Министерство образования и науки Российской Федерации
Южно-Уральский государственный университет
Кафедра прикладной математики

511(07)
Э157

А. Ю. Эвнин

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Учебное пособие

2-е издание, переработанное и дополненное

Челябинск
Издательский центр ЮУрГУ
2015

УДК 511(075.8)
Э157

Одобрено учебно-методической комиссией
факультета Математики, механики и компьютерных наук

Рецензенты:
доктор физ.-мат. наук *С. М. Воронин,* ЧелГУ,
доктор физ.-мат. наук *Н. Н. Осипов,* СибФУ (Красноярск)

Эвнин, А. Ю.

Э157 Элементы теории чисел: учебное пособие. – 2-е изд., перераб. и доп. / А. Ю. Эвнин. – Челябинск: Издательский центр ЮУрГУ, 2015. – 93 с.

Учебное пособие предназначно для студентов направлений «Математика и компьютерные науки», «Прикладная математика» и «Прикладная математика и информатика».

В пособии излагаются как традиционные темы теории чисел, так и вопросы, которые могут изучаться на факультативных занятиях и спецкурсах. Затронуты вопросы применения теории чисел в криптографии.

УДК 519.1(075.8)+511(075.8)

Предисловие

Учебное пособие предназначно для студентов направлений «Математика и компьютерные науки», «Прикладная математика» и «Прикладная математика и информатика».

В пособии излагаются как традиционные темы теории чисел (теорема о делении с остатком; алгоритм Евклида; основная теорема арифметики; сравнения по модулю; теорема Эйлера и малая теорема Ферма; линейные диофантовы уравнения с двумя переменным; квадратичные вычеты; дискретное логарифмирование), так и вопросы, которые могут служить темой изучения на факультативных занятиях и спецкурсах (уравнения Пелля, цепные дроби и наилучшие приближения иррациональных чисел; группа мультипликативных функций, формула обращения Мёбиуса и её применение к задаче о числе ожерелий; система криптографии с открытым ключом, тесты Люка – Лемера и Миллера – Рабина).

Объём пособия по сравнению с первым изданием увеличился более чем вдвое. По-новому излагается доказательство существования фундаментального решения уравнения Пелля (методом Вайлдбергера). Выведены явные формулы решения уравнения Пелля. Добавлены классические сюжеты про представимость чисел в виде суммы двух и четырёх квадратов. Затронуты вопросы применения теории чисел в криптографии.

Автор выражает особую благодарность рецензентам Николаю Николаевичу Осипову и Сергею Михайловичу Воронину за ценные замечания и предложения по тексту учебного пособия.

1. Теорема о делении с остатком

Пусть a и b — целые числа. Если существует такое целое число q, что $a = bq$, то говорят:

- *a делится на b*;
- *a кратно b*;
- *b делит a*;
- *b — делитель a*;

при этом пользуются обозначениями $a \vdots b$ или $b \mid a$.

Теорема 1.1. [Теорема о делении с остатком]
Пусть a — целое число, b — натуральное число. Тогда существуют единственные целые числа q и r такие, что $a = bq + r$, $0 \leqslant r < b$.

Доказательство. *Существование.* Пусть bq — наибольшее из чисел, кратных b и не превосходящих a. Тогда выполняется двойное неравенство $bq \leqslant a < b(q+1)$, а, значит, и $0 \leqslant a - bq < b$. Теперь если положить $r = a - bq$, то одновременно будем иметь:

$$a = bq + r, \;\; 0 \leqslant r < b.$$

Единственность. Пусть $a = bq_1 + r_1$ и $a = bq_2 + r_2$. Вычитая из первого равенства второе, получаем: $0 = b(q_1 - q_2) + r_1 - r_2$, или $b(q_1 - q_2) = r_2 - r_1$, откуда следует, что $r_1 - r_2$ делится на b. С другой стороны, из неравенств $0 \leqslant r_1 < b$ и $0 \leqslant r_2 < b$ вытекает неравенство $|r_1 - r_2| < b$. Сопоставляя два полученных факта, заключаем, что $r_1 = r_2$. Тогда $b(q_1 - q_2) = 0$, и так как $b \neq 0$ (b — *натуральное* число), приходим к равенству $q_1 = q_2$. Итак, любые два представления числа a в виде $a = bq + r$ совпадают. Единственность доказана. □

Замечание. Числа q и r из формулировки доказанной теоремы называют соответственно *частным* и *остатком от деления* a на b.

2. Наибольший общий делитель. Алгоритм Евклида

В этом параграфе все числа предполагаются натуральными.

Обозначим через $D(a)$ множество всех делителей числа a, а через $D(a_1, a_2, \ldots, a_n)$ — множество всех общих делителей чисел $a_1, a_2, \ldots, a_n$. Таким образом,

$$D(a_1, a_2, \ldots, a_n) = \bigcap_{i=1}^{n} D(a_i).$$

Заметим, что это множество конечно и не пусто (по крайней мере, оно содержит 1), поэтому в нем есть наибольший элемент, который будем обозначать $(a_1, a_2, \ldots a_n)$ и называть *наибольшим общим делителем* чисел $a_1, a_2, \ldots, a_n$.

Натуральные числа a и b называются *взаимно простыми,* если их наибольший общий делитель равен 1. Очевидно следующее утверждение.

Лемма 2.1. $a \vdots b \Leftrightarrow (a, b) = b.$

Лемма 2.2. *Пусть* $a = bq + r,\ 0 < r < b$. *Тогда* $(a, b) = (b, r)$.

Доказательство. Возьмём произвольный элемент $x \in D(a, b)$. Тогда $a \vdots x,\ b \vdots x$ и $r = a - bq \vdots x$. Таким образом, $x \in D(b, r)$.

Пусть теперь $x \in D(b, r)$. Тогда $b \vdots x, r \vdots x$ и $a = bq + r \vdots x$. Таким образом, $x \in D(a, b)$.

Доказано равенство множеств $D(b, r) = D(a, b)$, а, значит, и их максимальных элементов. Поэтому $(b, r) = (a, b)$. □

Пусть a не делится на b. Тогда имеет место представление a в виде $a = bq_0 + r_1,\ 0 < r_1 < b$. По лемме 2.2 $(a, b) = (b, r_1)$. Если b не делится на r_1, то имеем: $b = r_1 q_1 + r_2,\ 0 < r_2 < r_1$ и $(b, r_1) = (r_1, r_2)$. Продолжив данный процесс (а он называется *алгоритмом Евклида*), получим последовательность остатков (r_i), это — убывающая последовательность натуральных чисел. Она не может быть бесконечной, поэтому некоторый остаток r_n будет делителем предыдущего остатка r_{n-1}. Итак, выполняются следующие соотношения:

$$a = bq_0 + r_1,\ 0 < r_1 < b; \quad (a, b) = (b, r_1);$$

$$b = r_1 q_1 + r_2,\ 0 < r_2 < r_1; \quad (b, r_1) = (r_1, r_2);$$

$$r_1 = r_2 q_2 + r_3,\ 0 < r_3 < r_2; \quad (r_1, r_2) = (r_2, r_3);$$

$$\ldots$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n,\ 0 < r_n < r_{n-1};\ \ (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n);$$
$$r_{n-1} = r_n q_n;\ \ (r_{n-1}, r_n) = r_n.$$

(Последнее равенство справедливо в силу леммы 2.1).

Цепочка равенств

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n$$

доказывает следующую теорему.

Теорема 2.1. *Наибольший общий делитель двух чисел равен последнему ненулевому остатку в алгоритме Евклида, применённому к данным числам.*

Пример. Для нахождения (288,126) применим алгоритм Евклида к числам 288 и 126:

		288	126
	126	36	2
36	18	3	
0	2		

Последний ненулевой остаток равен 18; поэтому (288,126)=18.

Теорема 2.2. *Наибольший общий делитель двух чисел делится на любой из общих делителей этих чисел.*

Доказательство. Пусть $a \vdots x,\ b \vdots x$; $r_1, \ldots, r_n$ — остатки, возникающие при работе алгоритма Евклида. Тогда

$$r_1 = (a - bq_0) \vdots x,\ r_2 = (b - r_1 q_1) \vdots x,\ \ldots,\ r_n = (r_{n-2} - r_{n-1}q_{n-1}) \vdots x.$$

В силу предыдущей теоремы $r_n = (a, b)$. Таким образом, $(a, b) \vdots x$, что и требовалось доказать. □

Свойства наибольшего общего делителя

1. $(a, b) = (b, a)$.
2. $(ma, mb) = m(a, b)$.

