

АЛЕКСЕЙ НЕСТЕРЕНКО

ВВЕДЕНИЕ В СОВРЕМЕННУЮ КРИПТОГРАФИЮ

Теоретико-числовые алгоритмы

*Курс лекций для специалистов и магистрантов высших учебных
заведений*

редакция от 1 июля 2011 г.

ОГЛАВЛЕНИЕ

Оглавление	2
1 Элементарная теория делимости	5
1.1 Наибольший общий делитель	6
1.2 Алгоритм Эвклида	7
1.3 Простые числа	11
2 Сравнения	15
2.1 Сравнения первой степени	16
2.2 Китайская теорема об остатках	19
2.3 Функция Эйлера	22
2.4 Первообразные корни	25
2.5 Алгебраическое заключение	30
3 Многочлены	33
3.1 Элементарные операции	33
3.2 Алгоритм Эвклида для многочленов	37
3.3 Основная теорема арифметики для многочленов	40
3.4 Дифференцирование многочленов	43
3.5 Решение сравнений по составному модулю	44
4 Сравнения старших степеней	51
4.1 Квадратичные вычеты	51
4.2 Символ Якоби	59
4.3 Вычисление квадратного корня	64
4.4 Вероятностный алгоритм вычисления корней многочленов	72
4.5 Оценки числа решений в специальных случаях	77
5 Простые числа	79
5.1 Вероятностные тесты проверки простоты	81
5.1.1 Тест Соловея-Штрассена	82
5.1.2 Тест Миллера-Рабина	85
5.2 $N - 1$ методы доказательства простоты	90
5.3 $N + 1$ метод доказательства простоты	95
5.4 Алгоритмы построения простых чисел	102
5.4.1 Рекурсивный алгоритм построения простых по известному разложению $p - 1$	103

5.4.2	Алгоритм построения сильно простого числа	106
6	Непрерывные дроби	111
6.1	Конечные непрерывные дроби	112
6.2	Понятие подходящей дроби	113
6.3	Квадратичные иррациональности	119
6.4	Наилучшие приближения	129
7	Факторизация целых чисел	133
7.1	Метод пробного деления	133
7.2	Метод Ферма	134
7.2.1	Вычисление квадратного корня	135
7.2.2	Как быстро проверить, что число является полным квадратом	136
7.3	Метод Лемана	140
7.4	Метод Полларда-Флойда	143
7.5	Метод Brenta	145
7.6	$p - 1$ метод Полларда	146
7.7	$p + 1$ метод Вильямса	148
7.8	Оптимизация алгоритмов Полларда и Вильямса	150
7.8.1	Разностная схема	151
7.8.2	Метод согласования	152
7.8.3	Поиск пар простых чисел	153
7.8.4	Поиск циклов в последовательностях	154
7.9	Метод Женга	156
7.10	Метод Макки	158
8	Факторизация целых чисел II	163
8.1	Метод Крайчика	164
8.2	Метод непрерывных дробей	165
8.2.1	Первый вариант	166
8.2.2	Второй вариант	168
A	Случайные отображения	173
A.1	Орбиты элементов	173
A.2	Алгоритмы поиска циклов	177
A.2.1	Алгоритм Флойда	177
A.2.2	Алгоритм Brenta	178
A.2.3	Алгоритм Госпера	181
A.2.4	Алгоритм Ниваша	183

Список литературы	185
Индексный указатель	189

ЭЛЕМЕНТАРНАЯ ТЕОРИЯ ДЕЛИМОСТИ

Операция деления, деление с остатком - Наибольший общий делитель, его свойства - Алгоритм Эвклида - Теорема Ламе - Двоичный алгоритм Эвклида - Простые числа - Основная теорема арифметики.

Мы начнем изложение с простейших вопросов и рассмотрим множество целых чисел

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

Множество целых чисел образует кольцо относительно операций сложения и умножения. Введем на этом множестве операцию деления.

Определение 1.1. Пусть a, b целые числа. Мы будем говорить, что a делит b и использовать запись $a|b$, если найдется такое целое число d , что $ad = b$.

Хорошо известно, что операция деления не может быть определена для двух произвольных целых чисел a, b . Легко привести пример, например, число 3 не делит число 7, ибо нельзя найти целое число d такое, что $3d = 7$.

С другой стороны, мы можем ввести другую операцию — операцию деления с остатком, которая определена для любой пары целых чисел a, b . Нам потребуется следующая лемма

Лемма 1.1. Пусть a, b целые числа, тогда существуют единственные целые числа q, r такие, что

$$b = aq + r, \quad 0 \leq r < |a|. \quad (1.1)$$

Доказательство. Без ограничения общности будем считать, что $a > 0$. Тогда найдется наибольшее целое число q такое, что $aq \leq b$ и $b < a(q+1)$. Обозначая $r = b - aq$, получим неравенство $0 \leq r < a$ и представление (1.1).

Допустим, что представление (1.1) не единственно. Тогда найдутся такие целые числа q_1, r_1 , что выполнены равенства $b = aq_1 + r_1$ и

$$aq + r = aq_1 + r_1.$$

Из последнего равенства следует, что $a|(r_1 - r)$. Из определения чисел r, r_1 следует, что $|r_1 - r| < a$. Таким образом $r_1 - r = 0$ и $r_1 = r$, $q_1 = q$. Лемма доказана. \square

Определение 1.2. Пусть a, b целые числа. Мы будем называть целое число r , $0 \leq r < |a|$, остатком от деления b на a , если выполнено представление (1.1) или, что аналогично, $a|(b - r)$.

1.1 Наибольший общий делитель

Определение 1.3. Мы будем называть натуральное число d наибольшим общим делителем двух целых чисел a, b если

1. d является общим делителем, то есть $d|a, d|b$.
2. d является наибольшим, то есть для любого общего делителя c выполнено $c|d$.

Мы будем обозначать наибольший общий делитель двух целых чисел a, b символом $\text{НОД}(a, b)$.

Легко видеть, что данное определение неоднозначно. Действительно, для каждого $d > 0$, удовлетворяющего определению 1.3, существует целое число $-d$, которое удовлетворяет первому и второму условию определения 1.3. Далее мы будем считать, что $\text{НОД}(a, b) > 0$.

Определение 1.4. Если наибольший общий делитель двух целых чисел a, b равен единице, то они называются взаимно простыми числами.

Приведем несколько свойств наибольшего общего делителя, которые будут использованы нами в дальнейшем.

Лемма 1.2. Пусть a, b и c целые числа. Выполнены следующие утверждения.

1. $\text{НОД}(a, b) = \text{НОД}(b, a)$,
2. $\text{НОД}(-a, b) = \text{НОД}(a, b)$,
3. $\text{НОД}(a, a) = \text{НОД}(a, 0) = |a|$,
4. $\text{НОД}(ac, bc) = |c| \cdot \text{НОД}(a, b)$,
5. если $\text{НОД}(a, c) = 1$, то $\text{НОД}(a, cb) = \text{НОД}(a, b)$,
6. $\text{НОД}(a, b) = \text{НОД}(a \pm b, a)$,
7. $\text{НОД}(a, b) = \text{НОД}(a, r)$, где r остаток деления b на a .

Доказательство. Поскольку большинство утверждений леммы достаточно очевидно, поэтому мы докажем только последние два.

Пусть r остаток от деления числа b на a и, следуя лемме (1.1), $b = aq + r$, где $0 \leq r < |a|$. Обозначим $d = \mathbf{НОД}(a, b)$, тогда найдутся такие целые числа k, l , что $a = kd, b = ld$. Следовательно

$$a \pm b = d(k \pm l), \quad r = b - aq = d(l - kq)$$

и d является общим делителем чисел $a, b, a \pm b, r$. Покажем, что d наибольший делитель.

Пусть d_1 является общим делителем чисел $(a \pm b)$ и a . Тогда, что легко показать, d_1 делит и b , то есть является общим делителем чисел a и b и, следовательно, $d_1 | \mathbf{НОД}(a, b) = d$ и $d_1 \leq d$.

Аналогично, пусть d_2 является общим делителем чисел r и a . Тогда $a = d_2k_2, r = d_2r_2$ и выполнено равенство $b = qa + r = d_2(qa_2 + r_2)$, из которого следует, что $d_2 | b$. Таким образом d_2 является общим делителем чисел a, b и $d_2 | \mathbf{НОД}(a, b) = d$ и $d_2 \leq d$. \square

Если нам известны все общие делители чисел a и b , то вычисление наибольшего общего делителя не представляет труда: мы можем перебрать все делители и выбрать максимальный. Однако, на практике, нам неизвестны все общие делители. Более того, как мы покажем далее, задача поиска делителей значительно сложнее, чем вычисление наибольшего общего делителя.

Основываясь на утверждениях доказанной леммы, мы можем предъявить сразу несколько алгоритмов вычисления наибольшего общего делителя.

В начале заметим, что из второго и третьего утверждения леммы 1.2 следует, что нам достаточно ограничиться только натуральными числами a, b . Используя шестое утверждение можно получить простейший алгоритм вычисления наибольшего делителя, который использует только операцию вычитания натуральных чисел.

1.2 Алгоритм Эвклида

Основываясь на седьмом утверждении леммы 1.2, мы получим алгоритм, который принято называть алгоритмом Эвклида вычисления наибольшего общего делителя.

Будем считать, что $b > a > 0$. Используя деление с остатком, см. (1.1), определим $r_{-1} = b, r_0 = a$ и последовательность

$$\begin{aligned}
b &= aq_1 + r_1, \\
a &= r_1q_2 + r_2, \\
r_1 &= r_2q_3 + r_3, \\
&\dots \\
r_{k-1} &= r_kq_{k+1} + r_{k+1}, \\
&\dots \\
r_{n-1} &= r_nq_{n+1}, \quad r_{n+1} = 0, \quad n \in \mathbb{N}.
\end{aligned} \tag{1.2}$$

Теорема 1.1. Пусть $b > a > 0$ — целые числа. Определим последовательности $r_{-1}, r_0, \dots, r_{n+1}$ и q_1, \dots, q_{n+1} равенствами (1.2). Тогда найдется такое натуральное число n , что $r_{n+1} = 0$ и

$$r_n = \text{НОД}(a, b).$$

Доказательство. В силу леммы 1.1 для всех $n = 0, 1, \dots$ выполнено равенство $0 \leq r_{n+1} < r_n$. Следовательно члены последовательности r_{-1}, r_0, \dots убывают и найдется такой индекс, при котором последний остаток r_{n+1} окажется равным нулю.

Из седьмого и третьего утверждений леммы 1.2 следуют равенства

$$\text{НОД}(a, b) = \text{НОД}(r_1, a) = \dots = \text{НОД}(r_n, 0) = r_n$$

и утверждение теоремы. □

Вычисление последовательности остатков $r_{-1}, r_0, \dots, r_{n+1}$ и является алгоритмом Эвклида. Мы можем минимизировать количество используемых вспомогательных переменных и переписать алгоритм Эвклида в виде, который может быть легко запрограммирован.

Алгоритм 1.1 (Алгоритм Эвклида)

Вход: целые числа a, b такие, что $b > a > 0$.

Выход: $\text{НОД}(a, b)$ — наибольший общий делитель чисел a и b .

1. Определить $r_{-1} = b, r_0 = a$.

2. Пока $r_0 > 0$ выполнять

2.1. определить $q = \left\lfloor \frac{r_{-1}}{r_0} \right\rfloor$.

2.2. определить $r = r_{-1} - qr_0$ и присвоить $r_{-1} = r_0, r_0 = r$.

3. Определить $\text{НОД}(a, b) = r_{-1}$. □

Следующая теорема позволяет оценить число шагов алгоритма Эвклида.

Теорема 1.2 (Ламе, 1844). Пусть a, b целые числа и $b > a > 0$. Количество операций деления с остатком в алгоритме 1.1 может быть оценено сверху величиной $1 + c \log_2 b$, где c положительная, эффективно вычисляемая константа.

Для доказательства этой теоремы нам потребуется сделать небольшое отступление.

Определение 1.5. Мы будем называть рекуррентную последовательность целых чисел

$$\begin{aligned} A_0 &= 0, & A_1 &= 1, \\ A_{n+1} &= A_n + A_{n-1}, & \text{при } n &= 1, 2, \dots \end{aligned} \quad (1.3)$$

последовательностью Фибоначчи.

Лемма 1.3. Пусть $z = \frac{1+\sqrt{5}}{2}$ действительный, положительный корень уравнения $z^2 = z + 1$. Тогда для последовательности Фибоначчи при всех натуральных n выполнено неравенство

$$A_{n+1} \geq z^{n-1}.$$

Доказательство. При $n = 1$, очевидно, $A_2 = 1 > 0$ и утверждение леммы выполнено. Далее проведем доказательство по индукции. Пусть условие леммы выполнено для всех индексов, меньших либо равных n . Тогда, в силу выбора z , выполнено неравенство

$$A_{n+1} = A_n + A_{n-1} \geq z^{n-2} + z^{n-3} = z^{n-3}(z + 1) = z^{n-1}.$$

□

Доказательство теоремы Ламе. В начале мы докажем неравенство

$$r_{k-1} \geq A_{n+1-k}, \quad \text{при } k = 0, 1, \dots, n, \quad (1.4)$$

где последовательность r_{-1}, r_0, \dots, r_n определена равенством (1.2), а последовательность Фибоначчи A_1, A_2, \dots равенством (1.3).

При $k = n$ выполнено $r_{n-1} = r_n q_{n+1} \geq 1 = A_1$. Далее по индукции. Пусть для всех $n, n-1, \dots, k$ неравенство (1.4) выполнено. Тогда

$$r_{k-1} = r_k q_{k+1} + r_{k+1} \geq r_k + r_{k+1} \geq A_{n-k} + A_{n-(k+1)} = A_{n+1-k}.$$

Из неравенства (1.4) и леммы 1.3 при $k = 0$ получаем

$$b = r_{-1} \geq A_{n+1} \geq z^{n-1} \quad \text{или} \quad n \leq 1 + \log_z b.$$

Учитывая значение $z = \frac{1 + \sqrt{5}}{2}$, мы получаем неравенство

$$n \leq 1 + \frac{\log_2 b}{\log_2(1 + \sqrt{5})},$$

которое завершает доказательство теоремы. \square

Использование вычислительных машин накладывает специфические требования к реализуемым на них алгоритмам. Хорошо известно, что операция деления целых чисел в общем случае выполняется на ЭВМ достаточно медленно. Тем не менее, в частном случае, когда целое число делится на двойку, операция деления может быть реализована в виде двоичного сдвига и выполняется очень быстро.

Этот факт привел к разработке некоторого класса алгоритмов, в которых операция деления на произвольное целое число заменяется операцией деления на двойку. Одним из ярких представителей подобного рода алгоритмов является бинарный алгоритм вычисления наибольшего общего делителя двух целых чисел a, b .

Алгоритм 1.2 (Бинарный алгоритм вычисления НОД)

Вход: целые числа a, b такие, что $b > a > 0$.

Выход: НОД(a, b) – наибольший общий делитель чисел a и b .

1. Определить $x = b, y = a, c = 1$.

2. Пока $2|x$ и $2|y$ выполнять

2.1. определить $c = 2c, x = \frac{x}{2}$ и $y = \frac{y}{2}$.

3. Пока $x \neq y$ выполнять

3.1. Если $2|x$, то определить $x = \frac{x}{2}$ и вернуться на шаг 3.

3.2. Если $2|y$, то определить $y = \frac{y}{2}$ и вернуться на шаг 3.

3.3. Если $x > y$, то определить $x = \frac{x-y}{2}$ и вернуться на шаг 3.

3.4. Если $y > x$, то определить $y = \frac{y-x}{2}$ и вернуться на шаг 3.

4. Определить НОД(a, b) = cx . \square

Корректность данного алгоритма основывается на четвертом и пятом утверждениях леммы 1.2. Согласно четвертому утверждению, на втором шаге алгоритма мы вычисляем целую константу $c = 2^k$, при некотором целом $k \geq 0$, такую, что $c|a, c|b$ и НОД(a, b) = $c \cdot$ НОД(x, y), где $a = cx, b = cy$.

Поскольку x и y не могут быть одновременно четными, мы пользуемся либо пятым, либо шестым утверждением леммы 1.2 в зависимости от того делится x или y на двойку, либо x и y одновременно нечетные целые числа.

Для бинарного алгоритма вычисления наибольшего общего делителя не известен аналог теоремы Ламе, позволяющий точно оценить число делений на двойку. Вместе с тем, при каждом повторении второго или третьего шага алгоритма 1.2 либо x , либо y уменьшается вдвое. Таким образом, сложность бинарного алгоритма вычисления наибольшего общего делителя может быть оценена величиной $O(\log_2 b)$.

Лемма 1.4. Пусть a, b, u, v натуральные числа, $\text{НОД}(a, b) = 1$ и $au = bv$. Тогда $a|v$ и $b|u$.

Доказательство. Рассмотрим частный случай $a = b = 1$. Очевидно, что для него утверждение леммы выполнено. Далее будем рассматривать случай $a + b > 2$.

Предположим, что для всех пар a, b таких, что $\text{НОД}(a, b) = 1$ и $a + b < k$, $k > 2$, утверждение леммы выполнено. Покажем, что оно выполнено и для пары $a + b = k$.

Так как $\text{НОД}(a, b) = 1$, то $a \neq b$. Далее, без ограничения общности, будем считать, что $b > a > 0$. Из равенства $au = bv$ следует

$$(b - a)v = a(u - v).$$

Поскольку $\text{НОД}(b - a, a) = 1$, в силу шестого утверждения леммы 1.2, и $(b - a) + a = b < k$, то по предположению индукции $a|v$ или, что равносильно, найдется целое v_1 такое, что $v = v_1 a$. Таким образом, из равенства $au = bv$ следует равенство $au = bv_1 a$. Сокращая на $a \neq 0$, получаем утверждение леммы. \square

1.3 Простые числа

Простые числа играют основополагающую роль в криптографии. В этом разделе мы только сформулируем основные определения и докажем основную теорему арифметики. Позднее, мы посвятим изучению свойств простых чисел отдельную лекцию.

Определение 1.6. Натуральное число $p > 1$ называется простым, если оно не имеет других натуральных делителей, отличных от 1 и p .

Рассматривая ряд натуральных чисел, мы можем выделить в нем простые числа, а именно,

$$2, 3, 5, 7, 11, 13, 17, 23, \dots$$

Как мы покажем немного позже, этот ряд бесконечен.

Определение 1.7. *Натуральное число n называется составным, если оно имеет делитель, отличный от 1 и n .*

Из данного нами определения следует, что для составного числа n всегда найдутся такие натуральные числа a, b , что

$$n = ab \quad \text{и} \quad 1 < a < n, \quad 1 < b < n.$$

Лемма 1.5. *Наименьший, отличный от единицы натуральный делитель составного числа $n > 1$ есть простое число.*

Доказательство. Рассмотрим множество всех делителей числа n и выберем в нем наименьший делитель q . Тогда q является простым числом. В противном случае, существует натуральное число q_1 такое, что $q_1 | q$, $1 < q_1 < q$ и $q_1 | n$. Но это противоречит тому, что q наименьший делитель числа n . \square

Легко доказать следующую простую лемму.

Лемма 1.6. *Наименьший простой делитель p составного числа $n > 1$ удовлетворяет неравенству $p \leq \sqrt{n}$.*

Доказательство. Пусть $n = pt$, где p наименьший простой делитель числа n , тогда $n > t > p > 1$. Если мы предположим, что $p > \sqrt{n}$, то будет выполнено неравенство $n = pt > p^2 > (\sqrt{n})^2 = n$, противоречащее утверждению леммы. \square

Теперь мы докажем следующий результат, принадлежащий Эвклиду.

Теорема 1.3 (Эвклид). *Множество простых чисел бесконечно.*

Доказательство. Предположим, что утверждение теоремы неверно и существует лишь конечное число простых чисел, скажем p_1, \dots, p_n .

Рассмотрим целое число $N = p_1 \cdots p_n + 1$. Число N не делится на цело ни на одно простое число p_1, \dots, p_n , так как остаток от деления отличен от нуля и равен единице. Тогда, либо число N простое, либо согласно лемме 1.5 у него есть наименьший простой делитель, отличный от p_1, \dots, p_n . Таким образом мы нашли еще одно простое число, что противоречит нашему предположению. \square

Следующая теорема позволяет говорить о том, что множество простых чисел служит базой для генерации множества всех целых чисел.

Теорема 1.4 (Основная теорема арифметики). Пусть $n > 1$ натуральное число. Можно представить n в виде произведения простых сомножителей единственным образом, с точностью до перестановки сомножителей.

Доказательство. Согласно лемме 1.5 число n имеет наименьший простой делитель p_1 и выполнено равенство $n = p_1 a_1$. Если $a_1 > 1$, то применяя утверждение леммы к числу a_1 , аналогично, получаем равенство $a_1 = p_2 a_2$, где p_2 наименьший простой делитель числа a_1 . Если $a_2 > 1$, то продолжаем далее.

Поскольку числа a_1, a_2, \dots убывают, то на некотором шаге k процесс прервется и будет выполнено равенство $a_k = 1$. Для каждого простого p_j выполнено $p_j | n$, $1 \leq j \leq k$. Следовательно, для числа n выполнено равенство

$$n = p_1 \cdots p_k. \quad (1.5)$$

Покажем единственность представления (1.5). Пусть существует другое разложение числа n в произведение простых сомножителей, а именно $n = q_1 \cdots q_s$, тогда выполнено равенство

$$p_1 \cdots p_k = q_1 \cdots q_s. \quad (1.6)$$

Будем считать, что $s \geq k$. В противном случае, мы можем поменять местами обозначения k и s местами.

В силу того, что все числа, входящие в произведение (1.6), являются простыми, то из утверждения леммы 1.4 следует, что либо $p_1 = q_1$, либо $p_1 | q_2 \cdots q_s$. Применяя лемму 1.4 последовательно к произведению $q_j \cdots q_s$, $2 \leq j \leq s$, найдем такой индекс j , что $p_1 = q_j$. Переставляя множители q_j будем считать, что $j = 1$ и $p_1 = q_1$.

Теперь, сокращая обе части равенства (1.6) на $p_1 = q_1$, получим

$$p_2 \cdots p_k = q_2 \cdots q_s.$$

Применяя к полученному равенству рассуждения, аналогичные приведенным выше, мы получим равенство $p_3 \cdots p_k = q_3 \cdots q_s$. и так далее, до тех пор, пока не получим $p_{s+1} \cdots p_k = 1$.

В силу того, что все простые числа p_{s+1}, \dots, p_k больше единицы, то последнее равенство не возможно и мы получаем, что $k = s$ и разложения в равенстве (1.6) совпадают. \square

Перемножая в равенстве (1.5) одинаковые сомножители получим

$$n = \prod_{i=1}^r p_i^{\alpha_i}, \quad r \in \mathbb{N}, \quad (1.7)$$

где p_i различные простые числа, а α_i натуральные числа, кратности, с которыми простые числа входят в разложение (1.5).

Определение 1.8. *Полученное нами равенство (1.7) называется каноническим разложением натурального числа $n > 1$ на простые сомножители.*

СРАВНЕНИЯ

Вычеты по модулю целых чисел - Теорема о числе решений сравнения первой степени - Лемма Безу - Расширенный алгоритм Эвклида - Китайская теорема об остатках - Алгоритм Гарнера - Функция Эйлера - Теоремы Эйлера и Ферма - Первообразные корни - Теорема о существовании первообразного корня по модулю простого числа.

В этой лекции мы введем одно из фундаментальных понятий в алгебре и теории чисел, а именно, понятие вычета по модулю целого числа.

Определение 2.1. Пусть a, b целые числа, и $m > 0$ натуральное число. Мы будем говорить, что числа a и b сравнимы по модулю m и записывать $a \equiv b \pmod{m}$, если $m \mid (a - b)$ или, что аналогично, $a = b + km$ для некоторого целого значения k .

Легко показать, что выполнены следующие утверждения

Лемма 2.1. Пусть $m > 0$ натуральное число и a, b целые числа для которых выполнено сравнение $a \equiv b \pmod{m}$.

1. если $\text{НОД}(c, m) = 1$, то $ac \equiv bc \pmod{m}$,
2. пусть $\text{НОД}(a, b) = d$ и $d \mid m$, тогда $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$,
3. если существует целое число c такое, что $c \mid a$ и $c \mid m$, тогда $c \mid b$.

Из определения 2.1 следует, что решениями сравнения

$$x \equiv b \pmod{m}$$

являются все целые числа вида $b + km$, где k некоторое целое число. Данные числа образуют класс чисел по модулю m .

Определение 2.2. Любое число из класса $b + km$, $k \in \mathbb{Z}$, мы будем называть вычетом по модулю числа m . Вычет x , удовлетворяющий неравенству $0 \leq x < m$, будем называть наименьшим неотрицательным вычетом.

Возьмем из каждого класса по модулю m одного представителя — наименьшие неотрицательные вычеты. Легко видеть, что таких вычетов всего m штук и все они различны.

Определение 2.3. Мы будем называть *полной системой вычетов* — множество всех наименьших неотрицательных вычетов по модулю m .

В дальнейшем нам потребуется и другой способ определения представителей классов вычетов, основанный на величине абсолютного значения представителя.

Определение 2.4. Мы будем называть *абсолютно-наименьшим вычетом по модулю числа m* вычет x , если он удовлетворяет неравенству

1. $-\frac{m}{2} < x \leq \frac{m}{2}$ при четном m ,
2. $-\frac{m-1}{2} \leq x \leq \frac{m-1}{2}$ при нечетном m .

Определение 2.5. Аналогично определению 2.3, мы будем называть *полной системой абсолютно-наименьших вычетов* — множество всех абсолютно-наименьших вычетов по модулю m .

2.1 Сравнения первой степени

Рассмотрим сравнение

$$ax \equiv b \pmod{m}. \quad (2.1)$$

Мы будем искать решения данного сравнения не в целых числах, а в вычетах по модулю m . Будем считать, что вычеты x и x_1 различны, если они принадлежат разным классам вычетов. Верна следующая теорема

Теорема 2.1. Пусть a, b целые числа и $m > 0$ натуральное число. Тогда для числа решений N сравнения $ax \equiv b \pmod{m}$ выполнены равенства

1. $N = 1$, если $\text{НОД}(a, m) = 1$,
2. $N = d$, если $\text{НОД}(a, m) = d$ и $d|b$,
3. $N = 0$, в противном случае.

Доказательство. Начнем доказательство с первого утверждения теоремы. Допустим, что выполнено условие $\text{НОД}(a, m) = 1$ и существуют два решения x, x_1 сравнения (2.1), тогда $ax \equiv ax_1 \equiv b \pmod{m}$ или, что равносильно, $ax = b + km$, $ax_1 = b + k_1m$ при некоторых целых k, k_1 . Тогда $a(x - x_1) = m(k - k_1)$ и, в силу леммы 1.4, выполнено условие

$m|(x - x_1)$. Таким образом $x \equiv x_1 \pmod{m}$ и x, x_1 принадлежат одному классу вычетов по модулю m .

Пусть $\text{НОД}(a, m) = d$, тогда из третьего утверждения леммы 2.1 следует, что $d|b$. В противном случае решений нет.

Определим целые числа a_1, b_1, m_1 равенствами $a = da_1, b = db_1$ и $m = dm_1$. Тогда согласно второму леммы 2.1 следует, что любое решение сравнения (2.1) удовлетворяет сравнению $a_1x \equiv b_1 \pmod{m_1}$, число решений которого, согласно первому утверждению теоремы, равно одному.

Пусть x_1 решение сравнения $a_1x \equiv b_1 \pmod{m_1}$, тогда найдется целое число l такое, что $a_1x_1 = b_1 + m_1l$. Обозначим $x = x_1 + m_1k$, где k произвольное целое число, тогда из равенства

$$ax = da_1(x_1 + m_1k) = db_1 + dm_1l + dm_1k = b + m(l + k)$$

следует, что x удовлетворяет исходному сравнению $ax \equiv b \pmod{m}$. Поскольку число возможных значений k , позволяющих получить различные вычеты по модулю m , равно d , то и число решений исходного сравнения равно d . \square

Для поиска решений сравнения $ax \equiv b \pmod{m}$ предположим, для начала, что $\text{НОД}(a, m) = 1$, и рассмотрим вычет z , удовлетворяющий сравнению

$$az \equiv 1 \pmod{m}, \quad \text{НОД}(a, m) = 1. \quad (2.2)$$

Как следует из теоремы 2.1, z существует, единственен и решение x сравнения (2.1) определяется сравнением $x \equiv zb \pmod{m}$.

В случае, если $\text{НОД}(a, m) = d$ мы можем рассмотреть сравнение

$$a_1x \equiv b_1 \pmod{m_1},$$

где

$$a_1 = \frac{a}{d}, \quad b_1 = \frac{b}{d}, \quad m_1 = \frac{m}{d}, \quad a_1, b_1, m_1 \in \mathbb{Z}, \quad \text{НОД}(a_1, m_1) = 1,$$

решение которого сводится к первому случаю.

Так или иначе, но решение сравнения (2.1) сводится к решению сравнения $az \equiv 1 \pmod{m}$, где $\text{НОД}(a, m) = 1$. Верно следующее утверждение

Лемма 2.2 (Лемма Безу). Пусть a, m целые числа. Тогда найдутся такие целые z, w , что

$$az + mw = \text{НОД}(a, m). \quad (2.3)$$

Вместо доказательства леммы, мы приведем алгоритм поиска коэффициентов z, w в соотношении (2.3) и докажем его корректность. Для нас является важным, что из леммы Безу вытекает разрешимость сравнения (2.2)

Для вычисления чисел z, w , удовлетворяющих равенству (2.3), можно воспользоваться следующим алгоритмом, который принято называть расширенным алгоритмом Эвклида.

Алгоритм 2.1 (Расширенный алгоритм Эвклида)

Вход: целые числа a, m такие, что $m > a > 0$.

Выход: целые числа z, w такие, что $az + bw = \text{НОД}(a, m)$.

1. Определить $r_{-1} = m, r_0 = a, w_{-1} = 1, w_0 = 0, z_{-1} = 0, z_0 = 1$.

2. Пока $r_0 > 0$ выполнять

2.1. определить $q = \left\lfloor \frac{r_{-1}}{r_0} \right\rfloor$.

2.2. определить $r = r_{-1} - qr_0$ и присвоить $r_{-1} = r_0, r_0 = r$.

2.3. определить $z = z_{-1} - qz_0$ и присвоить $z_{-1} = z_0, z_0 = z$.

2.4. определить $w = w_{-1} - qw_0$ и присвоить $w_{-1} = w_0, w_0 = w$.

3. Определить $\text{НОД}(a, m) = r_{-1}, z = z_{-1}, w = w_{-1}$. □

Теорема 2.2. Пусть a, m целые числа, $m > a > 0$. Алгоритм 2.1 позволяет находить целые числа z, w , удовлетворяющие равенству

$$az + mw = \text{НОД}(a, m).$$

Доказательство. Алгоритм Эвклида вычисляет убывающую последовательность остатков $r_{-1} = m, r_0 = a, \dots, r_n, r_{n+1} = 0$. Расширенный алгоритм Эвклида добавляет вычисление еще двух последовательностей $\{z_n\}$ и $\{w_n\}$, удовлетворяющих следующему равенству

$$az_k + bw_k = r_k, \quad k = -1, 0, \dots, n.$$

Для $k = -1, 0$ данное равенство выполнено в силу выбора значений z_{-1}, z_0, w_{-1}, w_0 . Предположим, что оно выполнено и для всех индексов, не превосходящих некоторого индекса k . Тогда

$$\begin{aligned} az_{k+1} + mw_{k+1} &= a(z_{k-1} - q_k z_k) + m(w_{k-1} - q_k w_k) = \\ &= az_{k-1} + mw_{k-1} - q(az_k + mw_k) = r_{k-1} - qr_k = r_{k+1}. \end{aligned}$$

Поскольку $r_n = \text{НОД}(a, m)$, то утверждение теоремы выполнено. □

Заметим, что в случае, когда $\text{НОД}(a, m) = 1$ и мы хотим найти решение сравнения (2.2), нам достаточно вычислять последовательность $\{w_n\}$.

В дальнейшем, мы будем использовать для вычета z , являющегося решением сравнения $az \equiv 1 \pmod{m}$ обозначение $z \equiv a^{-1} \pmod{m}$.

2.2 Китайская теорема об остатках

Перейдем к рассмотрению систем сравнений, которые часто возникают при решении криптографических задач, а также при реализации на ЭВМ вычислений с большими целыми числами. Рассмотрим систему

$$\begin{cases} a_1x \equiv b_1 \pmod{m_1}, \\ \dots \\ a_kx \equiv b_k \pmod{m_k}. \end{cases}$$

Используя описанную выше технику, мы можем независимо свести каждое уравнение этой системы к системе, в которой в левой части сравнения вместо коэффициентов будут стоять единицы. Для нахождения решения полученной системы может быть использована следующая теорема.

Теорема 2.3 (Китайская теорема об остатках, 1247). *Пусть k натуральное число и m_1, \dots, m_k целые, взаимно простые числа, произведение которых равно $M = \prod_{j=1}^k m_j$. Тогда любого набора целых чисел a_1, \dots, a_k решение системы сравнений*

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \dots \\ x \equiv a_k \pmod{m_k}, \end{cases} \quad (2.4)$$

единственно по модулю M и удовлетворяет сравнению

$$x \equiv \sum_{i=1}^k a_i b_i c_i \pmod{M}, \quad (2.5)$$

где $b_i = \frac{1}{m_i} \left(\prod_{j=1}^k m_j \right) = \frac{M}{m_i}$ и $c_i \equiv b_i^{-1} \pmod{m_i}$.

Доказательство. В силу выбора параметров b_i, c_i для каждого члена суммы, стоящей в правой части сравнения (2.5), выполнены сравнения

$$a_i b_i c_i \equiv a_i \pmod{m_i}, \quad a_i b_i c_i \equiv 0 \pmod{m_j}, \quad j \neq i, \quad i = 1, \dots, k,$$

из которых следует, что x удовлетворяет системе уравнений (2.4).

Покажем, что данное решение по модулю M единственно. Для этого предположим, что существует другое решение, скажем, y . Тогда выполнены сравнения $x - y \equiv 0 \pmod{m_i}$ для $i = 1, \dots, k$, или

$$x - y = m_1 c_1 = m_2 c_2 = \dots = m_k c_k,$$

при некоторых целых значениях c_1, \dots, c_k . Поскольку все числа m_1, \dots, m_k взаимно просты, то применяя лемму 1.4, получаем, что $m_i | c_j$ при всех $i \neq j$, что равносильно $x - y \equiv 0 \pmod{M}$. Последнее сравнение завершает доказательство теоремы. \square

Следствие 1. Двум различным наборам чисел a_1, \dots, a_k и a'_1, \dots, a'_k соответствуют два различных решения x и x' системы (2.4).

Доказательство. Пусть наборы чисел a_1, \dots, a_k и a'_1, \dots, a'_k таковы, что найдется хотя бы один индекс $j, j = 1, \dots, k$ такой, что $a_j \not\equiv a'_j \pmod{m_j}$.

Определим, согласно (2.5), решения

$$x \equiv \sum_{i=1}^k a_i b_i c_i \pmod{M}, \quad x' \equiv \sum_{i=1}^k a'_i b_i c_i \pmod{M}$$

и предположим, что $x \equiv x' \pmod{M}$. Тогда для выбранного ранее индекса j будет выполнено $m_j | M$ и, следовательно, $x \equiv x' \pmod{m_j}$. Последнее сравнение равносильно $a_j \equiv a'_j \pmod{m_j}$, что противоречит нашему предположению. \square

Утверждение теоремы 2.3 позволяет предложить следующий алгоритм решения системы (2.4).

Алгоритм 2.2

Вход: целые числа k, m_1, \dots, m_k и a_1, \dots, a_k , удовлетворяющие теореме 2.3.

Выход: вычет $x, 0 \leq x < M$ — решение системы сравнений (2.4).

1. Определить $x = 0, i = 1$ и $M = \prod_{j=1}^k m_j$.

2. Пока $i \leq k$ выполнять

2.1. вычислить $b = \frac{M}{m_i}$ и определить $c \equiv b^{-1} \pmod{m_i}$.

2.2. вычислить $x \equiv x + a_i b c \pmod{M}$.

2.3. определить $i = i + 1$.

3. Вернуть значение x . \square

Остановимся на реализации шага 2.2. Нам надо добавить к текущему значению переменной x произведение $a_i b c$, для которого верна оценка сверху

$$0 \leq a_i b c < AM, \quad \text{где } A = \max_{i=1, \dots, k} a_i.$$

После сложения, нам необходимо произвести операцию деления по модулю числа M и вычислить вычет x .

Поскольку операция приведения по модулю M является достаточно трудоемкой, мы приведем другой алгоритм восстановления значения x по множеству известных остатков a_1, \dots, a_k . Он основывается на следующей теореме.

Теорема 2.4. Пусть m_1, \dots, m_k целые, взаимно простые числа, произведение которых равно $M = \prod_{j=1}^k m_j$. Пусть $x < M$ целое число, удовлетворяющее системе сравнений (2.4). Тогда найдутся такие целые x_1, \dots, x_k , что $x_i < m_i$ для всех $i = 1, \dots, k$ и

$$x = x_1 + x_2 m_1 + x_3 m_1 m_2 + \dots + x_k m_1 \cdots m_{k-1}. \quad (2.6)$$

Доказательство. Начнем с того, что определим константы b_1, \dots, b_k равенствами

$$b_1 = 1, \quad b_i = \prod_{j=1}^{i-1} m_j, \quad i = 2, \dots, k.$$

Теперь мы можем переписать равенство (2.6) в виде $x = \sum_{i=1}^{k-1} x_i b_i$. Введем еще один набор значений s_1, \dots, s_k , зависящий от величины x следующим образом: $s_i = \sum_{j=1}^i x_j b_j$, тогда $x = s_k$ и

$$s_1 = x_1, \quad s_i = s_{i-1} + x_i b_i, \quad \text{для всех } i = 2, \dots, k. \quad (2.7)$$

Теперь мы можем определить величины x_1, \dots, x_k используя следующее рекуррентное соотношение

$$x_1 = a_1, \quad x_i \equiv b_i^{-1}(a_i - s_{i-1}) \pmod{m_i}, \quad \text{при } i = 2, \dots, k, \quad (2.8)$$

где величина b_i^{-1} определяется из сравнения $b_i b_i^{-1} \equiv 1 \pmod{m_i}$. Поскольку $\text{НОД}(b_i, m_i) = 1$, то данное определение величины b_i^{-1} корректно. Заметим, что, в силу определения, для коэффициентов x_i выполнены неравенства $x_i < m_i$ для всех $i = 1, \dots, k$.

Изучая равенство (2.6), заметим, что для всех индексов $i = 1, \dots, k$ выполнено сравнение $x \equiv s_i \pmod{m_i}$. Тогда, из (2.7) и (2.8) получаем

$$x \equiv s_{i-1} + x_i b_i \equiv s_{i-1} + b_i^{-1}(a_i - s_{i-1}) b_i \equiv a_i \pmod{m_i},$$

и число x действительно удовлетворяет системе сравнений (2.4).

Нам осталось показать, что выполнено неравенство $x < M$. Для этого докажем, по индукции, что выполнено неравенство $s_i < m_i b_i$ для любого индекса $i = 1, \dots, k$. Для $s_1 = x_1 < m_1$ неравенство очевидно. Далее, пусть оно выполнено для всех индексов, меньших i . Тогда $s_{i-1} < m_{i-1} b_{i-1} = b_i$ и

$$s_i = s_{i-1} + x_i b_i < b_i + (m_i - 1) b_i < m_i b_i.$$

Применяя полученное неравенство к индексу $i = k$ получаем, что $x = s_k < m_k b_k = M$. Теорема доказана. \square

Основываясь на данной теореме, мы можем предложить эффективный алгоритм вычисления значения x . Отметим, что для случая $k = 2$ описание алгоритма может быть найдено в книге А.Сушкевича [30]. Добавим, что в англоязычной и переводной литературе этот алгоритм, применительно к произвольному значению k , носит имя американского математика Х. Гарнера [6].

Алгоритм 2.3 (Алгоритм Гарнера)

Вход: целые числа k, m_1, \dots, m_k и a_1, \dots, a_k , удовлетворяющие теореме 2.3.

Выход: $x, 0 \leq x < M$ — решение системы сравнений (2.4).

1. Определить $i = 2, b = 1, s = a_1 \pmod{m_1}$.
2. Пока $i \leq k$ выполнять
 - 2.1. определить $b = bm_{i-1}$ и $d \equiv b^{-1} \pmod{m_i}$,
 - 2.2. вычислить $x \equiv d(a_i - s) \pmod{m_i}$,
 - 2.3. вычислить $s = s + xb$ и положить $i = i + 1$.
3. Вернуть значение s . \square

Основное преимущество алгоритма Гарнера заключается в том, что в нем вычисления производятся с числами, не превышающими величину модуля M . Более того, не требуется операция приведения по модулю M , которая заменена операциями приведения по модулю множителей m_i , входящих в разложение числа M .

2.3 Функция Эйлера

Рассмотрим целое неотрицательное число t и его полную систему вычетов

$$0, 1, \dots, t - 1.$$

Среди этого множества выберем вычеты, взаимно простые с t .

Определение 2.6. Множество вычетов по модулю t , взаимно простых с модулем t , называется приведенной системой вычетов. Мощность этого множества обозначается символом $\varphi(t)$. Функция целочисленного аргумента $\varphi(t)$ называется функцией Эйлера.

Для вычисления значения функции Эйлера может быть использована следующая теорема.

Теорема 2.5. Пусть m натуральное целое число, для которого известно разложение на простые множители $m = \prod_{i=1}^r p_i^{\alpha_i}$, p_i — простые числа. Тогда

$$\varphi(m) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1}), \quad (2.9)$$

в частности, если p — простое, то

$$\varphi(p) = p - 1, \quad \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

Доказательство. Если p простое число, то среди чисел $0, 1, \dots, p - 1$ взаимно простых с p ровно $p - 1$ в силу условия $\text{НОД}(0, p) = p$ (см. третье утверждение леммы 1.2). Следовательно, $\varphi(p) = p - 1$.

Пусть $m = p^\alpha$ для некоторого целого $\alpha > 1$. Тогда для любого наименьшего неотрицательного вычета z , $0 \leq z < p^\alpha$, выполнено либо равенство $\text{НОД}(z, p^\alpha) = 1$, либо условие $p \mid \text{НОД}(z, p^\alpha)$. Поскольку среди чисел $0, 1, \dots, p^\alpha - 1$ чисел кратных p ровно $p^{\alpha-1}$, то мы получаем, что $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Для доказательства основного утверждения теоремы нам осталось доказать, что функция Эйлера мультипликативна, то есть для любых взаимно простых чисел a, b выполнено равенство

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Тогда подставляя в это равенство разложение m на множители, получим утверждение теоремы.

Пусть α один из вычетов по модулю a , а β , соответственно, вычет по модулю b . Тогда согласно китайской теореме об остатках, теорема 2.3, существует единственный вычет $\gamma \pmod{ab}$ такой, что

$$\gamma \equiv \alpha \pmod{a}, \quad \gamma \equiv \beta \pmod{b}.$$

В случае, если α не взаимно просто с a , $\text{НОД}(\alpha, a) > 1$ или β не взаимно просто с b , $\text{НОД}(\beta, b) > 1$, то мы сразу получаем, что $\text{НОД}(\gamma, ab) > 1$. И наоборот, $\text{НОД}(\gamma, ab) = 1$ только тогда, когда α и β взаимно просты, соответственно, с a и b .

Таким образом мы получаем взаимно однозначное соответствие между двумя множествами — множеством взаимно простых вычетов по модулю ab и множеством вычетов по модулю a и b , следовательно, $\varphi(ab) = \varphi(a)\varphi(b)$. Теорема доказана. \square

Вынося в равенстве (2.9) за скобки общий множитель m , мы получаем следующее

Следствие 1 (к теореме 2.5). Для $\varphi(m)$ выполнено равенство

$$\varphi(m) = m \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

Функция Эйлера играет важнейшую роль не только в теории чисел, но и в криптографии. Ее применение основывается на следующей важной теореме.

Теорема 2.6 (Теорема Эйлера). Пусть $a, m > 0$ взаимно простые целые числа, то есть $\text{НОД}(a, m) = 1$. Тогда

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Доказательство. Рассмотрим приведенную систему вычетов по модулю m

$$1, \dots, m-1,$$

состоящую из $\varphi(m)$ различных вычетов.

Домножим каждый из вычетов данной системы на a и получим тоже самое множество вычетов, только записанное в другом порядке. Это позволяет нам получить равенство

$$(1)a \cdot \dots \cdot (m-1)a \equiv 1 \cdot \dots \cdot m-1 \pmod{p}.$$

Сокращая на множитель, стоящий в правой части сравнения, получим утверждение теоремы. \square

Частным случаем теоремы Эйлера является хорошо известная малая теорема Ферма. Действительно, применяя утверждение теоремы 2.5, получим следующий результат.

Теорема 2.7 (Малая теорема Ферма). Пусть p простое число и a целое, взаимно простое с p число. Тогда выполнено сравнение

$$a^{p-1} \equiv 1 \pmod{p}.$$

Еще одним следствием теоремы Эйлера может служить способ вычисления обратного элемента по модулю составного числа. Если числа a и m взаимно просты, то для вычисления $a^{-1} \pmod{m}$ можно воспользоваться сравнением

$$a^{\varphi(m)} \equiv a \cdot a^{\varphi(m)-1} \equiv 1 \pmod{m},$$

откуда

$$a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}. \quad (2.10)$$

Вычисление по формуле (2.10) может быть использовано в тех ситуациях, когда не реализована операция деления с остатком, либо эта операция выполняется слишком медленно.

2.4 Первообразные корни

Рассмотрим вопросы связанные с понятием первообразного корня целого числа.

Определение 2.7. Пусть a и $m > 0$ целые взаимно простые числа. Мы будем называть показателем числа a по модулю m минимальное из целых чисел q таких, что $a^q \equiv 1 \pmod{m}$, и использовать обозначение

$$\text{ord}_m a = \min \{q \in \mathbb{Z}, q > 0 : a^q \equiv 1 \pmod{m}\}.$$

Из теоремы Эйлера (теорема 2.6) следует, что показатель числа a существует всегда, например, им может являться значение функции Эйлера.

Лемма 2.3. Пусть $a, m > 0$ целые числа такие, что $\text{НОД}(a, m) = 1$, и показатель числа a по модулю m равен q . Тогда выполнены следующие условия

1. Числа $1, a, a^2, \dots, a^{q-1}$ не сравнимы друг с другом по модулю m .
2. Если выполнено сравнение $a^k \equiv a^l \pmod{m}$, то $k \equiv l \pmod{q}$.
3. Пусть s натуральное число такое, что $a^s \equiv 1 \pmod{m}$, тогда $q|s$. В частности показатель q делит значение $\varphi(m)$ функции Эйлера.

Доказательство. Докажем первое утверждение леммы. Пусть найдутся такие показатели k и l , $0 \leq k < l < q$, что $a^k \equiv a^l \pmod{m}$. Тогда из сравнения $a^{l-k} \equiv 1 \pmod{m}$ и неравенства $l - k < q$ получаем, что q не является показателем числа a и противоречие условию леммы.

Для доказательства второго утверждения леммы, используя деление с остатком (см. лемму 1.1), получим представления $k = k_1q + r_1$, $0 \leq r_1 < q$ и $l = l_1q + r_2$, $0 \leq r_2 < q$.

Из сравнения $a^k \equiv a^l \pmod{m}$ следует, что

$$a^{r_1} \equiv (a^k)^q a^{r_1} \equiv (a^l)^q a^{r_2} \equiv a^{r_2} \pmod{m}.$$

Поскольку $r_1 < q$, $r_2 < q$, то из первого утверждения леммы следует равенство $r_1 = r_2$ и доказательство второго утверждения.

Третье утверждение леммы является частным случаем второго. Действительно из сравнения

$$a^s \equiv 1 \equiv a^0 \pmod{m},$$

получаем, что $s \equiv 0 \pmod{q}$ и $s = cq$, при некотором значении числа c , то есть $q|s$. \square

Из утверждения леммы следует, что для каждого целого числа a его показатель по модулю числа m является делителем значения функции Эйлера $\varphi(m)$. Таким образом множество всех возможных делителей числа $\varphi(m)$ образует множество всех возможных значений показателей. Следующее определение задает класс чисел, имеющих максимально возможное значение показателя.

Определение 2.8. Пусть $a, m > 0$ целые взаимно простые числа. Число a называется первообразным корнем по модулю m , если показатель a по модулю m равен $\varphi(m)$, то есть $\text{ord}_m a = \varphi(m)$.

Сделаем следующее замечание. В отечественной учебной литературе по криптографии термины «показатель числа» и «первообразный корень» не прижились. Обычно они заменяются их алгебраическими синонимами: «порядок элемента» и «примитивный элемент», вводимыми в случае, когда модуль m является простым числом.

Определение 2.9. Пусть a целое число, p простое число такие, что $\text{НОД}(a, p) = 1$. Тогда порядком числа a называется числа a по модулю p называется показатель числа a по модулю p , то есть минимальное из чисел q таких, что $a^q \equiv 1 \pmod{p}$

$$\text{ord}_p a = \min_{q>0} \{a^q \equiv 1 \pmod{p}\}.$$

Соответственно, a называется примитивным элементом по модулю p , если показатель числа a равняется $p - 1$, то есть a является первообразным корнем по модулю простого числа p .

Для проверки — является ли заданное число a первообразным корнем по модулю m можно воспользоваться следующей теоремой.

Теорема 2.8. Пусть $a, m > 0$ целые взаимно простые числа. Известно разложение числа m на простые сомножители $m = \prod_{i=1}^r q_i^{\alpha_i}$, где

q_1, \dots, q_r различные простые числа, а $\alpha_1, \dots, \alpha_r$ натуральные числа. Число a является первообразным корнем по модулю m тогда и только тогда, когда выполнены условия

$$a^{\frac{\varphi(m)}{q_1}} \not\equiv 1 \pmod{m}, \quad \dots, \quad a^{\frac{\varphi(m)}{q_r}} \not\equiv 1 \pmod{m}.$$

Доказательство. Если a первообразный корень по модулю m , то в силу определения первообразного корня, для любого $c \mid \text{ord}_m a = \varphi(m)$ выполнено $a^{\frac{\text{ord}_m a}{c}} \not\equiv 1 \pmod{m}$, следовательно, выполнено и утверждение теоремы.

Обратно, пусть для числа a выполнены условия теоремы и его показатель равен t . Тогда, из третьего утверждения леммы 2.3 следует, что найдется некоторое натуральное число c такое, что $ct = \varphi(m)$. Если $c = 1$, то показатель элемента a равен $\varphi(m)$, то есть он является первообразным корнем.

Допустим, что это не так, тогда выполнено неравенство $c > 1$. Обозначим какой-нибудь простой делитель числа c символом q , тогда $qut = \varphi(m)$ для некоторого целого числа u и выполнено сравнение

$$a^{\frac{\varphi(m)}{q}} \equiv (a^t)^u \equiv 1 \pmod{m},$$

что противоречит нашему предположению, поскольку мы предъявили простой делитель q для которого не выполнено условие теоремы. \square

Несмотря на то, что с помощью теоремы 2.8 мы можем проверить – является ли число первообразным корнем, мы пока не доказали теорему о существовании первообразного корня по заданному модулю m . Для произвольного значения m такой результат доказать нельзя, вместе с тем мы можем получить его для частных случаев.

Теорема 2.9. Пусть p простое число, тогда найдется целое число a , являющееся первообразным корнем по модулю p .

Перед доказательством теоремы, мы докажем некоторые свойства первообразных корней по модулю простого числа p .

Лемма 2.4. Пусть a, b целые числа, p простое число.

1. Если показатель числа a по модулю p равен xy , $\text{ord}_p a = xy$, то выполнено $\text{ord}_p a^x = y$.
2. Если $\text{ord}_p a = x$, $\text{ord}_p b = y$ и $\text{НОД}(x, y) = 1$, то $\text{ord}_p(ab) = xy$.

Доказательство. Докажем первое утверждение леммы. Предположим, что показатель числа a^x равен t , тогда $(a^x)^t \equiv a^{xt} \equiv 1 \pmod{p}$. Тогда, согласно второму утверждению леммы 2.3, выполнено $xt \equiv xy \pmod{xy}$ или $xt = xyc$ при некотором целом c . Сокращая на x получим, что $y|t$.

С другой стороны, из сравнения $1 \equiv a^{xy} \equiv (a^x)^y \pmod{p}$ следует, что $y \equiv t \pmod{t}$, следовательно, $t|y$. Таким образом $y = t$ и первое утверждение леммы доказано.