   Доказательство. Все равенства, возникающие при работе алгоритма Евклида, почленно умножаются на m при переходе от пары $\langle a, b\rangle$ к паре $\langle ma, mb\rangle$. □

3. *Если a и b взаимно просты, то $(ac, b) = (c, b)$.*

   Доказательство. Пусть $x \in D(ac, b)$. Тогда $ac \vdots x, b \vdots x, bc \vdots x$, т. е. $x \in D(ac, bc)$. По теореме 2.2 $(ac, bc) \vdots x$, и, в силу предыдущего свойства, $c(a, b) \vdots x$, но по условию $(a, b) = 1$. Таким образом, $c \vdots x$ и $x \in D(b, c)$. Пусть теперь $x \in D(b, c)$. Тогда $b \vdots x, c \vdots x, ac \vdots x$ и $x \in D(ac, b)$. Доказано, что $D(ac, b) = D(c, b)$, откуда следует требуемое. □

4. *Если числа a_1 и a_2 взаимно просты с b, то тем же свойством обладает и их произведение, т. е.*
   $(a_1, b) = 1, (a_2, b) = 1 \Rightarrow (a_1 a_2, b) = 1$.

   Это свойство вытекает из предыдущего.

5. *Пусть для $i = 1, 2, \ldots, n$ $(a_i, b) = 1$. Тогда* $\left(\prod\limits_{i=1}^{n} a_i, b\right) = 1$.

   Свойство легко доказать индукцией по n с помощью предыдущего свойства.

6. *Если $\forall i, j$ $(a_i, b_j) = 1$, то* $(\prod a_i, \prod b_j) = 1$.

   Следует из свойств 1 и 5.

7. $(a_1, a_2, \ldots, a_n) = ((\ldots((a_1, a_2), a_3), \ldots), a_n)$.

   Для доказательства достаточно использовать соотношение $D(a_1, a_2, \ldots, a_n) = D(a_1) \cap D(a_2) \cap \ldots \cap D(a_n)$ и свойство ассоциативности пересечения множеств.

3. $(k^a - 1, k^b - 1) = k^{(a,b)} - 1$

Вновь все числа, рассматриваемые в этом параграфе, предполагаются натуральными.

Пусть $k \geqslant 2$. Докажем справедливость формулы, вынесенной в заголовок параграфа.

Доказательство. Рассмотрим сначала случай, когда a кратно b. Имеем при этом $a = bq$ и $(a, b) = b$ (по лемме 2.1). Доказываемое равенство приобретает вид $(k^a - 1, k^b - 1) = k^b - 1$ и равносильно тому,

что $k^a - 1$ кратно $k^b - 1$.
С помощью алгебраического тождества

$$y^n - 1 = (y-1)(y^{n-1} + y^{n-2} + \ldots + y + 1)$$

получаем, что $k^a - 1 = k^{bq} - 1 = (k^b)^q - 1$ делится на $k^b - 1$.

Пусть теперь a не делится на b, т. е. $a = bq + r,\ 0 < r < b$. Имеем: $k^a - 1 = k^{bq+r} - 1 = k^r(k^{bq} - 1) + k^r - 1$. Как показано выше, $k^{bq} - 1$ делится на $k^b - 1$. Кроме того, $0 < k^r - 1 < k^b - 1$. Таким образом, остаток от деления $k^a - 1$ на $k^b - 1$ равен $k^r - 1$. Поэтому по лемме 2.2

$$(k^a - 1, k^b - 1) = (k^b - 1, k^r - 1).$$

Используя соотношения алгоритма Евклида

$$a = bq_0 + r_1, b = r_1q_1 + r_2, r_1 = r_2q_2 + r_3, \ldots,$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n, r_{n-1} = q_nr_n,$$

получаем цепочку равенств

$$(k^a - 1, k^b - 1) = (k^b - 1, k^{r_1} - 1) = (k^{r_1} - 1, k^{r_2} - 1) =$$

$$= \ldots = (k^{r_{n-1}} - 1, k^{r_n} - 1) = k^{r_n} - 1 = k^{(a,b)} - 1.$$

Таким образом, $(k^a - 1, k^b - 1) = k^{(a,b)} - 1$. □

Пример. $(288, 216) = 18 \Rightarrow (3^{288} - 1, 3^{126} - 1) = 3^{18} - 1$.

Важным следствием доказанного соотношения является следующее утверждение.

Если m и n взаимно просты, то взаимно простыми будут и числа $2^m - 1$ и $2^n - 1$.

Действительно,

$$(m, n) = 1 \Rightarrow (2^m - 1, 2^n - 1) = 2^{(m,n)} - 1 = 2^1 - 1 = 1.$$

4. Простые числа. Основная теорема арифметики

Натуральное число, большее 1, называется *простым*, если оно имеет ровно два делителя — 1 и само себя.

Натуральное число, большее 1, не являющееся простым, называется *составным*.

1 не является ни простым, ни составным числом.

Отметим, что число является простым тогда и только тогда, когда оно взаимно просто со всеми меньшими натуральными числами.

Теорема 4.1. *Множество простых чисел бесконечно.*

Доказательство. Предположим, что $F = \{n_1, n_2, \ldots, n_k\}$ — множество *всех* простых чисел ($n_1 = 2$, $n_2 = 3$, $n_3 = 5, \ldots$). Очевидно, что числа из F попарно взаимно просты; в силу последнего утверждения предыдущего параграфа при $i \neq j$ числа $2^{n_i} - 1$ и $2^{n_j} - 1$ также взаимно просты. Выберем теперь для каждого $i = 1, 2, ..., k$ какой-нибудь *простой* делитель p_i числа $2^{n_i} - 1$; числа $p_1, p_2, \ldots, p_k$ будут попарно различны. В результате образуется множество $G = \{p_1, p_2, \ldots, p_k\}$ простых чисел ($p_1 = 3, \quad p_2 = 7, \quad p_3 = 31, \ldots$). Все элементы G — суть *нечётные* числа. Поскольку множества F и G содержат поровну элементов, $2 \in F$ и $2 \notin G$, делаем вывод, что в G найдётся число, не входящее в F. Пришли к противоречию. Теорема доказана. □

Замечание. Классическое доказательство теоремы 4.1 состоит в следующем. Предполагая, что $A = \{p_1, p_2, \ldots, p_n\}$ — множество всех простых чисел, рассмотрим число $P = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Оно больше единицы, у него есть простой делитель, и этот делитель не входит в множество A. Противоречие!

С другими доказательствами данной теоремы можно познакомиться, прочитав статью [15].

Упражнение 1. Докажите, что множество простых чисел вида $4k + 3$ бесконечно.

Указание. Пусть $p_1 = 3$, $p_2 = 7$, $p_3 = 11$, $p_4 = 19$, ..., p_n — все простые числа вида $4k + 3$. Рассмотрите число $P = 4p_2p_3 \ldots p_n + 3$.

Теорема 4.2. [Основная теорема арифметики]
Любое натуральное число, большее 1, представимо в виде произведения простых чисел. Такое представление единственно с точностью до порядка сомножителей.

Доказательство. Существование и единственность указанного представления для простых чисел очевидно. Доказательство теоремы для составных чисел проводится методом математической индукции.

Пусть a — составное число. Предположим, что все натуральные числа от 2 до $a-1$ раскладываются, и при том единственным образом, в произведение простых чисел.

Докажем *существование* соответствующего разложения и для a. Наименьший делитель a, больший 1, обозначим p. Очевидно, p — простое число. Для некоторого натурального числа a_1 имеем $a = a_1 \cdot p$, причем $a_1 < a$. По предположению индукции a_1 раскладывается на простые множители, поэтому тем же свойством обладает и число a.

Единственность. Пусть существует два разложения составного числа a на простые множители:

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_m. \qquad (1)$$

Если $p_i \neq q_j$ для всех i и j, то имеем $\forall i, j \;\; (p_i, q_j) = 1$ и по свойству 6 из § 2

$$a = (a, a) = (p_1 \cdot p_2 \cdot \ldots \cdot p_n, q_1 \cdot q_2 \cdot \ldots \cdot q_m) = 1,$$

что противоречит неравенству $a > 1$. Значит, для некоторых i и j выполняется $p_i = q_j$. Пусть $a = a_1 \cdot p_i$. Сокращая части равенства (1) на общий множитель $p_i = q_j$, получим два разложения для числа a_1. Поскольку $a_1 < a$, эти разложения совпадают. Отсюда следует и единственность представления числа a в виде произведения простых чисел. Теорема доказана. □

Представление натурального числа в виде $a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$, где $p_1, p_2, \ldots, p_r$ — попарно различные простые числа, называют *каноническим разложением* числа a.

5. Сравнения и их свойства

В этом параграфе все числа предполагаются целыми.

Пусть m — натуральное число. Говорят, что *число a сравнимо с числом b по модулю m*, если их разность $a - b$ делится на m. При этом используется запись $a \equiv b (\mathrm{mod}\, m)$.

Например, $7 \equiv 1 (\mathrm{mod}\, 3)$; $\;12 \equiv -2 (\mathrm{mod}\, 7)$.

Очевидно, что

$$a \equiv b (\mathrm{mod}\, m) \;\; \Leftrightarrow \;\; \exists t \in \mathbb{Z} \;\; a = b + mt.$$

Имеет место следующее простое

Предложение. *$a \equiv b (\mathrm{mod}\, m)$ тогда и только тогда, когда a и b имеют одинаковые остатки от деления на m.*

Доказательство. Пусть a и b при делении на m дают остатки r_1 и r_2 соответственно:

$$a = mq_1 + r_1, \;\; 0 \leqslant r_1 < m; \;\; b = mq_2 + r_2, \;\; 0 \leqslant r_2 < m.$$

Если $a \equiv b (\mathrm{mod}\, m)$, то $(a-b) \vdots m$, т. е. $(m(q_1-q_2)+r_1-r_2) \vdots m$, откуда $(r_1-r_2) \vdots m$. С другой стороны, поскольку $0 \leqslant r_1,\ r_2 < m$, имеем $|r_1-r_2| < m$. Сопоставляя два последних утверждения, получаем, что $r_1-r_2=0$, поэтому $r_1=r_2$.

Обратно, при $r_1=r_2$ справедливо $a-b=m(q_1-q_2) \vdots m$. $\square$

Заметим, что всякое число сравнимо по модулю m со своим остатком от деления на m.

Свойства сравнений

1. $a \equiv a (\mathrm{mod}\, m)$ (рефлексивность).
2. $a \equiv b (\mathrm{mod}\, m) \Rightarrow b \equiv a (\mathrm{mod}\, m)$ (симметричность).
3. $a \equiv b (\mathrm{mod}\, m), b \equiv c (\mathrm{mod}\, m) \Rightarrow a \equiv c (\mathrm{mod}\, m)$ (транзитивность).

   Доказательство. Если $(a-b) \vdots m,\ (b-c) \vdots m$, то и

   $a-c=(a-b)+(b-c) \vdots m$. $\square$
4. $a_1 \equiv b_1 (\mathrm{mod}\, m),\ a_2 \equiv b_2 (\mathrm{mod}\, m) \Rightarrow a_1+a_2 \equiv b_1+b_2 (\mathrm{mod}\, m)$.

   Доказательство. Если $(a_1-b_1) \vdots m,\ (a_2-b_2) \vdots m$, то

   $(a_1+a_2)-(b_1+b_2)=(a_1-b_1)+(a_2-b_2) \vdots m$. $\square$
5. $a_1 \equiv b_1 (\mathrm{mod}\, m),\ a_2 \equiv b_2 (\mathrm{mod}\, m) \Rightarrow a_1 \cdot a_2 \equiv b_1 \cdot b_2 (\mathrm{mod}\, m)$.

   Доказательство. Числа a_1 и a_2 можно представить в виде $a_1=b_1+mt_1$ и $a_2=b_2+mt_2$; поэтому

   $a_1a_2-b_1b_2=(b_1+mt_1)(b_2+mt_2)-b_1b_2=(b_1t_2+t_2b_1+mt_1t_2)m \vdots m$. $\square$

   Таким образом, *сравнения по одинаковому модулю можно почленно складывать и умножать.*
6. $a \equiv b (\mathrm{mod}\, m) \Rightarrow ca \equiv cb (\mathrm{mod}\, m)$.

   Это свойство — следствие свойств 1, 5.
7. $a \equiv b (\mathrm{mod}\, m), n \in \mathbb{N} \Rightarrow a^n \equiv b^n (\mathrm{mod}\, m)$.

   Следствие предыдущего свойства.

8. Если $a \equiv b (\mathrm{mod}\, m)$ и $P(x)$ — многочлен с целыми коэффициентами, то $P(a) \equiv P(b) (\mathrm{mod}\, m)$.

   Следствие свойств 4, 6, 7.

Примеры решения задач

1. Доказать, что любое натуральное число сравнимо с суммой своих цифр по модулю 9.

Доказательство. Пусть число k имеет десятичную запись

$$k = \overline{a_{n-1}a_{n-2}...a_1a_0}.$$

Рассмотрим многочлен $P(x) = \sum\limits_{i=0}^{n-1} a_i x^i$, чьи коэффициенты суть цифры числа k. Очевидно, что $k = P(10)$, $P(1) = \sum\limits_{i=0}^{n-1} a_i$. Поскольку $10 \equiv 1 (\mathrm{mod}\, 9)$, получаем $P(10) \equiv P(1) (\mathrm{mod}\, 9)$, что и требовалось доказать. □

Частным случаем доказанного утверждения является известный из средней школы признак делимости на 9. Аналогично доказывается, что любое натуральное число сравнимо с суммой своих цифр по модулю 3.

2. Вывести признак делимости на 11.

Пусть, как и выше, $k = \overline{a_{n-1}a_{n-2}...a_1a_0}$, $P(x) = \sum\limits_{i=0}^{n-1} a_i x^i$. Так как $10 \equiv -1 (\mathrm{mod}\, 11)$, имеем $k = P(10) \equiv P(-1) (\mathrm{mod}\, 11)$. Заметим, что $P(-1) = a_0 - a_1 + a_2 - a_3 + ... + (-1)^{n-1} a_{n-1}$. Таким образом, число делится на 11 тогда и только тогда, когда делится на 11 знакочередующаяся сумма его цифр.

3. Десятичная запись числа состоит из 95 единиц и нескольких нулей. Может ли оно быть квадратом некоторого натурального числа?

Пусть k — данное число. Как отмечалось выше, число сравнимо с суммой своих цифр по модулю 3. Поэтому

$$k \equiv 95 \equiv 2 (\mathrm{mod}\, 3).$$

Выясним теперь, какие остатки может давать квадрат натурального числа n от деления на 3. Имеет место один из трех случаев: n сравнимо с 0, 1 или 2 по модулю 3.

Если $n \equiv 0 (\mathrm{mod}\, 3)$, то $n^2 \equiv 0 (\mathrm{mod}\, 3)$;
если $n \equiv 1 (\mathrm{mod}\, 3)$, то $n^2 \equiv 1 (\mathrm{mod}\, 3)$;
если $n \equiv 2 (\mathrm{mod}\, 3)$, то $n^2 \equiv 4 \equiv 1 (\mathrm{mod}\, 3)$.

Таким образом, квадрат натурального числа не может давать остаток 2 от деления на 3; ответ на вопрос задачи отрицательный.

4. Докажите самостоятельно, что квадрат натурального числа при делении на 4 может иметь остатки только 0 или 1.

5. Доказать, что $(3^{30} - 2^{30}) \vdots 7$.

Действительно, $3^{30} = 27^{10} \equiv (-1)^{10} \equiv 1 (\mathrm{mod}\, 7)$;
$2^{30} = 8^{10} \equiv 1^{10} \equiv 1 (\mathrm{mod}\, 7)$, откуда вытекает требуемое.

6. Доказать, что для любого натурального $n \quad (5^{2n+3} + 3^{n+3} \cdot 2^n) \vdots 19$.

Доказательство. $5^{2n+3} = 125 \cdot 25^n \equiv 11 \cdot 6^n (\mathrm{mod}\, 19)$.

$3^{n+3} \cdot 2^n = 27 \cdot 6^n \equiv 8 \cdot 6^n (\mathrm{mod}\, 19)$.

Складывая сравнения, получаем:
$5^{2n+3} + 3^{n+3} \cdot 2^n \equiv 19 \cdot 6^n \equiv 0 (\mathrm{mod}\, 19)$. □

7. Доказать, что для любого натурального n

$13 \cdot (-50)^n + 17 \cdot 40^n - 30 \vdots 1989$.

Доказательство. Разложим 1989 на взаимно простые множители: $1989 = 9 \cdot 13 \cdot 17$. Обозначим $a_n = 13 \cdot (-50)^n + 17 \cdot 40^n - 30$.

Докажем, что a_n делится на 9, 13 и 17.
Действительно, $a_n \equiv 4 \cdot 4^n + (-1) \cdot 4^n - 3 \equiv 3 \cdot (4^n - 1) (\mathrm{mod}\, 9)$.

Поскольку $4^n - 1 \equiv 1^n - 1 \equiv 0 (\mathrm{mod}\, 3)$, $3 \cdot (4^n - 1) \vdots 9$. Таким образом, $a_n \equiv 3 \cdot (4^n - 1) \equiv 0 (\mathrm{mod}\, 9)$, т. е. a_n делится на 9.
Делимость на 13 и 17 доказывается совсем просто:
$a_n \equiv 0 + 17 \cdot 1^n - 30 \equiv 0 (\mathrm{mod}\, 13)$; $a_n \equiv 13 \cdot 1^n + 0 - 30 \equiv 0 (\mathrm{mod}\, 17)$.
Итак, a_n делится на попарно взаимно простые числа 9, 13 и 17, поэтому a_n кратно их произведению — 1989. □

8. Найти остаток от деления на 3 числа $\prod\limits_{k=1}^{1000} (k^2 + 1)$. Имеем:

$$\prod_{k=1}^{1000} (k^2+1) \equiv ((1+1)(1+1) \cdot 1)^{333} \cdot (1+1) \equiv 4^{333} \cdot 2 \equiv 1^{333} \cdot 2 \equiv 2 (\mathrm{mod}\, 3).$$

Остаток равен 2.