Пусть показатель элемента ab равен t , тогда

$$1 \equiv ((ab)^t)^x \equiv a^{tx}b^{tx} \equiv b^{tx} \pmod{p}.$$

Используя второе утверждение леммы 2.3 получим, что $tx \equiv y \pmod{y}$ или $tx = yc$ при некотором целом c . Поскольку $\text{НОД}(x, y) = 1$, то из леммы 1.4 получаем, что $y|t$. Аналогично, заменяя в предыдущей цепочке сравнений x на y получаем, что $x|t$ и $xy|t$.

С другой стороны, из второго утверждения леммы 2.3 и сравнения

$$(ab)^{xy} \equiv 1 \pmod{p}$$

получаем, что $ab \equiv t \pmod{t}$ и $t|xy$, следовательно, $xy = t$. \square

Перед доказательством теоремы 2.9 нам потребуется дать еще одно определение.

Определение 2.10. Пусть a, b натуральные, отличные от нуля числа. Наименьшим общим кратным мы будем называть наименьшее натуральное число m такое, что $a|m$, $b|m$. Для обозначения наименьшего общего кратного мы будем использовать символ

$$\text{НОК}(a, b) = \min\{m \in \mathbb{N} : a|m, b|m\}.$$

Данное определение естественным образом обобщается на несколько целых чисел

$$\text{НОК}(a_1, \dots, a_k) = \min\{m \in \mathbb{N} : a_1|m, \dots, a_k|m\}.$$

Докажем несколько свойств, которым удовлетворяет наименьшее общее кратное.

Лемма 2.5. Верны следующие утверждения:

1. Любое общее кратное нескольких чисел a_1, \dots, a_k делится на их наименьшее общее кратное.

2. Наименьшее общее кратное взаимно простых чисел a_1, \dots, a_k равно их произведению, то есть $\text{НОК}(a_1, \dots, a_k) = \prod_{i=1}^k a_k$.

3. Если число b делится на каждое из попарно взаимно простых чисел a_1, \dots, a_k , то оно делится и на их произведение.

Доказательство. Начнем доказательство с первого утверждения леммы. Обозначим символом $m = \text{НОК}(a_1, \dots, a_k)$, а символом s — какое-нибудь произвольное общее кратное чисел a_1, \dots, a_k . Поскольку m наименьшее общее кратное, мы можем записать равенство

$$s = mq + r, \quad 0 \leq r < m,$$

где q, r некоторые натуральные числа. В силу определения общего делителя, находим, что $r = s - mq$ делится на каждое из чисел a_1, \dots, a_k и, следовательно, является их общим делителем. Но поскольку мы предположили, что $r < m$ и m — наименьший общий делитель, то данное свойство возможно только при $r = 0$. Первое утверждение доказано.

Согласно основной теореме арифметики, см. теорему 1.4, разложим a_1 в произведение простых чисел $a_1 = \prod_{i=1}^{k_1} p_i^{\alpha_i}$. Каждое $p_i^{\alpha_i}$ из этого произведения делит $\text{НОК}(a_1, \dots, a_k)$, в силу определения наименьшего общего кратного, но не делит остальные a_i при $i > 1$, в силу их взаимной простоты. Аналогичное свойство выполняется для всех $a_i, i = 2, \dots, k$.

Таким образом $\prod_i^k a_i$ делит $\text{НОК}(a_1, \dots, a_k)$. Поскольку $\prod_i^k a_i$ также является общим кратным чисел a_1, \dots, a_k , то второе утверждение леммы выполнено.

Третье утверждение леммы тривиально следует из двух первых. Действительно, из первого утверждения леммы следует, что b делится на $\text{НОК}(a_1, \dots, a_k)$, а в силу второго утверждения следует утверждение, поскольку $\text{НОК}(a_1, \dots, a_k) = \prod_i^k a_i$. \square

Теперь мы можем перейти собственно к доказательству теоремы 2.9.

Доказательство теоремы 2.9. Для доказательства теоремы нам достаточно предъявить число a , показатель которого по модулю p равняется $p - 1$.

Пусть $\{t_1, \dots, t_k\}$ множество различных показателей, которым принадлежат числа $1, 2, \dots, p - 1$. Определим $\tau = \text{НОК}(t_1, \dots, t_k)$ и разложим его в произведение простых делителей

$$\tau = q_1^{\alpha_1} \cdots q_r^{\alpha_r}.$$

В силу определения наименьшего общего кратного для множителя $q_1^{\alpha_1}$ найдется некоторый показатель $t_i, 1 \leq i \leq k$, такой, что $q_1^{\alpha_1} | t_i$ или, что

равносильно, $t_1 = c_1 q_1^{\alpha_1}$ для некоторого целого c_1 . Пусть a_1 целое число, показатель которого равен t_i . Тогда из первого утверждения леммы 2.4 получаем, что показатель числа $b_1 \equiv a_1^{c_1} \pmod{p}$ равен $q_1^{\alpha_1}$.

Выполняя аналогичные рассуждения далее, мы найдем для каждого простого делителя q_i числа τ число b_i такое, что $\text{ord}_p b_i = q_i^{\alpha_i}$ для всех $i = 1, \dots, r$.

Тогда, согласно второму утверждению леммы 2.4, показатель элемента $b \equiv b_1 \cdots b_r \pmod{p}$ равен τ . Из третьего утверждения леммы 2.3, получаем $\tau | \varphi(p) = p - 1$.

С другой стороны, в силу построения τ , для любого индекса i выполнено $t_i | \tau$, следовательно, для каждого целого b из интервала $1, \dots, p - 1$ найдется индекс i такой, что $\text{ord} b = t_i$ и $b^\tau \equiv 1 \pmod{p}$. Отсюда мы выводим, что $p - 1 | \tau$ и завершаем доказательство теоремы. \square

Теперь мы можем привести вероятностный алгоритм, который строит первообразный корень по модулю простого числа. Он опирается на утверждения теоремы 2.8.

Алгоритм 2.4 (Вычисление первообразного корня)

Вход: Целое число p и разложение значения $p - 1 = \prod_{i=1}^k q_i^{\alpha_i}$ на простые сомножители.

Выход: Число a такое, что $\text{ord}_p a = p - 1$.

1. Выбрать случайно элемент a , удовлетворяющий неравенству $1 \leq a < p$.
2. Определить $i = 1$.
3. Пока $i \leq k$ выполнять
 - 3.1. Если $a^{\frac{p-1}{q_i}} \equiv 1 \pmod{p}$, то вернуться на шаг 1.
4. Вернуть значение a . \square

2.5 Алгебраическое заключение

Полная система вычетов по модулю m образует аддитивную группу относительно операции сложения

$$k + l = (k + l) \pmod{m}, \quad k, l \in \mathbb{Z}_m = \{0, 1, \dots, m - 1\}.$$

Рассмотрим множество ненулевых элементов в \mathbb{Z}_m . Из леммы Безу, см. лемму 2.2, вытекает, что оно образует мультипликативную группу относительно операции умножения

$$k \cdot l = kl \pmod{m}, \quad k, l \in \mathbb{Z}_m$$

в случае, когда число m является простым.

Таким образом, мы получаем, что множество \mathbb{Z}_m образует поле. В случае, когда m составное множество \mathbb{Z}_m удовлетворяет аксиомам кольца. Мы не приводим доказательство сформулированных утверждений, поскольку оно носит технический характер и заключается в проверке выполнения условий определения поля или кольца.

Далее, в случае, когда множество \mathbb{Z}_m образует поле мы будем использовать обозначение \mathbb{F}_p , подчеркивая тем самым, что модуль по которому берутся вычеты является простым.

Описанный нами способ определения мультипликативной группы поля \mathbb{F}_p не является единственно возможным. Используя понятие первообразного корня можно определить на том же множестве групповую структуру другим способом.

Пусть p простое число, a — первообразный корень по модулю p . Рассмотрим множество целых чисел

$$1, a, a^2 \pmod{p}, \dots, a^{p-2} \pmod{p}.$$

Введем операцию умножения элементов группы следующим образом

$$a^k \cdot a^l \equiv a^{k+l} \pmod{p}.$$

Единицей группы является число 1. Обратным элементом к элементу a^k , очевидно, является элемент $a^l \pmod{p}$, где $l \equiv -k \pmod{p-1}$.

Для обозначения мультипликативной группы поля \mathbb{F}_p мы будем использовать символ \mathbb{F}_p^* .

МНОГОЧЛЕНЫ

Определение элементарных операций - Алгоритмы умножения многочленов - Операция деления с остатком - Алгоритм Эвклида - Лемма Безу - Основная теорема арифметики для многочленов - Теорема о числе корней многочленов - Теоремы о подъеме решений

В этой лекции мы формализуем наши знания о многочленах: введем формальное понятие многочлена от одной переменной, определим для многочленов операции сложения, умножения и деления с остатком, покажем, что для многочленов также можно доказать теорему об однозначном разложении на множители.

Мы введем понятие кольца многочленов и получим для него несколько результатов, аналогичных кольцу целых чисел. Это позволит нам ввести понятие поля, являющегося конечным расширением некоторого другого поля. Данные поля активно применяются в криптографических приложениях.

3.1 Элементарные операции

Мы будем обозначать символом \mathbb{U} произвольное коммутативное кольцо с единицей. В качестве примеров используемых нами колец можно рассмотреть кольцо целых чисел \mathbb{Z} , кольцо \mathbb{Z}_m вычетов по модулю целого числа m . Поскольку поля также являются и кольцами, в качестве кольца \mathbb{U} мы будем также рассматривать поля рациональных чисел \mathbb{Q} , действительных чисел \mathbb{R} , а также введенное нами в прошлой лекции конечное поле \mathbb{F}_p .

Определение 3.1. Пусть \mathbb{U} произвольное коммутативное кольцо с единицей, a, b — ненулевые элементы кольца \mathbb{U} .

Мы будем говорить, что a делит b и использовать обозначение $a|b$ или $b \equiv 0 \pmod{a}$, если в кольце \mathbb{U} найдется такой элемент d , что $ad = b$. Элемент a мы будем называть делителем числа b .

Очевидно, что для кольца целых чисел \mathbb{Z} это определение совпадает с введенным ранее определением 1.1.

Определение 3.2. Мы будем называть элемент ε кольца \mathbb{U} обратимым, если он является делителем единицы, то есть для него найдется некоторый элемент ε^{-1} того же кольца такой, что $\varepsilon\varepsilon^{-1} = 1$. Для

обозначения обратного элемента мы также будем использовать обозначение $\frac{1}{\varepsilon}$.

Относительно операции умножения обратимые элементы образуют группу. Это доказывается простой проверкой выполнения условий определения группы и оставляется для самостоятельного упражнения.

В кольце целых чисел \mathbb{Z} существует всего два обратимых элемента 1 и -1 , которые также содержатся и в любом другом кольце. В общем случае, произвольные кольца могут содержать более двух обратимых элементов, например, в кольце \mathbb{F}_p , являющемся полем, все отличные от нуля элементы обратимы.

Обратимый элемент ε делит любой элемент кольца \mathbb{U} . Действительно, для любого элемента a выполнено равенство $a = \varepsilon b$, где $b = a\varepsilon^{-1}$.

Множество обратимых элементов образует группу относительно операции умножения. Действительно, пусть a и b обратимые элементы кольца \mathbb{U} , тогда найдутся $a^{-1}, b^{-1} \in \mathbb{U}$ такие, что $aa^{-1} = 1, bb^{-1} = 1$. Следовательно, в силу коммутативности кольца \mathbb{U} , будет выполнено равенство $ab(a^{-1}b^{-1}) = 1$ из которого следует, что элемент $ab \in \mathbb{U}$ также является обратимым элементом.

Пример 3.1. Рассмотрим кольцо вычетов \mathbb{Z}_{15} . Тогда группа его обратимых элементов состоит из следующих вычетов

$$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Из леммы Безу, см. лемму 2.2, следует, что обратимыми элементами являются только вычеты, взаимно простые с модулем, то есть с 15. Количество таких чисел определяется значением функции Эйлера $\varphi(15)$ и, согласно теореме 2.5, равно 8.

Введем формальное определение кольца многочленов от одной переменной, которое будет многократно использовано нами в дальнейшем.

Определение 3.3. Пусть \mathbb{U} произвольное коммутативное кольцо с единицей и $n \geq 0$ целое число. Многочленом $a(x)$ от одной переменной x мы будем называть сумму

$$a(x) = \sum_{k=0}^n a_k x^k, \quad a_n \neq 0. \quad (3.1)$$

Значения $a_0, \dots, a_n \in \mathbb{U}$ мы будем называть коэффициентами многочлена, коэффициент a_n — старшим коэффициентом.

При некотором фиксированном значении $x \in \mathbb{U}$ значение многочлена мы будем называть значение выражения (3.1), принадлежащее кольцу \mathbb{U} .

Целое число n мы будем называть степенью многочлена и обозначать символом $\deg a(x) = n$. Многочлены степени один мы будем называть линейными.

Как следует из данного нами определения, почти все элементы кольца \mathbb{U} могут рассматриваться как многочлены нулевой степени. Это неверно лишь для нуля, ибо у него всегда выполнено $a_n = 0$. Поэтому мы будем дополнительно считать, что $\deg 0 = -1$.

Определение 3.4. Многочлен $a(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$, старший коэффициент которого равен единице называется унитарным¹.

Далее мы будем обозначать символом $\mathbb{U}[x]$ множество многочленов от одной переменной x с коэффициентами из кольца \mathbb{U} .

Пусть

$$a(x) = \sum_{k=0}^n a_k x^k, \quad b(x) = \sum_{k=0}^m b_k x^k.$$

два произвольных многочлена. Без ограничения общности будем считать, что $m \geq n$. Определим их сумму равенством

$$a(x) + b(x) = \sum_{k=0}^m (a_k + b_k) x^k,$$

где коэффициенты a_{n+1}, \dots, a_m полагаются равными нулю. Легко видеть, что $\deg(a(x) + b(x)) = \max\{\deg a(x), \deg b(x)\}$. Определим произведение многочленов равенством

$$a(x) \cdot b(x) = \sum_{k=0}^{n+m} c_k x^k, \quad \text{где } c_k = \sum_{i+j=k} a_i b_j, \quad k = 0, \dots, n+m,$$

также выполнено равенство $\deg a(x)b(x) = \deg a(x) + \deg b(x)$.

¹В русскоязычных изданиях нет устоявшегося названия для данного многочлена. В литературе по теории чисел традиционно используется понятие *примитивного* многочлена, в пособиях по алгебре — используются понятия *нормированного* или *приведенного* многочлена.

Введенные нами операции позволяют определить на множестве $\mathbb{U}[x]$ структуру коммутативного кольца, единица и ноль которого совпадают с единицей и нулем кольца \mathbb{U} . Доказательство этого утверждения проводится проверкой всех свойств, которым должно удовлетворять кольцо.

Согласно определению 3.1 мы будем говорить, что многочлен

$$a(x) = \sum_{k=0}^n a_k x^k$$

делит многочлен $b(x)$ если $a(x)u(x) = b(x)$ для некоторого многочлена $u(x) \in \mathbb{U}[x]$. Исходя из определения операции умножения многочленов мы сразу заключаем, что $\deg a(x) \leq \deg b(x)$.

Заметим, что если старший коэффициент a_n многочлена $a(x)$ является обратимым, то мы можем записать многочлен $a(x)$ в виде

$$a(x) = a_n u(x) = v(x)u(x),$$

где $v(x) = a_n$ и $u_x = \sum_{k=0}^n u_k x^k$ унитарный многочлен, коэффициенты которого определены равенствами $u_k = a_k a_n^{-1}$ для $k = 0, \dots, n$.

Таким образом многочлен $a(x) \in \mathbb{U}[x]$ с обратимым старшим коэффициентом может быть представлен в виде произведения многочлена нулевой степени, на унитарный многочлен степени, равной степени многочлена $a(x)$. Очевидно, что если кольцо \mathbb{U} является полем, то это верно для любого многочлена положительной степени.

Определение 3.5. Если многочлен $a(x) \in \mathbb{U}[x]$ называется неприводимым, если равенство $a(x) = u(x)v(x)$, где $u(x), v(x) \in \mathbb{U}[x]$ возможно только в том случае, когда один из многочленов $u(x), v(x)$ имеет нулевую степень и, таким образом, является элементом кольца \mathbb{U} .

Решение задачи о проверке является ли заданный многочлен неприводимым существенно зависит от кольца, над которым рассматривается многочлен. Как хорошо известно из курса алгебры, любой многочлен с коэффициентами из поля комплексных чисел является приводимым, поскольку раскладывается на линейные множители, см. [27, гл.6, § 3].

Для произвольного кольца это, конечно, не верно. Однако мы можем доказать теорему о разложении многочленов на множители, аналогичную основной теореме арифметики для целых чисел.

3.2 Алгоритм Эвклида для многочленов

Пусть $a(x)$ и $b(x)$ два многочлена из кольца $\mathbb{U}[x]$, при этом старший коэффициент многочлена $a(x)$ является обратимым, в частности, $a(x)$ может быть унитарным многочленом.

Аналогично кольцу целых чисел \mathbb{Z} , введем операцию деления многочленов с остатком и определим два многочлена $q(x), r(x)$ кольца $\mathbb{U}[x]$, удовлетворяющих равенству

$$b(x) = a(x)q(x) + r(x), \quad \deg r(x) < \deg a(x). \quad (3.2)$$

Многочлен $q(x)$ мы будем называть *частным* от деления, а многочлен $r(x)$ — *остатком* от деления многочленов.

Мы дадим определение операции деления с остатком при помощи следующего алгоритма, который часто называют «школьным алгоритмом деления многочленов».

Алгоритм 3.1 (Деление многочленов с остатком)

Вход: Многочлены $a(x) = \sum_{k=0}^n a_k x^k$, $b(x) = \sum_{k=0}^m b_k x^k$ и a_n обратим.

Выход: Многочлены $q(x), r(x)$ такие, что $b(x) = a(x)q(x) + r(x)$ и $\deg r(x) < \deg a(x)$.

1. Определить $n = \deg a(x)$ и $r(x) = b(x)$, $q(x) = 0$.
2. Определить $k = \deg r(x)$. Если выполнено $k < n$, то закончить алгоритм.
3. Определить $c = r_k a_n^{-1}$, где r_k старший коэффициент многочлена $r(x)$, и вычислить

$$r(x) = r(x) - c \cdot a(x) \cdot x^{k-n}, \quad q(x) = q(x) + c \cdot x^{k-n}.$$

Вернуться на шаг 2. □

Данный алгоритм выполнит операцию деления с остатком за конечное число шагов. Легко видеть, что после каждого выполнения третьего шага алгоритма степень многочлена $r(x)$ уменьшается. Поскольку степень многочлена является целым числом, то число шагов алгоритма конечно и не превышает величины $m - n$.

Лемма 3.1. *Полученное нами представление (3.2) единственно.*

Доказательство. Рассмотрим равенство

$$b(x) = a(x)q(x) + r(x) = a(x)q_1(x) + r_1(x),$$

где $\deg a(x) > \deg r(x)$, $\deg a(x) > \deg r_1(x)$. Следовательно, многочлен $a(x)$ делит разность многочленов $r_1(x) - r(x)$, то есть

$$a(x)(q(x) - q_1(x)) = (r_1(x) - r(x)). \quad (3.3)$$

В силу выбора многочленов $r(x), r_1(x)$, выполнено неравенство

$$\deg(r_1(x) - r(x)) \leq \max\{\deg r_1(x), \deg r(x)\} < \deg a(x),$$

следовательно, многочлен, стоящий справа в равенстве (3.3) имеет степень меньшую, чем многочлен стоящий слева. Таким образом равенство возможно только в том случае, если многочлены справа и слева равны нулю, откуда следует единственность представления (3.2). \square

Равенство (3.2) мы будем также записывать в виде

$$b(x) \equiv r(x) \pmod{a(x)},$$

используя обозначения, аналогичные кольцу целых чисел.

Операция деления с остатком, как следует из ее определения, может быть определена для любого многочлена $a(x)$ со старшим коэффициентом a_n , обратимым в кольце \mathbb{U} . Далее, нам потребуется, чтобы у многочленов обратимыми являлись все коэффициенты. Поэтому мы будем считать, что кольцо \mathbb{U} является *полем*.

Теперь мы можем ввести понятие наибольшего общего делителя двух многочленов.

Определение 3.6. Пусть $a(x)$ и $b(x)$ два многочлена из кольца $\mathbb{U}[x]$. Многочлен $u(x)$ называется наибольшим общим делителем многочленов $a(x), b(x)$ если

- многочлен $u(x)$ является общим делителем, то есть $u(x)|a(x)$, $u(x)|b(x)$, и
- для любого другого общего делителя $v(x)$ многочленов $a(x), b(x)$ выполнено $\deg u(x) > \deg v(x)$.

Мы будем использовать для обозначения наибольшего общего делителя обозначение, аналогичное принятому для целых чисел, то есть $u(x) = \mathbf{НОД}(a(x), b(x))$.

Введенное нами определение неоднозначно. Действительно, пусть выполнено равенство $u(x) = \mathbf{НОД}(a(x), b(x))$, тогда для любого обратимого элемента $\alpha \in \mathbb{U}$ будет выполнено $\alpha \cdot u(x) = \mathbf{НОД}(a(x), b(x))$. Поэтому, для определенности, мы будем считать, что наибольший общий делитель двух многочленов $a(x)$ и $b(x)$ является унитарным многочленом кольца $\mathbb{U}[x]$.

Определение 3.7. Пусть $a(x), b(x)$ многочлены из кольца $\mathbb{U}[x]$. Мы будем называть их взаимно простыми, если $\text{НОД}(a(x), b(x)) = 1$, то есть их наибольший общий делитель является унитарным многочленом степени ноль.

Свойства наибольшего общего делителя двух многочленов во многом аналогичны свойствам наибольшего общего делителя двух целых чисел. Сформулируем следующую лемму

Лемма 3.2. Пусть $a(x), b(x)$ два многочлена кольца $\mathbb{U}(x)$, старшие коэффициенты которых обратимы в кольце \mathbb{U} . Тогда выполнены следующие утверждения

1. $\text{НОД}(a(x), b(x)) = \text{НОД}(b(x), a(x))$,
2. $\text{НОД}(a(x), a(x)) = \text{НОД}(a(x), 0) = a_n^{-1}a(x)$, где a_n старший коэффициент многочлена $a(x)$,
3. $\text{НОД}(a(x), b(x)) = \text{НОД}(a(x), r(x))$, где $r(x)$ остаток от деления многочлена $b(x)$ на многочлен $a(x)$.

Доказательство данной леммы проводится аналогично доказательству леммы 1.2, поэтому мы его не приводим.

Для кольца многочленов, также как и для кольца целых чисел, существует алгоритм, основывающийся на последнем утверждении леммы 3.2 и позволяющий эффективно вычислять значение наибольшего общего делителя двух многочленов.

Алгоритм 3.2 (Алгоритм Эвклида для многочленов)

Вход: Многочлены $a(x), b(x)$ кольца $\mathbb{U}[x]$ такие, что их старшие коэффициенты обратимы в кольце \mathbb{U} и выполнено неравенство $\deg b(x) \geq \deg a(x) > 0$.

Выход: $\text{НОД}(a(x), b(x))$ – наибольший общий делитель многочленов $a(x)$ и $b(x)$.

1. Определить $u(x) = b(x), v(x) = a(x)$.
2. Пока $v(x) \neq 0$ выполнять
 - 2.1. используя алгоритм 3.1, определить многочлены $q(x), r(x)$, удовлетворяющие равенству $u(x) = v(x)q(x) + r(x)$.
 - 2.2. определить $u(x) = v(x)$ и $v(x) = r(x)$.
3. Определить $\text{НОД}(a(x), b(x)) = u_n^{-1}u(x)$, где u_n старший коэффициент многочлена $u(x)$. □

Корректность приведенного алгоритма, очевидно, следует из последнего утверждения леммы 3.2. Количество шагов алгоритма, то есть операций деления с остатком на втором шаге алгоритма, не превышает величины $\deg b(x)$.

3.3 Основная теорема арифметики для многочленов

Сформулируем аналог леммы Безу, см. лемму 2.2, для многочленов.

Лемма 3.3 (Лемма Безу для многочленов). Пусть $a(x)$ и $m(x)$ два многочлена из кольца $\mathbb{U}(x)$. Тогда найдутся такие взаимно простые многочлены $u(x)$ и $v(x)$ такие, что

$$a(x)v(x) + m(x)u(x) = \mathbf{НОД}(a(x), m(x)). \quad (3.4)$$

Доказательство. □

Теперь мы можем доказать теорему об однозначном разложении на множители для многочленов. Нам потребуется следующая лемма.

Лемма 3.4. Пусть $f(x)$ неприводимый многочлен из кольца $\mathbb{U}[x]$, который делит произведение многочленов $g(x)h(x)$ из $\mathbb{U}[x]$. Тогда либо $f(x)|g(x)$, либо $f(x)|h(x)$.

Доказательство. Из условия леммы следует, что найдется некоторый многочлен $t(x) \in \mathbb{U}[x]$ такой, что выполнено равенство

$$f(x)t(x) = g(x)h(x). \quad (3.5)$$

Пусть многочлен $f(x)$ не делит многочлен $g(x)$. Тогда, в силу неприводимости многочлена $f(x)$, выполнено $\mathbf{НОД}(f(x), g(x)) = 1$ и, в силу леммы Безу, см. лемму 3.3, найдутся такие многочлены $u(x), v(x) \in \mathbb{U}[x]$, что

$$u(x)f(x) + v(x)g(x) = 1.$$

Домножая последнее равенство на многочлен $h(x)$ и используя равенство (3.5) получаем

$$u(x)f(x)h(x) + v(x)f(x)t(x) = h(x) \quad \text{или} \quad f(x)r(x) = h(x),$$

где $r(x) = u(x)h(x) + v(x)t(x)$. Таким образом, согласно определению, многочлен $h(x)$ делится на многочлен $f(x)$. Лемма доказана. □

Теорема 3.1 (Основная теорема арифметики для многочленов). Пусть $f(x)$ произвольный многочлен из кольца $\mathbb{U}[x]$, $\deg f(x) > 0$. Тогда он может быть представлен в виде

$$f(x) = cf_1^{\alpha_1}(x) \cdots f_k^{\alpha_k}(x), \quad (3.6)$$

где $c \in \mathbb{U}$, а $f_1(x), \dots, f_k(x)$ различные унитарные неприводимые многочлены, $\alpha_1, \dots, \alpha_k$ натуральные числа. Более того, это разложение однозначно с точностью до перестановки множителей.

Доказательство. Мы проведем доказательство теоремы индукцией по степени многочлена $f(x)$. В случае, когда $\deg f(x) = 1$, $f(x) = a_1x + a_0$ мы тривиально получаем представление $f(x) = a_1(x + a_1^{-1}a_0)$.

Предположим теперь, что условие теоремы выполнено для всех многочленов степени, меньшей чем n . Рассмотрим многочлен $f(x)$ такой, что $\deg f(x) = n$. Если многочлен $f(x)$ неприводим, то мы получаем требуемое представление $f(x) = a_n(a_n^{-1}f(x))$, где a_n старший коэффициент многочлена $f(x)$ и многочлен $a_n^{-1}f(x)$ унитарен.

Если многочлен $f(x)$ приводим, то представим его в виде произведения $f(x) = g(x)h(x)$, где $\deg g(x) < n$, $\deg h(x) < n$. Согласно предположению индукции, многочлены $g(x), h(x)$ могут быть представлены в виде (3.6), следовательно, и многочлен $f(x)$ представим в виде (3.6).

Для доказательства единственности мы сделаем предположение о том, что многочлен $f(x)$ имеет два разложения вида (3.6)

$$f(x) = cf_1^{\alpha_1}(x) \cdots f_k^{\alpha_k}(x) = dh_1^{\beta_1}(x) \cdots h_s^{\beta_s}(x). \quad (3.7)$$

Поскольку все многочлены $f_1(x), \dots, f_k(x)$ и $h_1(x), \dots, h_s(x)$ унитарны мы получаем, что значения c и d совпадают. Без ограничения общности будем считать, что $s \geq k$ и рассмотрим неприводимый многочлен $f_1(x)$, стоящий в левой части равенства (3.7). В силу леммы 3.4 в правой части равенства (3.7) найдется многочлен $h_{i_1}(x)$ такой, что $f_1(x) | h_{i_1}(x)$. Поскольку многочлен $h_{i_1}(x)$ унитарен и не приводим, то условие делимости возможно только в случае, когда $f_1 = h_{i_1}(x)$.

Мы можем сократить равенство (3.7) на общий множитель и повторить эту процедуру далее для многочлена $f_2(x)$. Проведя k сокращений мы получим равенство

$$1 = f_1^{|\alpha_1 - \beta_1|}(x) \cdots f_k^{|\alpha_k - \beta_k|}(x) h_{k+1}^{\beta_{k+1}}(x) \cdots h_s^{\beta_s}(x).$$

Поскольку в левой части полученного равенства стоит многочлен нулевой степени мы получаем, что $k = s$, $\alpha_i = \beta_i$, $i = 1, \dots, k$, откуда вытекает утверждение теоремы. \square

Дадим еще одно важное определение.

Определение 3.8. Элемент $e \in \mathbb{U}$ называется корнем или нулем многочлена $f(x) \in \mathbb{U}[x]$, если $f(e) = 0$.

Теорема 3.2. *Элемент $e \in \mathbb{U}$ является корнем многочлена $f(x) \in \mathbb{U}[x]$ в том и только в том случае, когда многочлен $x - e$ делит $f(x)$.*

Доказательство. Применяя алгоритм 3.1 деления с остатком получим представление многочлена $f(x)$ в виде

$$f(x) = (x - e)q(x) + c,$$

где c некоторый элемент из \mathbb{U} . Подставляя в полученное равенство вместо переменной x значение e получаем $f(e) = c$. Таким образом, если элемент e является корнем многочлена $f(x)$ выполнено равенство $c = 0$ и теорема доказана. \square

Определение 3.9. *Пусть $e \in \mathbb{U}$ корень многочлена $f(x) \in \mathbb{U}[x]$. Мы будем называть кратностью корня e такое максимально возможное натуральное число α , что $(x - e)^\alpha | f(x)$.*

Теорема 3.3. *Пусть $f(x) \in \mathbb{U}[x]$ произвольный многочлен степени больше нуля, то есть $\deg f(x) = n > 0$. Тогда многочлен $f(x)$ может иметь не более n корней.*

Доказательство. Пусть $e_1, \dots, e_s \in \mathbb{U}$ корни многочлена $f(x)$. Тогда из теоремы 3.2 следует, что найдутся натуральные числа $\alpha_1, \dots, \alpha_s \geq 1$ такие, что

$$(x - e_i)^{\alpha_i} | f(x), \quad i = 1, \dots, s.$$

Рассматривая разложение многочлена $f(x)$ на неприводимые множители, согласно теореме 3.1, получим равенство

$$f(x) = a_n(x - e_1)^{\alpha_1} \cdots (x - e_s)^{\alpha_s} u(x),$$

где a_n старший коэффициент многочлена $f(x)$, а многочлен $u(x)$ либо равен 1, либо раскладывается в произведение неприводимых многочленов степени большей единицы. Учитывая, что степень многочлена $f(x)$ равна n мы получаем неравенство

$$\alpha_1 + \cdots + \alpha_s \leq n,$$

из которого следует утверждение теоремы. \square

3.4 Дифференцирование многочленов

Рассмотрим многочлен $f(x) = \sum_{k=0}^n a_k x^k$, $f(x) \in \mathbb{U}[x]$. Пусть $c \in \mathbb{U}$ произвольный, отличный от нуля элемент, тогда

$$f(x+c) = \sum_{k=0}^n a_k (x+c)^k = f(x) + cf_1(x) + c^2 f_2(x) + \dots$$

Мы разложили значение многочлена $f(x+c)$ по степеням c . Полученное равенство может быть также записано в виде

$$f(x+c) \equiv f(x) + cf_1(x) \pmod{c^2}, \quad c \neq 0. \quad (3.8)$$

Определение 3.10. Пусть $f(x), f_1(x) \in \mathbb{U}[x]$ многочлены, удовлетворяющие равенству (3.8). Мы будем называть многочлен $f_1(x)$ производной многочлена $f(x)$ и обозначать символом $f'(x)$.

Лемма 3.5. Пусть $f(x), g(x)$ два многочлена кольца $\mathbb{U}[x]$. Тогда выполнены следующие соотношения

1. $(f(x) + g(x))' = f'(x) + g'(x)$ (производная суммы),
2. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$ (производная произведения).

Доказательство. Доказательство первого утверждения следует из определения производной и соотношения

$$\begin{aligned} f(x+c) + g(x+c) &\equiv f(x) + cf'(x) + g(x) + cg'(x) \equiv \\ &(f(x) + g(x)) + c(f'(x) + g'(x)) \pmod{c^2}. \end{aligned}$$

Аналогично, доказательство второго утверждения следует из определения производной и соотношения

$$\begin{aligned} f(x+c)g(x+c) &\equiv (f(x) + cf'(x))(g(x) + cg'(x)) \equiv \\ &f(x)g(x) + c(f'(x)g(x) + f(x)g'(x)) \pmod{c^2}. \end{aligned}$$

□

Обобщая утверждения леммы, мы получаем равенства

$$(f_1(x) + \dots + f_k(x))' = f_1'(x) + \dots + f_k'(x), \quad (3.9)$$

$$(f_1(x) \cdots f_k(x))' = f_1'(x)f_2(x) \cdots f_k(x) + \dots + f_1(x) \cdots f_{k-1}'(x)f_k(x). \quad (3.10)$$

Из (3.10) получаем равенство

$$(ax^k)' = akx^{k-1}, \quad \text{для } a \neq 0, k > 0. \quad (3.11)$$

Из (3.9) и последнего равенства (3.11) следует соотношение

$$\begin{aligned} f'(x) &= \left(\sum_{k=0}^n a_k x^k \right)' = \sum_{k=1}^n k a_k x^{k-1} = \\ &= \sum_{k=0}^{n-1} (k+1) a_{k+1} x^k = n a_n x^{n-1} + \dots + 2 a_2 x + a_1, \end{aligned} \quad (3.12)$$

которое традиционно используется для определения производной многочлена $f(x)$.

3.5 Решение сравнений по составному модулю

В заключение лекции рассмотрим вопрос о нахождении корней многочлена. Выберем некоторое целое число $m > 0$ с известным разложением на простые множители

$$m = \prod_{i=1}^k p_i^{\alpha_i}, \quad \alpha_i \in \mathbb{N}, \quad \alpha_i > 0, \quad (3.13)$$

и будем считать, что $\mathbb{U} = \mathbb{Z}_m$.

Рассмотрим произвольный многочлен $f(x) \in \mathbb{Z}_m[x]$ и зададимся вопросом о том, как найти его корни в кольце \mathbb{Z}_m . Другими словами, необходимо найти все решения уравнения $f(x) \equiv 0 \pmod{m}$ в кольце \mathbb{Z}_m .

Теорема 3.4. Пусть $f(x) \in \mathbb{Z}_m[x]$ многочлен с целыми коэффициентами и $m > 0$ целое число, для которого известно разложение на простые множители (3.13). Тогда множества целых чисел, удовлетворяющих сравнению

$$f(x) \equiv 0 \pmod{m} \quad (3.14)$$

и системе сравнений

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}}, \\ \dots, \\ f(x) \equiv 0 \pmod{p_k^{\alpha_k}}, \end{cases} \quad (3.15)$$

совпадают.

Обозначим символом $N(m)$ число решений сравнения (3.14), тогда выполнено равенство

$$N(m) = N(p_1^{\alpha_1}) \cdots N(p_k^{\alpha_k}).$$

Доказательство. Пусть целое число e удовлетворяет сравнению (3.14). Тогда $m|f(e)$ и для любого индекса $i = 1, \dots, k$, выполнено $p_i^{\alpha_i}|f(e)$, таким образом, e удовлетворяет системе сравнений (3.15).

Обратно, если e удовлетворяет системе сравнений (3.15), то $p_i^{\alpha_i}|f(e)$ для любого $i = 1, \dots, k$, то есть $f(e)$ является общим кратным чисел $p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$. Согласно лемме 2.5 наименьшее кратное чисел $p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$ есть m . Следовательно, $m|f(e)$ и e является решением системы сравнений (3.15).

Пусть числа a_1, \dots, a_k являются решением системы сравнений (3.15). Согласно «китайской теореме об остатках» (см. теорему 2.3) найдется вычет e по модулю m такой, что $e \equiv a_i \pmod{p_i^{\alpha_i}}$ для всех $i = 1, \dots, k$. Тогда $f(e) \equiv f(a_i) \equiv 0 \pmod{p_i^{\alpha_i}}$ и, по доказанному ранее, e является решением сравнения (3.14). Таким образом мы предъявили способ построения решения сравнения (3.14) по известным решениям системы (3.15).

Далее, пусть числа a_1, \dots, a_k пробегают все возможные наборы значений, являющихся решением системы (3.15), тогда, согласно следствию к теореме 2.3, соответствующие им решения принимают различные значения по модулю m . Отсюда следует, что число решений сравнения (3.14) не менее $N(p_1^{\alpha_1}) \cdots N(p_k^{\alpha_k})$.

По доказанному ранее, каждое решение e сравнения (3.14) удовлетворяет системе сравнений (3.15) и, следовательно, ему соответствует некоторый набор чисел a_1, \dots, a_k . Это доказывает, что других решений, отличных от построенных, сравнение (3.14) не имеет. \square

Доказанная нами теорема сводит поиск корней сравнения (3.14) к поиску корней сравнения $f(x) \equiv 0 \pmod{p^\alpha}$ для некоторого простого числа p и натурального α .

Легко видеть, что если e является корнем $f(x) \pmod{p^\alpha}$, то это же значение должно являться корнем $f(x) \pmod{p}$: из условия $p^\alpha|f(e)$ очевидным образом следует условие $p|f(e)$.

Таким образом, существование корня многочлена $f(x) \pmod{p}$ становится необходимым признаком существования корня многочлена $f(x) \pmod{p^\alpha}$.

Предположим, что нам известен корень многочлена $f(x) \pmod{p}$. Следующая теорема дает ответ на вопрос — как найти корень многочлена $f(x) \pmod{p^\alpha}$.

Теорема 3.5. Пусть p простое число, $f(x)$ многочлен с целыми коэффициентами и e целое число, удовлетворяющее условиям

$$f(e) \equiv 0 \pmod{p}, \quad f'(e) \not\equiv 0 \pmod{p}.$$

Тогда при любом натуральном $\alpha \geq 1$ существует единственное решение сравнения

$$f(x) \equiv 0 \pmod{p^\alpha},$$

принадлежащее классу вычетов $x \equiv e \pmod{p}$.

Доказательство. Докажем теорему индукцией по степеням простого числа p . При $\alpha = 1$, утверждение теоремы, очевидно, выполняется.

Предположим, что утверждение теоремы выполнено для всех целых степеней, меньших либо равных α , и обозначим e_α корень многочлена $f(x) \pmod{p^\alpha}$, то есть $f(e_\alpha) \equiv 0 \pmod{p^\alpha}$ и $e_\alpha \equiv e \pmod{p}$.

Обозначим $e_{\alpha+1}$ корень многочлена $f(x) \pmod{p^{\alpha+1}}$ и будем искать его в виде

$$e_{\alpha+1} = e_\alpha + tp^k, \quad t \in \mathbb{Z}, \quad 0 \leq t < p. \quad (3.16)$$

Тогда $e_{\alpha+1} \equiv e_\alpha \equiv e \pmod{p}$. Воспользуемся равенством (3.8) и запишем сравнение

$$f(e_{\alpha+1}) = f(e_\alpha + tp^k) \equiv f(e_\alpha) + tp^\alpha f'(e_\alpha) \pmod{p^{2\alpha}}.$$

Поскольку мы считаем, что $e_{\alpha+1}$ является корнем, то мы можем записать равенство

$$0 = f(e_\alpha) + tp^\alpha f'(e_\alpha) + hp^{\alpha+1},$$

для некоторого целого значения h . Поскольку по предположению индукции $f(e_\alpha)$ делится на p^α , то, сокращая полученное равенство на p^α , получаем сравнение

$$t \equiv -\frac{f(e_\alpha)}{p^\alpha f'(e_\alpha)} \pmod{p}. \quad (3.17)$$

Поскольку $f'(e_\alpha) \not\equiv 0 \pmod{p}$, то значение неизвестного t единственным образом определяется сравнением (3.17) \square

Таким образом, если нам известны корни многочлена $f(x)$ по модулю простого числа p , то теорема 3.5 дает нам способ определения всех корней многочлена $f(x)$ по модулю p^α . Этот способ часто называют подъемом решения. Однако он не работает, если многочлен $f(x)$ имеет кратные корни.

Действительно, согласно основной теореме арифметики для многочленов, если e корень многочлена $f(x) \pmod{p}$, то

$$f(x) \equiv (x - e)^\gamma u(x) \pmod{p}, \quad \text{НОД}((x - e), u(x)) = 1$$

где натуральное число $\gamma \geq 1$ является кратностью корня e . Для производной многочлена выполнено сравнение

$$\begin{aligned} f'(x) &\equiv \gamma(x - e)^{\gamma-1}u(x) + (x - e)^\gamma u'(x) \equiv \\ &\equiv (x - e)^{\gamma-1}(\gamma u(x) + u'(x)) \pmod{p}, \end{aligned}$$

из которого следует, что при $\gamma > 1$, выполнено $f'(e) \equiv 0 \pmod{p}$ и условия теоремы 3.5 не выполнены.

Теорема 3.6. Пусть p простое число, $f(x)$ многочлен с целыми коэффициентами и e целое число, удовлетворяющее условиям

$$f(e) \equiv 0 \pmod{p}, \quad f'(e) \equiv 0 \pmod{p}.$$

Пусть $\beta \geq 1$ максимальное число такое, что $f(e) \equiv 0 \pmod{p^\beta}$. Тогда сравнение $f(x) \equiv 0 \pmod{p^\alpha}$ разрешимо только при $\alpha \leq \beta$ и корнем является значение e .

Доказательство. Очевидно, что при $\alpha \leq \beta$ из сравнения $f(e) \equiv 0 \pmod{p^\beta}$ следует утверждение теоремы. Покажем, что при $\alpha > \beta$ решений не существует.

Обозначим $e_{\beta+1} = e + tp^{\beta+1}$ и запишем сравнение

$$f(e_{\beta+1}) = f(e) + tp^{\beta+1}f'(e) \pmod{p^{2(\beta+1)}}.$$

Если $p^{\beta+1}$ не делит $f(e)$, то правая часть в приведенном сравнении не делится на $p^{\beta+1}$. Отсюда следует, что $f(e_{\beta+1})$ не делится на $p^{\beta+1}$, следовательно, теорема доказана. \square

Суммируя утверждения двух последних теорем, мы можем предложить алгоритм для поднятия решения.

Алгоритм 3.3

Вход: Простое число p , натуральное число $\alpha > 1$, многочлен $f(x)$ и целое число e такое, что $f(e) \equiv 0 \pmod{p}$.

Выход: Целое число e_α такое, что $f(e_\alpha) \equiv 0 \pmod{p^\alpha}$.

1. Вычислить многочлен $f'(x)$.
2. Если $f'(e) \equiv 0 \pmod{p}$, то перейти на шаг 7.
Иначе определить $e_k = e$ и $k = 1$.
3. Пока $k \leq \alpha$ выполнять
 - 3.1. Вычислить вычет $t \equiv -\frac{f(e_k)}{p^k f'(e_k)} \pmod{p}$ и определить $e_k = e_k + tp^k$.
 - 3.2. Вычислить $k = k + 1$.
4. Закончить алгоритм и вернуть значение $e_\alpha = e_k$.
5. Определить $\beta = 0$ и $t = f(e)$.
6. Пока $t \equiv 0 \pmod{p}$ выполнять
 - 6.1. Вычислить $t = \frac{t}{p}$ и $\beta = \beta + 1$.
7. Если $\beta > \alpha$, то закончить алгоритм с уведомлением о том, что решений нет.
Иначе закончить алгоритм и вернуть значение $e_\alpha = e$. □

Приведенный алгоритм проверяет значение производной многочлена $f(x)$ в точке e и, в зависимости от того, равно ли это значение нулю или нет, следует утверждением теорем 3.5 и 3.6.

Пример 3.2. Приведем пример применения данного алгоритма и найдем корни многочлена $f(x) = x^3 + 2x^2 + 3x + 2$ по модулю 49. Рассмотрим сравнение $f(x) \equiv 0 \pmod{7}$, которое имеет два корня $e = 6$ и $\hat{e} = 3$. Вычислим производную $f'(x) = 3x^2 + 4x + 3$ и определим кратности корней.

Поскольку $f'(6) = 135 \equiv 2 \pmod{7}$, то кратность первого корня $e = 6$ равна единице. Вычисляя $f'(3) = 42 \equiv 0 \pmod{7}$ получаем, что кратность второго корня $\hat{e} = 3$ больше единицы. Так как многочлен $f(x)$ имеет не более трех корней заключаем, что кратность корня $\hat{e} = 3$ равна двум.

Найдем корень e_2 многочлена $f(x)$ по модулю 49 такой, что $e_2 \equiv e \pmod{7}$. Для этого вычислим

$$t \equiv -\frac{f(6)}{7f'(6)} \equiv -\frac{308}{7 \cdot 132} \equiv 6 \pmod{7}.$$

и определим $e_2 = 6 + 6 \cdot 7 = 48$. Проверяя, получаем $f(48) \equiv f(-1) \equiv 0 \pmod{49}$, следовательно найденное нами значение e_2 действительно является корнем многочлена $f(x)$ по модулю 49.

Рассмотрим второй корень $\hat{e} = 3$. Поскольку $f'(3) \equiv 0 \pmod{7}$, нам достаточно вычислить $f(3) = 56$. Поскольку $f(3) \not\equiv 0 \pmod{49}$, то из утверждения теоремы 3.6 следует, что значения \hat{e}_2 такого, что $f(\hat{e}_2) \equiv 0 \pmod{49}$ и $\hat{e}_2 \equiv \hat{e} \pmod{7}$, не существует. Таким образом, исходное сравнение $f(x) \equiv 0 \pmod{49}$ имеет только одно решение и оно равно 48.

В следующей лекции мы подробно рассмотрим вопрос о том, как находить решения полиномиальных сравнений по простому модулю.

СРАВНЕНИЯ СТАРШИХ СТЕПЕНЕЙ

Определение квадратичного вычета - Символ Лежандра - Теорема о числе решений - Свойства символа Лежандра - Определение символа Якоби, его свойства - Алгоритм вычисления символа Якоби - Вычисление квадратного корня: частные случаи - Алгоритм Тонелли-Шенкса - Общее квадратное уравнение - Вероятностный алгоритм вычисления корней многочлена

В этой лекции мы будем рассматривать вопрос о нахождении корней многочленов по модулю простого числа p . В начале мы рассмотрим случай многочленов второй степени, а потом перейдем к поиску корней многочленов произвольной степени.

Мы начнем с самого простого случая, а именно, с уравнения

$$x^2 \equiv a \pmod{p}. \quad (4.1)$$

Для x , удовлетворяющего (4.1), мы будем использовать выражение «квадратный корень из a по модулю простого числа p ».

4.1 Квадратичные вычеты

Рассмотрим вопрос о разрешимости сравнения (4.1).

Лемма 4.1. Пусть p нечетное простое число, a — целое число, взаимно простое с p . Если сравнение (4.1) разрешимо, то оно имеет два различных решения.

Доказательство. В начале заметим, что из условия $\text{НОД}(a, p) = 1$ и третьего утверждения леммы 1.2 следует, что $a \not\equiv 0 \pmod{p}$.

Пусть x_1 — некоторое, отличное от нуля решение сравнения (4.1). Обозначим $x_2 \equiv -x_1 \pmod{p}$. Тогда x_2 также является решением сравнения (4.1), в силу того, что $(x_2)^2 \equiv (-x_1)^2 \equiv a \pmod{p}$.

Второе решение отлично от первого, так как в противном случае были бы выполнены сравнения

$$x_2 \equiv x_1 \pmod{p} \quad \text{или} \quad 2x_1 \equiv 0 \pmod{p},$$

что невозможно, так как $\text{НОД}(2, p) = \text{НОД}(x_1, p) = 1$ и $x_1 \not\equiv 0$. \square

В случае, когда p четное простое число, то есть $p = 2$, решения сравнения (4.1) легко выписать в явном виде. Действительно, для a возможно всего два варианта $a = 0$ или 1 , из чего вытекает, что $x \equiv a \pmod{2}$.

Определение 4.1. Пусть a, p — целые, взаимно простые числа. Мы будем называть целое число a квадратичным вычетом по модулю p , если разрешимо сравнение (4.1). В противном случае, мы будем называть число a квадратичным невычетом.

Следующая лемма позволяет получить узнать точное число квадратичных вычетов и квадратичных невычетов по модулю простого числа.

Лемма 4.2. Пусть p нечетное простое число. Среди чисел $1, 2, \dots, p-1$ содержится равное число квадратичных вычетов и квадратичных невычетов по модулю p .

Доказательство. Среди вычетов $1, 2, \dots, p-1$ квадратичными вычетами являются только те, квадраты которых сравнимы с числами

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2. \quad (4.2)$$

Для вычетов k таких, что $1 \leq k \leq \frac{p-1}{2}$, это очевидно. Для остальных вычетов, при $\frac{p-1}{2} < k \leq p-1$, выполнено

$$k^2 \equiv (p-k)^2 \equiv l^2 \pmod{p}, \quad \text{где } 1 \leq l < \frac{p-1}{2}.$$

Пусть среди чисел (4.2) найдется хотя бы одна пара совпадающих, то есть

$$k^2 \equiv l^2 \pmod{p}, \quad 1 \leq k < l \leq \frac{p-1}{2}.$$

Тогда сравнению $x^2 \equiv l^2 \pmod{p}$ удовлетворяет четыре решения: $k, l, -k$ и $-l$, что противоречет лемме 4.1.

Следовательно, числа (4.2) попарно несравнимы и среди всех вычетов по модулю p : $1, 2, \dots, p-1$ найдется ровно $\frac{p-1}{2}$ квадратичных вычетов. Остальные — квадратичные невычеты. \square

Введем в рассмотрение функцию, которая позволяет говорить о разрешимости сравнения (4.1) и проверять является ли целое число квадратичным вычетом или нет.

Определение 4.2. Пусть p нечетное простое число, a — целое число, взаимно простое с p . Мы будем называть символом Лежандра и обозначать символом $\left(\frac{a}{p}\right)$ функцию, удовлетворяющую равенству

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ квадратичный вычет,} \\ -1, & \text{если } a \text{ квадратичный невычет.} \end{cases}$$

Сформулируем теорему о числе решений сравнения (4.1).

Теорема 4.1. Пусть p нечетное простое число. Тогда число решений сравнения $x^2 \equiv a \pmod{p}$ равно

1. нулю, если $\left(\frac{a}{p}\right) = -1$,
2. единице, если $a \equiv 0 \pmod{p}$,
3. двум, если $\left(\frac{a}{p}\right) = 1$.

Доказательство. Доказательство первого и третьего утверждений теоремы, очевидно, следует из леммы 4.1 и определения символа Лежандра.

Нам осталось доказать второе утверждение при $a \equiv 0 \pmod{p}$. Легко видеть, что $x \equiv 0 \pmod{p}$ является решением сравнения (4.1). Пусть существует второе решение z такое, что $z \not\equiv 0 \pmod{p}$. Тогда равенство (4.1) можно записать в виде

$$z^2 = kp, \tag{4.3}$$

при некотором целом k .

Поскольку p простое число, то $\text{НОД}(z, p) = 1$ и из леммы 1.4 следует, что $k|z$. Тогда, сокращая в равенстве (4.3) множитель $z \neq 0$, получаем, что $z = lp$ или, что равносильно, $z \equiv 0 \pmod{p}$. Мы получили противоречие с выбором z , которое завершает доказательство теоремы. \square

Для проверки разрешимости сравнения (4.1) нам нужен эффективный алгоритм вычисления символа Лежандра. Этот алгоритм может быть сгенерирован на основе утверждений следующей леммы.

Лемма 4.3. Пусть p нечетное простое число, a целое число, взаимно простое с p , тогда для символа Лежандра $\left(\frac{a}{p}\right)$ выполнены следующие свойства.

1. если $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,
2. **Критерий Эйлера:** $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$,
3. $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,
4. если $a = bc$, $a \neq 0$, где b, c целые числа, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \left(\frac{c}{p}\right)$,

$$5. \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p},$$

6. **Квадратичный закон взаимности Гаусса:** если a и p — простые нечетные числа, то

$$\left(\frac{a}{p}\right) = (-1)^{\frac{a-1}{2} \frac{p-1}{2}} \left(\frac{p}{a}\right)$$

Доказательство. Первое утверждение леммы следует из того, что разрешимость сравнения (4.1) не зависит от представителя класса вычетов по модулю p .