9. Доказать, что уравнение $x^2 - 4x + 12y = 19$ не имеет решений в целых числах.

Действительно, если $(x; y)$ — решение данного уравнения, то $x^2 = 4x - 12y + 19 \equiv 3 (\mathrm{mod}\, 4)$, что противоречит результату 4).

6. Системы вычетов

Как показано в § 5, отношение сравнимости по модулю m обладает свойствами рефлексивности, симметричности и транзитивности; поэтому оно является отношением эквивалентности. Как известно, отношение эквивалентности порождает разбиение множества, на котором оно определено, на классы эквивалентности. В случае отношения сравнимости по модулю m классы эквивалентности называют *классами вычетов по модулю* m; каждое число, входящее в какой-нибудь из классов, называется *вычетом* этого класса.

Пусть $\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a (\mathrm{mod}\, m)\}$ — класс эквивалентности, порождённый элементом a.

Число классов вычетов по модулю m равно m. Действительно, остаток от деления целого числа на m принимает одно из значений $0, 1, \ldots, m-2$ или $m-1$ и поэтому каждое из чисел попадает в один из классов $\overline{0}, \overline{1}, \ldots, \overline{m-1}$, количество которых равно m.

Взяв по одному числу из каждого класса вычетов $x_1, x_2, \ldots, x_m$, получим систему представителей классов вычетов, или *полную систему вычетов по модулю* m.

Пример 1. Различные полные системы вычетов по модулю 7:
1) $0, 1, 2, 3, 4, 5, 6$; **2)** $-3, -2, -1, 0, 1, 2, 3$; **3)** $7, -6, 9, -4, 11, -2, 13$.

Лемма 6.1. *Числа $x_1, x_2, \ldots, x_m$ образуют полную систему вычетов по модулю m тогда и только тогда, когда они попарно не сравнимы по модулю m.*

Доказательство. Необходимость очевидна. Докажем достаточность. Если два числа не сравнимы по модулю m, то они попадают в разные классы вычетов. Так как всего классов вычетов m и рассматриваемых чисел m, то они составляют полную систему вычетов. □

Лемма 6.2. *Пусть $x_1, x_2, ..., x_m$ — полная система вычетов по модулю m, целое число a взаимно просто с m, b — произвольное целое*

число. Тогда числа $ax_1+b, ax_2+b, \ldots, ax_m+b$ *также образуют полную систему вычетов.*

Доказательство. Согласно лемме 6.1 достаточно убедиться в том, что $ax_i + b \not\equiv ax_j + b (\mathrm{mod}\, m)$ при $i \neq j$. Предположим (для приведения к противоречию), что $ax_i + b \equiv ax_j + b (\mathrm{mod}\, m)$. Тогда $a(x_i - x_j) \vdots m$, и, поскольку $(a, m) = 1$, имеем $(x_i - x_j) \vdots m$, что противоречит лемме 6.1. □

Лемма 6.3. *Пусть* $x \equiv a (\mathrm{mod}\, m)$. *Тогда* $(x, m) = (a, m)$.

Доказательство. Пусть r — остаток от деления a на m. Тогда по лемме 2.2 $(a, m) = (r, m)$. Но так как $x \equiv a (\mathrm{mod}\, m)$, при делении на m число x также имеет остаток r, и, следовательно, $(x, m) = (r, m)$, откуда и вытекает требуемое. □

Итак, числа из одного класса вычетов по модулю m имеют один и тот же наибольший общий делитель с m. Поэтому становится корректным следующее определение.

Вычет по модулю m называют *приведённым*, если он взаимно прост с m. Совокупность приведённых вычетов из разных классов вычетов называют *приведённой системой вычетов.*

Пример 2. При $m = 7$ приведённая система вычетов может выглядеть так: 1, 2, 3, 4, 5, 6; а при $m = 6$ так: 1, 5.

Функцией Эйлера $\varphi(m)$ называют число натуральных чисел, не превосходящих m и взаимно простых с m. Например,

$$\varphi(1) = 1;\ \varphi(2) = 1;\ \varphi(3) = 2;\ \varphi(4) = 2;\ \varphi(5) = 4;\ \varphi(6) = 2;\ \varphi(7) = 6.$$

Легко видеть, что если p — простое число, то $\varphi(p) = p - 1$.

Очевидно, что приведённая система вычетов по модулю m содержит $\varphi(m)$ чисел.

Лемма 6.4. *Пусть* a *взаимно просто с* m, $k = \varphi(m)$ *и* $x_1, x_2, \ldots, x_k$ *— приведённая система вычетов по модулю* m. *Тогда числа* $ax_1, ax_2, \ldots, ax_k$ *также образуют приведённую систему вычетов по модулю* m.

Доказательство. Так как числа a и x_i взаимно просты с m, таким же свойством обладает и их произведение ax_i. В силу леммы 6.2 числа $ax_1, ax_2, \ldots, ax_k$ принадлежат k разным классам вычетов, и, следовательно, в силу предыдущего, образуют приведённую систему вычетов. □

7. Теорема Эйлера

Пусть m — натуральное число, $k = \varphi(m)$, $x_1, x_2, \ldots, x_k$ — приведённая система вычетов по модулю m. Пусть a — какое-нибудь натуральное число, взаимно простое с m. Тогда в силу результатов предыдущего параграфа числа $ax_1, ax_2, \ldots, ax_k$ также образуют приведённую систему вычетов по тому же модулю. Поскольку ax_j — приведённый вычет, для некоторого числа $i_j \in \{1, 2, \ldots, k\}$ справедливо соотношение $ax_j \equiv x_{i_j} (\mathrm{mod}\, m)$. Числа $i_1, i_2, \ldots, i_k$ попарно различны и поэтому образуют перестановку чисел от 1 до k. Перемножив k полученных сравнений, получим

$$a^k \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_k \equiv x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_k} (\mathrm{mod}\, m).$$

Пусть $s = x_1 \cdot x_2 \cdot \ldots \cdot x_k$. Тогда произведение $x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_k}$ также равно s. Заметим, что поскольку делители s взаимно просты с m, число s также обладает этим свойством. Итак, $a^k s \equiv s (\mathrm{mod}\, m)$, отсюда $s(a^k - 1) \vdots m$, и, в силу взаимной простоты s и m, имеем $a^k - 1 \vdots m$. Доказана

Теорема 7.1. [Теорема Эйлера] *Если целое число a взаимно просто с натуральным числом m, то число $a^{\varphi(m)} - 1$ делится на m.*

Следствие [Малая теорема Ферма] *Пусть p — простое число, a — целое число, не кратное p. Тогда $a^{p-1} - 1$ делится на p.*

Заметим, что в условиях малой теоремы Ферма $a^p - a$ делится на p, но последнее справедливо и при a, кратном p. В связи с этим часто под малой теоремой Ферма понимают следующее легко запоминаемое утверждение:

Если p — простое число, то для любого целого a число $a^p - a$ делится на p.

Малая теорема Ферма дает лишь *необходимое* условие простоты числа. Нечётное число $m \geqslant 3$ называют *условно простым по базе a* (где $a = 2, 3, \ldots, m-1$), если $a^{m-1} \equiv 1 (\mathrm{mod}\, m)$. Простое число является условно простым по любой базе. Существуют, однако, составные числа m, являющиеся условно простыми по любой базе a, взаимно простой с m. Такие числа называют *числами Кармайкла.* Наименьшее из них — 561. В 1994 г. было доказано, что чисел Кармайкла бесконечно много.

В последние годы задача проверки простоты числа или — более широко — задача разложения числа на простые множители вновь

приобрела актуальность в связи с проблемами создания надежных шифров (см. § 23 и § 24).

8. Линейные диофантовы уравнения

Диофантовым[1] называют уравнение в целых числах вида

$$P(x_1, \ldots, x_n) = 0,$$

где P — многочлен от n переменных с целыми коэффициентами. Предметом изучения в этом параграфе будет служить линейное диофантово уравнение с двумя неизвестными

$$ax + by = c, \tag{1}$$

где a, b и c — целые константы, а x и y — неизвестные, или переменные. Решением (более точно, *частным решением*) уравнения, как известно, называют набор значений переменных, обращающих его в верное равенство. Стоит задача описания всех решений уравнения (1) в целых числах.

Если один из коэффициентов при неизвестных равен нулю, то уравнение фактически содержит лишь одно неизвестное. Поэтому будем считать, что $a \neq 0$ и $b \neq 0$. Более того, при необходимости меняя знак переменной, можно без ограничения общности считать в этом случае, что $a > 0$ и $b > 0$. Пусть d — наибольший общий делитель a и b. Тогда для любых целых x и y левая часть уравнения $ax + by$ делится на d. Если при этом c не делится на d, то уравнение не имеет (целых) решений. Если же c кратно d, т. е. $c = c_1 d$ для некоторого целого c_1, то, положив $a = a_1 d$, $b = b_1 d$ и сократив на d, уравнение (1) сведём к виду

$$a_1 x + b_1 y = c_1,$$

в котором коэффициенты при неизвестных являются взаимно простыми числами.

Теорема 8.1. *Уравнение (1) с взаимно простыми коэффициентами при неизвестных разрешимо в целых числах.*

Доказательство. Рассмотрим сначала уравнение

$$ax + by = 1. \tag{2}$$

[1] В честь древнегреческого математика Диофанта, жившего в III веке.

Построим цепочку делений с остатком

$$a = bq_0 + r_1, \quad 0 < r_1 < b;$$

$$b = r_1 q_1 + r_2, \quad 0 < r_2 < r_1;$$

$$r_1 = r_2 q_2 + r_3, \quad 0 < r_3 < r_2;$$

$$\dots$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad 0 < r_n < r_{n-1};$$

$$r_{n-1} = r_n q_n.$$

Последний ненулевой остаток, как известно, равен наибольшему общему делителю a и b, т. е. $r_n = 1$. Заметим, что каждый остаток r_i может быть представлен целочисленной линейной комбинацией чисел a и b:

$$r_i = \alpha_i a + \beta_i b.$$

Действительно,

$$r_1 = a - bq_0 = \alpha_1 a + \beta_1 b;$$

$$r_2 = b - r_1 q_1 = b - (\alpha_1 a + \beta_1 b) q_1 = \alpha_2 a + \beta_2 b;$$

$$\dots$$

$$r_{i+1} = r_{i-1} - r_i q_i = \alpha_{i-1} a + \beta_{i-1} b - (\alpha_i a + \beta_i b) q_1 = \alpha_{i+1} a + \beta_{i+1} b;$$

$$\dots$$

$$1 = r_n = \alpha_n a + \beta_n b.$$

Последнее равенство показывает, что пара целых чисел $(\alpha_n; \beta_n)$ является решением (2). Очевидно, что пара целых чисел $(c\alpha_n; c\beta_n)$ — суть решение (1). Теорема доказана. □

Пример 1. Найти какие-нибудь целые x и y, для которых

$$1000x + 73y = 1.$$

Применив алгоритм Евклида к паре чисел 1000 и 73, получим цепочку равенств

$$1000 = 73 \cdot 13 + 51; \quad 73 = 51 \cdot 1 + 22; \quad 51 = 22 \cdot 2 + 7; \quad 22 = 7 \cdot 3 + 1,$$

из которых имеем

$$1 = 22 - 7 \cdot 3 = 22 - 3(51 - 2 \cdot 22) = 7 \cdot 22 - 3 \cdot 51 = 7(73 - 51) - 3 \cdot 51 =$$

$$= 7 \cdot 73 - 10 \cdot 51 = 7 \cdot 73 - 10(1000 - 73 \cdot 13) = -10 \cdot 1000 + 137 \cdot 73.$$

Ответом в данной задаче может служить пара $(-10; 137)$.

Итак, мы теперь умеем находить *частное решение* уравнения (1) (в том случае, когда это диофантово уравнение разрешимо). О том, каким является *общее решение* (1) — множество всех (частных) решений, говорит

Теорема 8.2. *Пусть a и b — взаимно простые натуральные числа, $(x_0; y_0)$ — некоторое решение диофантова уравнения (1). Тогда множество всех решений (1) описывается формулами*

$$x = x_0 + bt, \quad y = y_0 - at, \tag{3}$$

где $t \in \mathbb{Z}$.

Доказательство. Очевидно, что для любого целого t значения x и y, определяемые формулами (3), дают решение (1). Действительно,

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 = c,$$

так как пара $(x_0; y_0)$ удовлетворяет (1) по условию теоремы.

Убедимся теперь в том, что *произвольное* решение (1) имеет вид (3) для некоторого целого t. Вычтя из (1) почленно равенство

$$ax_0 + by_0 = c,$$

получим равносильное уравнение $a(x - x_0) + b(y - y_0) = 0$, или

$$a(x - x_0) = b(y_0 - y). \tag{4}$$

Из того, что $a(x - x_0)$ кратно b и a взаимно просто с b, следует, что $(x-x_0) \vdots b$, т. е. для некоторого целого t имеем $x - x_0 = bt$, или $x = x_0 + bt$. Подставив выражение для x в (4), получим $abt = b(y_0 - y)$ и, поскольку $b \neq 0$, справедливо равенство $y_0 - y = at$, или $y = y_0 - at$. Теорема доказана. □

Пример 2. Общее решение рассматривавшегося выше уравнения $1000x + 73y = 1$ таково: $\{(-10 + 73t, 137 - 1000t) \mid t \in \mathbb{Z}\}$.

9. Примеры решения нелинейных уравнений в целых числах

В этом параграфе будут продемонстрированы некоторые методы решения уравнений в целых числах.

1) $3x^2 + 4xy - 7y^2 = 13$.

Решение сводится к небольшому перебору после разложения левой части на множители. Имеем

$$3x^2 + 4xy - 7y^2 = x(3x + 7y) - y(3x + 7y) = (x - y)(3x + 7y) = 13.$$

Если $(x; y)$ — решение этого уравнения, то $x - y$ — делитель 13, т. е. принимает значения $\pm 1, \pm 13$; при этом $3x + 7y$ равно соответственно $\mp 13, \mp 1$. Решив четыре полученные системы двух линейных уравнений с двумя неизвестными, увидим, что только в двух случаях x и y — целые.

Ответ: $(2; 1), (-2; -1)$.

2) $2x^2 - 2xy + 9x + y = 2$.

Выразим y через x:

$$y = \frac{2x^2 + 9x - 2}{2x - 1} = x + 5 + \frac{3}{2x - 1}.$$

Если x — целое число, то y будет целым лишь при $2x - 1 = \pm 1, \pm 3$.

Ответ: $(1; 9), (0; 2), (2; 8), (-1; 3)$.

3) $2^x - 15 = y^2$ $(x, y \in \mathbb{N})$.

Пусть сначала x — нечётное число: $x = 2k + 1$, $k \in \mathbb{N}_0$. Тогда $y^2 = 2^{2k+1} - 15 = 2 \cdot 4^k - 15 \equiv 2 \cdot 1^k \equiv 2 (\mathrm{mod}\, 3)$, что невозможно, поскольку, как было установлено ранее, квадрат натурального числа не может давать остаток 2 от деления на 3.

Если x — чётное число, то уравнение решается ранее использованным приёмом: при $x = 2k$, $k \in \mathbb{N}$

$$15 = 2^{2k} - y^2 = (2^k - y)(2^k + y).$$

Простейший перебор по делителям 15 дает следующий

Ответ: (4;1), (6;7).

4) $19x^2 - 93y^2 = 1993$.

Записав уравнение в виде $19(x^2 - 100) = 93(1 + y^2)$, видим, что $(1 + y^2) \vdots 19$, откуда $y^2 \equiv 18 (\mathrm{mod}\, 19)$. Проверим, возможно ли последнее. Рассмотрев полную систему вычетов по модулю 19 : $0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 8, \pm 9$, получим возможные

остатки от деления точного квадрата на 19: 0, 1, 4, 9, 16, 6, 17, 11, 7, 5. Число 18 не входит в это множество.

Ответ: решений в целых числах нет.

5) $\operatorname{arctg}\dfrac{1}{x}+\operatorname{arctg}\dfrac{1}{y}=\operatorname{arctg}\dfrac{1}{10}$. (1)

Взяв тангенс от обеих частей уравнения, получим в качестве его *следствия* алгебраическое уравнение

$$\frac{\dfrac{1}{x}+\dfrac{1}{y}}{1-\dfrac{1}{x}\cdot\dfrac{1}{y}}=\frac{1}{10},$$

откуда после несложных преобразований

$$y=10+\frac{101}{x-10},\quad xy\neq 1. \tag{2}$$

Поскольку $x-10$ — делитель простого числа 101, имеем $x-10=$ $=\pm1,\pm101$; значит, $(x;y)=(11;111),(9;-91),(111;11),(-91;9)$. Решено в целых числах уравнение (2). Для каждой найденной пары $(x;y)$ найдётся такое целое число k, что

$$\operatorname{arctg}\frac{1}{x}+\operatorname{arctg}\frac{1}{y}=\operatorname{arctg}\frac{1}{10}+\pi k.$$

Легко проверить, что как $\operatorname{arctg}\dfrac{1}{11}+\operatorname{arctg}\dfrac{1}{111}$, так и $\operatorname{arctg}\dfrac{1}{9}-$ $-\operatorname{arctg}\dfrac{1}{91}$ попадают в промежуток $(0,\pi)$, поэтому каждый раз вышеупомянутое k равно 0 и, следовательно, найденные решения (2) являются и решениями (1).