Перейдем к доказательству с критерия Эйлера. Поскольку $p-1$ является четным числом, то в силу малой теоремы Ферма, см. теорему 2.7, выполнено сравнение

$$a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

Тогда из леммы 1.4 следует, что для любого a , $\text{НОД}(a, p) = 1$, выполнено одно из сравнений

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \quad (4.4)$$

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad (4.5)$$

Пусть a квадратичный вычет по модулю p и x решение сравнения (4.1). Поскольку x взаимно просто с p , то применяя малую теорему Ферма, см теорему 2.7, получаем

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Следовательно, любой квадратичный вычет a удовлетворяет сравнению (4.4).

Оставшиеся $\frac{p-1}{2}$ значений удовлетворяют сравнению (4.5) и, согласно лемме 4.2, являются квадратичными невычетами. Критерий Эйлера доказан.

Третье утверждение леммы, очевидно, вытекает из второго и не требует отдельного доказательства.

Критерий Эйлера позволяет доказать и четвертое утверждение леммы. Действительно, если $a = bc$, то

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \left(b^{\frac{p-1}{2}}\right) \cdot \left(c^{\frac{p-1}{2}}\right) \equiv \left(\frac{b}{p}\right) \left(\frac{c}{p}\right) \pmod{p}.$$

Из четвертого утверждения леммы следует, что в числителе символа Лежандра можно отбросить любой квадратный множитель, то есть выполнено равенство

$$\left(\frac{a^2b}{p}\right) = \left(\frac{b}{p}\right).$$

□

Для доказательства двух последних утверждений леммы нам потребуются дополнительные усилия. Из достаточно обширного списка опубликованных на русском языке доказательств квадратичного закона взаимности, мы остановимся на классическом доказательстве, изложенном в книге [30]. Это третье доказательство квадратичного закона взаимности из шести, данных Гауссом, последняя его часть принадлежит Кронекеру.

В начале нам потребуется следующая лемма.

Лемма 4.4 (лемма Гаусса). Пусть p нечетное простое число, a целое число, взаимно простое с p , $\text{НОД}(a, p) = 1$, тогда для символа Лежандра $\left(\frac{a}{p}\right)$ выполнено равенство

$$\left(\frac{a}{p}\right) = (-1)^\mu,$$

где μ число отрицательных абсолютно-наименьших вычетов по модулю p (см. определение 2.4) среди чисел $a, 2a, \dots, \frac{p-1}{2}a$.

Доказательство. Обозначим символами

$$a_1, a_2, \dots, a_\lambda, -b_1, -b_2, \dots, -b_\mu, \tag{4.6}$$

абсолютно наименьшие вычеты чисел $a, 2a, \dots, \frac{p-1}{2}a$ по модулю p , то есть для всех $i = 1, \dots, \lambda, j = 1, \dots, \mu$ выполнено

$$-\frac{p-1}{2} \leq a_i \leq \frac{p-1}{2}, \quad -\frac{p-1}{2} \leq -b_j \leq \frac{p-1}{2}.$$

Мы считаем, что все a_i, b_j положительны, поэтому в (4.6) содержится λ положительных чисел и μ отрицательных и $\lambda + \mu = \frac{p-1}{2}$. Все числа

$$a_1, a_2, \dots, a_\lambda, b_1, b_2, \dots, b_\mu,$$

целые, положительные, различные по модулю p и меньшие, чем $\frac{p}{2}$, следовательно, ими исчерпывается множество всех целых чисел от 1 до $\frac{p-1}{2}$.

Перемножая их, получим равенство

$$a_1 a_2 \cdots a_\lambda b_1 b_2 \cdots b_\mu = \left(\frac{p-1}{2}\right)! \quad (4.7)$$

Каждое из чисел (4.6) сравнимо только с одним произведением ka , где $k = 1, \dots, \frac{p-1}{2}$, таким образом, с учетом равенства (4.7) получаем сравнение

$$\begin{aligned} \left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} &= a \cdot 2a \cdots \frac{p-1}{2} \equiv a_1 a_2 \cdots a_\lambda b_1 b_2 \cdots b_\mu (-1)^\mu \equiv \\ &\equiv \left(\frac{p-1}{2}\right)! (-1)^\mu \pmod{p}. \end{aligned}$$

Сокращая обе части сравнения на множитель $\left(\frac{p-1}{2}\right)!$ получаем сравнение,

$$(-1)^\mu \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

которое выполнено в силу критерия Эйлера, см. утверждение 2 леммы 4.3. Учитывая, что в правой и левой частях приведенного сравнения стоят числа, не превосходящие по абсолютной величине единицы, то разность между ними, по абсолютной величине, не превосходит двух и меньше любого нечетного простого числа p . Следовательно, мы можем заменить знак сравнения на знак равенства. Лемма доказана. \square

Завершение доказательства леммы 4.3. Рассмотрим остальные утверждения леммы 4.3. Для этого зафиксируем множество чисел $a, 2a, \dots, \frac{p-1}{2}a$ и разделим каждое из них с остатком на p

$$\begin{cases} a = q_1 p + r_1, \\ 2a = q_2 p + r_2, \\ \dots \\ \frac{p-1}{2}a = q_{\frac{p-1}{2}} p + r_{\frac{p-1}{2}}, \end{cases} \quad (4.8)$$

где $0 \leq r_k < p$, $1 \leq k \leq \frac{p-1}{2}$. В обозначениях леммы Гаусса (лемма 4.4) получаем, что остатки r_k совпадают со множеством чисел

$$a_1, a_2, \dots, a_\lambda, p - b_1, p - b_2, \dots, p - b_\mu,$$

следовательно, можно записать равенство

$$\sum_{k=1}^{\frac{p-1}{2}} r_k = A - B + \mu p, \quad A = a_1 + \dots + a_\lambda, \quad B = b_1 + \dots + b_\mu.$$

Сложим почленно все равенства в (4.8) и, учитывая равенство¹

$$1 + 2 + \dots + \frac{p-1}{2} = \left(1 + \frac{p-1}{2}\right) \frac{p-1}{4} = \frac{p^2-1}{8},$$

получим

$$a \left(\frac{p^2-1}{8} \right) = p \sum_{k=1}^{\frac{p-1}{2}} q_k + A - B + \mu p. \quad (4.9)$$

Из доказательства леммы Гаусса следует, что все числа a_1, \dots, a_λ и b_1, \dots, b_μ суть числа от 1 до $\frac{p-1}{2}$. Следовательно,

$$A + B = 1 + 2 + \dots + \frac{p-1}{2} = \frac{p^2-1}{8}, \quad \text{или} \quad A = \frac{p^2-1}{8} - B.$$

Подставляя в (4.9) полученные равенства и перенося $\frac{p^2-1}{8}$ в правую часть, получим

$$\frac{p^2-1}{8}(a-1) = p \sum_{k=1}^{\frac{p-1}{2}} q_k - 2B + \mu p. \quad (4.10)$$

Поскольку p нечетное число, то выполнено сравнение $p \equiv 1 \pmod{2}$. Пусть $a = 2$, тогда равенство (4.10) может быть записано в виде сравнения

$$\frac{p^2-1}{8} \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \mu \pmod{2}.$$

Заметим, что при $a = 2$ значения всех q_k , $1 \leq k \leq \frac{p-1}{2}$, определяемых равенствами (4.8), равны нулю. Это, очевидно, следует из того, все числа вида ka при всех $1 \leq k \leq \frac{p-1}{2}$ не превосходят величины p . Таким образом

$$\frac{p^2-1}{8} \equiv \mu \pmod{2}$$

¹Мы используем равенство $1 + 2 + \dots + m = \frac{m(m+1)}{2}$, при $m = \frac{p-1}{2}$

и, учитывая лемму Гаусса, мы завершаем доказательство пятого утверждения леммы

$$\left(\frac{2}{p}\right) = (-1)^\mu = (-1)^{\frac{p^2-1}{8}}.$$

Перейдем к доказательству последнего, шестого утверждения леммы доказательству квадратичного закона взаимности Гаусса. Пусть a нечетное простое число, отличное от p . Тогда равенство (4.10) может быть записано в виде сравнения

$$0 \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \mu \pmod{2} \quad \text{или} \quad \sum_{k=1}^{\frac{p-1}{2}} q_k \equiv \mu \pmod{2}.$$

В силу определения, выполнено равенство $q_k = \left[\frac{ka}{p}\right]$ и $\mu \equiv \sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]$, откуда, по лемме Гаусса, получаем

$$\left(\frac{a}{p}\right) = (-1)^\mu = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]}.$$

Аналогичными рассуждениями получаем равенство $\left(\frac{p}{a}\right) = (-1)^{\sum_{s=1}^{\frac{a-1}{2}} \left[\frac{sp}{a}\right]}$, следовательно

$$\left(\frac{a}{p}\right) \left(\frac{p}{a}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] + \sum_{s=1}^{\frac{a-1}{2}} \left[\frac{sp}{a}\right]}.$$

Нам осталось вычислить сумму, образующую степень, в которую возводится -1 , и показать, что выполнено равенство

$$\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right] + \sum_{s=1}^{\frac{a-1}{2}} \left[\frac{sp}{a}\right] = \frac{(p-1)(a-1)}{4}.$$

Для этого рассмотрим выражение

$$\frac{s}{a} - \frac{k}{p}, \quad \text{где} \quad 1 \leq k \leq \frac{p-1}{2}, \quad 1 \leq s \leq \frac{a-1}{2}. \quad (4.11)$$

Учитывая пределы для переменных k и s получим, что разность (4.11) может принимать $\frac{1}{4}(p-1)(a-1)$ различных от нуля значений. Подсчитаем количество положительных и отрицательных значений.

Пусть $\frac{s}{a} - \frac{k}{p} > 0$, то есть $k < \frac{sp}{a}$. Тогда, при фиксированном значении s переменная k может принимать значения $1, 2, \dots, \left\lfloor \frac{sp}{a} \right\rfloor$. Поскольку s принимает все значения, не превосходящие $\frac{a-1}{2}$ получим, что существует всего $\sum_{s=1}^{\frac{a-1}{2}} \left\lfloor \frac{sp}{a} \right\rfloor$ положительных значений разности (4.11).

Пусть $\frac{s}{a} - \frac{k}{p} < 0$, то есть $s < \frac{ka}{p}$. Аналогичными рассуждениями получаем, что существует $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor$ отрицательных значений разности (4.11). Тогда, из мощностных соображений, получаем равенство

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{s=1}^{\frac{a-1}{2}} \left\lfloor \frac{sp}{a} \right\rfloor = \frac{1}{4}(p-1)(a-1),$$

которое завершает доказательство леммы. \square

Скажем несколько слов о способах вычисления символа Лежандра. Наиболее очевидный способ заключается в использовании критерия Эйлера. Однако при больших значениях чисел a, p возведение в степень может быть реализовано только с использованием специальных вычислителей или ЭВМ.

Второй подход к вычислению символа Лежандра основывается на факторизации числа a на множители и последующем применении четвертого, пятого и шестого утверждений леммы. Поскольку задача факторизации является, в общем случае, значительно более сложной задачей, то подобный подход тоже не является эффективным.

Для быстрого вычисления символа Лежандра принято использовать его обобщение — символ Якоби. Использование вычислений с символом Якоби оказывается не только эффективнее, чем использование критерия Эйлера, но и позволяет вычислять символ Лежандра для достаточно больших значений p и a без использования специальных вычислителей.

4.2 Символ Якоби

Определение 4.3. Пусть $m > 0$ — нечетное целое число, для которого известно каноническое разложение на простые сомножители

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i},$$

где p_i — простые числа, α_i — целые неотрицательные числа, k — натуральное и $1 \leq i \leq k$.

Рассмотрим целое число a и определим символ Якоби равенством

$$\left(\frac{a}{m}\right) = \begin{cases} 0, & \text{если } \text{НОД}(a, m) > 1, \\ \left(\frac{a}{p_1}\right)^{\alpha_1} \dots \left(\frac{a}{p_k}\right)^{\alpha_k}, & \text{если } \text{НОД}(a, m) = 1, \end{cases}$$

где в последнем произведении используется символ Лежандра.

Символ Якоби вводится для эффективного вычисления символа Лежандра и не несет другой смысловой нагрузки.

Приведем пример и рассмотрим случай $m = pq$, где p, q — простые числа. Выберем квадратичный невычет a по модулям p и q , тогда каждое уравнение системы

$$\begin{cases} x^2 \equiv a \pmod{p}, \\ x^2 \equiv a \pmod{q}, \end{cases}$$

не имеет решений. Таким образом, система решений не имеет и, следовательно, сравнение $x^2 \equiv a \pmod{m}$ также не имеет решений. В то же время выполнено равенство $\left(\frac{a}{m}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{q}\right) = (-1)^2 = 1$.

Лемма 4.5. Пусть $m > 0$ — нечетное целое, a — произвольное целое число. Для символа Якоби $\left(\frac{a}{m}\right)$ выполнены следующие свойства

1. если $b \equiv a \pmod{m}$, то $\left(\frac{b}{m}\right) = \left(\frac{a}{m}\right)$,

2. $\left(\frac{1}{m}\right) = 1$, $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$,

3. если $a = 2$, то $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$,

4. если $a = bc$, то $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right) \left(\frac{c}{m}\right)$,

5. если n, m нечетные целые числа, то

$$\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2} \frac{m-1}{2}} \left(\frac{m}{n}\right).$$

Доказательство. Мы построим доказательство основываясь на утверждениях леммы 4.3.

Пусть $m = \prod_{i=1}^k p_i^{\alpha_i}$ — каноническое разложение числа m на простые сомножители. Для всех простых делителей p_i числа m из сравнения $b \equiv a$

(mod m) следует сравнение $b \equiv a \pmod{p_i}$. Тогда, в силу первого утверждения леммы 4.3, получаем равенство

$$\left(\frac{b}{m}\right) = \prod_{i=1}^k \left(\frac{b}{p_i}\right)^{\alpha_i} = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{\alpha_i} = \left(\frac{a}{m}\right)$$

из которого следует первое утверждение леммы.

Равенство $\left(\frac{1}{m}\right) = 1$ доказывается аналогично. Для доказательства равенства $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$ заметим, что выполнено равенство

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^r \left(\frac{-1}{p_i}\right) = (-1)^{\sum_{i=1}^r \frac{p_i-1}{2}} = (-1)^{2N + \sum_{i=1}^r \frac{p_i-1}{2}},$$

для произвольного целого значения N . Отметим, что произведение и суммирование производится по всем простым сомножителям m с учетом их кратности.

Воспользовавшись равенством

$$\begin{aligned} \frac{m-1}{2} &= \frac{p_1 \cdots p_r - 1}{2} = \\ &= \frac{\left(1 + 2 \cdot \frac{p_1 - 1}{2}\right) \cdots \left(1 + 2 \cdot \frac{p_r - 1}{2}\right) - 1}{2} = \\ &= \frac{p_1 - 1}{2} + \cdots + \frac{p_r - 1}{2} + 2N, \end{aligned}$$

получим равенство $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$, которое завершает доказательство второго утверждения леммы.

Третье утверждение леммы доказывается при помощи аналогичного технического приема. Выполнено равенство

$$\left(\frac{2}{m}\right) = \prod_{i=1}^r \left(\frac{2}{p_i}\right) = (-1)^{\sum_{i=1}^r \frac{p_i^2-1}{8}} = (-1)^{2N + \sum_{i=1}^r \frac{p_i^2-1}{8}},$$

для произвольного целого значения N .

Тогда, воспользовавшись равенством

$$\begin{aligned} \frac{m^2-1}{8} &= \frac{p_1^2 \cdots p_r^2 - 1}{8} = \\ &= \frac{\left(1 + 8 \cdot \frac{p_1^2 - 1}{8}\right) \cdots \left(1 + 8 \cdot \frac{p_r^2 - 1}{8}\right) - 1}{8} = \\ &= \frac{p_1^2 - 1}{8} + \cdots + \frac{p_r^2 - 1}{8} + 2N, \end{aligned}$$

получим третье утверждение леммы.

Легко заметить, что четвертое утверждение леммы доказывается аналогично первому. Действительно

$$\left(\frac{a}{m}\right) = \prod_{i=1}^k \left(\frac{ab}{p_i}\right)^{\alpha_i} = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{\alpha_i} \cdot \prod_{i=1}^k \left(\frac{b}{p_i}\right)^{\alpha_i} = \left(\frac{b}{m}\right) \left(\frac{c}{m}\right).$$

Согласно четвертому утверждению леммы получаем, что в случае, если $a = b^2c$ и $\text{НОД}(a, m) = 1$, то

$$\left(\frac{a}{m}\right) = \left(\frac{b^2c}{m}\right) = \left(\frac{c}{m}\right).$$

Последнее утверждение леммы является аналогом квадратичного закона взаимности Гаусса для символа Якоби. Пусть, как и ранее, $m = \prod_{i=1}^r p_i$ — каноническое разложение числа m на простые сомножители, с учетом их кратности, а $n = \prod_{i=1}^s q_i$ — разложение числа n . Тогда, следуя квадратичному закону взаимности, получим

$$\begin{aligned} \left(\frac{n}{m}\right) &= \prod_{i=1}^r \left(\frac{n}{p_i}\right) = \prod_{j=1}^s \prod_{i=1}^r \left(\frac{q_j}{p_i}\right) = \\ &= (-1)^{\sum_{j=1}^s \sum_{i=1}^r \frac{q_j-1}{2} \cdot \frac{p_i-1}{2}} \prod_{j=1}^s \prod_{i=1}^r \left(\frac{p_i}{q_j}\right) = \\ &= (-1)^{\left(\sum_{j=1}^s \frac{q_j-1}{2}\right) \cdot \left(\sum_{i=1}^r \frac{p_i-1}{2}\right)} \left(\frac{m}{n}\right). \end{aligned}$$

Аналогично рассуждениям, высказанным при доказательстве второго утверждения данной леммы, получим равенства

$$\frac{m-1}{2} = \sum_{i=1}^r \frac{p_i-1}{2} + 2N_1, \quad \frac{n-1}{2} = \sum_{i=1}^s \frac{q_i-1}{2} + 2N_2,$$

где N_1, N_2 некоторые целые числа, и равенство

$$\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}} \left(\frac{m}{n}\right)$$

которое завершает доказательство леммы. \square

Свойства символа Якоби, которые мы только что доказали, позволяют предложить алгоритм нахождения символа Якоби, который не использует полной факторизации числа. Этот алгоритм использует только

деление на двойку, что может быть программно реализовано как сдвиг вправо на один разряд.

Подставляя в символ Якоби вместо m простое число p мы получим способ вычисления символа Лежандра.

Пример 4.1. Перед тем как привести алгоритм, мы рассмотрим пример вычисления символа Якоби, использующий утверждения леммы 4.5.

$$\begin{aligned} \left(\frac{158}{57}\right) &= \left(\frac{44}{57}\right) = \left(\frac{2^2}{57}\right) \left(\frac{11}{57}\right) = \left(\frac{11}{57}\right) = \\ &= (-1)^{\frac{(11-1)(57-1)}{4}} \left(\frac{57}{11}\right) = \left(\frac{57}{11}\right) = \left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1. \end{aligned}$$

Теперь мы можем описать собственно алгоритм вычисления символа Якоби.

Алгоритм 4.1 (Вычисление символа Якоби)

Вход: нечетное целое число $m > 0$ и целое число a .

Выход: символ Якоби $\left(\frac{a}{m}\right)$.

1. Если $a = 0$, то определить $\left(\frac{a}{m}\right) = 0$ и закончить алгоритм.
2. Если $a < 0$, то определить $x = -a$, $y = m$, $s = (-1)^{\frac{m-1}{2}}$,
Иначе определить $x = a$, $y = m$, $s = 1$.
3. Вычислить $c \equiv x \pmod{y}$ и определить $x = c$, $t = 0$.
4. Если $x = 0$, то определить $\left(\frac{a}{m}\right) = 1$ и закончить алгоритм.
5. Пока $2|x$ выполнять
 - 5.1. Определить $x = \frac{x}{2}$ и $t = t + 1$.
6. Если t - нечетно, то определить $s = s \cdot (-1)^{\frac{y^2-1}{8}}$.
7. Если $a > 1$ то
 - 7.1. Определить $s = s \cdot (-1)^{\frac{x-1}{2} \frac{y-1}{2}}$.
 - 7.2. Определить $c = x$, $x = y$, $y = c$ и вернуться на шаг 3.
8. Определить символ Якоби равенством $\left(\frac{a}{m}\right) = s$ и закончить алгоритм. □

Сделаем некоторые замечания, касающиеся практической реализации изложенного алгоритма.

Значение $s = (-1)^{\frac{m-1}{2}}$ на втором шаге алгоритма может быть вычислено следующим образом: если m нечетное число и $m \equiv 1 \pmod{4}$, то $s = 1$, в противном случае $s = -1$.

Действительно, если $m \equiv 1 \pmod{4}$, то

$$m - 1 = 4k \quad \text{и} \quad (-1)^{\frac{m-1}{2}} = (-1)^{2k} = 1,$$

для некоторого целого числа k . Это же замечание относится и к седьмому шагу алгоритма.

Аналогично вычисляется множитель для s на шестом шаге алгоритма. Если m нечетное число, то $m = 4k \pm 1$ для некоторого целого числа k . Тогда

$$\frac{m^2 - 1}{8} = \frac{(4k \pm 1)^2 - 1}{8} = 2k^2 \pm k.$$

Получаем, что при четном k , выполнено равенство $(-1)^{\frac{m^2-1}{2}} = 1$, а при нечетном k — равенство $(-1)^{\frac{m^2-1}{2}} = -1$.

Таким образом, если $m \equiv 1, 7 \pmod{8}$, что равносильно тому, что k четно, то на шестом шаге алгоритма ни чего не происходит. В противном случае, когда $m \equiv 3, 5 \pmod{8}$, величина s меняет знак.

4.3 Вычисление квадратного корня

В предыдущем разделе мы рассмотрели вопрос разрешимости сравнения (4.1)

$$x^2 \equiv a \pmod{p},$$

где p нечетное простое число. Теперь мы покажем как найти решение данного сравнения.

Вначале нам потребуется получить несколько вспомогательных результатов.

Лемма 4.6. Пусть p нечетное простое число, a — целое число, взаимно простое с p . Если сравнение $x^2 \equiv a \pmod{p}$ разрешимо, то выполнены следующие утверждения

1. если $p \equiv 3 \pmod{4}$, то $x \equiv a^{\frac{p+1}{4}} \pmod{p}$,

2. если $p \equiv 5 \pmod{8}$, то

a) если $a^{\frac{p-1}{4}} \equiv 1 \pmod{p}$, то $x \equiv a^{\frac{p+3}{8}} \pmod{p}$,

b) если $a^{\frac{p-1}{4}} \equiv -1 \pmod{p}$, то

$$x \equiv 2a(4a)^{\frac{p-5}{8}} \pmod{p}.$$

Доказательство. Рассмотрим случай $p \equiv 3 \pmod{4}$. Если x удовлетворяет сравнению $x \equiv a^{\frac{p+1}{4}} \pmod{p}$, то, учитывая критерий Эйлера (см. лемму 4.3), получим

$$x^2 \equiv a^{\frac{p+1}{2}} \equiv a(a)^{\frac{p-1}{2}} \equiv a \left(\frac{a}{p} \right) \equiv 1 \pmod{p}.$$

Первое утверждение леммы доказано.

Для доказательства второго утверждения заметим, что если выполнено $p \equiv 5 \pmod{8}$, то $4|p-1$. Поскольку $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, то выполнено одно из двух сравнений

$$a^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}.$$

Рассмотрим случай $a^{\frac{p-1}{4}} \equiv 1 \pmod{p}$ и определим $x \equiv a^{\frac{p+3}{8}} \pmod{p}$, тогда

$$x^2 \equiv a^{\frac{p+3}{4}} \equiv \left(a^{\frac{p-1}{4}}\right) a \equiv a \pmod{p}.$$

В случае, когда $a^{\frac{p-1}{4}} \equiv -1 \pmod{p}$, определим x в соответствии с утверждением леммы, тогда

$$x^2 \equiv 4a^2 (4a)^{\frac{p-5}{4}} \equiv a (4a)^{1+\frac{p-5}{4}} \equiv a 2^{\frac{p-1}{2}} a^{\frac{p-1}{4}} \pmod{p}. \quad (4.12)$$

В силу второго и третьего утверждений леммы 4.3 следует, что

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \equiv -1 \pmod{p},$$

так как $\frac{p^2-1}{8}$ нечетно. Действительно, вспоминая, что $p \equiv 5 \pmod{8}$, получим $\frac{p^2-1}{8} = \frac{(5+8k)^2-1}{8} = 1 + 2(1 + 5k + 4k^2)$, для некоторого целого k . Тогда, возвращаясь к (4.12), получим сравнение

$$x^2 \equiv a 2^{\frac{p-1}{2}} a^{\frac{p-1}{4}} \equiv a(-1)(-1) \equiv a \pmod{p},$$

которое завершает доказательство леммы. □

Из утверждений леммы 4.6 следует, что остался лишь один случай, для которого неизвестен способ определения решения сравнения (4.1), а именно, случай $p \equiv 1 \pmod{8}$.

Мы начнем с доказательства одной «замечательной» леммы. Мы называем ее замечательной, поскольку она будет нами использована не только в данной, но и в последующих лекциях.

Лемма 4.7. Пусть $p = 2^n q + 1$ простое число, q нечетное целое и a целое число такое, что $\text{НОД}(a, p) = 1$. Тогда

1. либо $a^q \equiv 1 \pmod{p}$,
2. либо найдется такое целое число k , $0 \leq k < n$, что

$$a^{2^k q} \equiv -1 \pmod{p}.$$

Доказательство. В силу малой теоремы Ферма (см. теорему 2.7) выполнено сравнение

$$a^{p-1} - 1 \equiv a^{2^n q} - 1 \equiv \left(a^{2^{n-1}q} - 1\right) \left(a^{2^{n-1}q} + 1\right) \equiv 0 \pmod{p}. \quad (4.13)$$

Тогда, в силу леммы 1.4, либо правая скобка, либо левая скобка в сравнении (4.13) делится на p . Если это правая скобка, то выполнено сравнение $a^{2^{n-1}q} \equiv -1 \pmod{p}$ и $k = n - 1$. Если же это левая скобка, то мы получаем сравнение

$$a^{2^{n-1}q} - 1 \equiv \left(a^{2^{n-2}q} - 1\right) \left(a^{2^{n-2}q} + 1\right) \equiv 0 \pmod{p}.$$

Аналогично сравнению (4.13) получаем, что либо $a^{2^{n-2}q} \equiv -1 \pmod{p}$ и $k = n - 2$, либо $a^{2^{n-2}q} - 1 \equiv 0 \pmod{p}$.

Продолжим далее и, если не для одного $k = n - 2, \dots, 1$ не будет выполнено утверждение леммы, придем к сравнению

$$(a^q + 1)(a^q - 1) \equiv 0 \pmod{p},$$

из которого вытекает сравнение $a^q \equiv \pm 1 \pmod{p}$, а также доказательство леммы. \square

Из первого утверждения доказанной нами леммы получаем следующий результат. Если a квадратичный вычет по модулю p и выполнено первое утверждение леммы 4.7, то есть $a^q \equiv 1 \pmod{p}$, то решение сравнения $x^2 \equiv a \pmod{p}$ определяется сравнением

$$x \equiv a^{\frac{q+1}{2}} \pmod{p}.$$

Действительно,

$$x^2 \equiv \left(a^{\frac{q+1}{2}}\right)^2 \equiv a \cdot a^q \equiv a \pmod{p}.$$

Полученная нами формула является частным случаем более общей ситуации. Основная идея решения сравнения (4.1) заключается в следующем. Легко видеть, что для любого нечетного натурального q выполнено сравнение

$$\left(a^{\frac{q+1}{2}}\right)^2 \equiv a \cdot a^q \pmod{p}.$$

Предположим, что нам известен элемент w такой, что

$$w^2 a^q \equiv 1 \pmod{p}, \quad (4.14)$$

тогда решение сравнения (4.1) примет вид $x \equiv wa^{\frac{q+1}{2}} \pmod{p}$. Действительно,

$$x^2 \equiv w^2 a^{q+1} \equiv a \cdot w^2 a^q \equiv a \pmod{p}.$$

Рассмотренный нами выше случай выполняется при $w = 1$. Для поиска вычетов w , отличных от единицы, нам необходимо рассмотреть случай, когда выполнено второе утверждение леммы 4.7. Для этого нам потребуется еще одна лемма, которая описывает свойства элементов, показатели которых по модулю p являются степенями двойки.

Лемма 4.8. Пусть $p = 2^n q + 1$ простое число, q нечетное целое число и c — произвольный квадратичный невычет по модулю p . Выполнены следующие утверждения.

1. Обозначим $z \equiv c^q \pmod{p}$, тогда показатель z по модулю p равен 2^n , то есть $\text{ord}_p z = 2^n$.
2. Обозначим $z_k \equiv z^{2^k} \pmod{p}$, тогда $z_k \equiv z_{k-1}^2 \pmod{p}$ и $\text{ord}_p z_k = 2^{n-k}$.
3. Пусть u, v вычеты такие, что $\text{ord}_p u = \text{ord}_p v = 2^{k+1}$, тогда выполнено условие $\text{ord}_p(uv) | 2^k$.

Доказательство. Рассмотрим произвольный квадратичный невычет c по модулю p . Тогда $\left(\frac{c}{p}\right) = -1$ и из критерия Эйлера (см. лемму 4.3), малой теоремы Ферма (см. теорему 2.7) и сравнений

$$\begin{aligned} c^{\frac{p-1}{2}} &\equiv c^{2^{n-1}q} \equiv z^{2^{n-1}} \equiv -1 \pmod{p}, \\ c^{p-1} &\equiv c^{2^n q} \equiv z^{2^n} \equiv 1 \pmod{p}, \end{aligned}$$

следует, что $\text{ord}_p z = 2^n$, то есть первое утверждение леммы.

Легко видеть, что $z_k \equiv z^{2^k} \equiv \left(z^{2^{k-1}}\right)^2 \equiv z_{k-1}^2 \pmod{p}$. Более того, из первого утверждения леммы 2.4 следует, что

$$\text{ord}_p z_k = \text{ord}_p z^{2^k} = \frac{\text{ord}_p z}{2^k} = 2^{n-k},$$

то есть второе утверждение леммы.

Рассмотрим третье утверждение леммы. Поскольку $\text{ord}_p u = \text{ord}_p v = 2^{k+1}$, то выполнены сравнения

$$u^{2^k} \equiv -1 \pmod{p}, \quad v^{2^k} \equiv -1 \pmod{p}.$$

Перемножая указанные сравнения получим $(uv)^{2^k} \equiv 1 \pmod{p}$. Учитывая третье утверждение леммы 2.3 получим $\text{ord}_p(uv) | 2^k$. Лемма доказана. \square

Введенные нами в утверждении леммы вычеты z_k будут использованы для построения вычета w такого, что выполнено сравнение (4.14)

$$w^2 a^q \equiv 1 \pmod{p}.$$

При этом заметим, что выполнение данного сравнения равносильно выполнению равенства $\text{ord}_p(w^2 a^q) = 1$. Напомним, что в силу леммы 4.7, найдется такой индекс k , $0 \leq k < n$, что $a^{2^k q} \equiv -1 \pmod{p}$, следовательно, $\text{ord}_p a^q = 2^{k+1}$.

Определим конечную последовательность u_1, u_1, \dots, u_{r+1} сравнениями

$$\begin{aligned} u_1 &\equiv a^q \pmod{p}, \\ u_2 &\equiv z_{l_1} u_1 \pmod{p}, \\ &\dots \\ u_{r+1} &\equiv z_{l_r} u_r \pmod{p}, \end{aligned}$$

где индексы l_j выбираются из условия $\text{ord}_p u_j = \text{ord}_p z_{l_j}$, $j = 1, \dots, r$, а вычеты z_{j_j} определяются вторым утверждением леммы 4.8.

Из третьего утверждения леммы 4.8 следует, что

$$\text{ord}_p u_j \mid \text{ord}_p u_{j-1}, \quad \text{при } j = 2, \dots, r,$$

и выполнена цепочка неравенств

$$\text{ord}_p u_1 > \text{ord}_p u_2 > \dots > \text{ord}_p u_{r+1} = 1$$

для некоторого значения $r \geq 1$. Таким образом мы получаем, что

$$u_{r+1} \equiv z_{l_1} \cdots z_{l_r} \cdot a^q \equiv 1 \pmod{p}.$$

Вспомним, что из второго утверждения леммы 4.8 следуют сравнения $z_{l_j} \equiv z_{l_{j-1}}^2 \pmod{p}$ и обозначим $w = z_{l_1-1} \cdots z_{l_r-1}$. Тогда выполняется нужное нам сравнение (4.14)

$$z_{l_1} \cdots z_{l_r} \cdot a^q \equiv (z_{l_1-1} \cdots z_{l_r-1})^2 a^q \equiv w^2 a^q \equiv 1 \pmod{p}$$

и мы можем определить неизвестное x сравнением

$$x \equiv (z_{l_1-1} \cdots z_{l_r-1}) \cdot a^{\frac{q+1}{2}} \pmod{p}.$$

Мы рассмотрели все варианты, возникающие при вычислении решения сравнения $x^2 \equiv a \pmod{p}$. Суммируем все изложенное выше и приведем алгоритм, который позволяет находить решения рассматриваемого сравнения.

Алгоритм 4.2 (Алгоритм Тонелли-Шенкса)

Вход: нечетное простое число $p = 2^n q + 1$, q — нечетное целое и целое число a такое, что $\left(\frac{a}{p}\right) = 1$.

Выход: вычет x такой, что $x^2 \equiv a \pmod{p}$.

1. Если $p \equiv 3 \pmod{4}$, то определить $x \equiv a^{\frac{p+1}{4}} \pmod{p}$ и остановиться.
2. Если $p \equiv 5 \pmod{8}$ то
 - 2.1. Если $a^{\frac{p-1}{4}} \equiv 1 \pmod{p}$, то определить $x \equiv a^{\frac{p+3}{8}} \pmod{p}$ и остановиться.
 - 2.2. Если $a^{\frac{p-1}{4}} \equiv -1 \pmod{p}$, то определить $x \equiv 2a(4a)^{\frac{p-5}{8}} \pmod{p}$ и остановиться.
3. Выбирая случайным образом найти квадратичный невычет c и определить

$$z \equiv c^q \pmod{p}, \quad r = n.$$

4. Определить

$$t \equiv a^{\frac{q-1}{2}} \pmod{p}, \quad x \equiv at \pmod{p}, \quad b \equiv xt \pmod{p}.$$

5. Если $x \equiv 1 \pmod{p}$, то закончить вычисления,
Иначе вычислить наименьшее m такое, что $b^{2^m} \equiv 1 \pmod{p}$.
6. Определить $t \equiv z^{2^{r-m-1}} \pmod{p}$,

$$z \equiv t^2 \pmod{p}, \quad x \equiv xt \pmod{p}, \quad b \equiv bz \pmod{p}, \quad r = m$$

и вернуться на шаг 5. □

Приведенный алгоритм позволяет найти один корень уравнения $x^2 \equiv a \pmod{p}$, скажем e_1 . Второй корень e_2 , очевидно, находится из равенства $e_2 = p - e_1$.

Легко видеть, что случае $p \not\equiv 1 \pmod{8}$ трудоемкость приведенного алгоритма сравнима с трудоемкостью возведения вычета a в степень и может быть оценена величиной $O(\log p)$.

Теперь мы можем рассмотреть общий случай. Рассмотрим сравнение второй степени

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{4.15}$$

где p — нечетное простое число, $a \not\equiv 0 \pmod{p}$ и b, c — произвольные вычеты по модулю p .

Верна следующая теорема.

Теорема 4.2. Пусть p нечетное простое число, a, b, c целые числа и a взаимно просто с p . Пусть $D \equiv b^2 - 4ac \pmod{p}$. Тогда

1. если $\left(\frac{D}{p}\right) = -1$, то сравнение (4.15) не имеет решений,

2. если $D \equiv 0 \pmod{p}$, то сравнение (4.15) имеет единственное решение $e \equiv -\frac{b}{2a} \pmod{p}$,

3. если $\left(\frac{D}{p}\right) = 1$, то сравнение (4.15) имеет два различных решения e_1, e_2 , которые удовлетворяют сравнениям

$$e_1 \equiv \frac{-b - \xi}{2a} \pmod{p}, \quad e_2 \equiv \frac{-b + \xi}{2a} \pmod{p},$$

где $\xi^2 \equiv D \pmod{p}$.

Доказательство. Легко заметить, что решения сравнения $ax^2 + bx + c \equiv 0 \pmod{p}$ удовлетворяют также сравнению

$$x^2 + \frac{bx}{a} + \frac{c}{a} \equiv \left(x + \frac{b}{2a}\right)^2 - \left(\frac{D}{4a^2}\right) \equiv 0 \pmod{p}$$

и разрешимость сравнения (4.15) эквивалентна разрешимости сравнения

$$z^2 \equiv D \pmod{p}, \quad \text{где } z \equiv 2ax + b \pmod{p}.$$

Таким образом, мы свели поиск корней многочлена второй степени к поиску квадратных корней из D . Теперь все утверждения доказываемой нами теоремы вытекают из теоремы 4.1. \square

Мы доказали результат о разрешимости сравнения (4.15) по модулю простого числа p в зависимости от величины дискриминанта D . Теперь получим обратное утверждение — о разрешимости сравнения (4.15) для бесконечного множества простых чисел.

Теорема 4.3. Пусть сравнение $ax^2 + bx + c \equiv 0 \pmod{p}$ разрешимо для некоторого нечетного простого числа p , тогда оно разрешимо для всех простых чисел, сравнимых с p по модулю $4|D|$, где $D = b^2 - 4ac$.

Доказательство. Из утверждения теоремы 4.2 следует, что разрешимость исходного сравнения равносильна разрешимости сравнения $z^2 \equiv D \pmod{p}$. Таким образом, для доказательства нашей теоремы достаточно показать, что $\left(\frac{D}{p}\right) = \left(\frac{D}{p_1}\right)$ при $p_1 \equiv p \pmod{4|D|}$.

Разложим дискриминант D в произведение простых сомножителей, с учетом знака, то есть

$$D = (-1)^{\alpha_1} 2^{\alpha_2} \prod_{i=3}^k q_i^{\alpha_i},$$

при некотором натуральном k , где q_i различные нечетные простые числа, α_i неотрицательные целые числа, и рассмотрим несколько случаев.

Случай первый. Поскольку $p_1 \equiv p \pmod{4|D|}$, то $p_1 \equiv p \pmod{4}$ и выполнено сравнение $\frac{p_1-1}{2} \equiv \frac{p-1}{2} \pmod{2}$. Используя третье утверждение леммы 4.3, получаем

$$\left(\frac{-1}{p_1}\right) = (-1)^{\frac{p_1-1}{2}} = (-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right).$$

Случай второй. Предположим, что $\alpha_2 \geq 1$. Тогда $2|D$, выполнено сравнение $p_1 \equiv p \pmod{8}$ и $8|(p_1-p)$. Учитывая, что числа p, p_1 нечетны, мы получаем

$$\frac{p_1^2-1}{8} - \frac{p^2-1}{8} = (p_1+p)\frac{(p_1-p)}{8} \equiv 0 \pmod{2}.$$

Тогда, из пятого утверждения леммы 4.3, следует равенство

$$\left(\frac{2}{p_1}\right) = (-1)^{\frac{p_1^2-1}{8}} = (-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right).$$

Случай третий. Пусть q произвольный нечетный делитель числа D . Если $p_1 \equiv p \pmod{4|D|}$, то $p_1 \equiv p \pmod{q}$ и, в силу первого утверждения леммы 4.3, $\left(\frac{p_1}{q}\right) = \left(\frac{p}{q}\right)$.

С другой стороны, поскольку $4|(p_1-p)$, получаем

$$\frac{(p_1-1)(q-1)}{2} - \frac{(p-1)(q-1)}{2} = (q-1)\frac{(p_1-p)}{4} \equiv 0 \pmod{2}.$$

Воспользовавшись квадратичным законом взаимности, см. шестое утверждение леммы 4.3, запишем равенство

$$\left(\frac{q}{p_1}\right) = (-1)^{\frac{p_1-1}{2} \frac{q-1}{2}} \left(\frac{p_1}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).$$

Собирая все рассмотренные случаи вместе, получаем

$$\begin{aligned} \left(\frac{D}{p_1}\right) &= \left(\frac{-1}{p_1}\right)^{\alpha_1} \left(\frac{2}{p_1}\right)^{\alpha_2} \prod_{i=3}^k \left(\frac{q_i}{p_1}\right)^{\alpha_i} = \\ &= \left(\frac{-1}{p}\right)^{\alpha_1} \left(\frac{2}{p}\right)^{\alpha_2} \prod_{i=3}^k \left(\frac{q_i}{p}\right)^{\alpha_i} = \left(\frac{D}{p}\right). \end{aligned}$$

Теорема доказана. \square

Утверждение доказанной теоремы позволяет в явном виде определить множество всех простых чисел при которых разрешимо сравнение (4.15) при фиксированных значениях параметров a, b и c .

4.4 Вероятностный алгоритм вычисления корней многочленов

Теперь мы зафиксируем простое число p , рассмотрим произвольный многочлен $f(x) = \sum_{k=0}^n a_k x^k$ и зададимся вопросом о поиске решений сравнения

$$f(x) \equiv 0 \pmod{p}.$$

В случае, когда p есть маленькое простое число, мы можем в явном виде перебрать все значения $e = 0, 1, \dots, p-1$ и проверить, вычисляя значения $f(e) \pmod{p}$, какое из них является корнем многочлена. При больших значениях p , очевидно, перебор не является наилучшим способом вычисления корней многочленов.

Далее мы будем считать, что p нечетное, большое простое число. Нам потребуется несколько вспомогательных теоретических результатов.

Лемма 4.9. *Для каждого простого числа p справедливо сравнение*

$$x^p - x \equiv x(x-1)(x-2)\cdots(x-p+1) = \prod_{k=0}^{p-1} (x-k) \pmod{p}. \quad (4.16)$$

Доказательство. Согласно малой теореме Ферма, см. теорему 2.7, для каждого целого числа e , $0 \leq e < p$, выполнено сравнение $e^p \equiv e \pmod{p}$. Следовательно, каждое число e из указанного интервала является корнем многочлена $x^p - x$ в кольце $\mathbb{F}_p[x]$.

С другой стороны, согласно теореме 3.2, для каждого корня e многочлена $f(x)$ выполнено $f(x) \equiv 0 \pmod{x-e}$, то есть многочлен $x-e$ делит многочлен $f(x)$ нацело. Таким образом в поле $\mathbb{F}_p[x]$ многочлен $\prod_{k=0}^{p-1} (x-k)$ делит нацело многочлен $(x^p - x)$.

Поскольку степени обоих многочленов совпадают, а также совпадают коэффициенты при старших степенях, мы делаем вывод о том, что выполнено искомое сравнение (4.16). Лемма доказана. \square

Лемма 4.10. *Пусть $f(x)$ произвольный многочлен из $\mathbb{F}_p[x]$. Определим многочлен $h(x)$*

$$h(x) = \text{НОД}(x^p - x, f(x)).$$

Тогда каждый корень многочлена $h(x)$ является корнем многочлена $f(x)$ и наоборот, то есть множества корней многочленов $h(x)$ и $f(x)$ совпадают.

Доказательство. Согласно основной теореме арифметики для многочленов, см. теорему 3.1, мы можем представить $f(x) = \sum_{k=0}^n a_k x^k$ в виде

$$f(x) = a_n(x - e_1)^{\alpha_1} \cdots (x - e_r)^{\alpha_r} u(x),$$

где e_1, \dots, e_k различные корни многочлена $f(x)$, а многочлен $u(x) \in \mathbb{F}_p[x]$ является произведением неприводимых, то есть не имеющих корней в $\mathbb{F}_p[x]$, многочленов.

Согласно лемме 4.9 многочлен $x^p - x$ в кольце $\mathbb{F}_p[x]$ раскладывается в произведение p различных линейных множителей, следовательно

$$h(x) = \text{НОД}(x^p - x, f(x)) = (x - e_1) \cdots (x - e_r) \in \mathbb{F}_p[x].$$

Последнее равенство завершает доказательство леммы. □

Согласно утверждению последней леммы, мы можем свести задачу определения корней многочлена $f(x)$ к определению корней многочлена $h(x)$, раскладывающегося в произведение линейных множителей, такого, что $\deg h(x) \leq \deg f(x)$.

Теперь опишем вероятностный алгоритм поиска корней многочлена $h(x)$ по модулю простого нечетного числа p . Мы считаем, что $\deg h(x) = r > 1$, поскольку в противном случае, он либо является константой, при $\deg h(x) = 0$, либо линейен, то есть $h(x) = x - e$. В последнем случае вычисление корня тривиально.

Алгоритм 4.3 (Вычисление случайного корня многочлена)

Вход: Нечетное простое число p и многочлен $h(x) \equiv \prod_{k=1}^r (x - e_k) \pmod{p}$, раскладывающийся на линейные множители в $\mathbb{F}_p[x]$ с неизвестными значениями e_1, \dots, e_r .

Выход: Корень многочлена — одно из значений e_1, \dots, e_r .

1. Выбрать случайное значение $c \in \mathbb{F}_p$. Если $h(c) \equiv 0 \pmod{p}$, то закончить алгоритм и вернуть значение c в качестве корня многочлена $h(x)$.
2. Вычислить многочлен $d(x) \in \mathbb{F}_p[x]$

$$d(x) = \text{НОД}\left(h(x), (x - c)^{\frac{p-1}{2}} - 1\right)$$

3. Если $\deg d(x) < 1$ или $\deg d(x) = \deg h(x)$, то вернуться на шаг 1).
4. Если $\deg d(x) = 1$, то закончить алгоритм и вернуть в качестве корня значение свободного члена многочлена $d(x)$.
5. Определить $f(x) = d(x)$ и вернуться на шаг 1). □

Алгоритм 4.3 носит вероятностный характер. Алгоритм случайным образом находит какой-нибудь корень многочлена $h(x)$. При фиксированном числе выборов случайного значения c на первом шаге алгоритма, можно оценить вероятность успешного завершения алгоритма.

Лемма 4.11. Пусть многочлен $h(x)$ удовлетворяет входным данным алгоритма 4.3. Тогда выполнены следующие утверждения

1. алгоритм 4.3 действительно находит корень многочлена $h(x)$.
2. вероятность того, что на шаге 2 алгоритма будет найден многочлен $d(x)$ такой, что $\deg d(x) > 0$, не менее $1/2$.

Доказательство. Покажем, что алгоритм действительно позволяет найти корень многочлена $h(x)$. Завершение работы алгоритма на первом и четвертом шагах очевидно. В первом случае, мы в явном виде предъявляем корень, которым является значение e . Во втором случае, мы находим многочлен $d(x) = x - e$ такой, что $d(x)|h(x) = \prod_{k=1}^r (x - e_k)$. Следовательно, согласно теореме 3.2, значение e — свободный член многочлена $d(x)$ будет являться корнем многочлена $h(x)$.

Если многочлен $d(x) = \mathbf{НОД} \left(h(x), (x - c)^{\frac{p-1}{2}} - 1 \right)$ имеет степень большую единицы, то в силу того, что $d(x)|h(x)$, он является произведением линейных множителей, свободные члены которых являются корнями многочлена $h(x)$. Заметим, что $\deg d(x) < \deg h(x)$, следовательно, после присваивания на 5 шаге алгоритма, степень многочлена уменьшается. Таким образом, после не более чем r делений, мы получим в качестве $d(x)$ многочлен первой степени, что даст нам искомое значение корня.

Для доказательства первого утверждения леммы, нам осталось показать, что мы действительно на втором шаге вычислим многочлен $d(x)$ такой, $d(x)|f(x)$ и $\deg d(x) > 0$.

Поскольку мы считаем, что $\deg h(x) > 1$, то зафиксируем два произвольных корня e_1, e_2 и определим множество \mathcal{D}

$$\mathcal{D} = \{c \in \mathbb{F}_p : (e_1 - c)^{\frac{p-1}{2}} \not\equiv (e_2 - c)^{\frac{p-1}{2}} \pmod{p}\}.$$

Выберем некоторый вычет $c \in \mathcal{D}$ и рассмотрим многочлен

$$v(x) = (x - c)^{\frac{p-1}{2}} - 1, \quad \deg v(x) = \frac{p-1}{2}.$$

В силу критерия Эйлера и свойств символа Лежандра, см. лемму 4.3, для каждого вычета $e \in \mathbb{F}_p$, $e \not\equiv c \pmod{p}$, выполнено сравнение $v(e) \equiv 0 \pmod{p}$, либо сравнение $v(e) \equiv -2 \pmod{p}$. В первом случае, очевидно, получаем, что e является корнем многочлена $v(x)$ по модулю p .

Поскольку вычетов и невычетов по модулю p ровно $\frac{p-1}{2}$, то получаем, что многочлен $v(x)$ раскладывается произведение $\frac{p-1}{2}$ линейных множителей

$$v(x) = (x - \gamma_1) \cdots (x - \gamma_{\frac{p-1}{2}}),$$

где γ_i вычеты, такие что $\gamma_i - c$ является квадратичным вычетом по модулю p . В силу выбора элемента $c \in \mathcal{D}$ по крайней мере один корень многочлена $h(x)$ либо e_1 , либо e_2 входит в множество вычетов $\gamma_1, \dots, \gamma_{\frac{p-1}{2}}$. Следовательно, степень многочлена $d(x) = \text{НОД}(h(x), v(x))$ больше нуля. Первое утверждение леммы доказано.

Для утверждения второго утверждения леммы нам достаточно оценить мощность множества \mathcal{D} .

Рассмотрим многочлен $(e_1 - x)^{\frac{p-1}{2}} - (e_2 - x)^{\frac{p-1}{2}}$ степени $\frac{p-3}{2}$. Согласно теореме 3.3 в поле \mathbb{F}_p этот многочлен имеет не более $\frac{p-3}{2}$ корней. Поскольку корни рассматриваемого многочлена не принадлежат множеству \mathcal{D} , мы получаем что мощность множества \mathcal{D} удовлетворяет неравенству

$$|\mathcal{D}| \geq p - \frac{p-3}{2} = \frac{p+3}{2}.$$

Таким образом выбирая случайное значение c в интервале $0, \dots, p-1$ мы с вероятностью $\frac{p+3}{2p} > 1/2$ выберем значение, принадлежащее множеству \mathcal{D} . Из этого следует второе утверждение леммы. \square

Из утверждений доказанной леммы следует, что в среднем нам потребуется две попытки выбора значения c для того, чтобы разложить на множители многочлен $h(x)$ на втором шаге алгоритма 4.3. Учитывая, что полученное разложение может не дать нам многочлен первой степени, нам потребуется, в среднем, $2r$ попыток выбора значения c для того, чтобы определить корень многочлена $h(x)$. Таким образом, мы можем оценить среднюю трудоемкость алгоритма 4.3 величиной $O(\deg h(x))$.

Теперь суммируем полученные результаты. Пусть нам задан многочлен $f(x) = \sum_{k=0}^n a_k x^k$ с целыми коэффициентами и мы хотим не только найти его корни в поле \mathbb{F}_p , то есть решить сравнение $f(x) \equiv 0 \pmod{p}$, но и представить его в виде

$$f(x) \equiv a_n(x - e_1)^{\alpha_1} \cdots (x - e_r)^{\alpha_r} u(x) \pmod{p},$$

где $u(x)$ есть произведение неприводимых в $\mathbb{F}_p[x]$ многочленов. Для нахождения неизвестных значений $e_1, \dots, e_r, \alpha_1, \dots, \alpha_r$ и $u(x)$ можно предложить следующий алгоритм.

Алгоритм 4.4 (Вычисление всех корней многочлена)

Вход: Простое нечетное число p и многочлен $f(x) = \sum_{k=0}^n a_k x^k$ такой, что $a_n \not\equiv 0 \pmod{p}$.

Выход: Значения $e_1, \dots, e_r, \alpha_1, \dots, \alpha_r$ и многочлен $u(x) \in \mathbb{F}_p[x]$ такие, что выполнено сравнение $f(x) \equiv a_n(x - e_1)^{\alpha_1} \cdots (x - e_r)^{\alpha_r} u(x) \pmod{p}$.

1. Если $a_n \not\equiv 1 \pmod{p}$, то сделать многочлен $f(x)$ унитарным, то есть определить $f(x) \equiv a_n^{-1} f(x) \pmod{p}$.
2. Определить многочлены $u(x) = f(x)$ и $h(x) = \text{НОД}(x^p - x, f(x))$.
3. Если $\deg h(x) = 0$, то закончить алгоритм.
4. Используя алгоритм 4.3 вычислить $e \in \mathbb{F}_p$ такой, что $h(e) \equiv 0 \pmod{p}$ и определить $\alpha = 0$.
5. Пока $f(x) \equiv 0 \pmod{x - e}$ **выполнять**
 - 5.1. Определить $f(x) = \frac{f(x)}{(x-e)}$ и вычислить $\alpha = \alpha + 1$.
6. Вычислить $u(x) = \frac{u(x)}{(x-e)^\alpha}$ и $h(x) = \frac{h(x)}{(x-e)}$.
7. Добавить пару e, α в список корней и их кратностей и перейти на шаг 3. \square

Мы могли бы немного оптимизировать число делений многочлена $h(x)$, возникающих при вызове алгоритма 4.3. Это однако, привело бы нас к рекурсивной версии алгоритма. Поскольку рекурсии являются достаточно медленными при практической реализации на ЭВМ, мы пожертвовали возможностью снизить трудоемкость алгоритма за счет снижения времени его работы: не рекурсивная версия алгоритма, на практике, работает быстрее.

4.5 Оценки числа решений в специальных случаях

Докажем еще один результат о свойствах показателей по простому модулю p . Этот результат будет востребован нами при оценке числа решений полиномиального сравнения $x^m - 1 \equiv 0 \pmod{p}$.

Лемма 4.12. Пусть p нечетное простое число и q натуральное число такое, что $q|p-1$. Найдется вычет a по модулю p такой, что его показатель равен q , то есть $\text{ord}_p a = q$. Более того, множество вычетов

$$a^n \pmod{p}, \quad n = 0, 1, \dots, q-1, \quad \text{и} \quad \text{НОД}(n, q) = 1 \quad (4.17)$$

образует множество всех вычетов, показатель которых равен q . Мощность данного множества равна $\varphi(q)$.

Доказательство. В начале покажем, что для любого натурального q , удовлетворяющего условиям леммы, найдется вычет a , показатель которого равен q . Обозначим $p-1 = qt$ и b — первообразный корень по модулю p . Такой корень существует в силу доказанной нами ранее теоремы 2.9. Тогда, в силу первого утверждения леммы 2.4, получаем, что вычет $a \equiv b^t \pmod{p}$ имеет порядок равный q .

Зафиксируем найденный вычет a и рассмотрим уравнение $x^q \equiv 1 \pmod{p}$ относительно неизвестной x . Согласно теореме 3.3 найдется не более чем q различных вычетов по модулю p , удовлетворяющих данному уравнению. Все эти вычеты содержатся во множестве $a^n \pmod{p}$ при $n = 1, \dots, q-1$, поскольку для любого натурального n выполнено $(a^n)^q \equiv (a^q)^n \equiv 1 \pmod{p}$. Таким образом, любой вычет, показатель которого равен q , содержится в указанном множестве.

Обозначим символом d показатель элемента $a^n \pmod{p}$ при некотором фиксированном индексе n из множества $n = 1, \dots, q-1$. Тогда выполнено сравнение $a^{nd} \equiv 1 \pmod{p}$. Поскольку показатель элемента a равен q , то из третьего утверждения леммы 2.3 получаем, что $q|nd$ или, что равносильно, $nd = kq$ для некоторого натурального k .

Таким образом, равенство $n = q$ возможно только в том случае, когда $\text{НОД}(n, q) = 1$ и мы получаем утверждение нашей леммы. В силу определения функции Эйлера, получаем, что количество чисел n , для которых выполнено условие $\text{НОД}(n, q) = 1$ равно $\varphi(q)$. \square

Теперь докажем необходимый нам результат.

Теорема 4.4. Пусть p нечетное простое число, m натуральное число. Тогда многочлен $x^m - 1$ имеет q корней в поле $\mathbb{F}_p[x]$, где

$$q = \text{НОД}(m, p - 1).$$

Доказательство. Представим m в виде $m = k(p - 1) + r$ и $0 \leq r < p - 1$. Согласно малой теореме Ферма, см. теорему 2.7, для любого целого, взаимно простого с p , числа a выполнено $a^m \equiv (a^{p-1})^k \cdot a^r \equiv a^r \pmod{p}$. Следовательно, каждый корень исходного многочлена является корнем многочлена $x^r - 1 = 0$.

Пусть $q = \text{НОД}(r, p - 1)$ и выполнено равенство $r = qt$ для некоторого натурального t . Тогда, согласно предыдущей лемме, найдется вычет a , показатель которого по модулю p будет равен q , то есть $\text{ord}_p a = q$. Согласно первому утверждению леммы 2.3 получаем, что все вычеты

$$1, a, \dots, a^{q-1} \tag{4.18}$$

попарно несравнимы и выполнено $(a^n)^r \equiv (a^q)^{tn} \equiv 1 \pmod{p}$ при $n = 0, 1, \dots, q - 1$. Таким образом, множество (4.18) образует множество корней корней многочлена $x^r - 1$. Заметим, что не для всех вычетов из множества (4.18) показатель равен q — показатели некоторых элементов из (4.18) могут делить q .

Нам осталось показать, что у многочлена $x^r - 1$ не существует корней, отличных от множества (4.18). Предположим, что это не так, тогда найдется вычет b такой, что $b^r \equiv 1 \pmod{p}$. Пусть s показатель вычета b , тогда, в силу третьего утверждения леммы 2.3, выполнено $s|q$. Поскольку $s|p - 1$, мы получаем, что s является общим делителем чисел r и $p - 1$. В силу выбора, q является наибольшим делителем этих чисел, следовательно, $s|q$, и мы получаем, что b принадлежит множеству (4.18). Мы показали, что $d = \text{НОД}(r, p - 1) = \text{НОД}(m, p - 1)$. Теорема доказана. \square

ПРОСТЫЕ ЧИСЛА

Построение таблицы простых чисел - Вероятностные алгоритмы проверки на простоту - Тест Соловея-Штрассена - Тест Миллера-Рабина - Теорема Поклингтона и ее дополнения - Алгоритмы построения простых чисел - Рекуррентные последовательности Люка - Теорема Моррисона - Рекурсивный алгоритм построения простого числа с известным разложением $p-1$ - Алгоритм построения сильно простого числа.

В криптографических приложениях простые числа играют основополагающую роль, являясь долговременными параметрами криптографических схем. Данные параметры известны всем пользователям криптографических схем и подвергаются атакам нарушителей в первую очередь. В связи с этим, время действия открытых параметров ограничено, что вынуждает разработчиков криптографических схем достаточно часто вырабатывать новые, не использовавшиеся ранее простые числа, удовлетворяющие ряду ограничений.

Приведем пример. Согласно первой редакции стандарта Российской Федерации на электронную цифровую подпись ГОСТ Р 34.10-94, необходимо было строить два простых числа p, q , удовлетворяющих условиям

$$2^{1021} < p < 2^{1024}, \quad q^{254} < q < 2^{256}, \quad p \equiv 1 \pmod{q}.$$

Последняя редакция этого стандарта: ГОСТ Р 34.10-2001 накладывает другие условия на простые числа p, q :

$$2^{255} < p < 2^{256}, \quad 2^{254} < q < 2^{256}, \quad q \equiv 1 + t \pmod{p}, \quad |t| \leq 2\sqrt{p}.$$

При генерации простых чисел, как правило, возникает два вопроса:

- как построить простое число с заданными ограничениями на размер числа?
- как определить, является ли заданное целое число m простым или составным?

Данные вопросы тесно связаны между собой: как только у нас появляется критерий проверки простоты, мы сразу можем предложить алгоритм построения простого числа, основанный на данном критерии.

Кроме того, задача проверки простоты числа связана с задачей разложения на множители. Наиболее простой способ проверить является ли

число m составным или нет, это проверить утверждение леммы 1.6, то есть выяснить, существует ли у числа m простой делитель, не превосходящий величины \sqrt{m} . Если такого делителя нет, то число m является простым.

Для перебора всех возможных делителей нам потребуется сделать порядка $O(\sqrt{m})$ операций пробного деления числа m . При больших значениях числа m это сделать на практике не представляется возможным. Вместе с тем, пробное деление часто используется для проверки: есть ли у числа маленькие делители.

Приведем алгоритм построения таблицы всех простых чисел, ограниченных сверху некоторой величиной b . Такая таблица может быть использована как для реализации метода пробного деления, так и в некоторых алгоритмах разложения целых чисел на множители.

Алгоритм 5.1 (Алгоритм построения таблицы простых чисел)

Вход: Целое число $b > 0$.

Выход: Таблица простых чисел p_0, \dots, p_n таких, что $p_n < b$ и n размер таблицы простых чисел.

1. Присвоить начальным элементам массива значения

$$p_0 = 2, \quad p_1 = 3, \quad p_2 = 5, \quad p_3 = 7, \quad p_4 = 11, \quad p_5 = 13, \quad p_6 = 17.$$

2. Определить переменные $n = 8, h = 5, s = 25$.
3. Определить $p_n = p_n + 2$ и $k = 1$.
4. Если $p_n > b$, то завершить алгоритм и вернуть значение n .
5. Если $p_n > s$, то определить $s = s + h, h = h + 1, s = s + h$.
6. Пока $p_k \leq h$ выполнять
 - 6.1. Если $p_n \equiv 0 \pmod{p_k}$, то вернуться на шаг 3.
Иначе вычислить $k = k + 1$.
7. Определить $n = n + 1$ и вернуться на шаг 3. □

Приведенный алгоритм реализует циклическую проверку утверждения леммы 1.6 для всех нечетных чисел, не превосходящих заданной границы b . Это позволяет сказать, что его трудоемкость оценивается величиной $\frac{b\sqrt{b}}{2}$ операций деления чисел, не превосходящих величины b .

Отметим, что вычисление квадратного корня из целого числа является достаточно медленной процедурой. Для ее оптимизации на 5 шаге алгоритма мы выполняем итерационное вычисление значений, таких что $p_n < s = h^2$.

Далее, мы опишем вероятностные тесты, которые позволяют проверить простоту числа с некоторой вероятностью, а также алгоритмы, которые позволяют строго доказать простоту числа.

5.1 Вероятностные тесты проверки простоты

Процедуры строгого доказательства простоты заданного нечетного числа m являются достаточно трудоемкими и могут требовать больших вычислительных ресурсов. Гораздо эффективнее могут быть реализованы процедуры, которые проверяют не является ли число m составным с некоторой вероятностью — так называемые вероятностные тесты.

Данные тесты позволяют очень эффективно отбраковать составные числа, однако они не в состоянии строго доказать простоту числа, они лишь позволяют говорить, что число m не является составным с некоторой вероятностью.

Первая и наиболее очевидная идея построения подобного теста заключается в обращении малой теоремы Ферма. Действительно, если найдется целое, взаимно простое с m число a такое, что $a^{m-1} \not\equiv 1 \pmod{m}$, то из утверждения малой теоремы Ферма, см. теорему 2.7, следует, что число m составное.

Казалось бы, что еще надо? Однако в 1912 году Р. Кармайкл показал [4], что существуют составные числа m для которых обращение малой теоремы Ферма выполнено для любых взаимно простых с m чисел a . Теперь такие числа принято называть числами Кармайкла. Известно, что подобных чисел бесконечно много и все они имеют вид, описываемый следующей теоремой

Теорема 5.1 (Кармайкл, 1912). *Пусть задано m нечетное, составное число. Тогда*

1. *если p простое число и $p^2 \mid m$, то m не является числом Кармайкла,*
2. *если $m = p_1 \cdots p_k$ является произведением различных простых чисел, то для того, чтобы m было числом Кармайкла необходимо и достаточно, чтобы выполнялось условие $p_i - 1 \mid m - 1$ для всех $i = 1, \dots, k$,*
3. *если $m = p_1 \cdots p_k$ число Кармайкла, то $k \geq 3$.*

Как следует из результата Кармайкла, обращение теоремы Ферма работает не во всех случаях, а значит для построения теста требуется использовать другие математические результаты.

5.1.1 Тест Соловья-Штрассена

Тест Соловья-Штрассена был опубликован авторами в 1977 году в работе [20]. Он основывается на вычислении символа Лежандра для целого числа m , проверяемого на простоту.

Докажем следующий результат, лежащий в основе теста.

Теорема 5.2. Пусть m нечетное составное целое число. Тогда среди всех целых чисел a таких, что $0 < a < m$, не более половины будут удовлетворять условиям

1. $\text{НОД}(a, m) = 1$,
2. выполнено сравнение $a^{\frac{m-1}{2}} \equiv \left(\frac{a}{m}\right) \pmod{m}$, где символ $\left(\frac{a}{m}\right)$ означает символ Якоби.

Доказательство. В начале мы покажем, что найдется вычет a — целое, взаимно простое с m число, $0 < a < m$ такое, что второе условие теоремы будет не выполнено, то есть $a^{\frac{m-1}{2}} \not\equiv \left(\frac{a}{m}\right) \pmod{m}$.

Пусть $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ разложение составного числа m на простые, нечетные сомножители. Для начала рассмотрим случай, когда найдется такой индекс i , $1 \leq i \leq k$ такой, что $\alpha_i > 1$. Без ограничения общности будем считать, что $i = 1$.

Определим целое число a равенством

$$a = 1 + \frac{m}{p_1}, \quad (5.1)$$

тогда $a \equiv 1 \pmod{p_i}$ для всех индексов $1 \leq i \leq k$. Это позволяет нам записать равенство

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k} = 1.$$

Предположим, что для числа a выполнено сравнение $a^{\frac{m-1}{2}} \equiv 1 \pmod{m}$. Тогда, поскольку $p_1^{\alpha_1} | m$ получаем, что $a^{\frac{m-1}{2}} \equiv 1 \pmod{p_1^{\alpha_1}}$.

Обозначим символом d показатель числа a по модулю $p_1^{\alpha_1}$, то есть d минимальное целое такое, что $a^d \equiv 1 \pmod{p_1^{\alpha_1}}$. Используя утверждение леммы 2.3 получаем, что $d | \frac{m-1}{2}$ и, следовательно, $d | m - 1$.

В силу равенства (5.1) мы можем записать сравнение $a \equiv 1 + kp_1^{\alpha_1-1} \pmod{p_1^{\alpha_1}}$ для некоторого целого числа k такого, что $\text{НОД}(k, p_1) = 1$. Используя формулу бинома Ньютона, мы можем записать сравнение

$$1 \equiv a^d \equiv (1 + kp_1^{\alpha_1-1})^d \equiv 1 + kdp_1^{\alpha_1-1} \pmod{p_1^{\alpha_1}},$$

из которого следует, что $kdp_1^{\alpha_1-1} \equiv 0 \pmod{p_1^{\alpha_1}}$ или, что равносильно, $p_1|kd$. В силу взаимной простоты k и p_1 получаем, что $p_1|d|m-1$.

Вспоминая, что нечетное простое p_1 является делителем числа m и не может одновременно делить $m-1$ получаем, что наше предположение не верно и число a , определенное равенством (5.1), не удовлетворяет второму условию теоремы.

Теперь рассмотрим случай, когда составное число m раскладывается в произведение нечетных простых делителей в первой степени, то есть $m = p_1 \cdots p_k$. Определим целое число a как решение системы сравнений

$$\begin{cases} x \equiv s \pmod{p_1}, \\ x \equiv 1 \pmod{p_2}, \\ \dots \\ x \equiv 1 \pmod{p_k}, \end{cases} \quad (5.2)$$

где s произвольный квадратичный невычет по модулю p_1 . В силу определения, для числа a выполнено равенство

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right) = \left(\frac{s}{p_1}\right) = -1.$$

С другой стороны, $a^{\frac{m-1}{2}} \equiv 1 \pmod{p_i}$ для всех индексов i , $2 \leq i \leq k$. Следовательно, воспользовавшись китайской теоремой об остатках, см. теорему 2.3, получаем сравнение $a^{\frac{m-1}{2}} \equiv 1 \pmod{p_2^{\alpha_2} \cdots p_k^{\alpha_k}}$.

Последнее сравнение позволяет нам сделать вывод, что выполнено условие $a^{\frac{m-1}{2}} \not\equiv -1 \pmod{m}$, из которого следует, что определенное системой сравнений (5.2) число a также не удовлетворяет второму утверждению теоремы.

Нам осталось показать, что чисел, не удовлетворяющих условиям теоремы, достаточно много. Пусть w целое число, удовлетворяющее условиям теоремы. Рассмотрим вычет $u \equiv aw \pmod{m}$, где a вычет, построенный нами ранее, и предположим, что u также удовлетворяет условиям теоремы. Тогда выполнено сравнение

$$u^{\frac{m-1}{2}} \equiv \left(\frac{u}{m}\right) \pmod{m}$$

и мы можем записать равенства

$$\begin{aligned} \left(\frac{u}{m}\right) &= \left(\frac{a}{m}\right) \left(\frac{w}{m}\right), \\ u^{\frac{m-1}{2}} &\equiv a^{\frac{m-1}{2}} w^{\frac{m-1}{2}} \equiv a^{\frac{m-1}{2}} \left(\frac{w}{m}\right) \pmod{m}, \end{aligned}$$

из которых следует, что вычет a также удовлетворяет условиям теоремы, а это противоречит нашему построению.

Мы получили, что вычет u также не удовлетворяет условиям теоремы. В силу произвольности выбора вычета мы получаем, что для каждого вычета w , удовлетворяющего условиям теоремы, найдется вычет u , который не удовлетворяет условиям теоремы. Таким образом теорема доказана. \square

Теперь вернемся к вопросу о простоте числа m . Если число m простое, то оба условия доказанной нами теоремы, в силу свойств символа Якоби, будут выполнены. В случае, если число m составное, то найдется такой вычет a , что одно из условия теоремы будет не выполнено. При этом мы доказали, что таких вычетов не менее, чем вычетов, для которых утверждение теоремы выполнено.

Алгоритм 5.2 (Тест Соловея-Штрассена)

Вход: Целое число m .

Выход: Заключение о том, что число составное, либо заключение о том, что число не является составным с некоторой вероятностью.

1. Определить число итераций $k = 20$.
2. Вычислить случайное число a , $0 < a < m$.
3. Если $\text{НОД}(a, m) > 1$, то закончить алгоритм с уведомлением, что число m составное.
4. Если $a^{\frac{m-1}{2}} \not\equiv \left(\frac{a}{m}\right) \pmod{m}$, то закончить алгоритм с уведомлением, что число m составное.
5. Вычислить $k = k - 1$
6. Если $k = 0$, то закончить алгоритм с уведомлением, что число m вероятно простое.

Иначе вернуться на шаг 2. \square

Заметим, что вероятность принять составное число m за простое определяется числом итераций k и, очевидно, равняется $\frac{1}{2^k}$. Таким образом, если число m завершило тест с заключением, что оно вероятно простое, то оно является простым с вероятностью $1 - \frac{1}{2^k}$.

При практической реализации алгоритма, для снижения его трудоемкости, выбирают числа a не из интервала $0 < a < m$, а из меньшего интервала $0 < a < c$, где константа c определяет максимально возможное значение натурального числа, помещающегося в одном регистре процессора.

5.1.2 Тест Миллера-Рабина

Следующий тест может быть реализован на ЭВМ более эффективно, чем тест Соловея-Штрассена. Детерминированная версия данного теста была предложена Гари Миллером в 1976 году [15]. Позднее, в 1980 году, Майкл Рабин [19] предложил вероятностный алгоритм тестирования простоты и получил теоретическую оценку вероятности его успешного завершения.

Приведем результат Рабина, на котором основан тест проверки на простоту.

Теорема 5.3 (Рабин, 1980). Пусть m нечетное составное число такое, что $\text{НОД}(6, m) = 1$. Определим целые числа n, q равенством $m - 1 = 2^n q$ и будем говорить, что вычет a принадлежит множеству $\mathcal{S} \subset \mathbb{Z}_m$, если выполнено одно из двух условий

1. $a^q \equiv 1 \pmod{m}$,
2. $a^{2^k q} \equiv -1 \pmod{m}$ для некоторого целого индекса k , $0 \leq k < n$.

Тогда мощность множества \mathcal{S} не превосходит $\frac{m}{4}$.

Заметим, что если число m является простым, то, согласно лемме 4.7, условия теоремы 5.3 выполнены для всех целых чисел a взаимно простых с m . Именно это различие между простыми и составными числами лежит в основе теста, предложенного Миллером и Рабином.

Прежде чем приступать к доказательству теоремы 5.3, следуя статье [26], докажем несколько вспомогательных утверждений. Определим множество $\mathcal{A} \subset \mathbb{Z}_m$ вычетов a , удовлетворяющих одному из двух условий

1. $a^{m-1} \not\equiv 1 \pmod{m}$,
2. число a является первообразным корнем по модулю некоторого простого делителя p числа m и для любого целого z выполнено условие $a^z \not\equiv -1 \pmod{m}$.

Лемма 5.1. Для любого элемента $a \in \mathcal{A}$ и любого элемента $s \in \mathcal{S}$ выполнено условие $as \pmod{m} \notin \mathcal{S}$ или, на языке множеств, выполнено $a\mathcal{S} \cap \mathcal{S} = \emptyset$.

Доказательство. В начале заметим, что поскольку выполнено равенство $m - 1 = 2^n q$, то для любого $s \in \mathcal{S}$ выполнено $s^{m-1} \equiv 1 \pmod{m}$.

Теперь предположим, что $a \in \mathcal{A}$ удовлетворяет первому условию, то есть $a^{m-1} \not\equiv 1 \pmod{m}$. Тогда, очевидно,

$$(as)^{m-1} \equiv a^{m-1}s^{m-1} \equiv a^{m-1} \not\equiv 1 \pmod{m}$$

и вычет as не принадлежит множеству \mathcal{S} .

Второй случай, когда $a^{m-1} \equiv 1 \pmod{m}$ и $a^z \not\equiv -1 \pmod{m}$ для любого целого z , рассматривается несколько сложнее.

Предположим, что вычет as принадлежит множеству \mathcal{S} и рассмотрим четыре возможных варианта:

1. $s^q \equiv 1 \pmod{m}$ и $(as)^q \equiv 1 \pmod{m}$,
2. $s^q \equiv 1 \pmod{m}$ и $(as)^{2^l q} \equiv -1 \pmod{m}$, $0 \leq l < n$,
3. $s^{2^k q} \equiv -1 \pmod{m}$, $0 \leq k < n$ и $(as)^q \equiv 1 \pmod{m}$,
4. $s^{2^k q} \equiv -1 \pmod{m}$, $0 \leq k < n$ и $(as)^{2^l q} \equiv -1 \pmod{m}$, $0 \leq l < n$.

Для первого варианта сразу получаем, что $a^q \equiv 1 \pmod{m}$. Это не верно: в противном случае, $a^q \equiv 1 \pmod{p}$, поскольку $p|m$ и $p-1|q$, поскольку a первообразный корень по модулю p . Последнее условие не выполнено в силу того, что $p-1$ четно, а q нечетно.

Для второго варианта получаем $-1 \equiv a^{2^l q}(s^q)^{2^l} \equiv a^{2^l q} \pmod{m}$, что противоречит выбору a .

В третьем случае выразим из второго сравнения $s^q \equiv a^{-q} \pmod{m}$. Подставляя полученное выражение в первое сравнение, получим сравнение $a^{-2^k q} \equiv -1 \pmod{m}$, которое противоречит выбору a .

В последнем случае, если $l > k$, то, подставляя первое сравнение во второе, получим сравнение $a^{2^k q} \equiv -1 \pmod{m}$, которое противоречит выбору a . Если же $l \leq k$, выражая $s^{2^l q} \equiv -a^{2^l q} \pmod{m}$ и подставляя это выражение в первое сравнение, получим сравнение

$$\left(-a^{2^l q}\right)^{2^{k-l}} \equiv -1 \pmod{m},$$

которое также противоречит выбору a при $l < k$. Оставшийся вариант, при $k = l$, приводит нас к сравнению $a^{2^l q} \equiv 1 \pmod{m}$. Тогда, поскольку $p|m$, получаем $a^{2^l q} \equiv 1 \pmod{p}$, а поскольку a первообразный корень по модулю p , то $p-1|2^l q = 2^k q$. Последнее равенство влечет за собой сравнение $s^{p-1} \equiv s^{2^k q} \equiv 1 \pmod{p}$, которое противоречит выбору s .

Таким образом мы рассмотрели все возможные варианты и показали, что вычет as не принадлежит множеству \mathcal{S} . Лемма доказана. \square

Лемма 5.2. Пусть a и b два различных элемента из \mathbb{Z}_m . Элемент a обратим по модулю m , а элемент $b \in \mathcal{A}$. Тогда множества $a\mathcal{S}$ и $b\mathcal{S}$ не пересекаются, если $a^{-1}b \in \mathcal{A}$.

Доказательство. Предположим, что s_1, s_2 два элемента из множества \mathcal{S} такие, что $as_1 \equiv bs_2 \pmod{m}$. Поскольку a обратим, получаем, что $s_1 \equiv a^{-1}bs_2 \pmod{m}$, $s_1 \in \mathcal{S}$. Из предыдущей леммы получаем, что это невозможно, если $a^{-1}b \in \mathcal{A}$. Лемма доказана. \square

Доказательство теоремы 5.3. Способ доказательства теоремы зависит от разложения числа m на простые сомножители. В начале предположим, что число m обладает простым делителем p , то есть $p^\alpha | m$ при целом $\alpha > 1$.

Рассмотрим множество

$$\mathcal{G} = \left\{ 1 + k \frac{m}{p} \pmod{m}, \quad \text{для всех } 0 \leq k < p \right\}.$$

Легко видеть, что множество \mathcal{G} образует мультипликативную подгруппу порядка p в группе обратимых элементов \mathbb{Z}_m^* . Действительно, в силу определения, выполнено равенство

$$\begin{aligned} \left(1 + k \frac{m}{p} \right) \left(1 + h \frac{m}{p} \right) \pmod{m} = \\ \left(1 + (k + h) \pmod{p} \frac{m}{p} \right) \pmod{m}, \quad 0 \leq k, h < p, \end{aligned}$$

из которого мы получаем, что \mathcal{G} образует группу порядка p .

Пусть g отличный от единицы элемент группы \mathcal{G} . Рассмотрим сравнение

$$g^{m-1} \equiv \left(1 + k \frac{m}{p} \right)^{m-1} \pmod{m} \equiv 1 + k(m-1) \frac{m}{p} \pmod{m},$$

при некотором k таком, что $0 < k < p$. Поскольку $p | m$ и p не делит $(m-1)$, то мы можем считать, что m не делит $k(m-1) \frac{m}{p}$ и, следовательно, $g^{m-1} \not\equiv 1 \pmod{m}$.

Таким образом мы получили, что любой отличный от единицы элемент группы \mathcal{G} принадлежит множеству \mathcal{A} . Поскольку \mathcal{G} является группой, то мы получаем, что $a^{-1}b \in \mathcal{G} \supset \mathcal{A}$ для любых двух отличных от единицы элементов a, b группы \mathcal{G} .

Воспользовавшись утверждением леммы 5.2 получим, что множества aS и bS не пересекаются для любых двух элементов a, b группы \mathcal{G} . Следовательно,

$$\mathbb{Z}_m \supseteq \left| \bigcup_{g \in \mathcal{G}} gS \right| = |G| \cdot |S| = p|S|.$$

Вспоминая, что $\text{НОД}(6, m) = 1$ получаем неравенство $p \geq 5$ и условие

$$m = |\mathbb{Z}_m| > 4|S|,$$

которое завершает доказательство теоремы для составного числа m , делящегося, как минимум, на квадрат простого числа.

Теперь рассмотрим случай, когда составное число m не делится на квадрат простого числа, то есть $m = p_1 \cdots p_k$, где p_1, \dots, p_k различные простые числа, $k \in \mathbb{N}$. Без ограничения общности будем считать, что $p_1 < \cdots < p_k$.

Определим вычеты для каждого $i = 1, \dots, k$ определим вычет c_i по модулю m как решение системы сравнений

$$\begin{cases} x \equiv a_i \pmod{p_i}, \\ x \equiv 1 \pmod{p_j}, \quad \text{для всех } j, j \neq i, \end{cases}$$

где a_i первообразный корень по модулю простого числа p_i .

Сделаем предположение о том, что найдется целое число z такое, что $c_i^z \equiv -1 \pmod{m}$. Поскольку $p_j | m$, $j \neq i$, то должно быть выполнено сравнение $c_i^z \equiv -1 \pmod{p_j}$. Последнее сравнение ни когда не выполнено, в силу построения числа c_i . Таким образом, все вычеты $c_1, \dots, c_k \in \mathcal{A}$. Более того, вычеты c_1, \dots, c_k обратимы и $c_1^{-1}, \dots, c_k^{-1} \in \mathcal{A}$.

Рассмотрим вычет $d \equiv c_1 c_2 \pmod{m}$ и покажем, что $d \in \mathcal{A}$. При $k \geq 3$ доказательство этого факта аналогично доказательству того, что $c_i \in \mathcal{A}$. Рассмотрим случай $k = 2$.

Пусть выполнено сравнение $d^{m-1} \equiv 1 \pmod{m}$, тогда выполнено $a^{m-1} \equiv 1 \pmod{p_2}$, поскольку $p_2 | m$. Из последнего сравнения следует, что $p_2 - 1 | m - 1$, см. третье утверждение леммы 2.3, поскольку, в силу построения, $d \pmod{p_2}$ является первообразным корнем по модулю p_2 .

Запишем равенство

$$m - 1 = p_1 p_2 - 1 = p_1(p_2 - 1) - p_1 - 1, \quad \text{и} \quad p_1 - 1 < p_2 - 1,$$

из которого следует, что $m - 1$ не может делиться на $p_2 - 1$. Из полученного противоречия следует, что $d^{m-1} \not\equiv 1 \pmod{m}$, то есть $d \in \mathcal{A}$.

Для завершения доказательства рассмотрим четыре множества $S, c_1S, c_2S, dS \subset \mathbb{Z}_m$. В силу леммы 5.2 эти множества не пересекаются, следовательно $4|S| \leq |\mathbb{Z}_m|$. Теорема доказана. \square

Теорема Рабина в явном виде описывает множество вычетов (множество \mathcal{S}), которое должно использоваться для проверки, является ли число m составным или нет. Опишем алгоритм, реализующий данный тест.

Алгоритм 5.3 (Тест Миллера-Рабина)

Вход: Целое нечетное число m такое, что $\text{НОД}(6, m) = 1$.

Выход: Заключение о том, что число составное, либо заключение о том, что число не является составным с некоторой вероятностью.

1. Вычислить такие целые числа n, q , что $m - 1 = 2^n q$ и q — нечетно.
2. Определить $k = 20$ число попыток выбора случайного числа в теореме Рабина.
3. Вычислить $k = k - 1$. Если $k = 0$, то завершить алгоритм с заключением, что m вероятно простое число.
4. Выбрать случайный вычет $a \in \mathbb{Z}_m$ и вычислить $b \equiv a^q \pmod{m}$.
5. Если $b \equiv \pm 1 \pmod{m}$, то вернуться на шаг 3. В противном случае, определить счетчик $i = 0$.
6. **Пока $i < n$ выполнять**
 - 6.1. Вычислить $b \equiv b^2 \pmod{m}$.
 - 6.2. **Если $b \equiv -1 \pmod{m}$, то** вернуться на шаг 3. В противном случае вычислить $i = i + 1$.
7. Завершить алгоритм с заключением, что число m составное. \square

Сделаем несколько замечаний к данному алгоритму. Как следует из теоремы Рабина, мы можем принять составное число m за простое с вероятностью $\frac{1}{4}$. В алгоритме мы реализуем k попыток проверки условий теоремы, следовательно, общая вероятность принять составное число за простое составляет $\frac{1}{4^k}$.

Мы выбираем число k достаточно случайно, исходя из эффективности реализации теста Миллера-Рабина. Вместе с тем, необходимо заметить, что в детерминированном варианте данного теста, Миллер предложил, см. [15], перебирать все значения a от двойки до величины $\ln^2 m$. Он доказал, что в этом случае, при выполнении расширенной гипотезы Римана, число m будет простым.

И еще, на четвертом шаге алгоритма мы можем выбирать случайный вычет a не из всего кольца \mathbb{Z}_m , а из некоторого малого множества, например $1 < a < 2^w$, где w определяет разрядность регистров процессора ЭВМ, выполняющей вычисления. Это не изменит общей вероятности, однако несколько снизит трудоемкость алгоритма при возведении в степень на четвертом шаге алгоритма.

Как правило, число проходящее тест Миллера-Рабина, предварительно тестируются на наличие маленьких делителей методом грубой силы (пробных делений). Поэтому, в силу выбора небольших значений a , мы не стали добавлять в четвертый шаг алгоритма проверку условия $\text{НОД}(a, m) = 1$.

5.2 $N - 1$ методы доказательства простоты

Теперь мы перейдем к рассмотрению методов, позволяющих получить строгое доказательство простоты числа. Именно подобный класс методов используется на практике при построении простых чисел, используемых в криптографических схемах.

Методы доказательства простоты целых чисел, использующие разложение числа $m - 1$ на простые множители, были известны достаточно давно. Мы можем доказать хорошо известную теорему Э. Люка о простоте числа m , основанную на свойствах первообразных корней.

Теорема 5.4 (теорема Люка, 1876). Пусть $m > 1$ нечетное целое число. Если найдется такое целое число a , $\text{НОД}(a, m) = 1$, такое, что для любого простого делителя q числа $m - 1$ выполнены сравнения

$$a^{m-1} \equiv 1 \pmod{m}, \quad a^{\frac{m-1}{q}} \not\equiv 1 \pmod{m},$$

то m — простое число.

Доказательство. Пусть существует целое число a для которого выполнены условия теоремы. Тогда из утверждения теоремы 2.8 следует, что $\text{ord}_m a = m - 1$ и a является первообразным корнем по модулю m . Следовательно $\varphi(m) = m - 1$, а это возможно только в случае, когда m простое число. \square

Основываясь на теореме Люка мы можем предложить простой тест проверки простоты нечетного числа m , если известно разложение $m - 1$ на множители.

Алгоритм 5.4 (Алгоритм Люка для доказательства простоты)

Вход: Целое число m такое, что $m - 1 = \prod_{k=1}^n q_k^{\alpha_k}$

Выход: Заключение о том, является ли число m простым или составным.

1. Определить $c = 20$ и $k = 1$.
2. Выбрать случайно элемент $1 \leq a < m$. Если $\text{НОД}(a, m) > 1$, то закончить алгоритм с уведомлением, что число m составное.

3. Вычислить $c = c - 1$. Если $c = 0$, то завершить алгоритм с уведомлением, что алгоритм не может дать однозначного ответа на вопрос, составное число или нет.
4. Пока $k \leq n$ выполнять
 - 4.1. Если выполнено условие $a^{m-1} \not\equiv 1 \pmod{m}$, то закончить алгоритм с уведомлением, что число m составное.
 - 4.2. Если выполнено условие $a^{\frac{m-1}{q_k}} \equiv 1 \pmod{m}$, то вернуться на шаг 2.
 - 4.3. Вычислить $k = k + 1$.
5. Завершить алгоритм с уведомлением, что число m простое. □

Ситуация, когда нам полностью известно разложение числа $m - 1$ на простые множители, возникает не часто. Как правило, используемые нами методы разложения на множители позволяют получить лишь частичное разложение числа $m - 1$ на множители. Это вынуждает нас использовать более тонкие результаты, чем теорема Люка.

Итак, мы хотим проверить на простоту нечетное целое число $m > 0$. Запишем $m - 1$ в виде

$$m - 1 = fr, \quad \text{НОД}(f, r) = 1, \quad (5.3)$$

где f число с известным разложением на множители $f = \prod_{k=1}^n q_k^{\alpha_k}$, а r составное число с неизвестным разложением на множители. Заметим, что если число r простое, то мы получаем полное разложение числа $m - 1$ на простые сомножители, что позволяет нам воспользоваться теоремой Люка для проверки простоты m .

Дополнительно мы будем считать, что каждый простой делитель q числа r удовлетворяет неравенству $q > b$ для некоторого натурального числа b . В качестве границы b , на практике, можно выбрать величину

$$b = \max_k q_k,$$

то есть максимальное из простых чисел, входящих в разложение числа f . Впрочем, можно несколько увеличить эту границу, взяв в качестве величины b значение $\hat{q} - 1$, где \hat{q} следующее за максимальным q_k простое число.

Определим следующие условия

1. Для каждого простого числа q_k , $k = 1, \dots, n$, входящего в разложение числа f , найдется некоторое взаимно простое с m целое число a_k такое, что

$$a_k^{m-1} \equiv 1 \pmod{m} \quad \text{и} \quad \text{НОД}\left(a_k^{\frac{m-1}{q_k}} - 1, m\right) = 1. \quad (5.4)$$

2. Найдется некоторое взаимно простое с m целое число b такое, что

$$b^{m-1} \equiv 1 \pmod{m} \quad \text{и} \quad \text{НОД}\left(b^{\frac{m-1}{r}} - 1, m\right) = 1. \quad (5.5)$$

Выполнимость одного или двух указанных условий позволяет нам говорить о простоте числа m .

Теорема 5.5 (Поклингтон, 1918). Пусть m нечетное натуральное число, для которого выполнено условие (5.4) и p произвольный простой делитель числа m , тогда

$$p \equiv 1 \pmod{f}.$$

Доказательство. Пусть выполнены утверждения теоремы и p произвольный простой делитель числа m . Рассмотрим q_k некоторый простой делитель, входящий в разложение числа f , и обозначим символом t показатель числа a_k по модулю p .

Из первого утверждения теоремы следует, что $a_k^{m-1} \equiv 1 \pmod{p}$, тогда, согласно третьему утверждению леммы 2.3, $t|m-1$. Из второго утверждения теоремы получаем, что $a_k^{\frac{m-1}{q_k}} \not\equiv 1 \pmod{p}$, следовательно t не делит $\frac{m-1}{q_k}$. Поскольку $q_k^{\alpha_k} | m-1$, то из полученных условий вытекает, что $q_k^{\alpha_k} | t$.

С другой стороны, согласно малой теореме Ферма, см. теорему 2.7, выполнено $t|p-1$. Таким образом, мы получаем, что $q_k^{\alpha_k} | p-1$, что равносильно,

$$p \equiv 1 \pmod{q_k^{\alpha_k}}.$$

В силу произвольного выбора индекса k мы получаем, что последнее сравнение выполнено для всех индексов $k = 1, \dots, n$. Следовательно, по китайской теореме об остатках, см. теорему 2.3, выполнено сравнение $p \equiv 1 \pmod{f}$, поскольку $f = \prod_{k=1}^n q_k^{\alpha_k}$. Теорема доказана. \square

Доказанный нами результат был в последствии использован Д. Лемером для доказательства простоты целых чисел. Следуя статье [21], приведем несколько полезных для наших целей результатов.

Теорема 5.6 (Лемер, следствие теоремы Поклингтона, 1927). Пусть нечетное целое число $m > 0$. Если число m удовлетворяет условию теоремы 5.5 и $f^2 \geq \sqrt{m}$, то m - простое.

Доказательство. Если выполнены условия теоремы 5.5, то для любого простого делителя p числа m выполнено равенство $p = 1 + kf$ при

некотором $k \in \mathbb{Z}$. Следовательно, для любого простого делителя p выполнено неравенство $p = 1 + kf \geq 1 + \sqrt{m} > \sqrt{m}$, которое противоречит утверждению леммы 1.6. Полученное противоречие завершает доказательство. \square

Приведем пример использования данной теоремы.

Пример 5.1. Рассмотрим число $m = 156 \cdot 5^{202} + 1$. Используя вычисления на ЭВМ находим, что

$$13^m \equiv 1 \pmod{m} \quad \text{и} \quad \text{НОД}\left(13^{156 \cdot 5^{201}}, m\right) = 1,$$

следовательно всякий простой делитель p числа m имеет вид $p = 1 + k5^{202}$. Поскольку $5^{202} > \sqrt{m}$, то число m простое.

Теперь покажем как можно использовать для доказательства простоты введенное нами ранее условие (5.5).

Теорема 5.7. Пусть m нечетное натуральное число, для которого выполнено условие (5.5) и p произвольный простой делитель числа m , тогда

$$p \equiv 1 \pmod{q},$$

где q некоторый простой делитель числа r .

Доказательство. Пусть $p|m$. Обозначим символом t показатель элемента b по модулю простого числа p . Тогда из условия $b^{m-1} \equiv 1 \pmod{m}$ следует, что $b^{m-1} \equiv 1 \pmod{p}$ и $t|m - 1$. Из второго условия теоремы $\text{НОД}\left(b^{\frac{m-1}{r}}, m\right) = 1$ следует, что $b^{\frac{m-1}{r}} \not\equiv 1 \pmod{p}$ и t не делит $\frac{m-1}{r}$. Суммируя оба вывода получаем, что $\text{НОД}(t, r) > 1$, следовательно, найдется простой делитель q числа r такой, что $q|t$.

Поскольку $t|p - 1$ получаем, что $q|p - 1$ или, что равносильно, $p \equiv 1 \pmod{q}$. Теорема доказана. \square

Скомбинировав утверждения двух последних теорем, можно получить следующее утверждение.

Теорема 5.8. Пусть m нечетное натуральное число, для которого выполнены условия (5.4) и (5.5). Пусть p произвольный простой делитель числа m , тогда

$$p \equiv 1 \pmod{fq},$$

где q некоторый простой делитель числа r . Кроме того, если выполнено неравенство

$$(1 + fb)^2 > m, \quad (5.6)$$

то m простое число.

Доказательство данной теоремы очевидным образом основывается на утверждениях предыдущих теорем, и мы оставляем его читателю в качестве упражнения.

При больших значениях числа m не всегда удастся получить значения f и b , удовлетворяющие неравенству (5.6). В этом случае, можно воспользоваться утверждением следующей теоремы.

Теорема 5.9. Пусть m нечетное натуральное число, для которого выполнено условие (5.4) и неравенство $f^3 > m > f^2$. Определим целые, неотрицательные числа c_1, c_2 равенствами

$$c_1 \equiv \frac{m-1}{f} \pmod{f} \quad \text{и} \quad c_2 = \frac{m - c_1 f - 1}{f^2},$$

то есть разложим число m по степеням f . Число m простое тогда и только тогда, когда многочлен $f(x) = c_2 x^2 + c_1 x + 1 \in \mathbb{Z}[x]$ неприводим в кольце целых чисел.

Доказательство. Предположим, что число m составное и обозначим символом p_1 его простого делитель. Поскольку m удовлетворяет условию (5.4), то из теоремы Поклингтона, см. теорему 5.5, $p_1 = 1 + x_1 f$ для некоторого натурального x_1 .

Обозначим символом p_2 целое число, удовлетворяющее $p_2 = \frac{m}{p_1}$. Поскольку каждый простой делитель числа p_2 также является и делителем числа m , то для p_2 выполнено равенство $p_2 = 1 + x_2 f$ для некоторого натурального x_2 .

Легко видеть, что $p_2 < f^2$. В противном случае получаем противоречивое неравенство $m = p_1 p_2 = (1 + x_1 f)(1 + x_2 f) > f p_2 > f^3 \geq m$. Таким образом выполнено $f < p_2 < f^2$. Аналогичным способом выводим, что $f < p_1 < f^2$. Из полученных неравенств следуют неравенства $0 < x_1, x_2 < f$.

Вспомним, что число m удовлетворяет равенству $m = c_2 f^2 + c_1 f + 1$, где значения c_1 и c_2 определены в условии теоремы, и запишем систему уравнений, относительно неизвестных x_1, x_2

$$\begin{cases} x_1 + x_2 = c_1, \\ x_1 x_2 = c_2. \end{cases}$$

Решение указанной системы в целых числах равносильно поиску целых корней многочлена $f(x) = c_2x^2 + c_1x + 1 \in \mathbb{Z}[x]$. Если система разрешима в целых числах, то мы находим разложения числа m на множители. Если система не разрешима, то число m простое. Теорема доказана. \square

5.3 $N + 1$ метод доказательства простоты

Рассмотрим метод доказательства простоты числа m , использующий разложение $m+1$ на простые сомножители. Прежде чем сформулировать и доказать необходимое утверждение, мы дадим некоторые определения.

Определение 5.1. *Рассмотрим многочлен $f(x) = x^2 - ax + b$ с целыми коэффициентами такими, что $\text{НОД}(a, b) = 1$ и дискриминант многочлена $D = a^2 - 4b$ отличен от нуля. Обозначим*

$$\alpha = \frac{a + \sqrt{D}}{2}, \quad \beta = \frac{a - \sqrt{D}}{2}, \quad \alpha > \beta,$$

корни многочлена $f(x)$ и определим последовательности чисел U_n, V_n равенствами

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = \alpha^n + \beta^n, \quad n = 0, 1, \dots \quad (5.7)$$

Мы будем называть последовательности $\{U_n\}, \{V_n\}$ рекуррентными последовательностями Люка.

Данное нами определение рекуррентных последовательностей Люка не задает, в явном виде, соотношения между элементами последовательности. Следующая лемма позволяет предъявить данные соотношения, а также выявить ряд полезных свойств рекуррентных последовательностей Люка.

Лемма 5.3. *Пусть последовательности чисел $\{U_n\}, \{V_n\}$ определены равенствами (5.7). Тогда верны следующие утверждения.*

1. Для всех индексов $n = 0, 1, \dots$ значения U_n, V_n являются целыми числами. Более того выполнены рекуррентные соотношения

$$U_{n+1} = aU_n - bU_{n-1}, \quad V_{n+1} = aV_n - bV_{n-1}, \quad n = 1, 2, \dots \quad (5.8)$$

где $U_0 = 0, U_1 = 1, V_0 = 2, V_1 = a$.

2. Выполнены равенства

$$U_{2n} = U_n V_n, \quad V_{2n} = \frac{1}{2} (V_n^2 + D U_n^2) \quad (5.9)$$

3. Выполнены равенства

$$U_{n+1} = \frac{1}{2} (V_n + a U_n), \quad V_{n+1} = \frac{1}{2} (a V_n + D U_n) \quad (5.10)$$

4. Выполнены равенства

$$U_{k+l} = \frac{1}{2} (U_k V_l + U_l V_k), \quad V_{k+l} = \frac{1}{2} (V_k V_l + D U_k U_l) \quad (5.11)$$

5. Выполнено равенство $4b^n = V_n^2 - D U_n^2$.

6. Для любого индекса d такого, что $d|n$, выполнено $U_d|U_n$.

Доказательство. Прежде, чем переходить к доказательству перечисленных утверждений заметим, что для корней многочлена $f(x)$, в силу теоремы Виета, выполнены простые соотношения, которые будут использованы нами далее

$$\alpha + \beta = a, \quad \alpha\beta = b, \quad (\alpha - \beta)^2 = D. \quad (5.12)$$

Докажем первое утверждение леммы. Подставляя значения $n = 0, 1$ в соотношения (5.7) получим равенства $U_0 = 0, U_1 = 1$, а также, $V_0 = 2, V_1 = a$. Теперь, используя индуктивное предположение, докажем истинность соотношений (5.8). Учитывая (5.12), получаем равенства

$$\begin{aligned} aU_n - bU_{n-1} &= \frac{1}{\alpha - \beta} ((\alpha + \beta)(\alpha^n - \beta^n) - \alpha\beta(\alpha^{n-1} - \beta^{n-1})) = \\ &= \frac{1}{\alpha - \beta} (\alpha^{n+1} - \beta^{n+1}) = U_{n+1}, \end{aligned}$$

$$\begin{aligned} aV_n - bV_{n-1} &= (\alpha + \beta)(\alpha^n + \beta^n) - \alpha\beta(\alpha^{n+1} + \beta^{n+1}) = \\ &= \alpha^{n+1} + \beta^{n+1} = V_{n+1}. \end{aligned}$$

Из полученных равенств следует, что все элементы последовательностей $\{U_n\}, \{V_n\}$ выражаются через целые коэффициенты a, b и начальные значения U_0, U_1 и V_0, V_1 , то есть являются целыми числами.

Доказательства остальных утверждений леммы проводятся аналогичным способом. Действительно, с учетом (5.12), получаем равенства

$$U_{2n+1} = \frac{1}{\alpha - \beta} (\alpha^{2n} - \beta^{2n}) = \frac{1}{\alpha - \beta} (\alpha^n - \beta^n) (\alpha^n + \beta^n) = U_n V_n,$$

$$V_n^2 + DU_n^2 = (\alpha^n + \beta^n)^2 + (\alpha^n - \beta^n)^2 = 2(\alpha^{2n} + \beta^{2n}) = 2V_{2n}$$

из которых следует второе утверждение леммы.

Соотношения

$$\begin{aligned} V_n + aU_n &= (\alpha^n + \beta^n) + \frac{\alpha + \beta}{\alpha - \beta} (\alpha^n - \beta^n) = \\ &= \frac{1}{\alpha - \beta} ((\alpha - \beta)(\alpha^n + \beta^n) + (\alpha + \beta)(\alpha^n - \beta^n)) = \\ &= \frac{2}{\alpha - \beta} (\alpha^{n+1} - \beta^{n+1}) = 2U_{n+1}, \end{aligned}$$

$$\begin{aligned} aV_n + DU_n &= (\alpha + \beta)(\alpha^n + \beta^n) + (\alpha - \beta)(\alpha^n - \beta^n) = \\ &= 2(\alpha^{n+1} + \beta^{n+1}) = 2V_{n+1}, \end{aligned}$$

дают нам третье утверждение леммы.

Четвертое утверждение леммы вытекает из равенств

$$\begin{aligned} U_k V_l + U_l V_k &= \frac{1}{\alpha - \beta} ((\alpha^l + \beta^l)(\alpha^k - \beta^k) + (\alpha^k + \beta^k)(\alpha^l - \beta^l)) = \\ &= \frac{2}{\alpha - \beta} (\alpha^{k+l} - \beta^{k+l}) = 2U_{k+l}. \end{aligned}$$

$$\begin{aligned} V_k V_l + DU_k U_l &= (\alpha^k + \beta^k)(\alpha^l + \beta^l) + (\alpha - \beta)^2 \frac{(\alpha^k - \beta^k)(\alpha^l - \beta^l)}{\alpha - \beta} = \\ &= 2(\alpha^{k+l} + \beta^{k+l}) = 2V_{k+l}. \end{aligned}$$

Докажем пятое утверждение леммы. Для этого выразим α^n , β^n через U_n , V_n . Поскольку выполнены равенства (5.7), то

$$2\alpha^n = V_n - (\alpha - \beta)U_n, \quad 2\beta^n = V_n + (\alpha - \beta)U_n,$$

тогда, с учетом (5.12), получаем равенства

$$4b^n = (2\alpha^n)(2\beta^n) = V_n^2 - (\alpha - \beta)^2 U_n^2 = V_n^2 - DU_n^2,$$

и доказательство пятого утверждения леммы.

Доказательство последнего утверждения проведем по индукции. Рассмотрим U_d , тогда из второго утверждения леммы следует равенство $U_{2d} = U_d V_d$ и $U_d | U_{2d}$. Теперь предположим, что утверждение леммы выполнено для всех целых индексов $d, 2d, 3d, \dots, (k-1)d$. Покажем, что оно выполнено и для индекса kd .

Воспользовавшись четвертым утверждением леммы запишем равенство

$$2U_{kd} = U_d V_{(k-1)d} + V_d U_{(k-1)d}.$$

Поскольку, по предположению индукции, $U_d | U_{(k-1)d}$, то правая часть приведенного равенства делится на U_d и $U_d | U_{kd}$. Лемма доказана. \square

Приведем пример вычисления элементов рекуррентных последовательностей Люка.

Пример 5.2. Рассмотрим целые числа $a = 3$, $b = 1$ и построим элементы рекуррентных последовательностей Люка для всех $n = 0, 1, \dots, 12$. Согласно первому утверждению леммы, выполнены равенства

$$\begin{aligned}(U_0, V_0) &= (0, 2), \\ (U_1, V_1) &= (1, 3)\end{aligned}$$

Далее, воспользовавшись рекуррентными соотношениями (5.8), вычисляем

$$\begin{aligned}(U_2, V_2) &= (3, 7), \\ (U_3, V_3) &= (8, 18), \\ (U_4, V_4) &= (21, 47), \\ (U_5, V_5) &= (55, 123), \\ (U_6, V_6) &= (144, 322), \\ (U_7, V_7) &= (377, 843), \\ (U_8, V_8) &= (987, 2207), \\ (U_9, V_9) &= (2584, 5778), \\ (U_{10}, V_{10}) &= (6765, 15127), \\ (U_{11}, V_{11}) &= (17711, 39603), \\ (U_{12}, V_{12}) &= (46368, 103682)\end{aligned}$$

Понятно, что при больших значениях индекса n вычислить пару U_n, V_n с использованием соотношений (5.8) достаточно сложно. Тем не менее, мы можем предложить простой алгоритм, использующий соотношения (5.9) и (5.10), сложность которого оценивается величиной $O(\log_2 n)$, что

делает его пригодным для вычисления элементов последовательностей Люка с произвольно большим индексом.