10. Мультипликативные функции

Функция натурального аргумента $\theta(n)$ называется *мультипликативной*, если $\theta(1)=1$ и для любых взаимно простых чисел m и n выполняется равенство

$$\theta(m\cdot n)=\theta(m)\cdot\theta(n).$$

Простейшим примером мультипликативной функции является степенная функция $\theta(n) = n^\alpha$.

Пусть $n_1, n_2, \ldots, n_k$ — попарно взаимно простые числа. Индукцией легко доказать, что для любой мультипликативной функции справедливо соотношение

$$\theta(n_1 \cdot n_2 \cdot \ldots \cdot n_k) = \theta(n_1) \cdot \theta(n_2) \cdot \ldots \cdot \theta(n_k).$$

Из этого свойства вытекает, что мультипликативная функция однозначно определяется своими значениями на степенях простых чисел.

До конца этого параграфа будем считать, что n имеет каноническое разложение

$$n = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}.$$

Докажем сначала мультипликативность функции Эйлера (определение см. § 6).

Пусть m и n — взаимно простые числа. Чтобы подсчитать количество чисел, не превосходящих mn и взаимно простых с mn, расположим все числа от 1 до mn в виде прямоугольной таблицы

1	2	3	$\ldots$	n
$n+1$	$n+2$	$n+3$	$\ldots$	$2n$
$2n+1$	$2n+2$	$2n+3$	$\ldots$	$3n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$(m-1)n+1$	$(m-1)n+2$	$(m-1)n+3$	$\ldots$	mn

Любое натуральное число взаимно просто с mn тогда и только тогда, когда оно взаимно просто и с m, и с n (в силу взаимной простоты чисел m и n). Числа из каждого фиксированного столбца таблицы попарно сравнимы по модулю n; поэтому можно оставить в таблице только столбцы, первые элементы которых взаимно просты с n, не потеряв при этом ни одного интересующего нас числа. Число таких столбцов есть $\varphi(n)$. Элементы каждого столбца в силу леммы 6.2 образуют полную систему вычетов по модулю m. Поэтому ровно $\varphi(m)$ элементов каждого столбца взаимно просты с m. Таким образом, всего имеется $\varphi(n) \cdot \varphi(m)$ чисел не больше mn и взаимно простых с mn, т. е. $\varphi(mn) = \varphi(m) \cdot \varphi(n)$, что и требовалось доказать.

Используя свойство мультипликативности, нетрудно вывести формулу для вычисления $\varphi(n)$. Поскольку $\varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot \ldots \cdot \varphi(p_s^{k_s})$,

достаточно научиться вычислять функцию Эйлера от степени простого числа. Для этого заметим, что если p — простое число, то среди любых p последовательных натуральных чисел ровно $p-1$ чисел взаимно просты с p, а также с любой степенью p. Поэтому $\varphi(p^k) = \varphi(p \cdot p^{k-1}) = (p-1) \cdot p^{k-1}$. Таким образом,

$$\varphi(n) = \prod_{i=1}^{s} \varphi\left(p_i^{k_i}\right) = \prod_{i=1}^{s} (p_i - 1) \cdot p_i^{k_i - 1} = \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) \cdot p_i^{k_i} = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right).$$

Пример. $\varphi(24) = 24 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 8.$

Приведём эффектное **доказательство бесконечности множества простых чисел** с помощью функции Эйлера.

Предполагая, что множество простых чисел конечно и состоит из чисел $p_1, p_2, \ldots, p_s$, рассмотрим их произведение $P = p_1 \cdot p_2 \cdot \ldots \cdot p_s$. Ни одно число, кроме 1, не может быть взаимно просто с P, откуда $\varphi(P) = 1$. С другой стороны,

$$\varphi(P) = \varphi(p_1 p_2 \ldots p_s) = (p_1 - 1)(p_2 - 1) \ldots (p_s - 1) > 1.$$

Противоречие. □

Рассмотрим еще несколько задач, при решении которых возникают мультипликативные функции.

1) Найти $\tau(n)$ — число различных делителей натурального числа n (включая 1 и n).

Общий вид делителя n имеет вид

$$d = p_1^{r_1} p_2^{r_2} \ldots p_s^{r_s},$$

где для каждого i показатель степени r_i принимает значения $0, 1, \ldots, k_i$. Произвольный делитель числа n можно построить в результате выполнения процедуры из s действий, где i-е действие состоит в выборе r_i — показателя степени простого числа p_i. Поскольку i-е действие может быть выполнено $k_i + 1$ способами, применение правила произведения дает

$$\tau(n) = (k_1 + 1)(k_2 + 1) \ldots (k_s + 1) = \prod_{i=1}^{s} (k_i + 1).$$

Примеры. 1) $\tau\left(2^3 \cdot 3^4 \cdot 5^6\right) = 4 \cdot 5 \cdot 7 = 140$;
2) $\tau\left(2^3 \cdot 3^4 \cdot 4^5\right) = \tau(2^{13} \cdot 3^4) = 14 \cdot 5 = 70.$

2) Найти $\sigma(n)$ — сумму всевозможных делителей числа n.

Покажем, что

$$\sigma(n) = (1 + p_1 + p_1^2 + \ldots + p_1^{k_1}) \cdot \ldots \cdot (1 + p_s + p_s^2 + \ldots + p_s^{k_s}).$$

Действительно, раскрывая скобки и не меняя при этом порядка множителей, получим
$\sigma(n) = 1 \cdot 1 \cdot \ldots \cdot 1 + 1 \cdot 1 \cdot \ldots \cdot p_s + \ldots + p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$ — сумму всех делителей n. С помощью формулы суммы членов геометрической прогрессии получаем компактную формулу

$$\sigma(n) = \prod_{i=0}^{s} \frac{p_i^{k_i+1} - 1}{p_i - 1}.$$

Примеры. 1) $\sigma(12) = \sigma(2^2 \cdot 3) = \frac{2^3-1}{2-1} \cdot \frac{3^2-1}{3-1} = 7 \cdot 4 = 28$.
2) $\sigma(60) = \sigma(12) \cdot \sigma(5) = 28 \cdot 6 = 168$.

Проверка мультипликативности функций $\tau(n)$ и $\sigma(n)$ проводится непосредственной подстановкой.

С помощью функции $\sigma(n)$ вводятся *совершенные* и *дружественные* числа

Число m называется *совершенным*, если $\sigma(m) = 2m$.

Примеры совершенных чисел: 6, 28, 496, 8128, 33 550 336.

Число Мерсенна $M_n = 2^n - 1$.

Упражнение 2. Докажите, что при составном n число M_n также составное.

Упражнение 3. Докажите, что если M_n — простое число, то число $2^{n-1}M_n$ — совершенное.

Оказывается, что любое чётное[2] совершенное число имеет вид, указанный в предыдущем упражнении. Доказательство этого факта, открытого Эйлером, приводится в задачнике [24], а также в книге [20]. О том, как доказывают простоту чисел Мерсенна, см. §25.

Приведём некотрые интересные сведения, касающиеся чисел Мерсенна. В 1750 г. Эйлер установил, что M_{31} — простое число. Оно оставалось более 100 лет наибольшим известным простым числом. К началу 2016 г. найдено 49 простых чисел Мерсенна. За нахождение 45-го простого числа Мерсенна

[2]Существуют ли нечётные совершенные числа, до сих пор неизвестно. Установлено, что в промежутке от 1 до 10^{300} таких чисел нет.

$M_{43\,112\,609}$ проектом GIMPS[3] в 2009 году была получена премия в 100 000 долларов США, назначенная сообществом Electronic Frontier Foundation за нахождение простого числа, десятичная запись которого содержит не менее 10 миллионов цифр. На данный момент (май 2016 г.) наибольшим известным простым числом является число $M_{74\,207\,281}$, найденное 7 января 2016 года и содержащая в своей десятичной записи 22 338 618 цифр.

Числа m и n называются *дружественными*, если

$$\sigma(m) = \sigma(n) = m + n.$$

Примеры дружественных чисел: 220 и 284, 1184 и 1210.

11. Формула обращения Мёбиуса

Группа мультипликативных функций

Для дальнейшего нам понадобятся функции $E(n)$, $I(n)$, $J(n)$:

$$E(n) = 1 \ \ \forall n; \quad I(n) = n \ \ \forall n; \quad J(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n > 1 \end{cases}$$

и *функция Мёбиуса* $\mu(n)$, которая вводится следующим образом:

$\mu(1) = 1$;

если n делится на квадрат простого числа, то $\mu(n) = 0$;

если n свободно от квадратов и представимо в виде произведения s различных простых чисел, то $\mu(n) = (-1)^s$.

Мультипликативность этих функций очевидна.

Произведением Дирихле функций $f(n)$ и $g(n)$ называется функция

$$f \circ g(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Очевидно, что $J \circ f = f$ для любой функции $f(n)$.

Потренируемся в вычислении произведения Дирихле.

Упражнение 4. Проверьте, что

$$E \circ E = \tau; \quad I \circ E = \sigma; \quad I \circ I(n) = n\tau(n).$$

Упражнение 5. Докажите, что $\mu \circ E = J$.