Приводимый нами алгоритм вычисляет значение пары элементов U_{kn}, V_{kn} последовательности Люка для заданной начальной пары значений U_k, V_k и целочисленного индекса $n > 1$, представленного в двоичном представлении $n = \sum_{i=0}^{r-1} n_i 2^i$. Напомним, что, согласно (5.8), при $k = 1$ начальная пара последовательности Люка имеет вид $U_1 = 1, V_1 = a$.

Алгоритм 5.5 (Вычисление последовательностей Люка)

Вход: Целые числа a, b такие, что $\text{НОД}(a, b) = 1$, целочисленный индекс $n > 1$, представленный в двоичном представлении $n = \sum_{i=0}^{r-1} n_i 2^i$ и пара начальных значений последовательности U_k, V_k .

Выход: Пара элементов U_n, V_n рекуррентных последовательностей Люка.

1. Присвоить начальные значения переменным $s = 0, i = 0, D = a^2 - 4b$.
2. Пока $n_i = 0$ выполнять $s = s + 1, i = i + 1$.
3. Определить $U = U_k, V = V_k$ и вычислить $i = i + 1$.
4. Пока $i \leq r - 1$ выполнять

4.1. Используя равенства (5.9), вычислить

$$x = UV, \quad y = \frac{1}{2}(V^2 + DU^2), \quad U = x, \quad V = y.$$

4.2. Если $n_i = 1$, то, используя равенства (5.10), вычислить

$$x = \frac{1}{2}(V + aU), \quad y = \frac{1}{2}(aV + DU), \quad U = x, \quad V = y.$$

4.3. Вычислить $i = i + 1$.

5. Пока $s > 0$ выполнять

5.1. Используя равенства (5.9), вычислить

$$x = UV, \quad y = \frac{1}{2}(V^2 + DU^2), \quad U = x, \quad V = y.$$

5.2. Вычислить $s = s - 1$.

6. Завершить алгоритм и вернуть пару значений U, V . □

Используя приведенный алгоритм, для вычисления пары (U_{12}, V_{12}) из примера 5.2, нам потребуется вычислить лишь пары элементов $(U_1, V_1), (U_2, V_2), (U_3, V_3), (U_6, V_6)$ и (U_{12}, V_{12}) .

Теперь перейдем к доказательству результатов, которые потребуются для проверки простоты целых чисел.

Лемма 5.4. Пусть p нечетное простое, $\{U_n\}$ рекуррентная последовательность Люка с параметрами a, b и $b \not\equiv 0 \pmod{p}$. Пусть d минимальное целое число такое, что $U_d \equiv 0 \pmod{p}$. Тогда $U_n \equiv 0 \pmod{p}$ тогда и только тогда, когда $d|n$.

Доказательство. Если индекс $d|n$ то, согласно последнему утверждению леммы 5.3, $U_d|U_n$ и, очевидно, $U_n \equiv 0 \pmod{p}$.

Предположим обратное, пусть $n = kd + r$ для некоторого целого r такого, что $0 < r < d$.

Воспользовавшись четвертым утверждением леммы 5.3 получаем равенство $U_n = U_{kd}V_r + U_rV_{kd}$. Поскольку из предыдущих рассуждений и условия леммы следуют сравнения $U_n \equiv 0 \pmod{p}$ и $U_{kd} \equiv 0 \pmod{p}$, мы получаем $U_rV_{kd} \equiv 0 \pmod{p}$. Поскольку d выбрано минимальным, а $r < d$, то мы получаем, что $V_{kd} \equiv 0 \pmod{p}$.

Теперь воспользуемся пятым утверждением леммы 5.3 и получим сравнение

$$4b^{kd} = V_{kd}^2 - DU_{kd}^2 \equiv 0 \pmod{p}.$$

Поскольку p нечетно, то мы получаем, что $p|b$, а это противоречит условиям леммы. Лемма доказана. \square

Лемма 5.5. Пусть p нечетное простое число, удовлетворяющее условиям предыдущей леммы. Более того, $D = a^2 - 4b \not\equiv 0 \pmod{p}$. Обозначим $\Phi(p) = p - \left(\frac{D}{p}\right)$, где $\left(\frac{D}{p}\right)$ символ Лежандра. Тогда выполнено сравнение

$$U_{\Phi(p)} \equiv 0 \pmod{p}.$$

Доказательство. Напомним, что $U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$, где $\alpha = \frac{a + \sqrt{D}}{2}$, $\beta = \frac{a - \sqrt{D}}{2}$. Вычислим значение $\alpha^p \pmod{p}$. Для этого вычислим $\left(\frac{a + \sqrt{D}}{2}\right)^p = \frac{1}{2^p}(A_p + B_p\sqrt{D})$ и приведем по модулю p значения A_p и B_p .

Таким образом, используя малую теорему Ферма и критерий Эйлера, получаем сравнение

$$\begin{aligned} \alpha^p &\equiv \frac{1}{2^p}(a + \sqrt{D})^p \equiv \frac{1}{2} \left(a + D^{\frac{p-1}{2}} \sqrt{D} \right) \equiv \\ &\equiv \frac{1}{2} \left(a + \left(\frac{D}{p}\right) \sqrt{D} \right) \pmod{p}. \end{aligned}$$

Аналогичными рассуждениями, получаем сравнение

$$\beta^p \equiv \frac{1}{2} \left(a - \left(\frac{D}{p}\right) \sqrt{D} \right) \pmod{p}.$$

Мы можем переписать полученные сравнения в следующем виде

$$\begin{cases} \alpha^p \equiv \alpha \pmod{p}, & \beta^p \equiv \beta \pmod{p}, & \text{при } \left(\frac{D}{p}\right) = 1, \\ \alpha^p \equiv \beta \pmod{p}, & \beta^p \equiv \alpha \pmod{p}, & \text{при } \left(\frac{D}{p}\right) = -1, \end{cases}$$

Теперь вычислим значение $U_{\Phi(p)}$. При $\left(\frac{D}{p}\right) = -1$ получаем $\Phi(p) = p + 1$ и

$$U_{\Phi(p)} = \frac{1}{\alpha - \beta} (\alpha^{p+1} - \beta^{p+1}) \equiv \frac{1}{\alpha - \beta} (\beta\alpha - \alpha\beta) \equiv 0 \pmod{p}.$$

При $\left(\frac{D}{p}\right) = 1$ получаем $\Phi(p) = p - 1$ и

$$U_{\varphi(p)} = \frac{1}{\alpha - \beta} (\alpha^{p-1} - \beta^{p-1}) \equiv \frac{1}{\alpha - \beta} \left(\frac{\alpha}{\alpha} - \frac{\beta}{\beta}\right) \equiv 0 \pmod{p}.$$

Лемма доказана. □

Теперь сформулируем теорему, которая позволяет нам сделать вывод, о строении простых делителей числа m , по известным делителям числа $m + 1$.

Теорема 5.10 (Моррисон, 1975). *Пусть m нечетное целое число. Представим $m + 1$ в виде $m + 1 = fr$, где для числа f известно полное разложение на множители $f = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$.*

Пусть a, b произвольные целые числа такие, что $\text{НОД}(a, b) = 1$. Определим $\{U_n\}$ последовательность Люка, зависящую от параметров a, b . Если для каждого делителя q_i числа f будут выполнены условия

1. *Выполнено сравнение $U_{m+1} \equiv 0 \pmod{m}$,*
2. *Выполнено условие $\text{НОД}\left(U_{\frac{m+1}{q_i}}, m\right) = 1, i = 1, \dots, s,$*

то для каждого простого делителя p числа m такого, что $\left(\frac{D}{p}\right) \neq 0$, где $D = a^2 - 4b$ и $b \not\equiv 0 \pmod{p}$, будет выполнено сравнение

$$p \equiv \left(\frac{D}{p}\right) \pmod{f}.$$

Доказательство. Пусть для простого делителя q_i числа f выполнено первое условие теоремы, тогда $U_{m+1} \equiv 0 \pmod{m}$ и для любого простого делителя p числа m выполнено сравнение $U_{m+1} \equiv 0 \pmod{p}$. Пусть d минимальное целое число такое, что $U_d \equiv 0 \pmod{p}$, тогда, в силу леммы 5.4, $d|m + 1$.

Из второго условия теоремы получаем, что $U_{\frac{m+1}{q_i}} \not\equiv 0 \pmod{p}$, следовательно, $d \nmid \frac{m+1}{q_i}$. Сравнивая два полученных утверждения получаем, что $d|q_i^{\alpha_i}$.

С другой стороны, согласно лемме 5.5 выполнено $U_{\Phi(p)} \equiv 0 \pmod{p}$. Воспользовавшись еще раз утверждением леммы 5.4 получаем условие $d|\Phi(p)$. Таким образом, $d|\text{НОД}(q_i^{\alpha_i}, \Phi(p)) = q_i^{\alpha_i}$. Последнее равенство выполнено в силу простоты q_i .

Мы получили, что $q_i^{\alpha_i}|\Phi(p)$, что равносильно $\Phi(p) \equiv 0 \pmod{q_i^{\alpha_i}}$ или

$$p \equiv \left(\frac{D}{p}\right) \pmod{q_i^{\alpha_i}}.$$

Воспользовавшись китайской теоремой об остатках, мы получаем, что аналогичное сравнение выполнено и по модулю f . Теорема доказана. \square

Эта теорема имеет очевидное следствие, которое позволяет сделать вывод о простоте числа m .

Следствие 1. Пусть для числа m выполнены утверждения теоремы 5.10 и выполнено неравенство $f^2 > m$. Тогда число m простое.

Доказательство. Предположим, что число m составное и, без ограничения общности, имеет два простых делителя p и q . Если для числа m выполнены условия теоремы 5.10, то $p = \pm 1 + kf$, $q = \pm 1 + lf$ для некоторых целых чисел k, l и мы получаем, что $m = pq > f^2 > m$. Противоречие. \square

Мы можем воспользоваться для доказательства простоты числа m приведенным следствием следующим образом. Пусть нам известно частичное разложение числа $m + 1 = fr$ на простые множители, где $f = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$, $f^2 > m$.

Выберем целые числа a, b такие, что выполнены условия

$$\text{НОД}(a, b) = 1, \quad \text{НОД}(m, b) = 1, \quad \text{НОД}(m, a^2 - 4b) = 1,$$

и проверим условия теоремы 5.10. Если они выполнены, то число m простое. Отметим, что нам достаточно вычислять элементы рекуррентной последовательности по модулю m , поскольку в этом случае необходимые нам свойства делимости сохраняются.

5.4 Алгоритмы построения простых чисел

Основываясь на изложенных выше идеях, приведем несколько алгоритмов построения простых чисел, которые используются при генерации параметров криптографических схем.

Мы начнем с описания простого алгоритма, который позволяет строить простые числа p с известным разложением $p - 1$ на множители. Основная идея данного алгоритма заключается в поиске простых чисел в арифметических прогрессиях. Хорошо известен следующий результат.

Теорема 5.11 (Теорема Дирихле, см. [25], гл. 3). *Пусть арифметическая прогрессия задана соотношением $x_k = ak + b$, $k = 0, 1, \dots$, где параметры a, b натуральные, взаимно простые числа. Тогда среди чисел x_k бесконечно много простых.*

Как показывают практические вычисления, простые числа встречаются в арифметических прогрессиях достаточно часто. В комбинации с доказанными ранее результатами о простоте чисел, например теоремами Поклингтона или Моррисона, мы получаем достаточно удобный инструмент для построения больших простых чисел.

5.4.1 Рекурсивный алгоритм построения простых по известному разложению $p - 1$

В 1994 году в работе [14] Преда Михалеску (Preda Mihailescu) предложил алгоритм построения простых чисел, который использует поиск в арифметических прогрессиях. Метод доказательства простоты числа p состоит из трех последовательных шагов:

1. проверка делимости числа p на маленькие простые числа,
2. использование теста Миллера-Рабина, см. тест 5.3, для отбраковки составных чисел, имеющих большие простые делители,
3. использование теоремы Лемера, см. теорему 5.6, для доказательства простоты числа p .

В данном алгоритме мы будем искать простое число вида $p = kq + 1$, где q простое число, удовлетворяющее неравенству $q > \sqrt{p}$, а k произвольное четное целое число. Мы будем считать, что нам заданы два натуральных числа A, B таких, что $B > A + 1$, и будем искать простое число p , удовлетворяющее неравенству

$$A < p < B. \tag{5.13}$$

Из неравенства (5.13) мы можем получить оценки на q и k . Действительно, поскольку q целое, удовлетворяющее неравенству $q > \sqrt{p}$, то из

(5.13) следует оценка на q снизу

$$q \geq \lceil \sqrt{B} \rceil > \sqrt{p}.$$

Обозначим $q_A = \lceil \sqrt{B} \rceil$ и ограничим простое число q сверху, то есть $q_A \leq q \leq \alpha q_A$ для произвольного действительного числа $\alpha > 1$, тогда для k выполнены следующие оценки.

Если $k < \left\lfloor \frac{B-1}{\alpha q_A} \right\rfloor$, то выполнено

$$p = kq + 1 \leq k\alpha q_A + 1 < \alpha q_A \frac{B-1}{\alpha q_A} + 1 = B$$

и для p верна оценка сверху (5.13).

Аналогично, если $k \geq \left\lceil \frac{A}{q_A} \right\rceil$, то выполнено

$$p = kq + 1 > kq \geq kq_A \geq q_A \frac{A}{q_A} = A,$$

и для p верна оценка снизу (5.13). Исходя из того, что интервал для значений k не должен быть пустым, мы получаем оценку сверху на значение параметра α . Действительно, из неравенства $\left\lceil \frac{A}{q_A} \right\rceil < \left\lfloor \frac{B-1}{\alpha q_A} \right\rfloor$ получаем, что α ограничено сверху величиной $\frac{B-1}{A}$, то есть принадлежит интервалу

$$1 < \alpha < \frac{B-1}{A}. \quad (5.14)$$

Указанный интервал не пуст, поскольку величина $\frac{B-1}{A} > 1$ для всех натуральных значений A, B таких, что $B > A + 1$. В алгоритме мы будем использовать значение $\alpha = \frac{B+A-1}{2A}$, которое является серединой интервала (5.14).

Итак, мы будем искать простые числа в арифметической прогрессии $p_k = kq + 1$, перебирая все четные числа k в заданном интервале, последовательно увеличивая число k на двойку. Для отбраковки большей части составных чисел мы будем использовать пробное деление на маленькие простые числа.

Для того, чтобы оптимизировать данную процедуру заметим следующий простой факт. Предположим, что мы разделили число p на маленькие простые числа d_1, \dots, d_n и нашли остатки от деления $\delta_1, \dots, \delta_n$ такие, что $p \equiv \delta_n \pmod{d_n}$. Предположим, что найдется остаток $\delta_i \equiv 0 \pmod{d_i}$, $1 \leq i \leq n$, тогда число p делится на d_i и является составным.

Для проверки следующего числа заметим, что $p + 2 \equiv \delta_i + 2 \pmod{d_i}$ для всех i , $1 \leq i \leq n$. Таким образом, мы можем найти остатки от деления следующего числа на маленькие простые без деления большого числа, а лишь изменяя остатки от деления предыдущего числа. На практике мы будем выбирать число $n = 10$ и проверять делимость числа p на простые 3, 5, 7, 11, 13, 17, 19, 23, 29 и 31. Мы исключили из этого списка двойку, поскольку число p всегда нечетно.

Прежде чем приступить к описанию алгоритма заметим, что нам потребуется таблица всех простых чисел, не превосходящих некоторой величины, скажем 2^{16} . Построить эту таблицу можно, например, используя алгоритм 5.1.

Алгоритм 5.6 (Алгоритм построения простого числа)

Вход: Натуральные числа A, B такие, что $A + 1 < B$.

Выход: Простое число p такое, что $2^A < p < 2^B$.

1. Если $B \leq 2^{16}$, то выбрать случайным образом простое число p из таблицы простых чисел и завершить работу.
2. Определить переменные $q_A = \lceil \sqrt{B} \rceil$, $\alpha = \frac{B+A-1}{2A}$ и $k_1 = \lceil \frac{A}{q_A} \rceil$, $k_2 = \lfloor \frac{B-1}{q_A} \rfloor$.
3. Определить $k_n = k_2$. Используя этот же алгоритм 5.6, построить простое число q , удовлетворяющее неравенствам $q_A < q < \lfloor \alpha q_A \rfloor$.
4. Выбрать случайное число k в интервале $k_1 < k < k_n$. Если k нечетно, то положить $k = k - 1$. Определить $k_s = k_n$, $k_n = k$ и целое число $p = kq + 1$.
5. Для простых чисел $d_1 = 3, \dots, d_{10} = 31$ определить остатки $\delta_1, \dots, \delta_{10}$ от деления числа p на простые d_1, \dots, d_{10} , то есть $\delta_i \equiv p \pmod{d_i}$, $1 \leq i \leq 10$.
6. Вычислить $k = k + 2$, $p = p + 2q$ и $\delta_i = \delta_i + 2 \pmod{d_i}$ для всех i таких, что $1 \leq i \leq 10$.
7. Если $k > k_s$, то вернуться на шаг 4.
8. Если найдется индекс i , $1 \leq i \leq 10$ и $\delta_i = 0$, то вернуться на шаг 6.
9. Применить к числу p тест Миллера-Рабина, см. тест 5.3. Если тест не пройден, то вернуться на шаг 6.
10. Определить значение счетчика $n = 10$.
11. Вычислить случайное целое число a и $n = n - 1$.
12. Если $\text{НОД}(a^k - 1, p) = 1$ и $a^{p-1} \equiv 1 \pmod{p}$, то завершить алгоритм с уведомлением, что число p простое.
13. Если $n = 0$, то вернуться на шаг 6. Иначе, вернуться на шаг 11.

□

Как мы говорили выше, описанный алгоритм использует для доказательства простоты числа p утверждение теоремы Лемера, см. теорему 5.6. Вместе с тем, он может быть легко модифицирован таким образом, чтобы использовать утверждение теоремы 5.9.

Другой возможной модификацией данного алгоритма является использование теоремы Моррисона, см. теорему 5.10, и последовательно-

стей Люка для доказательства простоты числа p . Детальную проработку этих модификаций мы оставляем читателю.

5.4.2 Алгоритм построения сильно простого числа

Во многих приложениях возникает необходимость строить простые числа с дополнительными условиями. Дадим следующее определение.

Определение 5.2. Мы будем называть нечетное простое число p *сильно простым*, если найдутся такие нечетные простые числа q , s и r такие, что

$$p \equiv 1 \pmod{q}, \quad p \equiv -1 \pmod{s}, \quad q \equiv 1 \pmod{r}, \quad (5.15)$$

что равносильно равенствам

$$\begin{cases} p = kq + 1, \\ p = is - 1, \\ q = jr + 1, \end{cases}$$

для некоторых четных чисел i, j, k .

Поскольку предложенный нами ранее алгоритм 5.6 позволяет строить простые числа p , удовлетворяющие только первому и третьему из сравнений (5.15), то для построения строго простых чисел нам потребуется провести его некоторую модификацию.

В 1979 году Вильямс и Шмидт (Н.С. Williams & В. Schmid) в работе [23] предложили алгоритм, вариант которого мы приведем далее.

Предположим, что мы построили два простых числа r , s и хотим построить оставшиеся два простых числа p и q так, чтобы выполнялись сравнения (5.15). Для этого зафиксируем целое число $a \geq 1$, определим наименьшее положительное целое число x такое, что $x \equiv -\frac{(1+a)}{ar} \pmod{s}$, и будем искать простое число q в арифметической прогрессии

$$q = (ks + x)r + 1, \quad k = 0, 1, \dots$$

Для поиска такого числа q можно организовать переборный алгоритм, аналогичный алгоритму 5.6. Тогда, если число $p = 2aq + 1$ будет простым, мы найдем искомое строго простое число — это вытекает из сравнения

$$\begin{aligned} p = 2aq + 1 &= 2a((ks + x)r + 1) + 1 = \\ &= 2aksr + 2arx + (2a + 1) \equiv -1 \pmod{s}. \end{aligned}$$

Если $r > \sqrt{q}$, то мы можем воспользоваться теоремой Лемера для доказательства простоты как числа q , так и числа p .

Если $a = 1$, то простое число p удовлетворяет равенству $p = 2q + 1$. Простые числа p и q , удовлетворяющие этому равенству, называются *простыми-близнецами* и встречаются достаточно редко. Поэтому, при практических вычислениях, необходимо выбирать a достаточно большим.

Прежде, чем приводить алгоритм построения сильно простого числа p , приведем оценки сверху и снизу на параметры, которые нам необходимо определить. Как и раньше, мы будем строить простое число p , удовлетворяющее неравенству

$$A < p < B, \quad \text{тогда} \quad q_A = \left\lfloor \frac{A-1}{2a} \right\rfloor \leq q = \frac{p-1}{2a} \leq \left\lfloor \frac{B-1}{2a} \right\rfloor = q_B,$$

для некоторых целых A, B таких, что $B > A + 2a$. Заметим, что для выполнения условий теоремы Лемера, при доказательстве простоты p , нам необходимо выполнение условия $q > \sqrt{p}$. Так мы получаем оценку на a сверху, а именно

$$\frac{B-1}{2\sqrt{A}} > \frac{p-1}{2q} = a.$$

Теперь, как и в предыдущем алгоритме, получим оценки на r . Для выполнимости условий теоремы Лемера и доказательства простоты q , положим

$$r \geq \lceil \sqrt{q_A} \rceil = r_A,$$

тогда $\lfloor \alpha r_A \rfloor \geq r \geq r_A$ для некоторого действительного параметра $\alpha > 1$.

Если $ks + x \leq \left\lfloor \frac{q_B-1}{\alpha r_A} \right\rfloor$, тогда выполнена оценка сверху

$$q = (ks + x)r + 1 < \frac{q_B-1}{\alpha r_A} \alpha r_A + 1 \leq q_B.$$

Аналогично, если $ks + x \geq \left\lceil \frac{q_A}{r_A} \right\rceil$, то выполнена оценка снизу

$$q = (ks + x)r + 1 \geq \frac{q_A}{r_A} r_A + 1 > q_A.$$

Таким образом, мы получили ограничения сверху и снизу на размер перебираемого параметра k

$$\left\lfloor \frac{q_B-1}{\alpha r_A} \right\rfloor \geq (ks + x) \geq \left\lceil \frac{q_A}{r_A} \right\rceil. \quad (5.16)$$

Исходя из того, что перебираемый интервал не должен быть пустым, мы получим оценку сверху на параметр α . Действительно, указанный интервал не пуст при $\alpha < \frac{q_B-1}{q_A} < \frac{B-2a}{A}$. При практических вычислениях мы будем использовать значение $\alpha = \frac{q_B+q_A-1}{2q_A}$.

Исходя из неравенства (5.16), получаем оценки для k

$$\left\lfloor \frac{q_B - 1}{\alpha sr_A} \right\rfloor - x \geq k \geq \left\lceil \frac{q_A}{sr_A} \right\rceil - x,$$

а также оценку на s сверху. Поскольку, в силу построения, $s > x > 0$ и $k \geq 1$, то мы получаем неравенство

$$\frac{q_B - 1}{\alpha r_A} \geq \left\lfloor \frac{q_B - 1}{\alpha r_A} \right\rfloor \geq (k + 1)s > ks + x,$$

откуда следует неравенство $s < \left\lfloor \frac{q_B-1}{2\alpha r_A} \right\rfloor = s_A$, которое мы будем использовать для верхней оценки s . Для нижней оценки будем использовать величину¹ $\lceil \sqrt{s_A} \rceil$.

Алгоритм 5.7 (Алгоритм построения сильно простого числа)

Вход: Натуральные числа A, B такие, что $A + 2 < B$.

Выход: Сильно простое число p такое, что $A < p < B$.

1. Вычислить случайное натуральное число a такое, что $1 \leq a \leq \left\lfloor \frac{B-1}{2\sqrt{A}} \right\rfloor$.
2. Определить $q_A = \left\lfloor \frac{A-1}{2a} \right\rfloor$, $q_B = \left\lfloor \frac{B-1}{2a} \right\rfloor$, $r_A = \lceil \sqrt{q_A} \rceil$, $\alpha = \frac{q_B+q_A-1}{2q_A}$ и $s_A = \left\lfloor \frac{q_B-1}{2\alpha r_A} \right\rfloor$.
3. Используя алгоритм 5.6, вычислить простое число r , удовлетворяющее неравенствам $r_A < r < \lfloor \alpha r_A \rfloor$.
4. Используя алгоритм 5.6, вычислить простое число s , удовлетворяющее неравенствам $\lceil \sqrt{s_A} \rceil < s < s_A$.
5. Вычислить наименьшее положительное целое число x , удовлетворяющее сравнению $x \equiv -\frac{(1+a)}{ar} \pmod{s}$.
6. Определить $k_2 = \left\lfloor \frac{q_B-1}{\alpha sr_A} \right\rfloor - x$ и $k_1 = \left\lceil \frac{q_A}{sr_A} \right\rceil - x$.
7. Вычислить случайное число k , $k_1 \leq k \leq k_2$.
8. **Если** x - четно и k - четно, **то** положить $k = k + 1$ и перейти к шагу 10.
9. **Если** x - нечетно и k - нечетно, **то** положить $k = k + 1$.
10. Определить $q = (ks + x)r + 1$ и $p = 2aq + 1$.
11. Вычислить $k = k + 2$, $q = q + 2sr$ и $p = p + 4asr$.
12. Если $k > k_2$, то вернуться на шаг 3.
13. Применить к числу q тест Миллера-Рабина, см. тест 5.3. Если тест не пройден, то вернуться на шаг 11.
14. Применить к числу p тест Миллера-Рабина, см. тест 5.3. Если тест не пройден, то вернуться на шаг 11.

¹Нижняя граница для числа s определяется исходя из криптографических требований к конкретной криптографической системе.

15. Определить значение счетчика $n = 10$.
16. Вычислить случайное целое число a и $n = n - 1$.
17. Если $\text{НОД}(a^{ks+x} - 1, q) = 1$ и $a^{q-1} \equiv 1 \pmod{q}$, то перейти у к шагу 19.
18. Если $n = 0$, то вернуться на шаг 11. Иначе, вернуться на шаг 16.
19. Определить значение счетчика $n = 10$.
20. Вычислить случайное целое число a и $n = n - 1$.
21. Если $\text{НОД}(a^q - 1, p) = 1$ и $a^{p-1} \equiv 1 \pmod{p}$, то завершить алгоритм с уведомлением, что сильно простое число p построено.
22. Если $n = 0$, то вернуться на шаг 11. Иначе, вернуться на шаг 20. \square

Приведенный алгоритм имеет высокую трудоемкость и при практической реализации на ЭВМ может занимать достаточно много времени. В 1984 году Джон Гордон (John Gordon) в работе [7] предложил другой способ построения сильно простых чисел. Он основан на следующей лемме.

Лемма 5.6 (Лемма Гордона). *Простое число $p > 2$ является сильно простым и удовлетворяет сравнениям (5.15), тогда и только тогда, когда p имеет вид $p = u + 2kqs$, для натурального k и*

$$u = \begin{cases} w, & \text{если } w - \text{нечетно,} \\ w + qs, & \text{если } w - \text{четно,} \end{cases}$$

где $u \equiv s^{q-1} - q^{s-1} \pmod{qs}$.

Доказательство. Пусть $p = u + 2kqs$, для некоторого натурального k , тогда, в силу малой теоремы Ферма,

$$p \equiv u \equiv -q^{s-1} \equiv -1 \pmod{s}, \quad \text{и} \quad p \equiv u \equiv s^{q-1} \equiv 1 \pmod{q},$$

и сравнения (5.15) выполнены, если простое число q имеет большой простой делитель r .

Пусть π сильно простое число, не удовлетворяющее условиям леммы. В силу сравнений (5.15) $\pi - p \equiv 1 - 1 \equiv 0 \pmod{q}$ и $\pi - p \equiv -1 - (-1) \equiv 0 \pmod{s}$, следовательно, $\pi \equiv p \pmod{qs}$. Тогда $\pi \equiv w \pmod{rs}$ и имеет вид $\pi = u + 2kqs$ для некоторого натурального числа k . Лемма доказана. \square

Предложенный Гордоном алгоритм основывался на данной лемме и состоял из следующей последовательности действий. В начале, необходимо построить простые числа q, s, r , например, с использованием алгоритма 5.6, изложенного нами ранее. Далее, число p необходимо искать в арифметической прогрессии $p = u + 2kqs$. Для отсева составных чисел можно использовать тест Миллера-Рабина. Для доказательства простоты необходимо использовать алгоритмы доказательства простоты чисел произвольного вида.

НЕПРЕРЫВНЫЕ ДРОБИ

Определение непрерывной дроби - Понятие подходящей дроби - Теорема о наилучшем приближении - Квадратичные иррациональности и их свойства - Подходящие дроби и наилучшие приближения.

В этой лекции мы рассмотрим непрерывные дроби действительных чисел, или более точно, непрерывные дроби действительных квадратичных иррациональностей.

Далее нам понадобятся некоторые соотношения, возникающие при вычислении непрерывных дробей. Сейчас же мы приведем необходимые определения и доказательства.

Определение 6.1. Пусть α действительное число. Мы будем называть целой частью α , которую мы обозначаем символом $[\alpha]$, наибольшее целое число, меньшее, либо равное α . В частном случае: целая часть целого числа совпадает с ним.

Отметим, что α может быть как отрицательным, так и положительным числом. Например $[\sqrt{13}] = 3$, в то время как $[-\sqrt{13}] = -4$. В любом случае выполнено неравенство $[\alpha] \leq \alpha$.

Пусть α_0 действительное число и $\alpha_0 \neq 0$. Определим последовательность действительных чисел $\alpha_1, \alpha_2, \dots$ следующим рекуррентным соотношением

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n}, \quad \text{где } a_n = [\alpha_n]. \quad (6.1)$$

В случае, если α_n является целым числом, то есть выполнено равенство $a_n = \alpha_n$, мы будем считать, что последовательность (6.1) обрывается.

Записав равенство (6.1) в виде $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$, мы можем выразить число α_0 в виде

$$\alpha_0 = a_0 + \frac{1}{\alpha_1} = a_0 + \frac{1}{a_1 + \frac{1}{\alpha_2}} = \dots$$

или, в общем виде,

$$\alpha_0 = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{\alpha_n}}}}, \quad (6.2)$$

для произвольного индекса n .

Для упрощенной записи равенства (6.2) мы будем использовать обозначение $\alpha_0 = [a_0, a_1, \dots, a_{n-1}, \alpha_n]$.

Определение 6.2. Пусть $\alpha_0 \neq 0$ действительное число. Мы будем называть представление (6.2)

$$\alpha_0 = [a_0, a_1, \dots, a_{n-1}, \alpha_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{\alpha_n}}}},$$

$n = 1, 2, \dots$ непрерывной или цепной дробью числа α_0 . Элементы последовательности a_0, a_1, \dots мы будем называть неполными частными, а элементы последовательности $\alpha_1, \alpha_2, \dots$ полными частными.

Заметим, что из соотношения (6.1) и неравенства $[\alpha] \leq \alpha$ вытекает выполнимость следующих неравенств

$$0 \leq \alpha_n - [\alpha_n] < 1 \quad \text{и} \quad \alpha_n > 1, \quad a_n \geq 1 \quad \text{при} \quad n \geq 1. \quad (6.3)$$

6.1 Конечные непрерывные дроби

Остановимся на частном случае, когда последовательность полных частных $\alpha_0, \alpha_1, \dots, \alpha_n$ конечна. Верна следующая лемма.

Лемма 6.1. Пусть $\alpha_0 \neq 0$ действительное число. Последовательность полных частных $\alpha_1, \alpha_2, \dots$, определяемая соотношениями (6.1), обрывается тогда и только тогда, когда α_0 рациональное число.

Доказательство. Если последовательность конечна, то найдется индекс n , такой что α_n целое число и $\alpha_n = a_n$. Тогда $\alpha_{n-1} = a_{n-1} + \frac{1}{a_n}$ является рациональным числом. Выполняя аналогичные рассуждения для всех индексов, меньших n , получаем, что α_0 является рациональным числом.

Если α_0 рациональное число, то оно представимо в виде несократимой дроби $\alpha_0 = \frac{p}{q}$. Применим к числам p, q алгоритм Эвклида, см. алгоритм 1.1, а именно представим

$$p = a_0q + r_1, \quad \text{где } 0 \leq r_1 < q.$$

Тогда $\alpha_0 = \frac{p}{q} = a_0 + \frac{1}{\alpha_1}$, где $\alpha_1 = \frac{q}{r_1}$. Производя деление q на r_1 с остатком, получим

$$q = a_1r_1 + r_2, \quad \text{где } 0 \leq r_2 < r_1,$$

что равносильно $\alpha_1 = \frac{q}{r_1} = a_1 + \frac{1}{\alpha_2}$, где $\alpha_2 = \frac{r_1}{r_2}$.

Продолжая этот процесс, мы получим равенство

$$\alpha_n = \frac{r_{n-1}}{r_n},$$

где

$$\begin{aligned} r_{-1} &= p, \quad r_0 = q, \\ r_{n-1} &= a_n r_n + r_{n+1}, \quad 0 \leq r_{n+1} < r_n. \end{aligned}$$

Последовательность r_0, r_1, \dots образует строго убывающую последовательность неотрицательных целых чисел, следовательно, найдется такой индекс n , что $r_{n+1} = 0$. Из этого равенства следует, что $\alpha_n = a_n = \frac{r_{n-1}}{r_n}$ является целым числом. Последнее рассуждение завершает доказательство леммы. \square

Из утверждения доказанной нами леммы следует, что рассматриваемая последовательность $\alpha_1, \alpha_2, \dots$ бесконечна, если α_0 является действительной иррациональностью, то есть не может быть представлено в виде несократимой дроби.

6.2 Понятие подходящей дроби

Для каждого индекса n мы можем рассмотреть рациональную дробь $\frac{P_n}{Q_n}$, определяемую равенством

$$\frac{P_n}{Q_n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_n}}}} = [a_0, a_1, \dots, a_{n-1}, a_n]. \quad (6.4)$$

Определение 6.3. Пусть $\alpha_0 \neq 0$ действительное число. Дробь $\frac{P_n}{Q_n}$, определяемая равенством (6.4), называется подходящей дробью к числу α_0 .

Нам потребуются следующие леммы, описывающих свойства числителей и знаменателей подходящих дробей.

Лемма 6.2. Пусть $\alpha_0 \neq 0$ действительное число. Для числителей P_n и знаменателей Q_n подходящих дробей числа α_0 выполнены следующие рекуррентные соотношения

$$\begin{aligned} P_{n+1} &= a_{n+1}P_n + P_{n-1}, \\ Q_{n+1} &= a_{n+1}Q_n + Q_{n-1}, \end{aligned} \quad (6.5)$$

где $P_{-1} = 1$, $Q_{-1} = 0$, $P_0 = a_0$, $Q_0 = 1$.

Доказательство. Из определения подходящей дроби следуют равенства

$$\frac{P_0}{Q_0} = a_0, \quad \frac{P_1}{Q_1} = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1},$$

которые задают начальные значения для соотношений (6.5).

Проведем доказательство по индукции. Предположим, что утверждение леммы выполнено для всех индексов равных или меньших n , то есть выполнено равенство

$$\frac{P_n}{Q_n} = [a_0, a_1, \dots, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}}.$$

Тогда утверждение леммы следует из следующего равенства

$$\begin{aligned} \frac{P_{n+1}}{Q_{n+1}} &= [a_0, a_1, \dots, a_n, a_{n+1}] = \\ &= \left[a_0, a_1, \dots, a_n + \frac{1}{a_{n+1}} \right] = \frac{\left(a_n + \frac{1}{a_{n+1}} \right) P_{n-1} + P_{n-2}}{\left(a_n + \frac{1}{a_{n+1}} \right) Q_{n-1} + Q_{n-2}} = \\ &= \frac{a_{n+1} (a_n P_{n-1} + P_{n-2}) + P_{n-1}}{a_{n+1} (a_n Q_{n-1} + Q_{n-2}) + Q_{n-1}} = \frac{a_{n+1} P_n + P_{n-1}}{a_{n+1} Q_n + Q_{n-1}}. \end{aligned}$$

□

Основываясь на доказательстве леммы 6.2 легко заметить, что из равенства

$$[a_0, \dots, a_n] = \frac{a_n P_{n-1} + P_{n-2}}{a_n Q_{n-1} + Q_{n-2}},$$

следует равенство

$$\alpha_0 = [a_0, \dots, \alpha_{n+1}] = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}}. \quad (6.6)$$

Отметим, что неравенство (6.3) и формулы (6.5) позволяют заключить, что числители и знаменатели подходящих дробей удовлетворяют неравенствам

$$P_n > 0, \quad Q_n > 0.$$

Лемма 6.3. При всех индексах $n = 0, 1, \dots$ для числителей P_n и знаменателей Q_n подходящих дробей выполнено следующее соотношение

$$P_{n+1} Q_n - Q_{n+1} P_n = (-1)^n. \quad (6.7)$$

Доказательство. Используя равенства (6.5), получим следующие равенства

$$\begin{aligned} P_{n+1} Q_n - Q_{n+1} P_n &= (a_{n+1} P_n + P_{n-1}) Q_n - (a_{n+1} Q_n + Q_{n-1}) P_n = \\ &= -(P_n Q_{n-1} - Q_n P_{n-1}) = (-1)^2 (P_{n-1} Q_{n-2} - Q_{n-1} P_{n-2}) = \dots \\ &= (-1)^k (P_{n-k+1} Q_{n-k} - Q_{n-k+1} P_{n-k}), \end{aligned}$$

для любого $k = 1, 2, \dots$

Подставляя в полученные равенства $k = n + 1$ и начальные значения $P_{-1} = 1, P_0 = a_0, Q_{-1} = 0, Q_0 = 1$ из (6.5), получим равенство

$$P_{n+1} Q_n - Q_{n+1} P_n = (-1)^{n+2},$$

которое равносильно утверждению леммы. □

Заметим, что из равенства (6.7) следует, что подходящая дробь $\frac{P_n}{Q_n}$ несократима. Если предположить обратное, то найдется целое число d_n такое, что $\text{НОД}(P_n, Q_n) = d_n > 1$ и $d_n | (-1)^{n+1}$. Последнее условие невыполнимо.

Лемма 6.4. При всех индексах $n = 0, 1, \dots$ для числителей P_n и знаменателей Q_n подходящих дробей выполнено следующее соотношение

$$P_{n+1} Q_{n-1} - Q_{n+1} P_{n-1} = a_{n+1} (-1)^{n+1} \quad (6.8)$$

Доказательство. Для доказательства леммы домножим первое равенство в (6.5) на Q_{n-1} и вычтем из полученного второе равенство из (6.5), домноженное на P_{n-1} . Учитывая предыдущую лемму, получаем, с точностью до показателя степени при -1 , искомое равенство

$$P_{n+1}Q_{n-1} - Q_{n+1}P_{n-1} = a_{n+1}(P_nQ_{n-1} - Q_nP_{n-1}) = a_{n+1}(-1)^{n-1}.$$

□

Две последние леммы позволяют нам получить явное представление о расположении на действительной оси элементов последовательности подходящих дробей. Согласно утверждению леммы 6.3 выполнены неравенства $\frac{P_{2k+1}}{Q_{2k+1}} > \frac{P_{2k}}{Q_{2k}}$ при некотором натуральном k . Далее, из утверждения леммы 6.4 следует, что $\frac{P_{2k-1}}{Q_{2k-1}} > \frac{P_{2k+1}}{Q_{2k+1}}$ и $\frac{P_{2k+2}}{Q_{2k+2}} > \frac{P_{2k}}{Q_{2k}}$ при некотором натуральном k , то есть элементы последовательности с нечетными номерами образуют возрастающую подпоследовательность, а элементы с четными номерами — убывающую. Получаем цепочку неравенств

$$\dots \frac{P_{2k-1}}{Q_{2k-1}} > \frac{P_{2k+1}}{Q_{2k+1}} > \dots > \frac{P_{2k+2}}{Q_{2k+2}} > \frac{P_{2k}}{Q_{2k}} > \dots \quad (6.9)$$

из которой следует, что последовательность подходящих дробей сходится и имеет предел. Чему равен этот предел данной определяет теорема 6.1, к доказательству которой мы скоро приступим.

Лемма 6.5. *Для всех индексов $n = 1, 2, \dots$ знаменатели Q_n подходящих дробей удовлетворяют неравенству $Q_{n+1} > 2^{\lceil \frac{n}{2} \rceil}$ или, что равносильно*

$$\begin{cases} Q_{n+1} \geq 2^{\frac{n}{2}}, & \text{при четном } n, \\ Q_{n+1} \geq 2^{\frac{n+1}{2}}, & \text{при нечетном } n. \end{cases} \quad (6.10)$$

Доказательство. Из соотношений (6.3) и (6.5) следует неравенство

$$Q_{n+1} = a_{n+1}Q_n + Q_{n-1} \geq Q_n + Q_{n-1} \geq 2Q_{n-1} + Q_{n-2} \geq 2Q_{n-1}$$

из которого следует утверждение леммы: при нечетном n выполнено неравенство

$$Q_{n+1} \geq 2^{\frac{n+1}{2}} Q_0 = 2^{\frac{n+1}{2}},$$

а при четном n

$$Q_{n+1} \geq 2^{\frac{n}{2}} Q_1 \geq 2^{\frac{n}{2}}.$$

□

Теперь мы можем доказать теорему о приближении числа α_0 последовательностью подходящих дробей.

Теорема 6.1. Пусть $\alpha_0 \neq 0$ действительное число. Тогда последовательность подходящих дробей сходится к α_0 , то есть выполнено условие

$$\alpha_0 = \lim_{n \rightarrow \infty} \frac{P_n}{Q_n}.$$

Доказательство. Сначала мы покажем, что последовательность подходящих дробей сходится. Действительно, из леммы 6.3 получаем равенство

$$\left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = \frac{1}{Q_n Q_{n+1}} |P_{n+1} Q_n - Q_{n+1} P_n| = \frac{1}{Q_n Q_{n+1}}.$$

Из этого равенства и из утверждения леммы 6.5 следует, что последовательность подходящих дробей сходится, то есть

$$\lim_{n \rightarrow \infty} \left| \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} \right| = 0.$$

Нам осталось выяснить чему равен предел последовательности подходящих дробей. Учитывая равенство (6.6) и утверждение леммы 6.3 получим следующее равенство

$$\begin{aligned} \alpha_0 - \frac{P_n}{Q_n} &= \frac{1}{Q_n} (\alpha_0 Q_n - P_n) = \\ &= \frac{1}{Q_n} \left(Q_n \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}} - P_n \right) = \\ &= \frac{1}{Q_n} \left(\frac{Q_n P_{n-1} - P_n Q_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}} \right) = \frac{(-1)^n}{Q_n (\alpha_{n+1} Q_n + Q_{n-1})}. \end{aligned} \quad (6.11)$$

Вспоминая, что α_n и Q_n положительны при всех $n \geq 1$, получаем неравенство

$$\left| \alpha_0 - \frac{P_n}{Q_n} \right| = \frac{1}{Q_n (\alpha_{n+1} Q_n + Q_{n-1})} \leq \frac{1}{Q_n (\alpha_{n+1} Q_n + Q_{n-1})} = \frac{1}{Q_{n+1} Q_n} \quad (6.12)$$

из которого вытекает утверждение теоремы. \square

Из доказанной нами теоремы следует, что мы можем приблизить действительное число α_0 при помощи рациональной дроби с любой степенью точности. В качестве такой дроби выступает некоторая подходящая

дробь. Используя подходящие дроби можно производить эффективные вычисления с действительными числами, при некотором, заранее заданном, уровне погрешности вычислений.

Пример 6.1. Отойдём от общего случая и рассмотрим частный пример, а именно, разложим $\alpha_0 = \sqrt{29}$ в непрерывную дробь.

Используя равенства (6.1) и (6.5) запишем

$$\begin{aligned}\alpha_0 &= \sqrt{29} \sim 5.3851648, & a_0 &= \lfloor \sqrt{29} \rfloor = 5, & P_0 &= 5, & Q_0 &= 1, \\ \alpha_1 &= \frac{1}{\sqrt{29} - 5} = \frac{\sqrt{29} + 5}{(\sqrt{29} - 5)(\sqrt{29} + 5)} = \frac{\sqrt{29} + 5}{4}, \\ a_1 &= \lfloor \alpha_1 \rfloor = \left\lfloor \frac{\sqrt{29} + 5}{4} \right\rfloor = 2, & P_1 &= 11, & Q_1 &= 2, & \frac{P_1}{Q_1} &= 5.5,\end{aligned}$$

аналогично мы получим следующие равенства

$$\begin{aligned}\alpha_2 &= \frac{1}{\frac{\sqrt{29} + 5}{4} - 2} = \frac{\sqrt{29} + 3}{5}, & a_2 &= 1, & \frac{P_2}{Q_2} &= \frac{16}{3} = 5.333333, \\ \alpha_3 &= \frac{1}{\frac{\sqrt{29} + 3}{5} - 1} = \frac{\sqrt{29} + 2}{5}, & a_3 &= 1, & \frac{P_3}{Q_3} &= \frac{27}{5} = 5.4, \\ \alpha_4 &= \frac{1}{\frac{\sqrt{29} + 2}{5} - 1} = \frac{\sqrt{29} + 3}{4}, & a_4 &= 2, & \frac{P_4}{Q_4} &= \frac{70}{13} = 5.3846154, \\ \alpha_5 &= \frac{1}{\frac{\sqrt{29} + 3}{4} - 2} = \sqrt{29} + 5, & a_5 &= 10, & \frac{P_5}{Q_5} &= \frac{727}{135} = 5.3851852, \\ \alpha_6 &= \frac{1}{\sqrt{29} - 5} = \frac{\sqrt{29} + 5}{4}, & a_6 &= 2, & \frac{P_6}{Q_6} &= \frac{1524}{283} = 5.385159, \\ \alpha_7 &= \frac{1}{\frac{\sqrt{29} + 5}{4} - 2} = \frac{\sqrt{29} + 3}{5}, & a_7 &= 1, & \frac{P_7}{Q_7} &= \frac{2251}{418} = 5.3851675.\end{aligned}$$

Мы остановим наши вычисления и заметим, что выполнены равенства

$$\alpha_6 = \alpha_1, \quad \alpha_7 = \alpha_2, \quad \dots,$$

то есть наша последовательность полных частных зациклилась и имеет период равный 5. Мы можем записать непрерывную дробь для $\alpha_0 = \sqrt{29}$ в виде

$$\sqrt{29} = [5; 2, 1, 1, 2, 10, 2, 1, 1, 2, 10, \dots]$$

или, в ещё более короткой форме, $\sqrt{29} = [5; \overline{2, 1, 1, 2, 10}]$. Отметим, что всего за семь шагов мы получили очень хорошее приближение к α_0 . Действительно,

$$\left| \alpha_0 - \frac{P_7}{Q_7} \right| = 0.0000027 < \frac{1}{Q_8 Q_7} = \frac{1}{701 \cdot 418} = 0.0000034.$$

6.3 Квадратичные иррациональности

Напомним, что целое число D называется полным квадратом, если найдется целое число d такое, что $D = d^2$.

Определение 6.4. Действительное число α называется квадратичной иррациональностью, если найдутся такие целые, взаимно простые числа $u > 0, v, w$, что значение $v^2 - 4uw > 0$ не является полным квадратом, а α является одним из корней многочлена $f(x) = ux^2 + vx + w$, то есть $f(\alpha) = 0$.

Величина $D = v^2 - 4uw$ называется дискриминантом квадратичной иррациональности α .

Пример 6.2. Проиллюстрируем понятие квадратичной иррациональности. Легко видеть, что значение $\alpha = \sqrt{29}$ является корнем многочлена $f(x) = x^2 - 29$ и, соответственно, квадратичной иррациональностью. Также, квадратичной иррациональностью является корень многочлена $f(x) = 3x^2 - 5x - 7$ равный $\alpha = \frac{5 + \sqrt{109}}{2}$.

Из определения 6.4 следует, что любая квадратичная иррациональность может быть представлена в виде

$$\alpha = \frac{A + \sqrt{D}}{B}, \tag{6.13}$$

где A, B, D — целые числа, $D = v^2 - 4uw$ не является полным квадратом и

$$\begin{cases} A = -v, B = 2u, & \text{либо} \\ A = v, B = -2u, \end{cases}$$

в зависимости от того, какой из двух корней многочлена $f(x)$ выбирается.

Возникает вопрос: единственно ли указанное представление? Для ответа на него предположим, что равенство (6.13) не единственно, то есть найдется еще одна пара целых чисел C, E таких, что $\alpha = \frac{C + \sqrt{D}}{E}$. Тогда выполнено равенство

$$E(A + \sqrt{D}) = B(C + \sqrt{D}),$$

откуда

$$EA - BC = (B - E)\sqrt{D}. \quad (6.14)$$

В левой части равенства (6.14), в силу выбора значений A, B, C, E , находится целое число. В правой части — произведение целого числа на корень из N , не являющегося полным квадратом, то есть действительное число. Таким образом, равенство (6.14) может быть выполнено только в том случае, если в обеих его частях находятся нули. Из этого следует, что $B = E$, $A = C$ и представление (6.14) единственно.

Определение 6.5. Пусть $\alpha = \frac{A + \sqrt{D}}{B}$ квадратичная иррациональность — корень многочлена $f(x) = ux^2 + vx + w$. Тогда второй корень этого многочлена

$$\hat{\alpha} = \frac{A - \sqrt{D}}{B}$$

называется квадратичной иррациональностью, сопряженной с α .

Легко показать, что каждое действительное число, представимое в виде (6.13), является квадратичной иррациональностью. Введем многочлен с целыми коэффициентами

$$\begin{aligned} f(x) &= B^2(x - \alpha)(x - \hat{\alpha}) = \\ &= (Bx - A - \sqrt{D})(Bx - A + \sqrt{D}) = \\ &= (Bx - A)^2 - D = B^2x^2 - 2ABx + A^2 - D \end{aligned} \quad (6.15)$$

Получаем, что α является корнем многочлена $f(x)$ второй степени с целыми коэффициентами. Если $A^2 - D$ делится на B , то коэффициенты многочлена можно сократить на общий множитель.

Используя преобразование (6.1), разложим квадратичную иррациональность $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$, являющуюся корнем многочлена $f(x) = ux^2 + vx + w$, в непрерывную дробь.

Для полного частного α_1 выполнено равенство

$$\begin{aligned} \alpha_1 &= \frac{1}{\alpha_0 - a_0} = \frac{1}{\frac{A_0 + \sqrt{D}}{B_0} - a_0} = \frac{B_0}{(A_0 - a_0B_0) + \sqrt{D}} = \\ &= \frac{B_0(A_0 - a_0B_0) - B_0\sqrt{D}}{(A_0 - a_0B_0)^2 - D}. \end{aligned} \quad (6.16)$$

Обозначим символом $\hat{\alpha}_0 = \frac{A_0 - \sqrt{D}}{B_0}$ второй корень многочлена $f(x)$. Тогда, используя теорему Виета, получим равенство

$$\alpha_0 \hat{\alpha}_0 = \left(\frac{A_0 + \sqrt{D}}{B_0} \right) \left(\frac{A_0 - \sqrt{D}}{B_0} \right) = w,$$

откуда $A_0^2 - D = wB_0^2$. Обозначим $B_{-1} = -wB_0$ и получим $-B_{-1}B_0 = A_0^2 - D$. Подставляя полученное равенство в (6.16) и сокращая на $-B_0$ получим

$$\alpha_1 = \frac{(a_0B_0 - A_0) + \sqrt{D}}{2a_0A_0 - a_0^2B_0 + B_{-1}} = \frac{A_1 + \sqrt{D}}{B_1},$$

где

$$\begin{aligned} A_1 &= a_0B_0 - A_0, \\ B_1 &= a_0(2A_0 - a_0B_0) + B_{-1} = a_0(A_0 - A_1) + B_{-1}. \end{aligned}$$

Мы получили, что полное частное α_1 имеет такой же вид как α_0 и так же является квадратичной иррациональностью. Более того, значения A_1, B_1 могут быть выражены через значения A_0, B_0 и коэффициенты многочлена $f(x)$. Обобщим полученный результат и докажем следующую лемму

Лемма 6.6. Пусть $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$ квадратичная иррациональность, являющаяся корнем многочлена $f(x) = ux^2 + vx + w$, $D = v^2 - 4uw$, и $\alpha_0, \alpha_1, \dots, \alpha_n, \dots$ последовательность полных частных.