[3]GIMPS (Great Internet Mersenne Prime Search) — широкомасштабный проект распределённых вычислений по поиску простых чисел Мерсенна.

Доказательство. Отметим сразу, что

$$\mu \circ E(1) = \mu(1) \cdot E(1) = 1 \cdot 1 = 1.$$

Пусть теперь $n > 1$. Тогда $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, где $k \geqslant 1$. Поскольку $\mu(d) \neq 0$ только если число d свободно от квадратов, имеем:

$$\sum_{d|n} \mu(d) = \mu(1) + \sum \mu(p_i) + \sum \mu(p_i p_j) + \ldots + \mu(p_1 \dots p_k) =$$

$$= 1 - k + C_k^2 - C_k^3 - \ldots + (-1)^k = (1-1)^k = 0. \ \square$$

Операция $\circ$, очевидно, коммутативна. Докажем, что она также ассоциативна. Действительно,

$$(f \circ g) \circ h(n) = f \circ (g \circ h)(n) = \sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3).$$

Пользуясь ассоциативностью и предыдущими результатами, вычислим ещё несколько произведений Дирихле.

$$\mu \circ \tau = \mu \circ E \circ E = J \circ E = E; \quad \mu \circ \sigma = \mu \circ E \circ I = J \circ I = I.$$

Из мультипликативности функций $f(n)$ и $g(n)$ следует мультипликативность $f \circ g(n)$.

В самом деле, для взаимно простых n и m имеем

$$f \circ g(nm) = \sum_{d|nm} f(d) g\left(\frac{nm}{d}\right) = \sum_{d_1|n, d_2|m} f(d_1 d_2) g\left(\frac{nm}{d_1 d_2}\right) =$$

$$= \sum_{d_1|n, d_2|m} f(d_1) f(d_2) g\left(\frac{n}{d_1}\right) g\left(\frac{m}{d_2}\right) =$$

$$= \sum_{d_1|n} f(d_1) g\left(\frac{n}{d_1}\right) \sum_{d_2|m} f(d_2) g\left(\frac{m}{d_2}\right) = (f \circ g(n)) \cdot (f \circ g(m)).$$

Пусть $f(n)$ — мультипликативная функция. Найдём такую мультипликативную функцию $f'(n)$, что $f \circ f' = J$. Определим функцию $f'(n)$ следующими соотношениями. Пусть $f'(1) = 1$. При этом $f \circ f'(1) = f \cdot f'(1) = 1$. Для каждого простого числа p положим $f'(p) = -f(p)$. Тогда $f \circ f'(p) = 0$. Положив

$$f'(p^n) = -\left(f(p^n) + f(p^{n-1}) f'(p) + \ldots + f(p) f'(p^{n-1})\right),$$

мы добьёмся того, что $\forall n \quad f \circ f'(p^n) = 0$.

Теперь значения f' определены на всех степенях простых чисел и свойство мультипликативности полностью задаёт функцию f'.

Произведение Дирихле мультипликативных функций $\Phi = f \circ f'$ мультипликативно. Поскольку $\Phi(1) = 1$ и для любого простого числа p и любого натурального n справедливо $\Phi(p^n) = 0$,

$$\Phi(p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}) = \Phi(p_1^{n_1}) \cdot \ldots \cdot \Phi(p_k^{n_k}) = 0.$$

Значит, Φ и есть J. Доказано, что $f \circ f' = J$.

Мы установили следующий факт.

Теорема 11.1. *Мультипликативные функции образуют коммутативную группу с единичным элементом J и произведением Дирихле в качестве групповой операции.*

Следствие. *Из мультипликативности функций $f(n)$ и $f \circ g(n)$ следует мультипликативность $g(n)$.*

Доказательство. Пусть f' — мультипликативная функция со свойством $f \circ f' = J$. Тогда функция $g = J \circ g = (f' \circ f) \circ g = f' \circ (f \circ g)$ также мультипликативна. □

Функция $F = f \circ E$ называется *сумматорной функцией* для $f(n)$. Таким образом,

$$F(n) = \sum_{d|n} f(d),$$

где суммирование ведётся по всем делителям числа n (включая 1 и n).

Из предыдущего вытекает, что $f(n)$ — мультипликативная функция тогда и только тогда, когда мультипликативна её сумматорная функция $F(n)$. Докажем, что $\varphi \circ E = I$, т. е. что сумматорная функция для функции Эйлера имеет вид:

$$\sum_{d|n} \varphi(d) = n.$$

1-й способ. Представим число n в виде произведения простых чисел:

$$n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}.$$

Любой делитель d числа n имеет вид $d = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$, где для каждого i справедливо $0 \leqslant s_i \leqslant r_i$. Поэтому

$$\sum \varphi(d) = (1 + \varphi(p_1) + \ldots + \varphi(p_1^{r_1})) \ldots (1 + \varphi(p_k) + \ldots + \varphi(p_k^{r_k})).$$

В этом легко убедиться, раскрыв скобки.

Вычислим сумму в каждой скобке:

$$1+\varphi(p_i)+\ldots+\varphi(p_i^{r_i})=1+(p_i-1)+(p_i^2-p_i)+\ldots+(p_i^{r_i}-p_i^{r_i-1})=p_i^{r_i}.$$

Таким образом, $\sum\varphi(d)=\prod p_i^{r_i}=n$. $\square$

2-й способ. Рассмотрим дроби $\frac{1}{n},\frac{2}{n},\frac{3}{n},\ldots,\frac{n}{n}$. Сократим каждую дробь. Получатся дроби, знаменатели которых являются делителями числа n, причём количество дробей со знаменателем d равно $\varphi(d)$. А общее количество дробей равно n. $\square$

С помощью упражнения 5 по сумматорной функции можно найти исходную функцию.

Теорема 11.2. [Формула обращения Мёбиуса]

$$F=f\circ E \iff f=F\circ\mu.$$

Таким образом, найдено выражение функции $f(n)$ через её сумматорную функцию:

$$f(n)=\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right).$$

В качестве упражнения покажем, как можно получить выражение для функции Эйлера, зная её сумматорную функцию.

$$\varphi(n)=n\sum_{d|n}\frac{\mu(d)}{d}=n\prod_{p|n}\left(1-\frac{1}{p}\right).$$

Соотношение

$$\frac{\varphi(n)}{n}=\sum_{d|n}\frac{\mu(d)}{d} \tag{1}$$

пригодится нам в дальнейшем.

Упражнение 6. Убедившись в справедливости равенства

$$\prod_{d|n}d=n^{\tau(n)/2},$$

найдите сумматорную функцию для натурального логарифма.

Ответ: $\ln\circ E(n)=\frac{\tau(n)}{2}\cdot\ln n$.

Упражнение 7. Пусть

$$\Lambda(n) = \begin{cases} \ln p, & \text{если } n = p^k, \text{ где } p \text{ — простое }, k \in N; \\ 0 & \text{в противном случае.} \end{cases}$$

Докажите: 1) $\Lambda \circ E = \ln$; 2) $\Lambda = \ln \circ \mu$.

Задача о числе ожерелий

Имеется неограниченный запас бусинок k цветов. Сколько можно составить различных ожерелий из n бусинок (ожерелья, получающиеся друг из друга плоскими вращениями, не будем различать)?

Математической моделью ожерелья является понятие циклической последовательности.

На множестве (линейных) последовательностей длины n, элементы которых принимают значения из некоторого конечного множества, зададим отношение эквивалентности

$$(a_1, \ldots, a_n) \sim (a_i, a_{i+1}, \ldots, a_n, a_1, \ldots, a_{i-1}) \quad (i = 1, \ldots, n).$$

Класс эквивалентности назовём *циклической последовательностью*. Подсчитать число различных циклических последовательностей не так просто, поскольку в разных классах эквивалентности может быть разное число (линейных) последовательностей; например, постоянная циклическая последовательность порождается одной линейной последовательностью, а циклической последовательности из n попарно различных элементов соответствует n линейных последовательностей.

Период циклической последовательности $(a_1, \ldots, a_n)$ — наименьшее число d такое, что $a_{i+d} = a_i$ для всех i, где сложение ведётся по модулю n (т. е. если $i + d > n$, то $i + d$ заменяется на $i + d - n$). Ясно, что период d должен быть делителем числа n.

Обозначим через $T(n)$ количество циклических последовательностей длины n, а через $M(n)$ количество циклических последовательностей длины n и периода n. Тогда

$$T(n) = \sum_{d|n} M(d).$$

Пример. При $k = 2$ и $n = 4$ имеем

$$T(4) = M(1) + M(2) + M(4) = 2 + 1 + 3 = 6.$$

Пусть $M(d)$ — количество циклических последовательностей длины и периода d, элементы которых могут принимать k различных значений. Тогда

$$k^n = \sum_{d|n} dM(d). \tag{2}$$

Действительно, каждая циклическая последовательность длины и периода d порождает ровно d различных линейных последовательностей.