Тогда для каждого полного частного α_{n+1} выполнено равенство

$$\alpha_{n+1} = \frac{A_{n+1} + \sqrt{D}}{B_{n+1}},$$

где

$$\begin{aligned} A_{n+1} &= a_nB_n - A_n, \\ B_{n+1} &= a_n(A_n - A_{n+1}) + B_{n-1}, \end{aligned} \tag{6.17}$$

при $B_{-1} = -wB_0$, а также выполнено равенство

$$-B_nB_{n+1} = (A_{n+1}^2 - D).$$

Доказательство. Мы проведем доказательство по индукции. Выполнимость утверждений леммы для α_1 мы проверили выше. Предположим, что для всех индексов $1, \dots, n$ утверждение леммы выполнено, тогда,

аналогично (6.16), получаем

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n} = \frac{B_n}{(A_n - a_n B_n) + \sqrt{D}} = \frac{-B_n (A_{n+1} + \sqrt{D})}{A_{n+1}^2 - D}, \quad (6.18)$$

где $A_{n+1} = (a_n B_n - A_n)$.

Покажем, что $B_n | (A_{n+1}^2 - D)$. В силу предположения индукции выполнено $B_n | (A_n^2 - D)$. Тогда из (6.18) и следующего равенства

$$A_{n+1}^2 - D = (a_n B_n - A_n)^2 - D = a_n^2 B_n^2 - 2a_n A_n B_n + A_n^2 - D$$

следует, что $B_n | (A_{n+1}^2 - D)$. Обозначим $B_{n+1} = \frac{A_{n+1}^2 - D}{-B_n}$, тогда

$$-B_n B_{n+1} = (A_{n+1}^2 - D). \quad (6.19)$$

Подставляя (6.19) в (6.18) получим приведенное в утверждении леммы равенство $\alpha_{n+1} = \frac{A_{n+1} + \sqrt{D}}{B_{n+1}}$. Нам осталось получить рекуррентную формулу для B_{n+1} .

Из (6.18), с учетом изменения индексов в равенстве (6.19), получаем

$$\begin{aligned} B_{n+1} &= \frac{A_{n+1}^2 - D}{-B_n} = \frac{(a_n B_n - A_n)^2 - D}{-B_n} = \\ &= \frac{-B_n(2a_n A_n - a_n^2 B_n) + A_n^2 - D}{-B_n} = \\ &= a_n(2A_n - a_n B_n) + B_{n-1} = a_n(A_n - A_{n+1}) + B_{n-1}. \end{aligned}$$

□

Доказанная лемма определяет соотношения (6.17), которые используются для эффективного разложения квадратичной иррациональности в непрерывную дробь.

В рассмотренном нами ранее на стр. 118 примере разложение квадратичной иррациональности в непрерывную дробь оказалось периодично. Покажем, что это свойство верно для любой квадратичной иррациональности.

Для этого нам потребуется ввести еще одно определение и доказать две вспомогательные леммы.

Определение 6.6. Пусть α — квадратичная иррациональность и $\hat{\alpha}$, сопряженная с α . Тогда α называется приведенной квадратичной иррациональностью, если

$$\alpha > 1 \quad \text{и} \quad -1 < \hat{\alpha} < 0. \quad (6.20)$$

Лемма 6.7. Пусть $\alpha = \frac{A + \sqrt{D}}{B}$ приведенная квадратичная иррациональность. Тогда

$$\begin{aligned} 0 < A < \sqrt{D}, \\ 0 < B < 2\sqrt{D}. \end{aligned}$$

Доказательство. Если α приведенная квадратичная иррациональность, тогда из (6.20) вытекают следующие утверждения:

1. так как $\alpha - \hat{\alpha} = \frac{2\sqrt{D}}{B} > 0$ и $\sqrt{D} > 0$, то выполнено $B > 0$;
2. так как $\alpha - \hat{\alpha} = \frac{2\sqrt{D}}{B} > 1$, то выполнено $2\sqrt{D} > B$;
3. так как $\alpha + \hat{\alpha} = \frac{2A}{B} > 0$ и $B > 0$, то выполнено $A > 0$;
4. так как $\hat{\alpha} = \frac{A - \sqrt{D}}{B} < 0$ и $B > 0$, то выполнено неравенство $A < \sqrt{D}$ и лемма доказана.

□

Лемма 6.8. Пусть $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$ квадратичная иррациональность и $\hat{\alpha}_1, \hat{\alpha}_2, \dots$ сопряженные полных частных ее разложения непрерывную дробь. Тогда

1. для всех $n \geq 0$ выполнено равенство

$$\hat{\alpha}_{n+1} = \frac{1}{\hat{\alpha}_n - a_n}. \quad (6.21)$$

2. значение $\hat{\alpha}_{n+1}$ удовлетворяет равенству

$$\hat{\alpha}_{n+1} = -\frac{\hat{\alpha}_0 Q_{n-1} - P_{n-1}}{\hat{\alpha}_0 Q_n - P_n}. \quad (6.22)$$

Доказательство. Учитывая (6.19), первое утверждение леммы получаем из равенства

$$\begin{aligned} \frac{1}{\hat{\alpha}_n - a_n} &= \frac{B_n}{(A_n - a_n B_n) - \sqrt{D}} = \\ &= \frac{B_n (-A_{n+1} + \sqrt{D})}{A_{n+1}^2 - D} = \frac{-A_{n+1} + \sqrt{D}}{-B_{n+1}} = \hat{\alpha}_{n+1}. \end{aligned}$$

Докажем второе утверждение леммы. Используя первое утверждение леммы, разложим $\hat{\alpha}_0$ в непрерывную дробь

$$\hat{\alpha}_0 = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{\hat{\alpha}_{n+1}}}}}$$

Таким образом, последовательность подходящих дробей для $\hat{\alpha}_0$ совпадает с последовательностью подходящих дробей $\frac{P_n}{Q_n}$ для α_0 и, согласно (6.6), выполнено равенство

$$\hat{\alpha}_0 = \frac{\hat{\alpha}_{n+1} P_n + P_{n-1}}{\hat{\alpha}_{n+1} Q_n + Q_{n-1}}.$$

Выражая из него $\hat{\alpha}_{n+1}$ получим соотношение (6.22). □

Теорема 6.2. Пусть $\alpha = \frac{A + \sqrt{D}}{B}$ квадратичная иррациональность. Тогда ее непрерывная дробь периодична.

Доказательство. В начале предположим, что α_0 приведенная квадратичная иррациональность, то есть

$$\alpha_0 > 1, \quad a_0 \geq 1, \quad -1 < \hat{\alpha}_0 < 0.$$

Тогда из (6.3) следует, что $\alpha_1 > 1$. Далее, следуя равенству (6.21), получим

$$\frac{1}{\hat{\alpha}_1} = \hat{\alpha}_0 - a_0 < 0 - a_0 \leq -1,$$

следовательно $-1 < \hat{\alpha}_1 < 0$ и α_1 является приведенной квадратичной иррациональностью.

Продолжая далее, мы получим, что α_2 и все остальные полные частные $\alpha_n = \frac{A_n + \sqrt{D}}{B_n}$ являются приведенными квадратичными иррациональностями. Из леммы 6.7 следует, что значения A_n, B_n неотрицательны, ограничены сверху и бесконечная последовательность пар A_n, B_n принимает значения на конечном множестве. Следовательно найдется некоторый индекс n_0 такой, что $A_0 = A_{n_0}, B_0 = B_{n_0}$ и последовательность α_n заиклится или, другими словами, периодична.

Для завершения доказательства теоремы нам осталось показать, что для любой квадратичной иррациональности α_0 найдется такой индекс n_0 , что α_{n_0} является приведенной квадратичной иррациональностью.

Вначале рассмотрим частный случай. Пусть

$$\alpha_0 = A_0 + \sqrt{D}$$

и α_0 не является приведенной. Тогда $a_0 = A_0 + [\sqrt{D}]$ и равенство (6.21) позволяет записать неравенства

$$-1 < \hat{\alpha}_1 = \frac{1}{\hat{\alpha}_0 - a_0} = \frac{-1}{\sqrt{D} + [\sqrt{D}]} < 0.$$

Следовательно, α_1 приведенная квадратичная иррациональность.

Теперь перейдем к общему случаю. Рассмотрим равенство (6.22) и, учитывая равенство (6.11), полученное в ходе доказательства теоремы 6.1, при $n \geq 1$, получим

$$\begin{aligned} \hat{\alpha}_{n+1} &= -\frac{\hat{\alpha}_0 Q_{n-1} - P_{n-1}}{\hat{\alpha}_0 Q_n - P_n} = \\ &= -\frac{Q_{n-1}}{Q_n} \left(\frac{\hat{\alpha}_0 - \frac{P_{n-1}}{Q_{n-1}}}{\hat{\alpha}_0 - \frac{P_n}{Q_n}} \right) = -\frac{Q_{n-1}(1 + \omega_{n+1})}{Q_n}, \end{aligned} \quad (6.23)$$

где точное значение ω_{n+1} определено равенством

$$\omega_{n+1} = \frac{\left(\frac{(-1)^{n-1}}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} - \frac{(-1)^n}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \right)}{\hat{\alpha}_0 - \alpha_0 + \frac{(-1)^n}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})}} \quad (6.24)$$

Равенство (6.23) позволяет сделать следующее заключение. Если ω_{n+1} удовлетворяет неравенствам

$$-1 < \omega_{n+1} < \frac{Q_n}{Q_{n-1}} - 1, \quad (6.25)$$

то при $n \geq 1$ из (6.23) вытекают неравенства $-1 < \hat{\alpha}_{n+1} < 0$. Следовательно α_{n+1} приведенная квадратичная иррациональность и, как мы доказали ранее, ее разложение в непрерывную дробь периодически. Следовательно, периодически разложение для α_0 .

Нам осталось показать, что найдется индекс $n \geq 1$ для которого выполнены неравенства (6.25). Рассмотрим равенство (6.24) более подробно и обозначим символом δ_{n+1} числитель дроби, то есть

$$\delta_{n+1} = (-1)^{n-1} \left(\frac{1}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \right).$$

Поскольку α_n и Q_n положительные целые числа, то выполнено $|\delta_{n+1}| < 1$. Более того

$$\begin{aligned} |\delta_{n+1}| &= \frac{1}{Q_{n-1}(\alpha_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \leq \\ &\leq \frac{1}{Q_{n-1}(a_n Q_{n-1} + Q_{n-2})} + \frac{1}{Q_n(a_{n+1} Q_n + Q_{n-1})} = \\ &= \frac{1}{Q_n Q_{n-1}} + \frac{1}{Q_{n+1} Q_n} = \frac{1}{Q_n} \left(\frac{1}{Q_{n+1}} + \frac{1}{Q_{n-1}} \right). \end{aligned} \quad (6.26)$$

Обозначим $\gamma = \hat{\alpha}_0 - \alpha_0$ и рассмотрим знаменатель дроби (6.24), тогда

$$\begin{aligned} \left| \hat{\alpha}_0 - \alpha_0 + \frac{(-1)^n}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \right| &\geq \\ &|\gamma| - \frac{1}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})} \geq |\gamma| - \frac{1}{Q_{n+1} Q_n}. \end{aligned}$$

С учетом (6.26), мы получили следующее неравенство

$$\begin{aligned} |\omega_{n+1}| &\leq \frac{|\delta_{n+1}|}{|\gamma| - \frac{1}{Q_{n+1} Q_n}} \leq \\ &= \left(\frac{1}{Q_{n+1}} + \frac{1}{Q_{n-1}} \right) \frac{Q_{n+1}}{Q_{n+1} Q_n |\gamma| - 1} = \\ &= \frac{Q_{n+1} + Q_{n-1}}{Q_{n+1} Q_n Q_{n-1} |\gamma| - Q_{n-1}}. \end{aligned}$$

Полученное неравенство позволяет нам сделать вывод о том, что всегда найдется индекс n , при котором будут выполнены ограничения на

ω_{n+1} , то есть неравенства (6.25). Если $|\gamma|$ принимает большие значения, например $|\gamma| > 1$, то выполнение неравенств (6.25) очевидно. Более тонким является случай, когда значения $|\gamma|$ близки к нулю.

Предположим, что $|\gamma|$ ограничен снизу величиной

$$|\gamma| > \frac{3}{Q_n Q_{n-1}} = \frac{3Q_{n+1}}{Q_{n+1} Q_n Q_{n-1}} > \frac{Q_{n+1} + 2Q_{n-1}}{Q_{n+1} Q_n Q_{n-1}}$$

тогда выполнено $|\omega_{n+1}| < 1$.

В силу того, что Q_n образуют монотонно возрастающую последовательность, замечаем, что для сколь угодно малого значения $\gamma = \hat{\alpha}_0 - \alpha_0$ найдется такой индекс n , что будет выполнено неравенство $|\gamma| > \frac{3}{Q_n Q_{n-1}}$ и, следовательно, $|\omega_{n+1}| < 1$. \square

Доказанная нами теорема позволяет получить оценку на величину индекса n , начиная с которого полные частные α_n станут приведенными квадратичными иррациональностями.

Следствие 1. Пусть $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$ квадратичная иррациональность, являющаяся корнем многочлена $f(x) = ux^2 + vx + w$, $u, v, w \in \mathbb{Z}$, где $u > 0$ и $D = v^2 - 4uw$. Тогда α_n приведенная квадратичная иррациональность, если

$$n > \log_2 \left(\frac{6u}{\sqrt{D}} \right).$$

Доказательство. Вспомним, что

$$\gamma = \hat{\alpha}_0 - \alpha_0 = \pm \frac{2\sqrt{D}}{B_0} = \pm \frac{\sqrt{D}}{u},$$

тогда из условия леммы следуют неравенства

$$n > \log_2 \left(\frac{6u}{\sqrt{D}} \right) = \log_2 \left(\frac{6}{|\gamma|} \right) \quad \text{и} \quad 2^{n-1} > \frac{3}{|\gamma|}.$$

Из утверждения леммы 6.5 получаем

$$Q_n Q_{n-1} \geq 2^{n-1} > \frac{3}{|\gamma|} \quad \text{или} \quad |\gamma| > \frac{3}{Q_n Q_{n-1}}.$$

Таким образом $|\omega_{n+1}| < 1$ и лемма доказана. \square

Нам осталось доказать последнюю теорему, которая позволяет связать между собой числители и знаменатели подходящих дробей и коэффициенты A_n, B_n разложения квадратичной иррациональности в непрерывную дробь.

Теорема 6.3. Пусть $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$ действительная квадратичная иррациональность и $\alpha_1, \alpha_2, \dots$ последовательность полных частных, удовлетворяющих равенству

$$\alpha_n = \frac{A_n + \sqrt{D}}{B_n}.$$

Тогда для всех индексов $n = 1, 2, \dots$ числители P_n и знаменатели Q_n подходящих дробей для α_0 удовлетворяют равенству

$$(P_n B_0 - Q_n A_0)^2 - Q_n^2 D = (-1)^{n+1} B_0 B_{n+1}. \quad (6.27)$$

Доказательство. Согласно (6.6), для любого индекса $n = 0, 1, \dots$, мы можем записать равенство

$$\alpha_0 = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}}.$$

Вспоминая, что $\alpha_{n+1} = \frac{A_{n+1} + \sqrt{D}}{B_{n+1}}$, получим равенство

$$\frac{A_0 + \sqrt{D}}{B_0} = \frac{P_n(A_{n+1} + \sqrt{D}) + B_{n+1}P_{n-1}}{Q_n(A_{n+1} + \sqrt{D}) + B_{n+1}Q_{n-1}},$$

которое равносильно

$$\begin{aligned} B_0(P_n(A_{n+1} + \sqrt{D}) + B_{n+1}P_{n-1}) &= \\ &= (A_0 + \sqrt{D})(Q_n(A_{n+1} + \sqrt{D}) + B_{n+1}Q_{n-1}). \end{aligned}$$

Раскрывая в последнем равенстве скобки и приводя слагаемые со множителем \sqrt{D} , получим равенство

$$\begin{aligned} B_0 B_{n+1} P_{n-1} - A_0 A_{n+1} Q_n - A_0 B_{n+1} Q_{n-1} + B_0 P_n A_{n+1} - Q_n D &= \\ &= (A_0 Q_n + A_{n+1} Q_n + B_{n+1} Q_{n-1} - B_0 P_n) \sqrt{D}. \end{aligned}$$

Применяя к последнему равенству рассуждения, аналогичные тем, что были применены к равенству (6.14), получим, что правая и левая части равенства равны нулю. Это позволяет из правой части равенства получить выражение для знаменателя Q_{n-1}

$$Q_{n-1} = \frac{B_0 P_n - Q_n(A_0 + A_{n+1})}{B_{n+1}}, \quad (6.28)$$

а также, из левой части равенства, для числителя P_{n-1}

$$\begin{aligned} P_{n-1} &= \frac{A_0 A_{n+1} Q_n + A_0 B_{n+1} Q_{n-1} + Q_n D - B_0 P_n A_{n+1}}{B_0 B_{n+1}} = \\ &= \frac{Q_n (D - A_0^2) - B_0 P_n (A_{n+1} - A_0)}{B_0 B_{n+1}}. \end{aligned} \quad (6.29)$$

Теперь рассмотрим утверждение леммы 6.3 и равенство (6.7), в правой части которого индекс n заменен на индекс $n - 1$, а в левой $(-1)^{n-1}$ на $(-1)^{n+1}$

$$P_n Q_{n-1} - Q_n P_{n-1} = (-1)^{n+1}.$$

Подставляя в него полученные выше выражения (6.28), (6.29), запишем

$$\begin{aligned} P_n \frac{B_0 P_n - Q_n (A_0 + A_{n+1})}{B_{n+1}} - \\ - Q_n \frac{Q_n (D - A_0^2) - B_0 P_n (A_{n+1} - A_0)}{B_0 B_{n+1}} = (-1)^{n+1}. \end{aligned}$$

Домножая наше равенство на $B_0 B_{n+1}$, раскрывая скобки и сокращая подобные члены, получим окончательный результат

$$(P_n B_0 - Q_n A_0)^2 - Q_n^2 D = (-1)^{n+1} B_0 B_{n+1}.$$

□

В частном случае, когда $\alpha_0 = \sqrt{N}$, выражение (6.27) принимает вид

$$P_n^2 - Q_n^2 D = (-1)^{n+1} B_{n+1}, \quad (6.30)$$

поскольку $A_0 = 0$ и $B_0 = 1$.

6.4 Наилучшие приближения

В некоторых методах анализа криптографических схем нам требуется понятие «наилучшего приближения». Поэтому мы завершим эту лекцию результатами, связывающими понятия о непрерывных дробях и наилучших приближениях. При изложении, мы следуем монографии [28].

Определение 6.7. Пусть α действительное, отличное от нуля число. Рациональная дробь $\frac{P}{Q}$ называется наилучшим приближением к числу α , если любой другой дроби $\frac{A}{B} \neq \frac{P}{Q}$ такой, что $1 \leq B \leq Q$, выполнено неравенство

$$|B\alpha - A| > |Q\alpha - P|.$$

Наилучшее приближение есть несократимая дробь. Предположив обратное, получим $P = uA$, $Q = uB$ при $u > 1$, откуда вытекает неравенство $|Q\alpha - P| = u|B\alpha - A| > |B\alpha - A|$, противоречащее определению наилучшего приближения.

Теорема 6.4. *Всякое наилучшее приближение к действительному числу α есть подходящая дробь к нему. И наоборот, каждая подходящая дробь $\frac{P_n}{Q_n}$ к числу α при $n \geq 1$ есть наилучшее приближение.*

Прежде чем переходить к доказательству заметим, что данное нами определение 6.7 эквивалентно тому, что система неравенств

$$\begin{cases} |x - \alpha y| \leq |P - \alpha Q|, \\ 0 < y \leq Q \end{cases} \quad (6.31)$$

имеет единственное решение в целых числах $x = P$, $y = Q$. Нам понадобится следующая лемма.

Лемма 6.9. *Пусть $\frac{P_n}{Q_n}$, $\frac{P_{n+1}}{Q_{n+1}}$ две соседние подходящие дроби к числу α , причем $\frac{P_{n+1}}{Q_{n+1}} \neq \alpha$. Тогда система неравенств*

$$\begin{cases} |x - \alpha y| \leq |P_n - \alpha Q_n|, \\ 0 < y \leq Q_{n+1} \end{cases} \quad (6.32)$$

имеет лишь два решения в целых числах, а именно $x = P_n$, $y = Q_n$ и $x = P_{n+1}$, $y = Q_{n+1}$.

Доказательство. Пусть x, y целые числа, решения системы неравенств (6.32). Представим их в виде

$$\begin{aligned} x &= uP_n + vP_{n+1}, \\ y &= uQ_n + vQ_{n+1}. \end{aligned}$$

где u, v неизвестные значения. Выражая в явном виде неизвестные u, v и воспользовавшись равенством (6.7) получим

$$u = (-1)^n(yP_{n+1} - xQ_{n+1}), \quad v = (-1)^n(xQ_n - yP_n).$$

Следовательно, неизвестные u, v могут принимать только целые значения, поскольку $P_n, Q_n, P_{n+1}, Q_{n+1}, x, y \in \mathbb{Z}$.

Наборы $u = 0, v = 1$ и $u = 1, v = 0$ дают нам два решения неравенства (6.32), указанные в формулировке леммы. Покажем, что других решений не существует.

Предположим, что u и v имеют одинаковые знаки. Тогда из условия $y > 0$ следует, что $uQ_n + vQ_{n+1} > 0$ и $u > 0, v > 0$. Но тогда $y \geq Q_n + Q_{n+1}$, что противоречит второму неравенству в (6.32). Таким образом, нам осталось рассмотреть случай, когда u и v имеют разные знаки.

Из неравенств (6.9) и утверждения теоремы 6.1 получаем, что числа $P_n - \alpha Q_n$ и $P_{n+1} - \alpha Q_{n+1}$ тоже имеют разные знаки, поэтому выполнено неравенство

$$\begin{aligned} |x - \alpha y| &= |u(P_n - \alpha Q_n) + v(P_{n+1} - \alpha Q_{n+1})| = \\ &= |u||P_n - \alpha Q_n| + |v||P_{n+1} - \alpha Q_{n+1}| > |P_n - \alpha Q_n|, \end{aligned}$$

которое противоречит (6.32). Лемма доказана. \square

Перейдем к доказательству теоремы 6.4. Пусть $\frac{P}{Q}$ наилучшее приближение к числу α и n максимальный индекс такой, что $Q_n \leq Q$. Предположим, что

$$|P - \alpha Q| < |P_n - \alpha Q_n|, \quad (6.33)$$

тогда, согласно утверждению леммы 6.9, дробь $\frac{P}{Q}$ совпадает с одной из подходящих дробей $\frac{P_n}{Q_n}$ или $\frac{P_{n+1}}{Q_{n+1}}$. Если (6.33) не выполнено, то $|P - \alpha Q| \geq |P_n - \alpha Q_n|$ и, в силу того, что $\frac{P}{Q}$ — наилучшее приближение, выполнено $P = P_n, Q = Q_n$. В обоих случаях, первое утверждение теоремы выполнено.

Теперь докажем обратное утверждение и покажем, что для всех индексов $n \geq 0$ каждая подходящая дробь $\frac{P_{n+1}}{Q_{n+1}}$ является наилучшим приближением. Рассмотрим значения x, y , являющиеся решением системы сравнений

$$\begin{cases} |x - \alpha y| \leq |P_{n+1} - \alpha Q_{n+1}|, \\ 0 < y \leq Q_{n+1}. \end{cases} \quad (6.34)$$

Из неравенств (6.9) и утверждения теоремы 6.1 получаем, что выполнено $|P_n - \alpha Q_n| > |P_{n+1} - \alpha Q_{n+1}|$. Тогда из (6.34) следуют неравенства

$$\begin{cases} |x - \alpha y| \leq |P_n - \alpha Q_n|, \\ 0 < y \leq Q_{n+1}, \end{cases}$$

которым, согласно лемме 6.9, удовлетворяет не более двух решений, а именно пары P_n, Q_n и P_{n+1} и Q_{n+1} . Поскольку P_n, Q_n не удовлетворяет (6.34), то $\frac{P_{n+1}}{Q_{n+1}}$ наилучшее приближение. Теорема доказана. \square

В заключение лекции мы докажем еще одну теорему, которая будет использована нами позднее при обосновании алгоритмов факторизации целых чисел.

Теорема 6.5. Если несократимая дробь $\frac{P}{Q}$, при $Q > 0$, удовлетворяет неравенству

$$\left| \alpha - \frac{P}{Q} \right| < \frac{1}{2Q^2}, \quad (6.35)$$

то она есть наилучшее приближение к α .

Доказательство. Предположим, что целые числа $x = A$, $y = B$ удовлетворяют неравенствам (6.31), то есть

$$\begin{cases} |A - \alpha B| \leq |P - \alpha Q|, \\ 0 < B \leq Q. \end{cases}$$

Тогда рассмотрим разность целых чисел $AQ - BP$ и получим неравенство

$$\begin{aligned} |AQ - BP| &= |Q(A - \alpha B) - B(P - \alpha Q)| \leq \\ &\leq Q|A - \alpha B| + B|P - \alpha Q| \leq 2Q|P - \alpha Q| < 2Q^2 \left| \alpha - \frac{P}{Q} \right| < 1, \end{aligned}$$

из которого следует, что разность $AQ - BP$ равна нулю или, что равносильно, $AQ = BP$. Поскольку дробь $\frac{P}{Q}$ несократима, то числа P и Q взаимно просты и мы получаем, что $Q|B$. Поскольку $B < Q$, то получаем, что $B = Q$, откуда вытекает равенство $A = P$. Следовательно система неравенств (6.31) имеет только одно решение. Теорема доказана. \square

Заметим, что из утверждения теорем 6.4 и 6.5 следует, что всякая несократимая дробь $\frac{P}{Q}$, удовлетворяющая неравенству (6.35), является подходящей дробью к числу α .

ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ

Метод пробного деления - Метод Ферма - Метод Лемана - Метод Полларда - Метод Брента - $p-1$ метод Полларда - $p+1$ метод Вильямса - Оптимизация методов Полларда и Вильямса - Метод Женга - Метод Макки.

В этой лекции мы описываем элементарные методы разложения составного числа m на множители. Эти методы достаточно просты для изложения, но имеют высокую трудоемкость, что не позволяет их использовать для разложения чисел, используемых на практике. Тем не менее, излагаемые алгоритмы могут быть использованы в качестве составных частей в более сложных алгоритмах.

На протяжении всей лекции мы будем считать, что m нечетное, составное число. Вопрос о том, как определить: является ли число m составным или простым, мы рассматривали в предыдущей лекции.

Напомним, что под задачей факторизации мы подразумеваем нахождение таких простых чисел p_1, \dots, p_k , что число m может быть единственным образом представлено в виде произведения

$$m = \prod_{i=1}^k p_i^{\alpha_i} = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

где α_i натуральные числа. Такое представление, в силу основной теоремы арифметики, см. теорему 1.4, существует и единственно.

Для поиска всех простых делителей числа m нам необходимо найти два делителя числа m , быть может и не простых, а потом применить процедуру поиска делителей к каждому из найденных делителей. Далее мы будем описывать алгоритмы предполагая, что нам достаточно найти два произвольных делителя числа m .

7.1 Метод пробного деления

Метод пробного деления является самым простым и очевидным алгоритмом поиска делителей числа m . Метод заключается в последовательном делении числа m на числа, не превосходящие величины $\lceil \sqrt{m} \rceil$. Такая оценка сверху верна в силу леммы 1.6 из которой следует, что любой простой делитель p числа m удовлетворяет неравенству $p \leq \sqrt{m}$.

С теоретической точки зрения, достаточно делить число m только на простые числа. Однако для этого необходимо иметь заранее подготовленную таблицу всех простых чисел от 2 до $\lceil \sqrt{m} \rceil$ включительно. Данная таблица может быть построена с помощью алгоритма 5.1, приведенного нами в предыдущей лекции. Однако при больших значениях числа m такая таблица занимала бы в ЭВМ слишком большой объем памяти.

На практике вырабатывается таблица простых в небольшом диапазоне, например до 2^{16} , и проверка проводится только для маленьких чисел. Поиск больших делителей выполняется другими алгоритмами.

7.2 Метод Ферма

Авторство метода, который мы излагаем далее, приписывается известному математику Пьеру Ферма (Pierre de Fermat). Он заметил, что составное число всегда может быть представлено в виде разности двух квадратов и предложил, основанный на этом наблюдении, простой способ поиска делителей.

Пусть $m = pq$, где p, q натуральные, не обязательно простые, делители числа m , и $p > q$. Тогда

$$m = x^2 - y^2, \quad \text{где} \quad x = \frac{p+q}{2}, \quad y = \frac{p-q}{2}. \quad (7.1)$$

Метод разложения на множители Ферма заключается в переборе всех возможных значений величины x и проверке: является ли число $m - x^2$ полным квадратом. Если это условие выполнено, то делители p, q удовлетворяют равенствам $p = x + y$, $q = x - y$.

Алгоритм 7.1 (Алгоритм факторизации Ферма)

Вход: Целое составное число $m > 0$.

Выход: Натуральный делитель $p > 1$ числа m .

1. Вычислить наименьшее целое число h такое, что $h^2 \geq \sqrt{m}$, то есть $h = \lceil \sqrt{m} \rceil$.
2. Если $h^2 = m$, то определить $p = h$ и завершить алгоритм.
3. Определить $x = h$, $v = x^2 - m$ и счетчик $k = 0$.
4. Пока $k > 0$ выполнять
 - 4.1. Если величина v является полным квадратом, то определить $y = \sqrt{v}$, $p = x + y$ и закончить алгоритм.
 - 4.2. Вычислить $k = k + 1$, $x = x + 1$ и $v = v + 2h + 1$.

□

Легко показать, что количество проверок числа v (количество повторений на четвертом шаге алгоритма) не превосходит величины $y = \frac{p-q}{2}$.

Поскольку выполнено неравенство $p > h > q$, мы можем оценить величину k следующим образом. Согласно шагу 4.2 приведенного алгоритма, в момент нахождения делителя выполнено равенство $x = h + k$, получаем

$$k = x - h = p - y - h < p - q - y = \frac{p - q}{2}.$$

Далее, мы рассмотрим несколько вопросов, которые влияют на быстродействие алгоритма Ферма при его практической реализации на ЭВМ.

7.2.1 Вычисление квадратного корня

На первом шаге, а также при проверке, является ли число v квадратом, необходимо вычислять квадратный корень из большого целого числа. Для реализации этой операции мы можем использовать арифметику большой точности для действительных чисел и вычислять действительный корень, например, с помощью алгоритма Ньютона. Эта достаточно медленная операция может быть заменена аналогичным алгоритмом, использующим вычисления только с целыми числами и вычисляющим такое целое число h , что $h^2 \leq m < (h + 1)^2$, то есть $h = \lfloor \sqrt{m} \rfloor$.

Алгоритм 7.2 (Вычисление целозначного квадратного корня)

Вход: Натуральное число $m > 0$.

Выход: Натуральное число h , удовлетворяющее неравенствам $h^2 \leq m < (h + 1)^2$.

1. Определить $x = m$.
2. Вычислить¹ $y = \left\lfloor \frac{x + \lfloor \frac{m}{x} \rfloor}{2} \right\rfloor$.
3. Если $y < x$, то положить $x = y$ и вернуться на шаг 2. В противном случае, положить $h = x$ и завершить алгоритм. □

Докажем, что приведенный алгоритм действительно находит целое число h такое, что $h = \lfloor \sqrt{m} \rfloor$. Для начала отметим, что для любого значения $x > 0$ выполнено неравенство

$$\frac{x + \frac{m}{x}}{2} > \sqrt{m}, \quad \text{при } m > 0. \quad (7.2)$$

Действительно, из неравенства $(x^2 - m)^2 > 0$ следует, что

$$x^4 - 2x^2m + m^2 > 0 \quad \text{или} \quad x^4 + 2x^2m + m^2 > 4x^2m,$$

тогда $(x^2 + m)^2 > 4x^2m$ или $x^2 + m > 2x\sqrt{m}$. Последнее неравенство равносильно (7.2).

¹При программировании на ЭВМ, операцию деления на двойку целесообразно реализовывать как операцию сдвига.

Таким образом мы получаем, что на каждом шаге алгоритма 7.2 для неизвестного x выполнено неравенство $x \geq h$. В силу условия на третьем шаге алгоритма мы получаем, что последовательность значений x убывает. Покажем, что алгоритм остановится только при выполнении условия $x = h$.

Предположим, что это не так. Тогда выполнены неравенства $y \geq x$, $x > h$ и

$$y - x = \left\lfloor \frac{x + \lfloor \frac{m}{x} \rfloor}{2} \right\rfloor - x = \left\lfloor \frac{\lfloor \frac{m}{x} \rfloor - x}{2} \right\rfloor = \left\lfloor \frac{m - x^2}{2x} \right\rfloor.$$

Поскольку $x > h$ и x целое число, то $x^2 > h^2 \geq m$, следовательно, $m - x^2 < 0$ и $y - x < 0$. Таким образом, мы получили противоречие нашему предположению $y \geq x$.

7.2.2 Как быстро проверить, что число является полным квадратом

Сделаем еще одно замечание, касающееся вопроса о проверке: является ли целое число v , вырабатываемое в алгоритме Ферма, полным квадратом. Для предварительного отсева, перед использованием алгоритма 7.2, можно воспользоваться следующим утверждением.

Теорема 7.1. *Целое число $v > 0$ является полным квадратом тогда и только тогда, когда число v является квадратичным вычетом по модулю любого нечетного простого числа p .*

Прежде, чем переходить к доказательству теоремы, нам потребуется следующая лемма.

Лемма 7.1. *Пусть q_1, \dots, q_r различные нечетные простые числа, $\varepsilon_1, \dots, \varepsilon_r$ набор знаков, принимающих значения ± 1 . Тогда существует бесконечно много простых чисел p таких, что выполнены равенства*

$$\left(\frac{p}{q_1} \right) = \varepsilon_1, \dots, \left(\frac{p}{q_r} \right) = \varepsilon_r,$$

где $\left(\frac{p}{q_i} \right)$ — символ Лежандра для всех $i = 1, \dots, r$.

Доказательство. Для любого индекса $i = 1, \dots, r$ найдется некоторое натуральное число b_i , $0 < b_i < q_i$, удовлетворяющее условию $\left(\frac{b_i}{q_i} \right) = \varepsilon_i$. Заметим, что в силу леммы 4.2, таких чисел будет ровно $\frac{q_i - 1}{2}$.

Рассмотрим систему сравнений

$$\{x \equiv b_i \pmod{q_i} \quad i = 1, \dots, r. \quad (7.3)$$

Поскольку числа q_1, \dots, q_r взаимно просты, то используя китайскую теорему об остатках, см. теорему 2.3, получим, что существует целое число x_0 , для которого система (7.3) эквивалентна сравнению

$$x \equiv x_0 \pmod{q_1 \cdots q_r}.$$

Воспользуемся утверждением теоремы Дирихле, см. теорему 5.11, из которого следует, что в арифметической последовательности

$$x_k = kq_1 \cdots q_r + x_0$$

найдется бесконечно много простых чисел p , удовлетворяющих сравнению $p \equiv x_0 \pmod{q_1 \cdots q_r}$.

Для каждого такого простого числа, используя свойства символа Лежандра, см. лемму 4.3, получаем равенства

$$\left(\frac{p}{q_i}\right) = \left(\frac{x_0}{q_i}\right) = \left(\frac{b_i}{q_i}\right) = \varepsilon_i, \quad i = 1, \dots, r,$$

из которых вытекает утверждение леммы. □

Доказательство теоремы 7.1. Если число является полным квадратом, то утверждение теоремы очевидно, в силу определения квадратичного вычета. Теперь предположим, что число v не является полным квадратом и покажем, что в этом случае существует бесконечное число простых чисел p , для которых v не является квадратичным вычетом.

Прежде всего заметим, что если $v = ab^2$, то любого нечетного простого p выполнено равенство $\left(\frac{v}{p}\right) = \left(\frac{a}{p}\right)$ и нам достаточно рассматривать числа v , которые раскладываются в произведение простых чисел в первой степени, то есть $v = 2q_1 \cdots q_r$, где q_1, \dots, q_r различные нечетные простые.

Зафиксируем некоторый набор знаков $\varepsilon_1, \dots, \varepsilon_r$, принимающих значения ± 1 , такой, что число значений -1 в нем нечетное количество. Согласно доказанной нами лемме, найдется бесконечное множество простых чисел p таких, что $p \equiv x_0 \pmod{q_1 \cdots q_r}$ и

$$\left(\frac{p}{q_i}\right) = \left(\frac{x_0}{q_i}\right) = \left(\frac{b_i}{q_i}\right) = \varepsilon_i, \quad i = 1, \dots, r.$$

Выберем из этого множества простые числа, удовлетворяющие условию $p \equiv 1 \pmod{8}$. Согласно теореме Дирихле, их также бесконечно много, поскольку они принадлежат арифметической прогрессии $x_0 + k8q_1 \cdots q_r$. Тогда числа $\frac{p-1}{2}$ и $\frac{p^2-1}{8}$ четные и выполнено равенство

$$\left(\frac{v}{p}\right) = \left(\frac{2}{p}\right) \prod_{i=1}^r \left(\frac{q_i}{p}\right) = (-1)^{\frac{p^2-1}{8}} \prod_{i=1}^r \left(\frac{p}{q_i}\right) (-1)^{\frac{p-1}{2} \frac{q_i-1}{2}} = \prod_{i=1}^r \varepsilon_i = -1,$$

то есть число v является квадратичным невычетом. Теорема доказана. \square

Из утверждения теоремы следует, что мы можем реализовать следующую процедуру проверки чисел v . В начале мы проверяем выполнимость утверждения теоремы для некоторого заранее выбранного множества простых, а после, в случае если v окажется квадратичным вычетом по модулю этих простых, с помощью алгоритма 7.2 вычисляем целочисленный квадратный корень.

Заметим, что для проверки утверждения теоремы 7.1 необязательно вычислять символ Лежандра. Можно заранее для каждого простого числа p определить множество чисел на интервале $1, \dots, p-1$, являющихся квадратичными вычетами по модулю p и проверять, принадлежит ли $v \pmod{p}$ этому множеству.

Можно оценить эффективность данной процедуры по отбраковке чисел, не являющихся полными квадратами. Докажем следующую теорему.

Теорема 7.2. Пусть v натуральное число, которое не является полным квадратом. Тогда не менее чем для половины нечетных простых чисел p будет выполнено условие $\left(\frac{v}{p}\right) = -1$.

Доказательство. Пусть, как и в предыдущей теореме, число v раскладывается в произведение $v = 2q_1 \cdots q_r$, где q_1, \dots, q_r различные нечетные простые. Пусть $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_r$ знаки ± 1 , которые соответствуют символам Лежандра, то есть

$$\left(\frac{2}{p}\right) = \varepsilon_0, \quad \left(\frac{q_1}{p}\right) = \varepsilon_1, \quad \dots, \quad \left(\frac{q_r}{p}\right) = \varepsilon_r$$

для некоторого простого числа p и $\left(\frac{v}{p}\right) = \prod_{i=0}^r \varepsilon_i$.

Простые числа p , для которых выполнено условие $\left(\frac{v}{p}\right) = -1$, принадлежат бесконечной арифметической прогрессии $\{x_0 + k8q_1 \cdots q_r\}$, где

$k = 0, 1, \dots$, для некоторого целого x_0 , взаимно простого с $8q_1 \cdots q_r$. Количество таких прогрессий ограничено и равно

$$\varphi(8q_1 \cdots q_r) = 4 \prod_{i=1}^r (q_i - 1),$$

где $\varphi(\cdot)$ — функция Эйлера.

Покажем, что число прогрессий, при которых значение символа Лежандра $\left(\frac{v}{p}\right) = -1$ совпадает с числом прогрессий, при которых $\left(\frac{v}{p}\right) = 1$.

Значение величины x_0 , как следует из доказательства предыдущей теоремы, определяется как решение системы сравнений

$$\begin{cases} x \equiv b_0 \pmod{8}, \\ x \equiv b_i \pmod{q_i}, \quad i = 1, \dots, r, \end{cases} \quad (7.4)$$

где величины b_i определяют знак символов Лежандра $\left(\frac{2}{p}\right)$ и $\left(\frac{q_i}{p}\right)$, для $i = 1, \dots, r$. При этом ровно половина чисел из интервала $0 < b_i < q_i$ соответствует знаку $\varepsilon_i = 1$, а другая половина — знаку $\varepsilon_i = -1$. Отметим, что $b_i \neq 0$, поскольку в этом случае решение системы (7.4) кратно q_i и не может являться простым числом.

Для случая двойки, аналогично, два значения 1, 7 соответствуют знаку $\varepsilon_0 = 1$ и два значения 3, 5 — знаку $\varepsilon_0 = -1$. Таким образом, для любого набора знаков $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_r$ ровно половина значений x_0 таких, что $0 < x_0 < 8q_1 \cdots q_r$, $\text{НОД}(x_0, 8q_1 \cdots q_r) = 1$, позволит нам определить последовательность простых чисел, для которой символ Лежандра $\left(\frac{v}{p}\right) = -1$. Соответственно, другая половина таких чисел даст нам последовательность, для которой символ Лежандра $\left(\frac{v}{p}\right) = 1$. Теорема доказана². □

Из доказанной теоремы следует, что в случае, если число v не является полным квадратом, то вероятность его отбраковки составляет $\frac{1}{2}$. Более того, если мы получим, что символ Лежандра $\left(\frac{v}{p}\right) = 1$ для k различных простых чисел, то вероятность того, что число v является полным квадратом близка к единице и равна $1 - \frac{1}{2^k}$.

²Собственно говоря, мы доказали более слабый результат о совпадении числа последовательностей, которые содержат простые числа, по модулю которых v является квадратичным вычетом или невычетом. С другой стороны, поскольку простые числа распределены в арифметических последовательностях равномерно, см. [29, §7, гл.4], из этого следует утверждение теоремы.

7.3 Метод Лемана

В настоящее время алгоритм Шермана Лемана (R. Sherman Lehman) носит число исторический интерес и, как правило, не используется на практике. Вместе с тем, он был первым детерминированным алгоритмом факторизации целых чисел, имеющим оценку сложности меньшую, чем корневая от величины раскладываемого на множители числа. Впервые метод был описан в 1974 году в работе [11].

Метод Лемана развивает идеи, заложенные в алгоритме Ферма и ищет делители числа m , используя равенство

$$x^2 - y^2 = 4bm, \quad (7.5)$$

для некоторого целого числа b . Он основан на следующей теореме.

Теорема 7.3. Пусть $m = pq$ составное число, являющееся произведением двух нечетных взаимно простых чисел, удовлетворяющих неравенствам $\sqrt[3]{m} < p < q < \sqrt[3]{m^2}$. Тогда, найдутся натуральные числа x , y и $b \geq 1$ такие, что

1. выполнено равенство $x^2 - y^2 = 4bm$ при $b < \sqrt[3]{m}$,
2. выполнено неравенство $0 \leq x - \lfloor \sqrt{4bm} \rfloor < \frac{\sqrt[6]{m}}{4\sqrt{b}} + 1$.

В начале докажем следующую лемму.

Лемма 7.2. Пусть выполнены условия теоремы 7.3. Тогда найдутся натуральные числа r , s такие, что

$$rs < \sqrt[3]{m} \quad \text{и} \quad |pr - qs| < \sqrt[3]{m}.$$

Доказательство. Для доказательства леммы разложим рациональное число $\frac{q}{p}$ в непрерывную дробь. Символами $\frac{P_n}{Q_n}$ мы будем обозначать подходящие дроби к $\frac{q}{p}$. В силу леммы 6.1 число подходящих дробей конечно и $\frac{P_t}{Q_t} = \frac{q}{p}$ для некоторого индекса t .

Согласно определению подходящей дроби и ограничениям на числа p , q получаем, что

$$P_0 = \left\lfloor \frac{q}{p} \right\rfloor < \frac{q}{p} < \frac{\sqrt[3]{m^2}}{\sqrt[3]{m}} = \sqrt[3]{m}, \quad Q_0 = 1,$$

то есть выполнено неравенство $P_0Q_0 < \sqrt[3]{m}$. С другой стороны, $P_tQ_t = pq > p > \sqrt[3]{m}$. Следовательно, найдется максимальный индекс n такой, что

$$P_nQ_n < \sqrt[3]{m}, \quad P_{n+1}Q_{n+1} > \sqrt[3]{m}, \quad 0 \leq n < t. \quad (7.6)$$

Определим в качестве исходных значений $r = P_n$, $s = Q_n$ и покажем, что они удовлетворяют утверждению леммы.

Первое неравенство очевидным образом выполняется в силу выбора значений r, s . Для доказательства второго неравенства рассмотрим два случая. В начале предположим, что выполнено неравенство $\frac{q}{p} \geq \frac{P_{n+1}}{Q_{n+1}}$, которое может быть переписано в виде

$$\frac{p}{Q_{n+1}} \leq \frac{q}{P_{n+1}}. \quad (7.7)$$

Воспользовавшись равенством (6.12) получим, что

$$\left| \frac{q}{p} - \frac{P_n}{Q_n} \right| \leq \frac{1}{Q_n Q_{n+1}}, \quad (7.8)$$

тогда, учитывая (7.6), (7.7) и (7.8), получим

$$\begin{aligned} |pr - qs| &= |pP_n - qQ_n| = pQ_n \left| \frac{q}{p} - \frac{P_n}{Q_n} \right| \leq \frac{p}{Q_{n+1}} = \\ &= \sqrt{\frac{p}{Q_{n+1}}} \sqrt{\frac{p}{Q_{n+1}}} \leq \sqrt{\frac{p}{Q_{n+1}}} \sqrt{\frac{q}{P_{n+1}}} = \sqrt{\frac{m}{P_{n+1}Q_{n+1}}} < \\ &< \frac{\sqrt{m}}{\sqrt[6]{m}} = \sqrt[3]{m}. \end{aligned}$$

Рассмотрим второй случай, при котором выполнены неравенства

$$\frac{P_{n+1}}{Q_{n+1}} > \frac{q}{p} > \frac{P_n}{Q_n}. \quad (7.9)$$

Тогда, переворачивая данное неравенство и учитывая утверждение леммы 6.3, получаем

$$\frac{Q_n}{P_n} - \frac{p}{q} < \frac{Q_n}{P_n} - \frac{Q_{n+1}}{P_{n+1}} = \frac{(-1)^{n+1}}{P_n P_{n+1}} \quad (7.10)$$

Кроме того, из (7.9) следует неравенство $pP_{n+1} > qQ_{n+1}$ или

$$\frac{p}{Q_{n+1}} > \frac{q}{P_{n+1}}. \quad (7.11)$$

Теперь, учитывая (7.6), (7.10) и (7.11), получим

$$\begin{aligned} |pr - qs| &= |pP_n - qQ_n| = qP_n \left| \frac{p}{q} - \frac{Q_n}{P_n} \right| < \frac{q}{P_{n+1}} = \\ &= \sqrt{\frac{q}{P_{n+1}}} \sqrt{\frac{q}{P_{n+1}}} < \sqrt{\frac{q}{P_{n+1}}} \sqrt{\frac{p}{Q_{n+1}}} = \sqrt{\frac{m}{P_{n+1}Q_{n+1}}} < \\ &< \frac{\sqrt{m}}{\sqrt[6]{m}} = \sqrt[3]{m}. \end{aligned}$$

Лемма доказана. □

Доказательство теоремы 7.3. Пусть p, q нечетные делители числа m . Определим числа $x = pr + qs$ и $y = pr - qs$, где r, s удовлетворяют утверждению леммы 7.2, тогда выполнено равенство

$$x^2 - y^2 = (pr + qs)^2 - (pr - qs)^2 = 4rspq = 4bm,$$

где $b = rs$. В силу леммы 7.2, целое число b удовлетворяет неравенству $b < \sqrt[3]{m}$, а кроме того, $y < \sqrt[3]{m}$. Первое утверждение теоремы выполнено.

Для доказательства второго утверждения определим целое число k равенством

$$k = x - \lfloor \sqrt{4bm} \rfloor = pr + qs - \lfloor \sqrt{4bm} \rfloor$$

и покажем, что оно удовлетворяет заданному ограничению.

В начале заметим, что поскольку $x^2 = 4bm + y^2$, то $x \geq \sqrt{4bm}$ и величина $k \geq 0$. Далее, используя оценку сверху на величину y , получаем

$$\begin{aligned} (\sqrt[3]{m})^2 > y^2 &= x^2 - 4bm = \\ &= (pr + qs + \sqrt{4bm})(pr + qs - \sqrt{4bm}) \geq \\ &\geq 2\sqrt{4bm}(pr + qs - \sqrt{4bm}) \geq 2\sqrt{4bm}(k - 1). \end{aligned}$$

Тогда выполнено

$$k < \frac{(\sqrt[3]{m})^2}{2\sqrt{4bm}} + 1 = \frac{\sqrt[6]{m}}{4\sqrt{b}} + 1.$$

Теорема доказана. \square

Используя утверждения доказанной нами теоремы, Леман предложил следующий алгоритм поиска делителей числа m .

Алгоритм 7.3 (Алгоритм Лемана)

Вход: Натуральное нечетное число m .

Выход: Простое число p такое, что $p|m$, либо заключение о том, что число m простое.

1. Для всех p от 2 до $\lfloor \sqrt[3]{m} \rfloor$ выполнить

1.1. Если $m \equiv 0 \pmod{p}$, то вернуть p в качестве делителя числа m и завершить алгоритм.

2. Для всех b от 1 до $\lfloor \sqrt[3]{m} \rfloor$ выполнить

2.1. Определить $k = 0$ и $D = \lfloor \frac{\sqrt[6]{m}}{4\sqrt{b}} \rfloor + 1$.

2.2. Определить $x = \lfloor \sqrt{4bm} \rfloor + k$ и $v = x^2 - 4bm$.

2.3. Если v является полным квадратом³, то определить

$$p = \text{НОД}(m, x \pm \sqrt{v})$$

и завершить алгоритм.

³Очевидно, что проверку можно производить используя методы, описанные нами ранее в разделах 7.2.1 и 7.2.2.

- 2.4. Определить $k = k + 1$.
- 2.5. Если $k \geq D$, то вычислить новое значение d . В противном случае, вернуться на шаг 2.2.
3. Завершить алгоритм с уведомлением, что число m простое. \square

Описанный нами алгоритм в начале проверяет, имеет ли число m простые делители, не превосходящие величины $\lceil \sqrt[3]{m} \rceil$, а потом устраивает перебор значений b и k для проверки выполнимости утверждений теоремы 7.3. В случае, если искомые значения x , y не найдены, то мы получаем, что число m простое. Таким образом, приведенный алгоритм может рассматриваться как тест числа m на простоту. Алгоритм, очевидно, является детерминированным, поскольку однозначно дает ответ на вопрос, является ли число m составным или простым.

Оценим трудоемкость алгоритма 7.3. На первом шаге нам потребуется произвести $\lceil \sqrt[3]{m} \rceil$ операций деления для поиска маленьких делителей числа m .

Трудоемкость второго шага оценивается в операциях тестирования числа v , определяемого на шаге 2.2, на то, является ли оно полным квадратом. В начале заметим, что для всех $b > \frac{\sqrt[6]{m}}{4}$ выполняется только две проверки: для $k = 0$ и $k = 1$. Тогда, трудоемкость второго этапа оценивается сверху величиной

$$\frac{\sqrt[6]{m}}{4} \sum_{b=1}^{\lfloor \sqrt[6]{m} \rfloor} \frac{1}{\sqrt{b}} + 2(\lceil \sqrt[3]{m} \rceil - \lfloor \sqrt[6]{m} \rfloor) < 3\lceil \sqrt[3]{m} \rceil.$$

Таким образом, трудоемкость всего алгоритма есть величина $O(\sqrt[3]{m})$.

7.4 Метод Полларда-Флойда

Описанные нами ранее алгоритмы факторизации носили детерминированный характер и позволяли после фиксированного числа шагов либо найти нетривиальные делители числа m , либо доказать, что число m простое.

Теперь мы перейдем к рассмотрению вероятностных алгоритмов, обладающих следующими свойствами. Во-первых, для алгоритма можно определить лишь среднее число шагов алгоритма, точное число шагов является случайной величиной и зависит от используемых в алгоритме генераторов псевдослучайных чисел. Во-вторых, если алгоритм не сможет определить делители числа m , то нельзя будет ни чего сказать о том, является ли число m простым.

Мы начнем изложения с метода, предложенного Дж. Поллардом в 1974 году в работе [18]. Метод основывается на свойствах случайных отображений конечного множества в себя, которые подробно рассматриваются нами в приложении А.

Пусть, как и ранее, m нечетное, составное число, которое мы хотим разложить на множители. Фиксируем некоторый многочлен $f(x) \in \mathbb{Z}[x]$ с целыми коэффициентами, степени большей единицы. В своей работе Поллард предложил выбрать многочлен вида $f(x) = x^2 + 1$. Данный многочлен задает отображение кольца вычетов по модулю m в себя

$$f(x) \pmod{m} : \mathbb{Z}_m \rightarrow \mathbb{Z}_m.$$

Выберем произвольный элемент x_0 кольца \mathbb{Z}_m и рассмотрим его орбиту, порожденную многочленом $f(x)$, то есть последовательность элементов кольца, определенных соотношением

$$x_{n+1} = f(x_n) \pmod{m}, \quad n = 0, 1, \dots$$

Поскольку число элементов кольца \mathbb{Z}_m конечно, то найдутся такие целые индексы τ и λ , что для всех индексов $n \geq \lambda$ будет выполнено сравнение

$$x_n \equiv x_{n+\tau} \pmod{m}. \quad (7.12)$$

Величина τ называется периодом (длиной цикла) последовательности $\{x_n\}_0^\infty$, а величина λ — длиной подхода к периоду.

Пусть p произвольный простой делитель числа m , тогда из сравнения (7.12) следует, что $x_n \equiv x_{n+\tau} \pmod{p}$ и многочлен $f(x)$ порождает последовательность вычетов кольца \mathbb{Z}_p , которая зациклится, то есть найдутся такие индексы $j > i$, что

$$x_j \equiv x_i \pmod{p}. \quad (7.13)$$

Последнее сравнение позволяет нам найти нетривиальный делитель числа m . Действительно, из (7.13) получаем, что $\text{НОД}(m, x_j - x_i) = p$, если $x_j \not\equiv x_i$. Таким образом, метод Полларда сводится к поиску таких индексов i, j , для которых выполнено сравнение (7.13).

Для поиска необходимых индексов i, j Поллард предложил использовать метод Флойда поиска циклов в последовательностях, см. раздел А.2.1, а именно, вычислять две последовательности $\{x_n\}_0^\infty$ и $\{x_{2n}\}_0^\infty$ и находить простой делитель p проверкой условия

$$\text{НОД}(m, z) > 1, \quad \text{где } z \equiv (x_{2n} - x_n) \pmod{m}.$$

Искомый делитель будет найден в том случае, когда период последовательности $\{x_n \pmod{p}\}_0^\infty$ будет делить значение индекса n .

Исходя из геометрических соображений, данный метод часто называют ρ -методом Полларда или методом Полларда-Флойда. Мы суммируем приведенные выше рассуждения в виде алгоритма.

Алгоритм 7.4 (ρ -метод Полларда (метод Полларда-Флойда))

Вход: Целое составное число m .

Выход: Целое, быть может составное число p такое, что $p|m$.

1. Зафиксировать некоторый многочлен второй степени $f(x) \in \mathbb{Z}[x]$, например, $f(x) = x^2 + 1$.
2. Выбрать случайный вычет $x \in \mathbb{Z}_m$ и определить $z = x$, $p = 1$.
3. Вычислить $x \equiv f(x) \pmod{m}$, $y \equiv f(z) \pmod{m}$, $z \equiv f(y) \pmod{m}$.
4. Вычислить $p = \text{НОД}(m, z - x \pmod{m})$.
5. Если $p > 1$, то завершить работу, в противном случае вернуться на шаг 3. \square

Оценка числа шагов данного алгоритма следует из оценки длины периода последовательности $\{x_n \pmod{p}\}_0^\infty$, см. теорему A.1, и, в среднем, составит величину порядка $O(\sqrt{p}) \sim O(\sqrt[4]{m})$.

7.5 Метод Брента

Метод Полларда-Флойда выполняет вычисления до тех пор, пока не будет найден нетривиальный делитель числа m , при этом оценка среднего числа шагов алгоритма зависит от размера делителя p . В 1980 году в работе [2] Ричард Брент (Richard P. Brent) предложил использовать этот факт для реализации теста, который позволяет определить, если ли у составного числа m небольшие простые делители.

Метод Брента является достаточно простой модификацией метода Полларда-Флойда и вычисляет лишь конечное число элементов последовательности

$$x_{n+1} = f(x_n) \pmod{m}, \quad n = 0, 1, \dots$$

для некоторого полинома $f(x) \in \mathbb{Z}[x]$

$$f(x) \pmod{m} : \mathbb{Z}_m \rightarrow \mathbb{Z}_m.$$

Для поиска совпадающих элементов последовательности $\{x_n\}_{n=0}$ используется алгоритм, детальное обоснование которого приводится нами в разделе A.2.2.

Основываясь на утверждении теоремы A.2, Brent предложил искать совпадение элементов последовательности $\{x_n \pmod{p}\}_0$ путем проверки условия

$$x_n \equiv x_{2^k-1} \pmod{p},$$

для всех индексов n таких, что $2^k \leq n < 2^{k+1}$, $k = 0, 1, \dots$. Как и ранее, проверка выполняется путем вычисления

$$\text{НОД}(m, z), \quad \text{где } z \equiv x_n - x_{2^k-1} \pmod{m}.$$

Алгоритм 7.5 (Алгоритм Брента)

Вход: Целое составное число m и натуральное число $c \geq 1$.

Выход: Либо целое, быть может составное, число p такое, что $p|m$, либо заключение о том, что делитель не найден.

1. Зафиксировать многочлен $f(x) \in \mathbb{Z}[x]$, например, $f(x) = x^2 + 1$.
2. Выбрать случайный вычет $x \in \mathbb{Z}_m$ и определить $z = 0$, $n = 0$ и $k = 0$, $t = 1$.
3. Вычислить $x \equiv f(x) \pmod{m}$, $n = n + 1$.
4. Если $n = t$, то определить $z = x$ и $k = k + 1$, $t = 2t$.
5. Если $k > c$, то завершить алгоритм с уведомлением о неудаче.
Иначе вернуться на шаг 3.
6. Вычислить $p = \text{НОД}(m, z - x)$.
7. Если $m > p > 1$, то делитель найден и алгоритм завершает работу. В противном случае, вернуться на шаг 3. □

Параметр c определяет трудоемкость алгоритма — количество его шагов не превышает величины $B = 2^c$. Тогда, учитывая утверждение теоремы A.1, можно ожидать, что алгоритм Брента сможет найти делитель p , не превосходящий величины $O(B^2)$.

В оставшейся части лекции, мы рассмотрим алгоритмы, которые позволяют эффективно раскладывать на множители числа m частного вида. В этих алгоритмах используются некоторые свойства числа m , которые существенно снижают трудоемкость разложения на множители.

7.6 $p - 1$ метод Полларда

Один из первых подходов к разложению на множители чисел частного вида был предложен Джоном Поллардом (John M. Pollard) в 1974 году работе [18]. Пусть m натуральное, нечетное, составное число, которое мы хотим разложить на множители и p некоторый простой делитель числа m , то есть $p|m$.

Пусть a натуральное число, тогда, согласно третьему утверждению леммы 2.3, $\text{ord}_p a$ — показатель a по модулю p делит число $p - 1$, то есть

$\text{ord}_p a | (p-1)$. Согласно малой теореме Ферма, см. теорему 2.7, выполнено сравнение $a^{p-1} \equiv 1 \pmod{p}$. Таким образом, для любого натурального k такого, что $\text{ord}_p a | (p-1) | k$ выполнено

$$a^k \equiv (a^{\text{ord}_p a})^t \equiv 1 \pmod{p}, \quad \text{при } k = t \text{ord}_p a,$$

что равносильно $a^k - 1 \equiv 0 \pmod{p}$. Последнее условие позволяет заключить, что

$$p | \text{НОД}(m, a^k - 1 \pmod{m}). \quad (7.14)$$

Для выбора числа k Поллардом была предложена следующая идея. Из основной теоремы арифметики, см. теорему 1.4, следует, что для числа $p - 1$ существует разложение на простые множители

$$p - 1 = \prod_{i=1}^s p_i^{\alpha_i}, \quad s \in \mathbb{N},$$

где $p_1 = 2$, а остальные p_i нечетны и не превосходят некоторой величины b_p . Легко видеть, что $b_p \leq \frac{p-1}{2}$.

Выберем в качестве k произведение всех маленьких простых чисел

$$k = \prod_i p_i^{\alpha_i}, \quad \text{где } p_i \leq B = \max_{p|m} \{b_p\}, \quad (7.15)$$

а величины α_i принимают достаточно большие значения. В этом случае выполнено $p - 1 | k$ и делитель p может быть найден из условия (7.14).

При разложении числа m на множители, нам не известно точное значение величины B . Исходя из тривиальной оценки сверху на величину b_p можно считать, что $B \sim \sqrt[4]{m}$. Однако в этом случае величина B принимает очень большое значение и вычисление значения $a^k - 1 \pmod{m}$ становится более трудоемким, чем поиск делителей числа m пробным делением.

На практике величина B выбирается почти произвольным образом, в зависимости от быстродействия вычислительного средства, реализующего алгоритм, например, $B = 10^6$.

Собственно алгоритм факторизации реализуется в виде теста — если для некоторого делителя p числа m , при k удовлетворяющем (7.15), выполнено условие (7.14), то делитель будет найден. В противном случае, алгоритм завершит свою работу с уведомлением о неудаче.

Алгоритм 7.6 ($p - 1$ алгоритм факторизации Полларда)

Вход: Целое составное число m , границы B и $s \in \mathbb{N}$.

Выход: Целое, быть может составное, число p такое, что $p|m$.

1. Используя алгоритм 5.1, построить все простые числа, не превосходящие величины B и определить величину $k = \prod_i p_i^{\alpha_i}$, где $p_i \leq B$, при некоторых натуральных значениях⁴ величин α_i . Определить $i = 0$.
2. Вычислить $i = i + 1$, положить $a = p_i$ (при $i = 1$ значение параметра a должно равняться 2).
3. Если $\text{НОД}(a, m) > 1$, то завершить алгоритм с результатом $p = a$.
4. Вычислить $p = \text{НОД}(m, a^k - 1 \pmod{m})$.
5. Если $m > p > 1$, то завершить алгоритм.
6. Если $i < c$, то вернуться на шаг 2. В противном случае, завершить алгоритм с уведомлением о неудаче. \square

Введенная нами в алгоритме граница c задает количество перебираемых чисел a , для которых проверяется выполнение условия (7.14). При практической реализации алгоритма эта величина может принимать небольшие значения, например 10.

Как можно заметить, $p - 1$ метод Полларда представляет собой аналог алгоритма пробного деления, изложенного нами в начале лекции. Только в методе Полларда мы ищем перебором не делители числа m , а делители числа $p - 1$, собранные в виде произведения в число k . Немного позже мы опишем процедуры оптимизации алгоритма 7.6, в которых перебор делителей числа $p - 1$ будет предъявлен в явном виде.

7.7 $p + 1$ метод Вильямса

Данный метод был предложен Хью Вильямсом (Hugh Williams) в 1982 году работе [22] и опирается на идеи, аналогичные $p - 1$ методу Полларда. Пусть m нечетное составное число, которое мы хотим разложить на множители. Мы будем применять метод Вильямса в том случае, когда хотя бы один простой делитель p числа m имеет вид

$$p \pm 1 = \prod_i p_i^{\alpha_i}, \quad (7.16)$$

где p_i маленькие простые числа. Другими словами, как и в методе Полларда, найдется небольшое натуральное число B , например $B = 10^6$. При этом все p_i , определяемые равенством (7.16), удовлетворяют условию $p_i < B$.

Ранее, в 5-й лекции, мы ввели последовательности Люка. Напомним, что для двух целых взаимно простых чисел a, b рекуррентной

⁴На практике для нескольких маленьких простых, например 2, ..., 31, величины α_i принимают значения не превосходящие 10, для всех остальных простых — значения α_i равны единице.

последовательностью Люка называется последовательность пар целых чисел U_n, V_n , определяемых равенствами (5.8)

$$U_{n+1} = aU_n - bU_{n-1}, \quad V_{n+1} = aV_n - bV_{n-1}, \quad n = 1, 2, \dots$$

где $U_0 = 0, U_1 = 1, V_0 = 2, V_1 = a$. Для эффективного вычисления значений пар U_n, V_n , можно использовать алгоритм 5.5, описанный нами ранее.

Пусть p нечетный, простой делитель числа m . Для заданной последовательности Люка, с параметрами a и $b, b \not\equiv 0 \pmod{p}$, определим $\Phi(p) = p - \left(\frac{D}{p}\right)$, где D удовлетворяет равенству $D = a^2 - 4b$ и условию $D \not\equiv 0 \pmod{p}$. Согласно утверждению леммы 5.5 выполнено условие $U_{\Phi(p)} \equiv 0 \pmod{p}$.

Пусть k произвольное натуральное число такое, что $\Phi(p) | k$. Тогда, из шестого утверждения леммы 5.3 следует, что $U_{\Phi(p)} | U_k$, откуда вытекает, что $U_k \equiv 0 \pmod{p}$.

Суммируя, мы получаем, что в случае выполнения условия $\Phi(p) | k$, искомый делитель числа m удовлетворяет условию

$$p | \text{НОД}(m, U_k). \tag{7.17}$$

Для поиска нетривиального делителя p числа m можно предложить следующий алгоритм, основывающийся на проверке условия (7.17). Он основан на выборе случайной пары числе a, b и вычислении элемента последовательности Люка U_k при k , удовлетворяющем равенству

$$k = \prod_i p_i^{\alpha_i}, \quad \text{где } p_i \leq B. \tag{7.18}$$

Алгоритм Вильямса является вероятностным и представляет собой тест. Если выполнено условие $\Phi(p) | k$ или, что равносильно: либо $p - 1 | k$, либо $p + 1 | k$, то алгоритм сможет найти делитель числа m . В противном случае, алгоритм завершится с уведомлением о неудаче.

Алгоритм 7.7 ($p + 1$ алгоритм факторизации Вильямса)

Вход: Целое составное число m , границы B и $c \in \mathbb{N}$.

Выход: Целое, быть может составное, число p такое, что $p | m$.

1. Используя алгоритм 5.1, построить все простые числа, не превосходящие величины B и определить величину $k = \prod_i p_i^{\alpha_i}$, где $p_i \leq B$, при некоторых натуральных значениях⁵ величин α_i . Определить $i = 0$.

⁵Выбор натуральных значений α_i может быть произведен, аналогично $p - 1$ методу Полларда, см. сноску на 148-й странице.

2. Вычислить $i = i + 1$, выбрать случайные, взаимно простые значения a , b и определить $D = a^2 - 4b$.
3. Если $p = \text{НОД}(m, b) > 1$, то завершить алгоритм.
4. Если $p = \text{НОД}(m, D) > 1$, то завершить алгоритм.
5. Используя алгоритм 5.5 вычислить элемент U_k последовательности Люка с параметрами a и b . При этом все вычисления величин можно проводить по модулю факторизуемого числа m .
6. Если $p = \text{НОД}(m, U_k) > 1$, то завершить алгоритм.
7. Если $i < c$, то вернуться на шаг 2. В противном случае, завершить алгоритм с уведомлением о неудаче. \square

Как и в $p - 1$ методе Полларда, нами введена граница c , которая задает количество перебираемых последовательностей Люка, для которых проверяется выполнение условия (7.17). При практической реализации алгоритма эта величина может принимать небольшие значения, например 10.

В заключение заметим, что метод Вильямса является расширением метода Полларда, поскольку он также применим для случая, когда для некоторого простого делителя p числа m значение $p - 1$ раскладывается в произведение маленьких простых чисел. Однако вычисление последовательности Люка является более трудоемким, чем модульное возведение малого числа в степень k . В связи с этим, иногда, при практическом тестировании больших составных чисел метод Вильямса не используют, ограничиваясь более простым $p - 1$ методом Полларда.

7.8 Второй этап: оптимизация алгоритмов Полларда и Вильямса

Предложенные нами ранее алгоритмы Полларда, алгоритм 7.6, и Вильямса, алгоритм 7.7, могут быть оптимизированы путем добавления второго этапа. Предположим, что некоторого простого делителя p разложение (7.16) имеет вид

$$p \pm 1 = q \cdot \prod_{i=1}^s p_i^{\alpha_i}, \quad \text{где } p_i < B \text{ и } B < q. \quad (7.19)$$

То есть в разложение чисел $p \pm 1$ входит один простой делитель, превосходящий заданную нами границу B . В этом случае, мы можем реализовать второй этап указанных алгоритмов 7.6 и 7.7, который выполняется после пятого и шестого шага, соответственно.

Для поиска простого делителя q предположим, что он ограничен сверху некоторой величиной B_1 , например, $B_1 = 10^8$. Перебирая все простые простые числа q_1, \dots, q_l на интервале $B \leq q_1 < q_2 < \dots < q_l \leq B_1$, мы можем проверить, для метода Полларда, выполнимость условия

$$\text{НОД}\left(m, (a^k)^{q_i} - 1 \pmod{m}\right) > 1,$$

где величина k определяется на первом этапе алгоритма. Если условие выполнено, то $p - 1 | kq_i$ и мы найдем нетривиальный делитель числа m . Аналогично, для метода Вильямса, нам надо проверять выполнимость условия

$$\text{НОД}(m, U_{kq_i}) > 1.$$

В случае его выполнения, мы получаем, что $\Phi(p) | kq_i$ и мы находим нетривиальный делитель числа m . Для вычисления U_{kq_i} можно использовать алгоритм 5.5 с начальными значениями U_k, V_k . Далее мы опишем несколько способов, позволяющих оптимизировать перебор простых чисел на интервале от B до B_1 .

7.8.1 Разностная схема

Для снижения трудоемкости описанной выше процедуры перебора, Поллард предложил использовать модификацию, использующую то, что разности между двумя соседними простыми числами принимают небольшие значения.

Пусть q_1, \dots, q_l все простые числа в интервале от B до B_1 . Определим разности между простыми числами

$$r_{i+1} = q_{i+1} - q_i \quad \text{для всех } i = 1, \dots, l - 1.$$

Обозначим $b \equiv a^k \pmod{m}$, тогда вычисление вычетов $(a^k)^{q_i} \equiv b^{q_i} \pmod{m}$ в алгоритме Полларда может быть реализовано последовательно, то есть

$$b^{q_{i+1}} \equiv b^{q_i+r_i} \equiv b^{q_i} b^{r_i} \pmod{m}.$$

Величины $b^{r_i} \pmod{m}$ могут быть вычислены перед выполнением второго этапа алгоритма и сохранены в памяти ЭВМ.

Эта же идея применима и для алгоритма Вильямса. Воспользовавшись соотношениями (5.11) мы можем записать равенства

$$U_{kq_{i+1}} = \frac{1}{2} (U_{kq_i} V_{kr_i} + U_{kr_i} V_{kq_i}), \quad V_{kq_{i+1}} = \frac{1}{2} (V_{kq_i} V_{kr_i} + DU_{kq_i} U_{kr_i}),$$

которые позволяют выразить пару $U_{kq_{i+1}}, V_{kq_{i+1}}$ через пары U_{kq_i}, V_{kq_i} и U_{kr_i}, V_{kr_i} . Величины U_{kr_i}, V_{kr_i} также могут быть вычислены и сохранены в памяти ЭВМ перед началом выполнения второго этапа. Мы не приводим в явном виде реализацию второго этапа для алгоритмов Полларда и Вильямса, оставляя ее в качестве упражнения читателю.

7.8.2 Метод согласования

Опишем другой подход к перебору всех простых чисел q_1, \dots, q_l в интервале от B до B_1 . Этот подход основан на методе согласования⁶.

Определим натуральное число $h = \lceil \sqrt{B_1} \rceil$, тогда любое простое число q из интервала $B \leq q \leq B_1$ может быть представлено в виде

$$q = uh + v, \quad \text{где } u, v \in \mathbb{N}, \quad \left\lfloor \frac{B}{h} \right\rfloor \leq u < h, \quad v < h. \quad (7.20)$$

Применим полученное равенство к алгоритму Полларда. Пусть выполнено условие $p - 1 \mid kq$, тогда $(a^k)^q \equiv 1 \pmod{p}$, что равносильно,

$$(a^k)^q (a^k)^{-v} \equiv (a^{kh})^u \pmod{p} \quad \text{или} \quad (a^k)^{-v} - (a^{kh})^u \equiv 0 \pmod{p}.$$

Последнее сравнение позволяет нам найти нетривиальный делитель числа m , путем вычисления

$$\text{НОД}(m, d^v - (b^h)^u \pmod{m}), \quad \text{где } b \equiv a^k, d \equiv b^{-1} \pmod{m},$$

при некоторых натуральных u, v .

Реализация второго этапа алгоритма может выглядеть следующим образом. В начале вычисляются значения $(b^h)^u \pmod{m}$ для всех u , удовлетворяющих неравенствам (7.20). Вычисленные значения сохраняются в памяти ЭВМ. После этого, для всех $v = 1, 2, \dots, h$ вычисляются значения вычетов $d^v \pmod{m}$ и проверяется условие

$$m > \text{НОД}(m, d^v - (b^h)^u \pmod{m}) > 1.$$

Если оно выполнено, то нетривиальный делитель числа m найден.

Соотношение (7.20) может быть использовано и при реализации метода Вильямса. Действительно, следуя (7.17), мы используем тот факт, что $p \mid \text{НОД}(m, U_{kq})$, для некоторого простого q , удовлетворяющего равенству (7.20).

⁶В англоязычных публикациях этот метод, применительно к $p - 1$ методу Полларда, принято называть «усложненным стандартным продолжением» — improved standard continuation.

Воспользовавшись равенствами (5.11) мы можем записать

$$2U_{kq} = (U_{khu}V_{kv} + U_{kv}V_{khu}).$$

Таким образом, мы можем предварительно вычислить значения U_{khu} , V_{khu} , для всех u удовлетворяющих неравенствам (7.20), и сохранить их в памяти ЭВМ. После этого, для всех $v = 1, 2, \dots, h$ вычисляются значения элементов последовательности Люка U_{kv} , V_{kv} и проверяется условие

$$m > \text{НОД}(m, U_{khu}V_{kv} + U_{kv}V_{khu}) > 1.$$

Если оно выполнено, то нетривиальный делитель числа m найден. Заметим, что поскольку m нечетно, то мы уменьшаем вычисления и заменяем величину U_{kq} величиной $2U_{kq}$.

Для снижения множества перебираемых значений можно использовать следующую идею. Выберем параметр h в равенстве (7.20) равным не $h = \lceil \sqrt{B_1} \rceil$, а ближайшим к $\lceil \sqrt{B_1} \rceil$ целым числом, кратным⁷ $2 \cdot 3 \cdot 5 \cdot 7 = 210$. При этом интервал для величины u принимает вид $\lfloor \frac{B}{h} \rfloor \leq u \leq \lceil \frac{B_1}{h} \rceil$. Поскольку число $q = uh + v$ должно быть простым, то параметр v не может принимать значения кратные 2, 3, 5 и 7.

Перебор таких значений v может быть организован аналогично методу решета, примененного нами в алгоритме 5.6. Положим $v = 1$ и $\delta_3 = \delta_5 = \delta_7 = 1$. Мы будем прибавлять к v двойку, поскольку значение v должно быть нечетно. При каждом увеличении v на двойку мы вычисляем $\delta_p = \delta_p + 2 \pmod{p}$, при $p = 3, 5, 7$. Если все δ_p отличны от нуля, то значение v может быть использовано. В противном случае, вычисляется следующее значение.

7.8.3 Поиск пар простых чисел

Следующая идея, развивающая метод согласования, была предложена Питером Монтогмери (Peter Montgomery) в статье [16]. Пусть, как и в методе согласования, нам задано целое число h — ближайшее к $\lceil \sqrt{B_1} \rceil$ и кратное 210.

Простое число q из интервала $B \leq q \leq B_1$, которое нам необходимо определить, может быть представлено в виде (7.20). Кроме того, мы можем определить парное ему число q_1 , удовлетворяющее равенствам

$$q = uh + v, \quad q_1 = uh - v, \quad \left\lfloor \frac{B}{h} \right\rfloor \leq u \leq \left\lceil \frac{B_1}{h} \right\rceil, \quad v < h. \quad (7.21)$$

⁷Очевидно, что при реализации алгоритма мы можем использовать и другие значения, например, 30, 2310 или $30030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$.

Пусть выполнено условие $p - 1 | kq$ и $(a^k)^q \equiv 1 \pmod{p}$. Обозначим, как и ранее $b \equiv a^k \pmod{m}$, тогда

$$\begin{aligned} b^{(uh)^2} - b^{v^2} &\equiv b^{v^2} \left(b^{(uh)^2 - v^2} - 1 \right) \equiv b^{v^2} \left(b^{(uh-v)(uh+v)} - 1 \right) \equiv \\ &\equiv b^{v^2} \left((b^q)^{q_1} - 1 \right) \equiv 0 \pmod{p} \end{aligned} \quad (7.22)$$

Таким образом, сравнение (7.22) позволяет нам найти нетривиальный делитель числа m путем проверки условия

$$m > \text{НОД} \left(m, b^{(uh)^2} - b^{v^2} \pmod{m} \right) > 1. \quad (7.23)$$

Второй этап реализуется следующим образом. В начале, по заданной таблице простых чисел, строится множество пар u, v , удовлетворяющих условиям (7.21). При этом, для некоторых простых чисел парные к ним не будут простыми, тем не менее, такие пары мы также будем использовать. Поскольку процесс построения не зависит от числа m , раскладываемого на множители, то он может быть выполнен предварительно.

Далее, перебирая все пары из построенного множества, мы проверяем выполнимость условия (7.23): в начале мы фиксируем значение u и перебираем все допустимые значения v . После чего, переходим к следующему значению u .

Для уменьшения трудоемкости вычисления величин $b^{(hu)^2} \pmod{m}$ для всех u , последовательно пробегающих интервал $\left[\frac{B}{h} \right] \leq u \leq \left[\frac{B_1}{h} \right]$, можно воспользоваться следующим сравнением

$$b^{(h(u+1))^2} \equiv b^{(hu)^2} \cdot (b^{hu})^2 \cdot b^h \pmod{m},$$

основываясь на котором, мы можем вычислить следующее значение с использованием предыдущего, одного возведения в квадрат и одного модульного умножения.

Отметим, что в силу сложности соотношения (7.22), подход, основанный на переборе пар простых чисел, практически не применим при реализации метода Вильямса.

7.8.4 Поиск циклов в последовательностях

Последний подход, так же как и изложенный ранее метод факторизации Полларда-Флойда, основан на свойствах случайных отображений конечного множества в себя. Пусть, как и ранее, на первом этапе алгоритма Полларда мы вычислили элемент $b \equiv a^k \pmod{m}$ и хотим найти простое число q такое, что $B \leq q \leq B_1$ и $b^k \equiv 1 \pmod{p}$.

Рассмотрим псевдо-случайную последовательность элементов

$$b_{i+1} \equiv b_i^{s_i} \pmod{m}, \quad s_i \equiv b_i \pmod{M}, \quad i = 0, 1, \dots,$$

где $b_0 = b$, а M некоторая маленькая константа, например 16.

Если мы рассмотрим каждый элемент этой последовательности по модулю некоторого простого числа p , являющегося делителем числа m , то данная последовательность заиклится. В приложении А мы подробно рассматриваем свойства таких последовательностей. Для поиска цикла мы можем использовать метод Флойда, то есть искать пару значений

$$b_i \equiv b_{2i} \pmod{p} \quad (7.24)$$

для некоторого индекса i . Последнее сравнение равносильно тому, что

$$p \mid \text{НОД}(m, b_i - b_{2i} \pmod{m}). \quad (7.25)$$

Поскольку нам неизвестно точное значение простого числа q , то мы не можем определить мощность множества $\{b, b^2, \dots, b^q \equiv 1 \pmod{p}\}$. Поэтому мы будем проверять выполнение условия (7.25) для всех индексов i от 1 до $\lceil \sqrt{B_1} \rceil$. Такая оценка сверху, очевидным образом, следует из свойств псевдослучайных последовательностей, рассмотренных нами в приложении А.

Данный подход может быть достаточно просто перенесен на алгоритм Вильямса. Определим множество $U_{kB}, U_{k(B+1)}, \dots, U_{kB_1}$ элементов последовательности Люка, которому принадлежит элемент U_{kq} для некоторого простого числа q такого, что $B \leq q \leq B_1$ и $p \mid \text{НОД}(m, U_{kq})$.

Мы будем искать совпадение двух элементов на введенном множестве, при этом, величина $B_1 - B$ задает мощность нашего множества.

Элементами нашей последовательности будут пары (U, V) элементов последовательности Люка. Начальный элемент последовательности имеет вид (U_k, V_k) . Тогда остальные элементы последовательности определяются по следующему правилу

$$s = B + (U_i \pmod{(B_1 - B)}), \quad U_{i+1} = U_{ks}, \quad V_{i+1} = V_{ks}.$$

Мы выбираем значение степени s таким образом, чтобы оно удовлетворяло неравенству $B \leq s < B_1$. В этом случае, условие (7.25) принимает вид

$$p \mid \text{НОД}(m, U_i - U_{2i} \pmod{m}), \quad (7.26)$$

для некоторого индекса i , которое может быть проверено для всех индексов, не превосходящих $\lceil \sqrt{B_1} \rceil$.

7.9 Метод Женга

В 2001 году в статье [24] Женг (Zhenxiang Zhang) опубликовал алгоритм, который позволяет, при некоторых дополнительных условиях, эффективно раскладывать на множители составные числа, используемые в схеме RSA. Для описания алгоритма и его модификаций нам потребуется следующая лемма.

Лемма 7.3. *Рассмотрим составное число m , являющееся произведением двух нечетных простых чисел p и q , для которых выполнено неравенство $p < q$, а также найдутся целые числа r, s , удовлетворяющие равенству $q = s(p - 1) - r$ при $0 < r \leq \frac{p-3}{2}$.*

Рассмотрим множество M , содержащее в себе все взаимно простые с m вычеты a такие, что $a^{m+r} \equiv 1 \pmod{m}$. Тогда выполнены следующие условия.

1. *Мощность множества M не превосходит величины $\frac{\varphi(m)}{2}$.*
2. *Для любого натурального числа b , взаимно простого с m , и не принадлежащего множеству M выполнено условие*

$$p = \text{НОД}(m, b^{m+r} - 1 \pmod{m}). \quad (7.27)$$

Доказательство. Множество M образовано вычетами кольца \mathbb{Z}_m , являющимися корнями многочлена $x^{m+r} - 1$. Согласно теореме 3.4, эти вычеты удовлетворяют системе сравнений

$$\begin{cases} (x^{m+r} - 1) \equiv 0 \pmod{p}, \\ (x^{m+r} - 1) \equiv 0 \pmod{q}. \end{cases} \quad (7.28)$$

Количество решений первого сравнения приведенной системы, согласно теореме 4.4, равно

$$\text{НОД}(m + r, p - 1) = \text{НОД}(s(p - 1), p - 1) = p - 1.$$

Учитывая, что $q - 1 = s(p - 1) - (r + 1)$ получаем,

$$\begin{aligned} \text{НОД}(m + r, q - 1) &= \text{НОД}(s(p - 1), s(p - 1) - (r + 1)) = \\ &= \text{НОД}(s(p - 1), r + 1) < r + 1 \leq \frac{p - 1}{2} < \frac{q - 1}{2}. \end{aligned}$$

Таким образом, число решений системы (7.28) и, соответственно, мощность множества M , оценивается величиной

$$\text{НОД}(m - r, p - 1) \text{НОД}(m - r, q - 1) < \frac{(p - 1)(q - 1)}{2} = \frac{\varphi(m)}{2}.$$

Первое утверждение леммы доказано.

Для доказательства второго утверждения рассмотрим взаимно простой с m вычет b , не принадлежащий множеству M . Тогда выполнено сравнение $b^{m+r} \not\equiv 1 \pmod{m}$. С другой стороны, используя малую теорему Ферма, см. теорему 2.7, получаем

$$b^{m+r} \equiv (b^p)^qb^r \equiv b^qb^r \equiv b^{s(p-1)-r}b^r \equiv b^{-r}b^r \equiv 1 \pmod{p}.$$

Таким образом $p \mid (b^{m+r} - 1) \pmod{m}$. Последнее утверждение завершает доказательство леммы. \square

Метод применения данной леммы для разложения числа m на множители выглядит следующим образом. Выберем случайный вычет b . Если он не взаимно прост с m , мы получаем нетривиальный делитель. В противном случае, с вероятностью, большей $\frac{1}{2}$ будет выполнено условие $\text{НОД}(m, b^{m+r} - 1 \pmod{m}) = p$ при некотором значении r . Для его поиска необходимо перебрать все значения, удовлетворяющие неравенству $0 < r \leq \frac{p-3}{2}$.

В общем случае, мы получаем трудоемкость сравнимую с трудоемкостью тотального перебора. Однако при малых значениях величины r алгоритм может привести к разложению числа m на множители.

Для оптимизации предложенного метода мы можем его скомпилировать с изложенным ранее $p - 1$ методом Полларда, см. раздел 7.6. Более того, мы будем рассматривать его как еще один вариант второго этапа метода Полларда, см. раздел 7.8.

Пусть $k = \prod_i p_i^{\alpha_i}$ — произведение маленьких простых чисел p_i , не превосходящих некоторой заранее заданной границы B . Пусть выполнены условия

$$p - 1 = ud, \quad k = ut, \quad d, u, t \in \mathbb{N}, \quad (7.29)$$

то есть величина $p - 1$ раскладывается в произведение маленьких простых чисел, входящих в разложение числа k и некоторого натурального числа d , каждый простой делитель которого превышает величину B , то есть $\text{НОД}(d, k) = 1$. Подобная ситуация возникает на втором этапе $p - 1$ -метода Полларда.

Рассмотрим для наибольшего делителя q числа m два представления

$$q = s(p - 1) - r, \quad q = ld - z, \quad 0 < r \leq \frac{p-3}{2}, \quad 0 \leq z < d. \quad (7.30)$$

Теперь мы можем записать сравнение

$$\begin{aligned} (a^k)^m &\equiv (a)^{kq} \equiv a^{kld}(a^k)^{-z} \equiv a^{utld}(a^k)^{-z} \equiv \\ &\equiv (a^{p-1})^{lt}(a^k)^{-z} \equiv (a^k)^{-z} \pmod{p} \end{aligned}$$

из которого следует $(a^k)^{m+z} \equiv 1 \pmod{p}$. Согласно доказанной ранее лемме, с вероятностью $\frac{1}{2}$ выполнено условие $(a^k)^{m+z} \not\equiv 1 \pmod{m}$ и мы получаем утверждение, аналогичное (7.27), а именно

$$p = \mathbf{НОД}(m, (a^k)^{m+z} - 1 \pmod{m}). \quad (7.31)$$

Полученное равенство существенно снижает границу для перебора значений z , поскольку $0 \leq z < d$. Однако она все равно остается достаточно высокой, поскольку $d > B$.

Надо заметить, что алгоритм Женга должен рассматриваться как частный случай $p-1$ -метода Полларда. Действительно, на втором этапе мы пользуемся пытаемся найти простое число d , для которого выполнено сравнение $(a^k)^d \equiv 1 \pmod{p}$ и $p-1 = d \cdot \mathbf{НОД}(p-1, k)$.

В случае выполнимости условия $(a^k)^{m+z} \equiv 1 \pmod{p}$ получаем, что должно быть выполнено условие $d|m+z$. Это действительно так, поскольку из (7.30) следует равенство

$$m+z = p(ld-z) + z = dlp - (p-1)z = d(lp-uz).$$

Обозначим $\xi = \mathbf{НОД}(l, u) = \mathbf{НОД}(l, \frac{p-1}{d})$, тогда $m+z \equiv 0 \pmod{\xi}$, что позволяет существенно снизить перебор возможных значений z и ограничиться только неотрицательными величинами z , удовлетворяющими сравнению $z \equiv -m \pmod{\xi}$. На практике величина ξ нам неизвестна, однако если она не велика, то есть величина l имеет маленькие простые делители, мы можем искать возможные значения неизвестной z в арифметических прогрессиях

$$z \equiv -m \pmod{\xi}, \quad \xi = 2, 3, 5, \dots$$

7.10 Метод Макки

В 1999 году в работе [13] Джеймс Макки (James McKee) доказал следующий результат.

Лемма 7.4 (Лемма Макки). Пусть m нечетное составное число, для которого выполнено $m = pq$ и $2\sqrt[4]{m} < p < q$. Определим $h = \lfloor \sqrt{m} \rfloor$ и выберем произвольное натуральное число $s \geq 1$. Тогда найдется s наборов натуральных чисел k, x, y, v , удовлетворяющих условиям

$$x^2 - y^2 = mv^2, \quad \text{где } x = hv + k, \quad (7.32)$$

а также

1. v четно и удовлетворяет неравенствам $2 \leq v \leq \sqrt[4]{m} + 2(c - 1)$,
2. выполнено неравенство $|y| < c^2\sqrt{m}$,
3. выполнены неравенства $0 < kv < c^4\sqrt{m}$,
4. выполнено условие $1 < \mathbf{НОД}(x + y, m) < m$.

Доказательство. Пусть ξ произвольное целое, отличное от нуля число. Определим значения x , y и v равенствами

$$x = q + \xi^2 p, \quad y = q - \xi^2 p, \quad v = 2\xi, \quad (7.33)$$

тогда для k выполнено $k = x - hv = q + \xi^2 p - 2h\xi$, а также выполнено равенство (7.32). Действительно,

$$x^2 - y^2 = (q + \xi^2 p)^2 - (q - \xi^2 p)^2 = 4\xi^2 p q = mv^2.$$

Таким образом, равенство (7.32) выполнено для любого целого ξ и величин x , y и v , определенных равенствами (7.33).

Поскольку значения x , y не зависят от знака ξ , мы ограничимся только положительными значениями ξ и покажем, что найдется c значений ξ , для которых выполнены утверждения леммы.

Рассмотрим величину $r = \left\lfloor \sqrt{\frac{q}{p}} \right\rfloor$ и определим величины ξ равенствами

$$\xi = r + i, \quad \text{для } i = 0, 1, \dots, c - 1. \quad (7.34)$$

Поскольку выполнены ограничения $2\sqrt[4]{m} < p < q$, то мы получаем неравенство

$$1 \leq r \leq \sqrt{\frac{q}{p}} < \sqrt{\frac{m^{\frac{3}{4}}}{4m^{\frac{1}{4}}}} = \frac{\sqrt[4]{m}}{2}, \quad (7.35)$$

из которого вытекает оценка $2 \leq v = 2\xi < \sqrt[4]{m} + 2(c - 1)$ и первое утверждение леммы.

Получим оценки для величины y , которая может принимать как положительные, так и отрицательные значения. Действительно, учитывая (7.34) и (7.35) получаем, что при $i = 0$ выполнено неравенство $\xi^2 \leq \frac{q}{p}$ и $y = q - \xi^2 p \geq 0$. В остальных случаях, при $i > 0$, получаем $\xi^2 > \frac{q}{p}$ и $y = q - \xi^2 p < 0$. В обоих случаях выполнено неравенство

$$y = q - \xi^2 p \geq q - p \left(\sqrt{\frac{q}{p}} + i \right)^2 = - (2i\sqrt{m} + pi^2).$$

Следовательно, учитывая интервал возможных значений i , получаем неравенство

$$|y| \leq 2i\sqrt{m} + pi^2 < \sqrt{m}(1 + 2i + i^2) \leq c^2\sqrt{m},$$

из которого следует второе утверждение леммы.

Для доказательства третьего утверждения леммы заметим, что

$$k = x - hv = q + \xi^2 p - 2h\xi = (\sqrt{q} - \xi\sqrt{p})^2 + 2\xi(\sqrt{m} - h) > 0. \quad (7.36)$$

Последнее неравенство верно, поскольку ξ положительно и $\sqrt{m} \geq h$, таким образом k является суммой двух положительных величин.

Предположим, что $k \leq v$ тогда, учитывая первое утверждение леммы, получаем

$$kv \leq v^2 \leq (\sqrt[4]{m} + 2(c-1))^2 < c^4\sqrt{m}.$$

Запишем равенство (7.32) в виде

$$mv^2 + y^2 = x^2 = (k + hv)^2 = k^2 + 2hkv + h^2v^2 \quad (7.37)$$

и рассмотрим случай $k > v$. Поскольку $h + \frac{k^2}{v^2} > h + 1 > m$, то выполнено неравенство $hv^2 + k^2 > mv^2$. Тогда, из (7.37), следует неравенство

$$kv = \frac{1}{2h} (y^2 + mv^2 - h^2v^2 - k^2) < \frac{y^2}{2h} < c^4\sqrt{m},$$

которое завершает доказательство третьего утверждения леммы.

Последнее утверждение леммы следует из равенств (7.33). Поскольку $x + y = 2q$ и m нечетно, получаем равенство $q = \mathbf{НОД}(x + y, m)$, которое позволяет нам найти нетривиальный делитель числа m . \square

Утверждение доказанной леммы может быть использовано для разложения числа m на множители с помощью алгоритма, аналогичного алгоритмам Ферма или Лемана. В качестве упражнения читателю предлагается разработать данный алгоритм и показать, что его трудоемкость не меньше, чем у метода Лемана.

Для уменьшения трудоемкости перебора можно воспользоваться равенством (7.36). Обозначим

$$\lambda = \sqrt{q} - \xi\sqrt{p}, \quad \mu = \sqrt{\frac{q}{p}},$$

тогда

$$\sqrt{p} = \frac{\lambda}{\mu - \xi}, \quad \sqrt{q} = \frac{\lambda\mu}{\mu - \xi}, \quad \sqrt{m} = \frac{\lambda^2\mu}{(\mu - \xi)^2}.$$

Последнее равенство позволяет нам записать $\lambda^2 = \frac{(\mu-\xi)^2}{\mu}\sqrt{m}$. Тогда, из (7.36), получаем выражение

$$k = \frac{(\mu - \xi)^2}{\mu}\sqrt{m} + 2\xi(\sqrt{m} - h),$$

где $\xi = \lfloor \mu \rfloor + i, i = 0, 1, \dots, c-1$. Мы получили точное значение величины k в зависимости от величины μ и, тем самым, определили область перебора возможных значений k . К сожалению, на практике точное значение величины μ бывает известно не всегда.

В своей работе [13] Макки предложил отличный от описанного выше способ поиска величин k и v , основанный на вычислении наилучших приближений для рациональных чисел. Запишем равенство (7.32) в виде

$$y^2 = x^2 - mv^2 = (hv + k)^2 - mv^2. \tag{7.38}$$

для натуральных чисел k, v , удовлетворяющих условиям леммы 7.4.

Пусть $z \leq y$ — некоторый делитель числа y такой, что выполнены неравенства $z > v$ и $z^2 \geq 2kv$.

Предположим, что v делит z , тогда $v|y$, кроме того, из равенства $x^2 = y^2 + mv^2$ следует, что $v|x$. Используя обозначения введенные при доказательстве леммы 7.4 запишем $v = 2\xi$, тогда $2\xi = v|(x + y) = 2q$, следовательно, $\xi|q$ и $\xi|m$. Мы получили, что величина ξ является делителем числа m и $\xi \leq \frac{\sqrt[4]{m}}{2} + (c - 1)$. С другой стороны, число m не имеет делителей, меньших, чем $2\sqrt[4]{m}$. Таким образом, при $c \leq \frac{3}{2}\sqrt[4]{m}$ величина v не делит z .

Далее, из равенства (7.38) получаем, что $z^2|(hv+k)^2 - mv^2$. Последнее условие равносильно сравнению

$$(hv + k)^2 \equiv mv^2 \pmod{z^2}.$$

Поскольку $\text{НОД}(v, z) = 1$, то последнее сравнение равносильно

$$\left(h + \frac{k}{v}\right)^2 \equiv m \pmod{z^2}.$$

Мы получили, что числа k, v , удовлетворяющие равенству (7.38), связаны соотношением $k = k_0v - lz^2$, где величина l является целым числом, удовлетворяющим неравенству $l > 0$, а k_0 является решением сравнения $(h + x)^2 \equiv m \pmod{z^2}$.

Предположим, что $l = 0$, тогда $k = k_0v$ и величина v делит k . Тогда, из равенства (7.38) следует, что $v|y$. Аналогично предыдущим рассуждениям получаем, что $v|x$ и $\xi = \frac{v}{2}$ делит m , то есть противоречие условию

леммы 7.4. Далее предположим, что выполнено неравенство $l < 0$, тогда

$$k = k_0v - lz^2 = k_0v + |l|z^2 \geq |l|z^2 \geq 2|l|kv \geq 4|l|k \quad \text{или} \quad |l| \leq \frac{1}{4}.$$

Поскольку l целое число, то последнее неравенство влечет за собой равенство $l = 0$, которое противоречит нашему предположению. Таким образом

$$k = k_0v - lz^2, \quad l > 0.$$

Поскольку $z^2 > 2kv$, то выполнено неравенство $\frac{1}{2v} > \frac{k}{z^2}$. Учитывая, что $k = k_0v - lz^2 > 0$, получаем

$$\frac{1}{2v^2} > \frac{k}{z^2v} = \frac{k_0v - lz^2}{z^2v} = \frac{k_0}{z^2} - \frac{l}{v} > 0.$$

Таким образом, согласно теореме 6.5, дробь $\frac{l}{v}$ является наилучшим приближением к величине $\frac{k_0}{z^2}$.

Воспользовавшись утверждением теоремы 6.4 мы получим, что дробь $\frac{l}{v}$ является подходящей дробью и может быть вычислена при помощи соотношений (6.5).

Алгоритм, предложенный Макки, состоял из следующей последовательности действий.

1. Фиксировать значение величины c , например, $c = \lceil \log_2 m \rceil$.
2. Выбрать случайное, простое число z , удовлетворяющее условиям $2c^2 \sqrt[4]{m} < z < c\sqrt{m}$ и $\left(\frac{m}{z}\right) = 1$.
3. Используя метод, полученный при доказательстве теоремы 3.5, вычислить k_0 , удовлетворяющее сравнению $(h + x)^2 \equiv m \pmod{z^2}$.
4. Используя соотношения (6.5) вычислить все подходящие дроби $\frac{P_n}{Q_n}$ к величине $\frac{k_0}{z^2}$.
5. Для каждой вычисленной дроби определить

$$v = Q_n, \quad k = k_0v - P_n z^2, \quad x = hv + k, \quad t = x^2 - mv^2.$$

6. Если t является полным квадратом, вычислить $y = \sqrt{t}$ и определить q — делитель числа m равенством $q = \text{НОД}(m, x + y)$.
7. Если для всех подходящих дробей делитель q не найден, то выбрать новое значение величины z .

ФАКТОРИЗАЦИЯ ЦЕЛЫХ ЧИСЕЛ II

Основная лемма - решето Крайчика - Метод непрерывных дробей - метод Моррисона-Брилхарда - линейное решето Шреппеля - квадратичное решето - дальнейшие модификации метода квадратичного решета.

В этой лекции мы опишем современные методы разложения целых чисел на множители. Рассматриваемые методы могут быть применены к произвольным целым числам, для которых не известно какой-либо дополнительной информации о делителях.

Докажем лемму, утверждения которой используются всеми методами настоящей лекции. Лемма является обобщением равенств используемых в алгоритмах Ферма и Лемана.

Лемма 8.1 (Лемма о факторизации). Пусть m нечетное составное число и x, y вычеты по модулю m такие, что $x \not\equiv \pm y \pmod{m}$ и

$$x^2 \equiv y^2 \pmod{m}, \quad (8.1)$$

тогда будет выполнено условие $1 < \text{НОД}(x - y, m) < m$.

Доказательство. Согласно основной теореме арифметики, представим m в виде $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, где p_1, \dots, p_n различные нечетные простые числа, $\alpha_1, \dots, \alpha_n$ натуральные числа. Тогда сравнение (8.1) позволяет нам записать равенство

$$(x - y)(x + y) = kp_1^{\alpha_1} \cdots p_n^{\alpha_n},$$

для некоторого целого числа k .

Предположим, что выполнено условие $\text{НОД}(x - y, m) = 1$. Тогда, согласно лемме 1.4, выполнено $p_i^{\alpha_i} | x + y$ для любого индекса $i = 1, \dots, n$. Следовательно $m | (x + y)$, что равносильно сравнению $x \equiv -y \pmod{m}$. Последнее сравнение противоречит условию леммы.

Далее, предположим, что выполнено условие $\text{НОД}(x - y, m) = m$. Аналогичными рассуждениями получаем, что $m | (x - y)$, то есть сравнение $x \equiv y \pmod{m}$ и противоречие условиям леммы. Таким образом, величина $\text{НОД}(x - y, m)$ не превосходит m и не равна 1 или m . Лемма доказана. \square

Согласно доказанной лемме для разложения числа m на множители достаточно найти пару вычетов x, y , удовлетворяющих условиям леммы. Легко заметить, что рассмотренные ранее равенства (7.1), (7.5) и (7.32), являются частным случаем сравнения (8.1).

8.1 Метод Крайчика

Еще в докомпьютерную эпоху, в 1926 году в монографии [10] Морис Крайчик¹ предложил последовательность действий, позволяющую для заданного составного числа m найти пару x, y , удовлетворяющую сравнению (8.1), и разложить число m на множители.

1. Вычислить множество пар целых чисел u, v , удовлетворяющих сравнению $u \equiv v \pmod{m}$.
2. Определить полное или частичное разложение чисел u, v на множители для каждой пары u, v .
3. С помощью известного разложения на множители, выбрать те пары u, v , произведение которых позволит получить сравнение (8.1).
4. Разложить число m на множители.

В своей работе Крайчик не предъявил конкретный алгоритм поиска пар чисел u, v и алгоритмический способ составления из найденных соотношений сравнения (8.1). Тем не менее, Крайчик заметил, что в случае, когда одно из чисел является полным квадратом, то есть выполнено сравнение $u^2 \equiv v \pmod{m}$, получить сравнение (8.1) несколько проще.

Пример 8.1. Приведем пример и разложим составное число $m = 1081$ на множители, используя метод Крайчика. Рассмотрим равенства

$$\begin{aligned} 1081 - 81 &= 1000, \\ 1081 - 960 &= 121, \\ 1081 - 720 &= 361, \\ 1089 - 1081 &= 8, \\ 1156 - 1081 &= 75. \end{aligned}$$

Раскладывая на множители в приведенных равенствах слагаемые, отличные от 1081, мы можем записать следующие сравнения

$$\begin{aligned} -3^4 &\equiv 2^3 \cdot 5^3 \\ -2^6 \cdot 3 \cdot 5 &\equiv 11^2 \\ -2^4 \cdot 3^2 \cdot 5 &\equiv 19^2 \\ 3^2 \cdot 11^2 &\equiv 2^3 \\ 2^2 \cdot 17^2 &\equiv 3 \cdot 5^2, \end{aligned} \tag{8.2}$$

¹Крайчик, Морис Борисович, родился в Минске 21 апреля 1882 г., еще до революции уехал в Бельгию, где учился и работал в университете города Льеж. Автор книг по теории чисел. Умер в Брюсселе 19 августа 1957.

рассматриваемые по модулю 1081. Можно заметить, что правая или левая часть каждого из сравнений в (8.2), согласно замечанию Крайчика, является полным квадратом.

Перемножая первое, третье и четвертое сравнения из (8.2), получим

$$(-1)^2 \cdot 3^4 \cdot 2^4 \cdot 3^2 \cdot 5 \cdot 3^2 \cdot 11^2 \equiv 2^3 \cdot 5^3 \cdot 19^2 \cdot 2^3 \pmod{1081}$$

или, сокращая на $2^4 \cdot 5$,

$$3^8 \cdot 11^2 \equiv 2^2 \cdot 5^2 \cdot 19^2 \pmod{1081}.$$

Последнее сравнение равносильно $891^2 \equiv 190^2 \pmod{1081}$. Мы получили сравнение вида (8.1), которое не может быть использовано для разложения числа 1081 на множители. Действительно, поскольку выполнено равенство $891 + 190 = 1081$, мы получаем противоречие с условием леммы 8.1.

Попробуем перемножить первое, второе, четвертое и пятое сравнения из (8.2). Получим

$$(-1)^2 \cdot 3^4 \cdot 2^6 \cdot 3 \cdot 5 \cdot 3^2 \cdot 11^2 \cdot 2^2 \cdot 17^2 \equiv 2^3 \cdot 5^3 \cdot 11^2 \cdot 2^3 \cdot 3 \cdot 5^2 \pmod{1081}$$

или, сокращая на $2^6 \cdot 3 \cdot 5 \cdot 11^2$,

$$2^2 \cdot 3^6 \cdot 17^2 \equiv 5^4 \cdot 11^2 \pmod{1081}.$$

Последнее сравнение равносильно $918^2 \equiv 25^2 \pmod{1081}$. Вычислим $918 - 25 = 893$ и найдем $\text{НОД}(893, 1081) = 47$. Величина 47 является делителем числа 1081. Другим делителем числа 1081, как легко проверить, является число 23.

8.2 Метод непрерывных дробей

Как мы видели ранее, метод Крайчика сводит задачу факторизации числа m к задаче факторизации нескольких чисел, а именно, пар u, v , связанных соотношением $u^2 \equiv v \pmod{m}$.

Величина v является величиной такого же порядка, как и m . Поэтому наивное применение метода Крайчика может привести к многократному разложению на множители чисел, сравнимых по величине с m .

Используя соотношения, возникающие при разложении квадратичных иррациональностей в непрерывные дроби, в 1931 году Лемер и Пауэрс (D.H. Lehmer & R.E. Powers) в работе [12] предложили два варианта

генерации указанных сравнений. Оба варианта обладают тем свойством, что величины, которые необходимо раскладывать на множители, не превосходят $2\sqrt{m}$.

Пусть $f(x) = ax^2 + bx + c$ многочлен второй степени с целыми коэффициентами, дискриминант которого $D = b^2 - 4ac > 0$, а кроме того, величина $D \equiv 0 \pmod{m}$ и не является полным квадратом. Следуя разделу 6.3, определим квадратичную иррациональность $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$ — корень многочлена $f(x)$, и разложим α в непрерывную дробь

$$\alpha_0 = [a_0, a_1, \dots, a_{n-1}, \alpha_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{\alpha_n}}}}$$

где $a_n = \lfloor \alpha_n \rfloor$ и $\alpha_n = \frac{A_n + \sqrt{D}}{B_n}$, $n = 0, 1, \dots$ и коэффициенты A_n, B_n удовлетворяют рекуррентным соотношениям (6.17)

$$\begin{aligned} A_{n+1} &= a_n B_n - A_n, \\ B_{n+1} &= a_n (A_n - A_{n+1}) + B_{n-1}, \end{aligned}$$

где $B_{-1} = -cB_0$.

8.2.1 Первый вариант

Согласно доказанной нами ранее лемме 6.6, для коэффициентов A_n, B_n выполнено равенство (6.19)

$$-B_n B_{n+1} = A_{n+1}^2 - D.$$

Поскольку $D \equiv 0 \pmod{m}$, то мы получаем сравнение

$$-B_n B_{n+1} \equiv A_{n+1}^2 \pmod{m}. \quad (8.3)$$

Полученное сравнение имеет вид $u^2 \equiv v \pmod{m}$, предложенный Крайчиком, и может быть использовано для факторизации числа m .

Согласно следствию 1 к теореме 6.2, найдется индекс n_0 такой, что для всех индексов $n \geq n_0$, квадратичная иррациональность α_n будет приведенной, см. определение на стр. 123. Тогда, согласно лемме 6.7, для величин A_n, B_n будут выполнены неравенства

$$0 < A_n < \sqrt{D}, \quad 0 < B_n < 2\sqrt{D}.$$

Вычисляя последовательно полные частные $\alpha_1, \alpha_2, \dots$ мы будем получать сравнения (8.3) для $n = 0, 1, \dots$. Комбинируя эти сравнения аналогично тому, как это делалось в методе Крайчика, получим искомое сравнение $x^2 \equiv y^2 \pmod{m}$.

Пример 8.2. Проиллюстрируем изложенный метод и разложим на множители число $m = 1081$.

Выберем многочлен $f(x) = 11x^2 + 5x - 24$, дискриминант которого $D = 25 + 4 \cdot 11 \cdot 24 = 1081$, следовательно, $D > 0$ и $D \equiv 0 \pmod{1081}$.

Определим начальную квадратичную иррациональность α_0 — положительный корень многочлена $f(x)$ равенством $\alpha_0 = \frac{-5 + \sqrt{1081}}{22}$, и $a_0 = \lfloor \alpha_0 \rfloor = 1$, где $A_0 = -5, B_0 = 22$.

Воспользовавшись равенством (6.1), запишем

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{27 + \sqrt{1081}}{16}, \quad a_1 = \lfloor \alpha_1 \rfloor = 3,$$

то есть $A_1 = 27, B_1 = 16$. Продолжая вычисления, находим

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{21 + \sqrt{1081}}{40}, \quad a_2 = 1, \quad A_2 = 21, \quad B_2 = 40,$$

$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{19 + \sqrt{1081}}{18}, \quad a_3 = 2, \quad A_3 = 19, \quad B_3 = 18,$$

$$\alpha_4 = \frac{1}{\alpha_3 - a_3} = \frac{17 + \sqrt{1081}}{44}, \quad a_4 = 1, \quad A_4 = 17, \quad B_4 = 44.$$

Воспользовавшись выражением (8.3), мы можем записать следующие сравнения для $n = 0, 1, 2, 3$

$$\begin{aligned} -2^5 \cdot 11 &\equiv 3^6 \pmod{1081}, \\ -2^7 \cdot 5 &\equiv 3^2 \cdot 7^2 \pmod{1081}, \\ -2^4 \cdot 3^3 \cdot 5 &\equiv 19^2 \pmod{1081}, \\ -2^3 \cdot 3^2 \cdot 11 &\equiv 17^2 \pmod{1081}. \end{aligned} \tag{8.4}$$

Перемножая первое и четвертое сравнения получим

$$(-1)^2 \cdot 2^5 \cdot 11 \cdot 2^3 \cdot 3^2 \cdot 11 \equiv 3^6 \cdot 17^2 \pmod{1081}$$

или, приводя подобные множители и сокращая на 3^2 ,

$$2^8 \cdot 11^2 \equiv 3^4 \cdot 17^2 \pmod{1081} \quad \text{или} \quad 176^2 \equiv 153^2 \pmod{1081}.$$

Мы получили сравнение вида (8.1), используя которое, находим нетривиальный делитель числа 1081. Действительно, $\text{НОД}(176 - 153, 1081) = 23$. Легко проверить, что второй делитель числа 1081 равен 47.

8.2.2 Второй вариант

Второй вариант, предложенный Лемером и Пауэрсом, заключался в следующем. Пусть, как и ранее, $\alpha_0 = \frac{A_0 + \sqrt{D}}{B_0}$ — квадратичная иррациональность, раскладываемая в непрерывную дробь. Рассмотрим последовательность полных частных $\alpha_1, \alpha_2, \dots, \alpha_n = \frac{A_n + \sqrt{D}}{B_n}, \dots$, а также последовательность подходящих дробей $\frac{P_n}{Q_n}, n = 0, 1, \dots$, числители и знаменатели которых определяются равенствами (6.5)

$$\begin{aligned} P_{n+1} &= a_{n+1}P_n + P_{n-1}, \\ Q_{n+1} &= a_{n+1}Q_n + Q_{n-1}, \end{aligned}$$

где $a_n = [\alpha_n]$ и $P_{-1} = 1, Q_{-1} = 0, P_0 = a_0, Q_0 = 1$. Согласно доказанной нами ранее теореме 6.3 выполнено равенство (6.27)

$$(P_n B_0 - Q_n A_0)^2 - Q_n^2 D = (-1)^{n+1} B_0 B_{n+1}.$$

Поскольку мы предположили, что $D \equiv 0 \pmod{m}$, то последнее равенство позволяет записать сравнение

$$(P_n B_0 - Q_n A_0)^2 \equiv (-1)^{n+1} B_0 B_{n+1} \pmod{m}. \quad (8.5)$$

Данное сравнение имеет вид $u^2 \equiv v \pmod{m}$, предложенный Крайчиком, и может быть использовано для факторизации числа m .

Разложение квадратичной иррациональности в непрерывную дробь периодически, см. теорему 6.2. Поэтому количество соотношений, которые можно получить с помощью данного метода, ограничено, и их может оказаться недостаточно для набора соотношений и построения сравнения (8.1).

В той же работе [12] Лемер и Пауэрс показали, что оба варианта алгоритма эквивалентны: если один вариант алгоритма найдет решение, то и второй вариант также найдет решение. Как показывают практические эксперименты, для больших значений m , оба варианта алгоритма всегда находят разложение числа m на множители.

В 1975 году Моррисон и Бриллхарт в работе [3] реализовали второй вариант алгоритма Лемера и Пауэrsa на ЭВМ и применили его к факторизации седьмого числа Ферма $F_7 = 2^{2^7} + 1$.

Моррисон и Бриллхарт впервые предложили алгоритм построения сравнения (8.1) по заданному множеству сравнений вида (8.3) или (8.5), и ввели понятие «факторная база».

Напомним, что величина D является дискриминантом многочлена $f(x)$ второй степени, корень которого раскладывается в непрерывную дробь. Для дискриминанта выполнено равенство $D = kt$ при некотором натуральном числе k .

Определение 8.1. Мы будем называть множество \mathcal{B}_B факторной базой, если оно содержит целое число -1 и простые числа p такие, что

1. p ограничено сверху, то есть $p \leq B$,
2. выполнено равенство $\left(\frac{D}{p}\right) = 1$, то есть число D является квадратичным вычетом по модулю p .

Пусть в ходе выполнения первого или второго варианта алгоритма найдено сравнение вида $u^2 \equiv v \pmod{D}$. Факторная база \mathcal{B}_B представляет собой множество возможных делителей числа v , не превосходящих заданной величины B .

Рассмотрим более детально получаемые сравнения. В случае первого варианта алгоритма получаемые сравнения следуют из равенства (6.19), то есть $D = u^2 + v$. В случае второго варианта алгоритма — из равенства (6.27), то есть $q^2 D = u^2 \pm v$, где q знаменатель некоторой подходящей дроби. Если мы обозначим символом p произвольный простой делитель числа v , то в обоих случаях выполнено сравнение $D \equiv w^2 \pmod{p}$ для некоторого вычета w . Таким образом, мы получили, что величина D является квадратичным вычетом по модулю любого простого числа, делящего v . Это объясняет введенное нами второе условие в определении факторной базы.

Опишем способ, который предложили Моррисон и Бриллхарт для построения сравнения (8.1) по множеству сравнений вида $u^2 \equiv v \pmod{D}$, вырабатываемых в ходе выполнения алгоритма. Каждому найденному сравнению, в котором

$$v = (-1)^{\gamma_0} \prod_{i=1}^s p_i^{\gamma_i}, \quad p_i \in \mathcal{B}_B, \quad \gamma_i \in \mathbb{N}, \quad (8.6)$$

сопоставим вектор

$$e = (\gamma_0, \gamma_1 \pmod{2}, \dots, \gamma_s \pmod{2}). \quad (8.7)$$

Вектор e содержит нули и единицы, то есть степени простых, входящих в разложение v , взятые по модулю 2.

Предположим, что мы нашли r сравнений,

$$u_i^2 \equiv v_i \pmod{D}, \quad i = 1, \dots, r, \quad (8.8)$$

правые части которых удовлетворяют равенству (8.6). Каждому сравнению будет соответствовать свой вектор e_i вида (8.7) и квадрат u_i^2 .

Образуюем из векторов e_i прямоугольную матрицу размера $(r \times s)$, элементами которой являются нули и единицы. Строкам матрицы будет соответствовать вектор (u_1^2, \dots, u_r^2) , состоящий из левых частей сравнений (8.8).

Используя алгоритм Гаусса в поле \mathbb{F}_2 , приведем полученную матрицу к диагональному виду. При этом, каждой операции сложения строк матрицы будет соответствовать операция умножения элементов вектора (u_1^2, \dots, u_r^2) с теми же индексами, что и у складываемых строк.

При $r > s + 1$ ранг матрицы не превосходит s , поэтому мы вправе ожидать, что после приведения матрица будет содержать в себе линейно-зависимые строки, состоящие из одних нулей.

Каждая строка, состоящая из одних нулей, представляет собой разложение некоторого числа на простые множители, принадлежащие факторной базе. При этом все множители входят в разложение в четной степени, то есть произведение является полным квадратом. Полученный квадрат будет сравним с элементом вектора (u_1^2, \dots, u_r^2) с индексом, совпадающим с индексом нулевой строки.

Для иллюстрации изложенного метода, воспользуемся вторым вариантом метода непрерывных дробей и разложим на множители число $m = 1081$.

Пример 8.3. Рассмотрим, как и в предыдущем примере, многочлен $f(x) = 11x^2 + 5x - 24$ и разложим в непрерывную дробь его положительный корень $\alpha_0 = \frac{-5 + \sqrt{1081}}{22}$. Напомним, что дискриминант выбранного нами многочлена $D = m = 1081$. Выполним последовательно несколько шагов.

Шаг первый. Выберем в качестве границы $B = 15$ и определим факторную базу

$$\mathcal{B}_{15} = \{-1, 2, 3, 5, 11\}.$$

Простые числа 7 и 13 не входят в факторную базу, поскольку $\left(\frac{1081}{7}\right) = \left(\frac{1081}{13}\right) = -1$. Это объясняет, почему простые 7, 13 не появлялись ранее в сравнениях (8.2) и (8.4).

Шаг второй. Разложим α_0 в непрерывную дробь и выработаем необходимые сравнения. Поскольку факторная база содержит только 5 эле-

ментов, то нам будет достаточно вычислить 6 сравнений, в которых правая часть удовлетворяет равенству (8.6).

Используя вычисления, проведенные в предыдущем примере, получим последовательность A_i, B_i для $i = 0, \dots, 6$.

$$\begin{aligned} A_0 &= -5, B_0 = 22, \\ A_1 &= 27, B_1 = 16, A_2 = 21, B_2 = 40, A_3 = 19, B_3 = 18, \\ A_4 &= 17, B_4 = 44, A_5 = 27, B_5 = 8, A_6 = 29, B_6 = 30. \end{aligned}$$

Кроме того, вычислим последовательность подходящих дробей

$$\begin{aligned} \frac{P_0}{Q_0} &= a_0 = 1, \\ \frac{P_1}{Q_1} &= \frac{4}{3}, \frac{P_2}{Q_2} = \frac{5}{4}, \frac{P_3}{Q_3} = \frac{14}{11}, \frac{P_4}{Q_4} = \frac{19}{15}, \frac{P_5}{Q_5} = \frac{147}{116}, \frac{P_6}{Q_6} = \frac{313}{247}. \end{aligned}$$

Теперь, используя сравнение (8.5) мы можем записать следующие сравнения. При $n = 0$ получаем

$$(1 \cdot 22 + 1 \cdot 5)^2 \equiv -22 \cdot 16 \pmod{1081} \quad \text{или} \quad 27^2 \equiv -2^5 \cdot 11 \pmod{1081}.$$

Используя полученное разложение замечаем, что правой части сравнения соответствует вектор $e_0 = (1, 1, 0, 0, 1)$. При $n = 1$

$$(4 \cdot 22 + 3 \cdot 5)^2 \equiv 22 \cdot 40 \pmod{1081} \quad \text{или} \quad 103^2 \equiv 2^4 \cdot 5 \cdot 11 \pmod{1081}.$$

Аналогично, получаем вектор $e_1 = (0, 0, 0, 1, 1)$. При $n = 2$

$$(5 \cdot 22 + 4 \cdot 5)^2 \equiv -22 \cdot 18 \pmod{1081} \quad \text{или} \quad 130^2 \equiv -2^2 \cdot 3^2 \cdot 11 \pmod{1081}.$$

Аналогично, получаем вектор $e_2 = (1, 0, 0, 0, 1)$. При $n = 3$

$$(14 \cdot 22 + 11 \cdot 5)^2 \equiv 22 \cdot 44 \pmod{1081} \quad \text{или} \quad 363^2 \equiv 2^3 \cdot 11^2 \pmod{1081}.$$

Аналогично, получаем вектор $e_3 = (0, 1, 0, 0, 0)$. При $n = 4$

$$(19 \cdot 22 + 15 \cdot 5)^2 \equiv -22 \cdot 8 \pmod{1081} \quad \text{или} \quad 493^2 \equiv -2^4 \cdot 11 \pmod{1081}.$$

Вектор $e_4 = (1, 0, 0, 0, 1)$.

Шаг третий. Составим из полученных векторов двоичную матрицу размером (5×5) .

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Этой матрице соответствует вектор левых частей сравнений

$$(27^2, 103^2, 130^2, 363^2, 493^2).$$

Прибавим к пятой строке третью и получим матрицу

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

которой соответствует вектор $(27^2, 103^2, 130^2, 363^2, 311^2)$, поскольку $311 \equiv 130 \cdot 493 \pmod{1081}$.

Прибавим к первой строке третью и четвертую строки матрицы. Получим матрицу

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

которой соответствует вектор $(712^2, 103^2, 130^2, 363^2, 311^2)$, поскольку выполнено сравнение $712 \equiv 27 \cdot 130 \cdot 363 \pmod{1081}$.

Шаг четвертый. Мы получили матрицу у которой первая и пятая строки состоят из одних нулей. Каждая такая строка даст нам сравнение вида (8.1). Действительно перемножая первое, третье и четвертое сравнения получаем

$$712^2 \equiv (-1)^2 2^{10} \cdot 3^2 \cdot 11^4 \pmod{1081} \quad \text{или} \quad 712^2 \equiv 806^2 \pmod{1081}.$$

Теперь вычисляем $\text{НОД}(806 - 712, 1081) = 47$ и находим делитель числа 1081. Другой делитель числа 1081 равен 23.

Воспользуемся второй нулевой строкой полученной матрицы. Перемножая третье и пятое сравнения, получим

$$311^2 \equiv (-1)^2 \cdot 2^6 \cdot 3^2 \cdot 11^2 \pmod{1081} \quad \text{или} \quad 311^2 \equiv 264^2 \pmod{1081}.$$

Также как и ранее, вычисляем $\text{НОД}(311 - 264, 1081) = 47$ и находим нетривиальный делитель числа 1081.

СЛУЧАЙНЫЕ ОТОБРАЖЕНИЯ

Орбиты элементов - циклы и подходы - теорема о математическом ожидании длин циклов и подходов - алгоритмы Флойда, Брента, Госпера и Ниваша для поиска длин циклов в последовательностях.

В этом приложении мы приведем несколько формальных определений и опишем свойства случайных отображений конечного множества в себя. Мы опишем несколько алгоритмов поиска длин циклов в последовательностях, которые используются нами при реализации и исследовании сложности большого класса криптографических алгоритмов.

А.1 Орбиты элементов

Рассмотрим произвольное конечное множество \mathcal{M} , состоящее из m элементов, и дадим несколько определений.

Определение А.1. Мы будем обозначать символом \mathcal{F}_m множество всех функций, отображающих элементы множества \mathcal{M} в себя

$$\mathcal{F}_m = \{f : \mathcal{M} \rightarrow \mathcal{M}\}.$$

Отметим, что любую функцию $f \in \mathcal{F}_m$ можно определить аналитически или задать таблицей

$$\begin{pmatrix} a_0 & a_1 & \dots & a_{m-1} \\ f(a_0) & f(a_1) & \dots & f(a_{m-1}) \end{pmatrix}$$

Мы допускаем возможность возникновения у функции f коллизии, то есть существования двух элементов $a, b \in \mathcal{M}$ таких, что $f(a) = f(b)$ при $a \neq b$.

Зафиксируем некоторое отображение $f \in \mathcal{F}_m$, выберем элемент a из множества \mathcal{M} и рассмотрим последовательность элементов $\{a_n\}_{n=0}$, определяемую равенствами

$$a_0 = a, \quad a_{n+1} = f(a_n), \quad n = 0, 1, \dots \quad (\text{A.1})$$

Определение А.2. Пусть a некоторый элемент из \mathcal{M} и $f \in \mathcal{F}_m$ некоторое фиксированное отображение. Орбитой элемента a называется последовательность $\{a_n\}_{n=0}$, определяемая равенством (A.1).

Сформулируем важное наблюдение. В силу того, что множество \mathcal{M} конечно, орбита каждого элемента a зациклится, то есть найдется индекс λ такой, что для всех индексов $n \geq \lambda$ будет выполнено равенство

$$a_n = a_{n+\tau}, \quad (\text{A.2})$$

при некоторой натуральной величине τ .

Определение А.3. Мы будем называть элементы $a_0, a_1, \dots, a_{\lambda-1}$ *подходом к циклу*, значение λ — *длиной подхода*, наименьшее из всех возможных значений τ , удовлетворяющих равенству (A.2) — *длиной цикла* последовательности $\{a_n\}_{n=0}$ или, другими словами, орбиты элемента a .

Пример А.1. Поясним введенные выше определения. Рассмотрим в качестве множества \mathcal{M} кольцо вычетов \mathbb{Z}_{11} и зафиксируем отображение f , задаваемое таблицей

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 4 & 10 & 2 & 5 & 1 & 1 & 8 & 5 & 3 & 9 \end{pmatrix}$$

Тогда орбита элемента $a = 0$ будет иметь следующий вид

$$\begin{aligned} a_0 &= 0, \\ a_1 &= f(0) = 6, \\ a_2 &= f(6) = 1, \\ a_3 &= f(1) = 4, \\ a_4 &= f(4) = 5, \\ a_5 &= f(5) = 1, \\ a_6 &= f(1) = 4, \quad \dots \end{aligned}$$

Схематично, орбиту элемента $a = 0$ можно нарисовать следующим образом

$$\underbrace{0 \rightarrow 6}_{\text{подход}} \rightarrow \underbrace{1 \rightarrow 4 \rightarrow 5}_{\text{цикл}} \rightarrow \dots$$

В нашем примере длина подхода $\lambda = 2$, а длина цикла $\tau = 3$. Кроме того заметим, что элемент $a = 0$ не является результатом действия функции f и может появиться только в одном месте орбиты — в ее начале.

Определение А.4. Пусть $f \in \mathcal{F}_m$ некоторое фиксированное отображение множества \mathcal{M} в себя. Элемент $a \in \mathcal{M}$ называется *терминальным*, если не существует элемента $b \in \mathcal{M}$ такого, что $a = f(b)$.

Элементы, не являющиеся терминальными, естественно назвать образами на множестве \mathcal{M} .

Согласно данному определению, в рассматриваемом нами примере элементы 0 и 7 являются терминальными. Остальные элементы — образами множества \mathbb{Z}_{11} .

Поскольку мы допускаем, что отображение $f \in \mathcal{F}_m$ может реализовывать коллизии на множестве \mathcal{M} , мы должны допустить возможность того, что один цикл может иметь несколько подходов. Действительно, легко заметить, что орбита элемента $a = 7$ имеет вид

$$\underbrace{7 \rightarrow 8}_{\text{подход}} \rightarrow \underbrace{5 \rightarrow 1 \rightarrow 4}_{\text{цикл}} \rightarrow \dots$$

и сходится к тому же циклу, что и орбита элемента $a = 0$.

Определение А.5. Пусть $f \in \mathcal{F}_m$ некоторое фиксированное отображение множества \mathcal{M} в себя. Мы будем называть область связности или, другими словами, связной компонентой множества \mathcal{M} , цикл и множество его подходов.

Легко видеть, что в примере А.1 отображение f разбивает множество \mathbb{Z}_{11} на две связные компоненты. Одна состоит из рассмотренного ранее цикла и двух его подходов, вторая — из цикла длины 4 без подходов

$$\underbrace{2 \rightarrow 10 \rightarrow 9 \rightarrow 3}_{\text{цикл}} \rightarrow \dots$$

Приведем, без доказательства, основное утверждение.

Теорема А.1. Пусть $f \in \mathcal{F}_m$ некоторое отображение, являющееся реализацией случайной величины, равномерно распределенной на множестве \mathcal{F}_m . Выполнены следующие утверждения.

1. Обозначим символом $M(f, m)$ математическое ожидание числа областей связности, на которые разбивается множество \mathcal{M} , тогда

$$\lim_{m \rightarrow \infty} \frac{M(f, m)}{\frac{1}{2} \ln m} = 1.$$

2. Обозначим символом $T(f, m)$ математическое ожидание числа терминальных элементов множества \mathcal{M} , тогда

$$\lim_{m \rightarrow \infty} \frac{T(f, m)}{\frac{m}{e}}, \quad \text{где } e = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n$$

основание натурального логарифма.

3. Обозначим символом $S(f, m)$ математическое ожидание числа образов множества \mathcal{M} , то есть элементов, не являющихся терминальными, тогда

$$\lim_{m \rightarrow \infty} \frac{S(f, m)}{\left(\frac{e-1}{e}\right) m} = 1.$$

4. Обозначим символом $\tau(f, m)$ математическое ожидание длины цикла произвольной орбиты множества \mathcal{M} , тогда

$$\lim_{m \rightarrow \infty} \frac{\tau(f, m)}{\sqrt{\frac{\pi m}{8}}} = 1.$$

5. Обозначим символом $\lambda(f, m)$ математическое ожидание длины подхода к циклу произвольной орбиты множества \mathcal{M} , тогда

$$\lim_{m \rightarrow \infty} \frac{\lambda(f, m)}{\sqrt{\frac{\pi m}{8}}} = 1.$$

Проведем эксперимент и применим утверждения теоремы к определенному в примере A.1 отображению f . Легко видеть, что изучаемые нами параметры принимают следующие значения.

1. Согласно утверждению теоремы, математическое ожидание числа компонент связности должно принимать значение $M = \frac{\ln 11}{2} = 1.19$. Точное значение равно двум.
2. Математическое ожидание числа терминальных элементов $T = \frac{11}{e} = 4.04$. Точное значение равно двум.
3. Математическое ожидание длины цикла и длины подхода к циклу равно $\sqrt{\frac{11\pi}{8}} = 2.08$. Точное значение длин подходов равно двум, а средняя длина цикла равна трем с половиной.

Приведенный пример показывает, что утверждения теоремы носят асимптотический характер и при малых значениях m могут не выполняться.

А.2 Алгоритмы поиска циклов

Пусть зафиксированы некоторое отображение $f : \mathcal{M} \rightarrow \mathcal{M}$ и начальный элемент $a \in \mathcal{M}$. Рассмотрим последовательность $\{a_n\}_{n=0}$, определяемую равенствами (A.1)

$$a_0 = a, \quad a_{n+1} = f(a_n), \quad n = 0, 1, \dots$$

Далее мы будем рассматривать задачу определения точного значения длины цикла τ для заданной последовательности $\{a_n\}_{n=0}$.

Известно несколько алгоритмов решения данной задачи. Первый и самый известный алгоритм был предложен в 1968 году Робертом Флойдом (Robert W Floyd), см. [9, п.3.1, задача 6b]. Годом позже Дональдом Кнутом (Donald Knuth) был опубликован, см. [9, п.3.1, задача 7b], алгоритм Ричарда Брента (Richard P. Brent).

Однако наиболее эффективный способ решения поставленной задачи заключается в использовании алгоритма, предложенного в 1972 году Биллом Госпером (Ralph William Gosper, Jr.), см. [1, п.132].

Стоит также отметить еще один алгоритм, который был предложен Габриэлом Нивашем (Gabriel Nivasch) в 2004 году [17] и основан на очень красивой идее поиска минимального элемента, лежащего внутри цикла. Алгоритм имеет сравнимую с методом Госпера трудоемкость и объем используемой памяти. Опишем более подробно перечисленные алгоритмы.

А.2.1 Алгоритм Флойда

Алгоритм Флойда является самым простым и хорошо известным. Он основан на выполнении следующего условия: если выполнено равенство

$$a_n = a_{2n}, \tag{A.3}$$

то величина τ делит n . Для вычисления τ можно использовать следующий алгоритм.

Алгоритм А.1 (Алгоритм Флойда)

Вход: Отображение $f : \mathcal{M} \rightarrow \mathcal{M}$ и начальный элемент a_0 .

Выход: Значение длины цикла τ .

1. Определить начальные значения: $a \leftarrow a_0$ и $b \leftarrow f(a)$.
2. Пока $a \neq b$ выполнять $a = f(a)$, $c = f(b)$ и $b = f(c)$.
3. Определить $b = f(a)$ и $\tau = 1$.
4. Пока $a \neq b$ выполнять $b = f(b)$ и $\tau = \tau + 1$. □

Второй шаг алгоритма выполняется до тех пор, пока не будет найдено равенство (A.3), при этом точное значение индекса n не вычисляется. Поскольку задача поиска всех делителей числа n , в общем случае, является весьма трудоемкой, то, на четвертом шаге алгоритма, мы вычисляем точное значение τ непосредственным перебором.

Легко видеть, что минимально возможное значение индекса n , при котором выполняется равенство $a_n = a_{2n}$, равно $\tau \lceil \frac{\lambda}{\tau} \rceil$. Таким образом трудоемкость алгоритма Флойда равна $\tau (3 \lceil \frac{\lambda}{\tau} \rceil + 1)$ операций вычисления функции f .

A.2.2 Алгоритм Brenta

Прежде чем описывать алгоритм вычисления длины цикла последовательности (A.1), мы докажем теорему, утверждения которой служат его обоснованием. При доказательстве теоремы мы будем следовать идеям, высказанным в монографии [5, п.8.2.2]. Определим функцию целочисленного аргумента

$$l(n) = 2^{\lfloor \log_2 n \rfloor}, \quad n = 1, 2, \dots,$$

которая возвращает максимальное целое число, являющееся степенью двойки и не превосходящее числа n . Из определения функции $l(n)$ следует, что $l(n) \leq n < 2l(n)$. Определим параметр k равенством

$$k = \lceil \log_2 \max\{\lambda + 1, \tau\} \rceil,$$

где τ означает длину цикла, а λ длину подхода к циклу в последовательности, порожденной элементом a_0 . Из определения параметра k следуют неравенства $\tau \leq 2^k$ и $\lambda \leq 2^k - 1$. Определим индекс n_0 равенством

$$n_0 = 2^k + \tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil - 1 \quad (\text{A.4})$$

Теорема A.2. *Выполнены следующие утверждения*

1. Верны неравенства $2^k \leq n_0 < 2^{k+1}$,
2. Для индекса n_0 выполнено равенство $a_{n_0} = a_{l(n_0)-1}$,
3. Выполнено $\frac{3}{2}l(n_0) \leq n_0 < 2l(n_0)$.

Доказательство. Начнем с доказательства первого утверждения теоремы. Поскольку длина цикла τ является целым числом, то $\tau \geq 1$. Поскольку неравенство $\left\lceil \frac{l(\lambda)+1}{\tau} \right\rceil \geq 1$ выполнено по определению, то неравенство $2^k \leq n_0$ очевидно. Для оценки сверху заметим, что нам достаточно показать, что

$$\tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil \leq 2^k,$$

тогда $n_0 \leq 2 \cdot 2^k - 1 < 2^{k+1}$.

1. В начале рассмотрим случай, когда $\tau > l(\lambda)$. Тогда выполнено $\tau \geq l(\lambda) + 1$ и $\frac{l(\lambda)+1}{\tau} \leq 1$. Следовательно

$$\left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil = 1 \quad \text{и} \quad \tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil = \tau \leq 2^k.$$

Последнее неравенство выполнено в силу выбора параметра k .

2. Рассмотрим второй случай $\tau \leq l(\lambda)$. Тогда выполнено

$$\left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil = \frac{l(\lambda) + 1 + \delta}{\tau} \leq \frac{l(\lambda) + \tau}{\tau} \leq \frac{2l(\lambda)}{\tau},$$

при некотором натуральном $\delta < \tau$. Полученное неравенство позволяет записать¹

$$\tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil \leq 2l(\lambda) = 2^{\lceil \log_2 \lambda \rceil + 1} = 2^{\lceil \log_2(\lambda+1) \rceil} \leq 2^k.$$

Мы получили, что для обоих случаев выполнено необходимое неравенство, таким образом первое утверждение теоремы доказано.

Для доказательства второго утверждения теоремы заметим, что из первого утверждения следует

$$k \leq \log_2 n_0 < k + 1 \quad \text{и} \quad l(n_0) = 2^k.$$

Тогда разность $n_0 - (l(n_0) - 1) = \tau \left\lceil \frac{l(\lambda)+1}{\tau} \right\rceil$ кратна длине цикла τ , то есть равенство $a_{n_0} = a_{l(n_0)-1}$ действительно имеет место.

Нам осталось доказать последнее утверждение теоремы. Оценка сверху тривиально вытекает из определения функции $l(n)$. Для получения нижней оценки заметим справедливость неравенств

¹Мы пользуемся равенством $\lceil \log_2 \lambda \rceil + 1 = \lceil \log_2(\lambda + 1) \rceil$, которое выполнено при натуральных значениях λ .

$$\tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil - 1 \geq \tau - 1 = 2^{\log_2 \tau} - 1 \geq 2^{\lceil \log_2 \tau \rceil - 1} \quad (\text{A.5})$$

$$\tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil - 1 \geq l(\lambda) = 2^{\lceil \log_2 \lambda + 1 \rceil - 1}. \quad (\text{A.6})$$

Следовательно, выполнено неравенство $\tau \left\lceil \frac{l(\lambda)+1}{\tau} \right\rceil - 1 \geq 2^{k-1}$, откуда следует

$$n_0 = 2^k + \tau \left\lceil \frac{l(\lambda) + 1}{\tau} \right\rceil - 1 \geq 2^k + 2^{k-1} = \frac{3l(n_0)}{2}$$

и доказательство последнего утверждения теоремы. \square

Доказанная нами теорема в явном виде задает значение индекса n_0 которое необходимо вычислить для определения длины цикла. К сожалению, на практике, нам неизвестно значение n_0 .

Основываясь на утверждениях доказанной теоремы, Brent предложил следующую идею: для поиска значения, кратного величине τ , нам необходимо воспользоваться тем фактом, что $a_{n_0} = a_{2^k-1}$ при некотором натуральном значении k таком, что $3 \cdot 2^{k-1} \leq n_0 < 2^{k+1}$.

Алгоритм А.2 (Алгоритм Брента)

Вход: Отображение $f : \mathcal{M} \rightarrow \mathcal{M}$ и начальный элемент a_0 .

Выход: Значение длины цикла τ .

1. Определить начальные значения: $c = a_0$, $a = f(a_0)$, $n = 1$ и $t = 1$.
2. **Если** $a = c$, **то** вернуть значение $\tau = 1$ и завершить алгоритм.
3. **Если** $n = t$, **то** положить $c = a$ и вычислить $t = 2t$.
4. Определить $a = f(a)$ и вычислить $n = n + 1$.
5. **Если** $n \geq 3t/4$, **то** проверить выполняется, ли равенство $a = c$. Если нет, то вернуться на шаг 3.
6. Определить $\tau = 1$ и $a = f(c)$.
7. **Пока** $a \neq c$ **выполнять** $a = f(a)$ и $\tau = \tau + 1$. \square

Алгоритм Брента, как и алгоритм Флойда, не позволяет в явном виде определить значение длины цикла τ . На пятом шаге приведенного алгоритма мы находим совпадение $a_{n_0} = a_{2^k-1}$ для некоторого натурального числа k . Последние два шага приведенного алгоритма позволяют определить значение τ в явном виде. Как и ранее, мы не вычисляем значение $n_0 + 1 - 2^k$, кратное величине τ , а находим искомую величину простым перебором.

Для оценки трудоемкости алгоритма Брента заметим, что из третьего утверждения теоремы А.2 и определения величины k следует оценка

снизу

$$n_0 \geq \frac{3l(n_0)}{2} = \frac{3}{2} \cdot 2^k \geq \frac{3}{2} \max\{\lambda + 1, \tau\},$$

для числа шагов, необходимых для поиска совпадения на пятом шаге алгоритма. Таким образом, общая трудоемкость алгоритма Brenta составит не менее $\tau + \frac{3}{2} \max\{\lambda + 1, \tau\}$ операций вычисления функции f .

А.2.3 Алгоритм Госпера

Пусть $n > 0$ натуральное число. Для описания алгоритма нам потребуется определить множество $M(n)$, элементами которого являются целые числа $n_{k,h}$, удовлетворяющие условиям

$$\begin{cases} n_{k,h} = 2^k - 1 + h2^{k+1}, & k = 0, 1, \dots \\ n_{k,h} < n \leq n_{k,h+1}, \end{cases} \quad (\text{A.7})$$

при неотрицательных целых значениях параметров k, h . Очевидно, что при фиксированном n , множество $M(n)$ конечно и содержит не более $\lceil \log_2 n \rceil + 1$ чисел. Например, для $n = 16$ множество $M(16)$ имеет вид

$$M(16) = \{n_{0,7} = 14, n_{1,3} = 13, n_{2,1} = 11, n_{3,0} = 7, n_{4,0} = 15\}.$$

Теорема А.3. Пусть параметры λ и τ определяют длину подхода к циклу и длину цикла последовательности (A.1). Тогда найдутся натуральные индексы r и $n = r + \tau$ такие, что

1. r принадлежит множеству $M(n)$,
2. $\lambda + \tau \leq n < \lambda + 2\tau$.

Доказательство. Определим параметр k как наименьшее целое число, удовлетворяющее неравенствам $2^k \leq \tau < 2^{k+1}$ и рассмотрим целые числа

$$r = 2^k \left\lceil \frac{\lambda + 1}{2^k} \right\rceil - 1 \quad \text{и} \quad n = r + \tau.$$

Очевидно, что $r < n$ для любого целого $\tau \geq 1$. Представим $\lceil \frac{\lambda+1}{2^k} \rceil = 2^l s$, где $l \geq 0$ целое число и $s = 2h + 1$ нечетное целое число. Тогда r имеет вид

$$r = 2^{k+l} s - 1 = 2^{k+l} (2h + 1) - 1 = 2^{k+l} - 1 + h2^{k+l+1}.$$

Поскольку выполнено неравенство

$$r + 2^{k+l+1} \geq r + 2^{k+1} > r + \tau = n$$

мы получаем, что индекс r принадлежит множеству $M(n)$. Первое утверждение теоремы доказано.

Для доказательства второго утверждения теоремы получим оценки снизу и сверху на величину r . Воспользовавшись неравенством

$$x \leq [x] < x + 1,$$

выполненным для любого действительного $x > 0$, получим

$$\begin{aligned} \lambda = 2^k \left(\frac{\lambda + 1}{2^k} \right) - 1 &\leq 2^k \left[\frac{\lambda + 1}{2^k} \right] - 1 = r \\ &< 2^k \left(\frac{\lambda + 1}{2^k} + 1 \right) - 1 = \lambda + 2^k \leq \lambda + \tau, \end{aligned}$$

то есть неравенство $\lambda \leq r < \lambda + \tau$, из которого следует утверждение теоремы. \square

При поиске длины цикла последовательности (A.1) утверждение теоремы в явном виде задает нам множество индексов $M(n)$ среди которых необходимо искать индекс r такой, что $a_r = a_n$. Более того, теорема позволяет получить оценку сверху на максимальное число элементов последовательности (A.1), которые необходимо вычислить для нахождения указанного равенства.

Для реализации алгоритма Госпера нам потребуется массив T из $[\log_2 m] + 1$ элементов множества \mathcal{M} , в котором мы будем хранить элементы последовательности (A.1) с индексами из множества $M(n)$, а также функция² натурального аргумента x , определяемая следующим образом

$$\text{ntz}(x) = k, \quad \text{если} \quad \begin{cases} x \equiv 0 \pmod{2^k}, \\ x \not\equiv 0 \pmod{2^{k+1}}. \end{cases}$$

Мы используем значение функции $\text{ntz}(n + 1)$ для того, чтобы узнать индекс элемента a_n (значение параметра k) в массиве T .

²В работе [1] Госпер называет эту функцию — функцией «линейки».

Алгоритм А.3 (Алгоритм Госпера)

Вход: Отображение $f : \mathcal{M} \rightarrow \mathcal{M}$ и начальный элемент a_0 .

Выход: Значение длины цикла τ .

1. Определить начальные значения: $a = a_0$, $n = 1$, $t = 1$ и $T[0] = a_0$.
2. Вычислить $a = f(a)$.
3. Для всех k от 0 до $t - 1$ выполнить
 - 3.1. Если $T[k] = a$, то положить $\tau = n - 2^k \left(1 + \left\lfloor \frac{n - 2^k + 1}{2^k} \right\rfloor \right) + 1$ и завершить алгоритм.
4. Вычислить $n = n + 1$ и $k = \text{ntz}(n)$.
5. Если $k = t$, то вычислить $t = t + 1$.
6. Определить $T[k] = a$ и вернуться на шаг 2. □

На четвертом шаге приведенного алгоритма мы определяем значение длины цикла τ , которое в явном виде нам неизвестно, но может быть вычислено с использованием значений k и n . Действительно, из (A.7) следует, что величина $h = \left\lfloor \frac{n - (2^k - 1)}{2^{k+1}} \right\rfloor$, величина $r = 2^k - 1 + h2^{k+1}$. Поскольку $\tau = n - r$, то мы получаем равенство, приведенное выше.

Как следует из утверждения теоремы A.3, алгоритму потребуется не более $\lambda + 2\tau$ операций вычисления функции f для нахождения длины цикла τ .

A.2.4 Алгоритм Ниваша

Алгоритм Ниваша основан на очень простой идее. Пусть на множестве \mathcal{M} задано отношение упорядоченности, то есть для любых двух элементов $a, b \in \mathcal{M}$ определена функция $h : \mathcal{M} \times \mathcal{M} \rightarrow \{-1, 0, 1\}$ такая, что

$$h(a, b) = \begin{cases} -1, & \text{если } a < b, \\ 0, & \text{если } a = b, \\ 1, & \text{если } a > b. \end{cases}$$

В этом случае, в цикле последовательности (A.1) может быть определен наименьший элемент a_l такой, что $h(a_l, a_n) = -1$ для всех индексов $n = \lambda, \dots, \lambda + \tau - 1$ при $n \neq l$. Идея Ниваша заключается в том, что минимальный элемент может быть определен при первом проходе цикла, тогда на втором проходе цикла будет найдено совпадение.

Для реализации поиска минимального элемента нам потребуется массив T , элементами которого будут являться пары (a_n, n) содержащие значение элемента последовательности и его индекс. Мы будем обозначать символом $T[i].a$ значение элемента последовательности, содержащееся в

i -й ячейке массива, аналогично $T[i].n$ будет означать индекс сохраненного в ячейке элемента последовательности.

Алгоритм А.4 (Алгоритм Ниваша)

Вход: Отображение $f : \mathcal{M} \rightarrow \mathcal{M}$ и начальный элемент a_0 .

Выход: Значение длины цикла τ .

1. Определить значения $a = a_0$, $n = 0$, $k = 1$ и $T[0] = (a_0, 0)$.
2. Определить $a = f(a)$, $n = n + 1$ и $i = k$.
3. **Пока** ($i \geq 0$ и $h(a, T[i].a) = -1$) **выполнять** $i = i - 1$.
4. **Если** $h(a, T[i].a) = 0$, **то** определить $\tau = n - T[i].n$ и завершить алгоритм.
5. **Если** $h(a, T[i].a) = 1$, **то** определить новое значение $T[i+1].a = a$, $T[i+1].n = n$ и $k = i + 2$.
6. Вернуться на шаг 2. □

Легко видеть, что количество вычислений функции f в приведенном алгоритме не превышает величины $\lambda + 2\tau$, то есть длины подхода и двух циклов последовательности (A.1). Массив T реализует собой стек, в котором хранятся элементы последовательности, отсортированные по возрастанию. Каждый новый вырабатываемый элемент a помещается в стек. Если в нем есть элементы, большие чем a , то они удаляются.

Если предположить, что элементы последовательности (A.1) являются реализацией некоторой случайной, равномерно распределенной на множестве \mathcal{M} величины, то, как показано в [8, п.1.2.10], с ростом индекса n размер стека растет как величина порядка $O(\log_2 n)$. Таким образом, мы можем считать, что величина стека в алгоритме Ниваша составляет $\lceil \log_2(\lambda + 2\tau) \rceil$ элементов, каждый из которых хранит элемент последовательности (A.1) и его индекс.

Для сравнения, сведем в одну таблицу различные характеристики описанных нами выше алгоритмов. Во второй колонке мы приводим оценку трудоемкости алгоритма, измеряемую в количестве вычислений функции f . В третьей колонке содержится количество ячеек памяти, необходимых для вычисления длины цикла τ .

Алгоритм	Трудоемкость	Объем памяти
Флойд	$\tau \left(3 \left\lceil \frac{\lambda}{\tau} \right\rceil + 1 \right)$	3
Брент	не менее $\tau + \frac{3}{2} \max\{\lambda + 1, \tau\}$	4
Госпер	не более $\lambda + 2\tau$	$\lceil \log_2 m \rceil + 4$
Ниваш	не более $\lambda + 2\tau$	$2 \lceil \log_2(\lambda + 2\tau) \rceil$

СПИСОК ЛИТЕРАТУРЫ

- [1] *Beeler M., Gosper R., Schroepfel R.* HACKMEM: Tech. Rep. AIM 239: MTI, 1972.
- [2] *Brent R. P.* An improved monte-carlo factorization algorithm // *BIT*. — 1980. — Vol. 20. — Pp. 176–184.
- [3] *Brillhart M. M. . J.* A method of factoring and the factorization of f_7 . // *Mathematics Of Computation*. — 1975. — Vol. 29. — Pp. 183–205.
- [4] *Carmichael R.* The Theory Of Numbers. — New York: J. Willey & Sons, 1914. — P. 95.
- [5] *Cohen H.* A Course In Computational Algebraic Number Theory. — 3rd edition. — New York: Springer, 1996. — P. 545.
- [6] *Garner H.* The residue number system // *IRE Transactions on Electronic Computers*. — 1957. — Vol. EC-8, no. 2. — Pp. 140–147.
- [7] *Gordon J.* Strong RSA keys // *Electronic Letters*. — 1984. — Vol. 20, no. 12. — Pp. 514–516. — June 1984.
- [8] *Knuth D. E.* Fundamental Algorithms. — Addison-Wesley Professional, 1969. — Vol. 1 of *The Art of Computer Programming*.
- [9] *Knuth D. E.* Seminumerical Algorithms. — Addison-Wesley Professional, 1969. — Vol. 2 of *The Art of Computer Programming*.
- [10] *Kraitchik M.* Théorie des Nombres. Tome I et II. — Paris: Gauthier-Villars, 1926.
- [11] *Lehman S.* Factoring large integers // *Mathematics Of Computation*. — 1974. — Vol. 28, no. 126. — Pp. 637–646.
- [12] *Lehmer D., Powers R.* On factoring large numbers // *Bulletin Of the American Mathematical Society*. — 1931. — Vol. 37, no. 9. — Pp. 770–776.
- [13] *McKee J.* Speeding fermat’s factoring algorithm // *Mathematics Of Computation*. — 1999. — Vol. 68, no. 228. — Pp. 1729–1737.

- [14] *Mihailescu P.* Fast generation of provable primes using search in arithmetic progressions // *Advances in Cryptology – CRYPTO '94.* — Vol. 839 Of Lecture Notes Of Computer Science. — Springer, 94. — Pp. 282–293.
- [15] *Miller G.* Riemann's hypothesis and tests for primality // *Journal of Computer and System Sciences.* — 1976. — Vol. 13, no. 3. — Pp. 300–317.
- [16] *Montgomery P.* Speeding the Pollard and elliptic curve methods of factorization // *Mathematics Of Computation.* — 1987. — Vol. 48. — Pp. 243–264.
- [17] *Nivash G.* Cycle detecting using a stack // *Journal Information Processing Letters.* — 2004. — Vol. 90.
- [18] *Pollard J.* Theorems on factorization and primality testing // *Proceedings of the Cambridge Cambridge Philosophical Society.* — 1974. — Vol. 76. — Pp. 521–528.
- [19] *Rabin M.* Probabilistic algorithm for testing primality // *Journal of Number Theory.* — 1980. — Vol. 12, no. 1. — Pp. 128–138.
- [20] *Solovay R., Strassen V.* A fast monte-carlo test for primality // *SIAM Journal on Computing.* — 1977. — Vol. 6, no. 1. — Pp. 84–85.
- [21] *Williams H.* Primality testing on a computer // *Ars Combinatoria.* — 1978. — Vol. 5. — Pp. 127–185.
- [22] *Williams H.* A $p + 1$ method of factoring // *Mathematics Of Computation.* — 1982. — Vol. 39, no. 159. — Pp. 225–234.
- [23] *Williams H., Schmid B.* Some remarks cocerning the MIT public-key cryptosystem // *BIT.* — 1979. — Vol. 19. — Pp. 525–538.
- [24] *Zhang Z.* Using Lucas sequences to factor large integers near group orders // *Fibonacci Quarterly.* — 2001. — Vol. 39. — Pp. 228–237.
- [25] *Галочкин А., Нестеренко Ю., Шидловский А.* Введение в теорию чисел. — М.: Изд-во Московского Университета, 1984. — С. 152.
- [26] *Гашков С.* Упрощенное обоснование вероятностного теста Миллера-Рабина для проверки простоты чисел // *Дискретная математика.* — 1998. — Т. 10, № 4. — С. 35–38.

-
- [27] *Кострикин А.* Введение в алгебру. — М.: Наука, 1977. — С. 495.
- [28] *Нестеренко Ю.* Теория чисел. — М.: Издательский дом «Академия», 2008. — С. 272.
- [29] *Прахар К.* Распределение простых чисел. — М.: Мир, 1967. — С. 512.
- [30] *Сушкевич А.* Теория чисел. Элементарный курс. — Харьков: Изд-во Харьковского университета, 1954.

ИНДЕКСНЫЙ УКАЗАТЕЛЬ

алгоритм

Эвклида, 8, 113

для многочленов, 39

расширенный, 18

Гарнера, 22

Тонелли-Шенкса, 68

бинарный НОД, 10

деления многочленов, 37

доказательства простоты

Лемана, 142

Люка, 90

факторизации

ρ -метод Полларда, 145

$p - 1$ Полларда, 147

Брента, 146

Ферма, 134

Крайчика, 164

Лемана, 142

Полларда-Флойда, 145, 154

Вильямса, 149

с помощью непрерывных дробей,
165

поиска длин циклов

Брента, 180

Флойда, 177

Госпера, 183

Ниваша, 184

построения

простого числа, 105

сильно простого числа, 108

таблицы простых чисел, 80

решения

системы сравнений, 20

вычисления

квадратного корня, 135

первообразного корня, 30

последовательности Люка, 99

символа Якоби, 63

случайного корня многочлена, 73

всех корней многочлена, 75

целая часть, 111

частные

неполные, 112

полные, 112

число

Кармайкла, 81

простое, 11

составное, 12

взаимно простое, 6

делитель

наибольший общий (НОД), 6

многочленов, 38

дискриминант

иррациональности

квадратичной, 119

длина

цикла, 144, 174

подхода к циклу, 144, 174

дробь

цепная, 112

непрерывная, 112

подходящая, 114

элемент

обратимый, 33

образ, 175

примитивный, 26

терминальный, 174

факторная база, 169

функция

Эйлера, 22, 139

группа

аддитивная, 30

мультипликативная, 30

обратимых элементов, 34

иррациональность

действительная, 113

квадратичная, 119

приведенная, 123

сопряженная, 120

коллизия, 173

компонента

связная, 175

корень

многочлена, 41

первообразный, 26

кратное

наименьшее

общее (НОК), 28

- кратность
 - корня, [42](#)
- критерий
 - Эйлера, [53](#)
- квадрат
 - полный, [119](#)
- лемма
 - Безу, [17](#)
 - для многочленов, [40](#)
 - Гаусса, [55](#)
 - Гордона, [109](#)
 - Макки, [158](#)
 - о факторизации, [163](#)
- многочлен, [34](#)
 - линейный, [35](#)
 - неприводимый, [36](#)
 - нормированный, [35](#)
 - приведенный, [35](#)
 - унитарный, [35](#)
- наилучшее приближение, [129](#)
- невычет
 - квадратичный, [52](#)
- нуль
 - многочлена, [41](#)
- область связности, [175](#)
- орбита
 - элемента, [173](#)
- период, [174](#)
- подход
 - к циклу, [174](#)
- показатель
 - числа, [25](#)
- порядок
 - элемента, [26](#)
- последовательность
 - рекуррентная
 - Фибоначи, [9](#)
 - Люка, [95](#), [148](#)
- производная
 - многочлена, [43](#)
- символ
 - Лежандра, [52](#)
 - Якоби, [60](#)
- система вычетов
 - абсолютно-наименьших
 - полная, [16](#)
 - полная, [16](#)
 - приведенная, [22](#)
- степень
 - многочлена, [35](#)
- теорема
 - Дирихле, [103](#)
 - Эйлера, [24](#)
 - Эвклида, [12](#)
 - Ферма, [24](#)
 - Кармайкла, [81](#)
 - Ламе, [9](#)
 - Лемана, [140](#)
 - Лемера, [92](#)
 - Люка, [90](#)
 - Моррисона, [101](#)
 - Поклингтона, [92](#)
 - Рабина, [85](#)
 - Виета, [121](#)
 - арифметики основная, [13](#)
 - для многочленов, [40](#)
 - китайская
 - об остатках, [19](#)
 - о полном квадрате, [136](#)
- тест
 - Миллера-Рабина, [89](#)
 - Соловея-Штрассена, [84](#)
- вычет
 - абсолютно-наименьший, [16](#)
 - квадратичный, [52](#)
 - наименьший
 - неотрицательный, [15](#)
- задача
 - факторизации, [133](#)
 - поиска длины цикла, [177](#)
- закон
 - взаимности
 - квадратичный, [54](#)
- значение
 - многочлена, [35](#)