Введём функции $m(n) = nM(n)$ и $h(n) = k^n$. Формула (2) говорит о том, что $h = m \circ E$. Применим формулу обращения Мёбиуса:

$$m = h \circ \mu; \quad nM(n) = \sum_{d|n} \mu(d) k^{\frac{n}{d}}.$$

Таким образом,

$$M(n) = \frac{1}{n} \sum_{d|n} \mu(d) k^{\frac{n}{d}}.$$

Всё готово для того, чтобы подсчитать общее количество циклических последовательностей длины n.

Теорема 11.3.

$$T(n) = \frac{1}{n} \sum_{d|n} \varphi(d) k^{\frac{n}{d}}.$$

Доказательство.

$$\sum_{d|n} M(d) = \sum_{d|n} \frac{1}{d} \sum_{c|d} \mu(c) k^{\frac{d}{c}} = \sum_{d|n} \frac{1}{d} \sum_{c|d} \mu\left(\frac{d}{c}\right) k^c = \sum_{c|n} \frac{k^c}{c} \sum_{c|d} \frac{c}{d} \mu\left(\frac{d}{c}\right) =$$

$$= \sum_{c|n} \frac{k^c}{c} \sum_{e|\frac{n}{c}} \frac{\mu(e)}{e} = \sum_{c|n} \frac{k^c}{c} \frac{\varphi(n/c)}{n/c} = \frac{1}{n} \sum_{c|n} k^c \varphi\left(\frac{n}{c}\right) = \frac{1}{n} \sum_{d|n} \varphi(d) k^{\frac{n}{d}}.$$

В процессе выкладок мы меняли порядок суммирования, а также применили тождество (1). □

Упражнение 8. Составляются ожерелья из бусин трёх цветов. Каждое ожерелье состоит из 1) 5; 2) 6; 3) 7; 4) 8 бусин. Не будем различать ожерелья, получающиеся друг из друга поворотом в плоскости. Пользуясь предыдущей теоремой, найдите число различных ожерелий.

Ответ: 1) 51; 2) 130; 3) 315; 4) 834.

Замечание. Задачу о числе ожерелий можно также решить с помощью теории Пойа [12, 24].

12. Уравнение Пелля

Одним из немногих хорошо изученных нелинейных диофантовых уравнений является уравнение Пелля:

$$x^2 - my^2 = 1, \tag{1}$$

где m — натуральное число, не являющееся полным квадратом. Как известно, число $\sqrt{m}$ будет при этом иррациональным.

При любом m пары чисел $(1;0)$ и $(-1;0)$ являются решениями уравнения (1). Назовём такие решения *тривиальными*. Остальные решения уравнения Пелля — *нетривиальные*. Как мы увидим позднее, нетривиальные решения всегда существуют.

Всякое решение (1) с натуральными значениями переменных x и y будем называть *натуральным* решением, а натуральное решение с наименьшим возможным значением x — *фундаментальным* решением. В дальнейшем нам пригодится следующий простой факт.

Если $(a;b)$ и $(c;d)$ — натуральные решения уравнения (1), то

$$a < c \iff b < d, \quad a = c \iff b = d, \quad a > c \iff b > d.$$

Таким образом, на множестве натуральных решений естественным образом вводится отношение порядка: будем говорить, что решение $(a;b)$ *меньше* решения $(c;d)$, если $a < c$ (при этом и $b < d$).

Ясно, что если $(a;b)$ — натуральное решение, то решениями (1) будут также пары $(a;-b)$, $(-a;b)$ и $(-a;-b)$. С другой стороны, если $(c;d)$ — произвольное нетривиальное решение диофантова уравнения (1), то $(|c|;|d|)$ — натуральное решение. Таким образом, решая уравнение Пелля, достаточно найти все его натуральные решения.

Рассмотрим числовое множество

$$\mathbb{Z}\left[\sqrt{m}\right] = \{x + y\sqrt{m} \mid x, y \in \mathbb{Z}\}.$$

Несложно видеть, что это множество содержит 0 и 1 и замкнуто относительно операций сложения и умножения. Поэтому $\mathbb{Z}\left[\sqrt{m}\right]$ — коммутативное кольцо с единицей.

Заметим, что соответствие

$$(x;y) \to x + y\sqrt{m}$$

между $\mathbb{Z}^2$ и $\mathbb{Z}[\sqrt{m}]$ является взаимно однозначным. Действительно, если $x_1 + y_1\sqrt{m} = x_2 + y_2\sqrt{m}$ и $y_1 \neq y_2$, то $\sqrt{m} = \dfrac{x_1 - x_2}{y_2 - y_1}$, что противоречит иррациональности числа $\sqrt{m}$. Поэтому число $z \in \mathbb{Z}[\sqrt{m}]$ представляется в виде $x + y\sqrt{m}$ единственным способом.

Указанное соответствие позволяет *отождествлять* пару целых чисел $(x;y)$ с числом $z = x + y\sqrt{m}$. Ниже иногда мы будем говорить, что $z = x + y\sqrt{m}$ — решение уравнения (1), имея в виду, что таковым на самом деле является пара $(x;y)$.

Введём на кольце $\mathbb{Z}[\sqrt{m}]$ операцию *сопряжения*:

$$\overline{x + y\sqrt{m}} = x - y\sqrt{m}.$$

Очевидно, что сопряжённое к сопряжённному есть исходное число: $\overline{\overline{z}} = z$. Докажем, что сопряжённое к произведению есть произведение сопряжённых: $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$. Действительно,

$$\overline{\left(x_1 + y_1\sqrt{m}\right)\left(x_2 + y_2\sqrt{m}\right)} = \overline{x_1x_2 + y_1y_2m + (x_1y_2 + y_1x_2)\sqrt{m}} =$$

$$= x_1x_2 + y_1y_2m - (x_1y_2 + y_1x_2)\sqrt{m} = \left(x_1 - y_1\sqrt{m}\right)\left(x_2 - y_2\sqrt{m}\right).$$

Введём *норму* числа $z = x + y\sqrt{m}$:

$$||z|| = z \cdot \overline{z} = x^2 - my^2.$$

Решить уравнение Пелля означает найти все числа с единичной нормой.

Отметим свойства нормы: сопряжённые числа имеют одинаковые нормы; норма произведения равна произведению норм. Действительно,

$$||\overline{z}|| = \overline{z} \cdot \overline{\overline{z}} = \overline{z} \cdot z = ||z||;$$

$$||z_1 \cdot z_2|| = z_1 \cdot z_2 \cdot \overline{z_1 \cdot z_2} = z_1 \cdot z_2 \cdot \overline{z_1} \cdot \overline{z_2} = z_1 \cdot \overline{z_1} \cdot z_2 \cdot \overline{z_2} = ||z_1|| \cdot ||z_2||.$$

Легко видеть, что числа с единичной нормой образуют мультипликативную группу. Элементом, обратным к числу z, является сопряжённое число $\overline{z}$. Если $(x_1;y_1)$ — решение уравнения (1), и

$$z_1 = x_1 + y_1\sqrt{m}, \quad z_k = z_1^k = x_k + y_k\sqrt{m},$$

то $(x_k; y_k)$ — также решение (1). Другими словами, степень каждого решения является решением. Оказывается, что степени фундаментального решения исчерпывают множество натуральных решений уравнения Пелля. Об этом говорит следующая теорема.

Теорема 12.1. *Пусть $(x_1; y_1)$ — фундаментальное решение, а $(x; y)$ — произвольное натуральное решение уравнения (1). Тогда для некоторого натурального k имеет место равенство*

$$z = x + y\sqrt{m} = \left(x_1 + y_1\sqrt{m}\right)^k.$$

Доказательство. Пусть, как и выше,

$$z_k = \left(x_1 + y_1\sqrt{m}\right)^k = x_k + y_k\sqrt{m}.$$

Возникают две бесконечные возрастающие последовательности натуральных чисел:

$$x_1 < x_2 < \ldots < x_k < \ldots; \quad y_1 < y_2 < \ldots < y_k < \ldots.$$

Если решение уравнения (1) $z = x + y\sqrt{m}$ не является степенью числа z_1, то найдётся такое число n, что $x_n < x < x_{n+1}$. При этом выполняются также неравенства $y_n < y < y_{n+1}$ и

$$z_1^n < z < z_1^{n+1}. \tag{2}$$

Умножив неравенство (2) на $\overline{z}_1{}^n$, получим

$$1 < X + Y\sqrt{m} < z_1, \tag{3}$$

где $X + Y\sqrt{m} = (x + y\sqrt{m})\,(x_1 - y_1\sqrt{m})^n$. Число $X + Y\sqrt{m}$, будучи произведением чисел с единичной нормой, также имеет единичную норму:

$$\left(X + Y\sqrt{m}\right)\left(X - Y\sqrt{m}\right) = 1. \tag{4}$$

Из соотношений (3) и (4) следует, что

$$0 < X - Y\sqrt{m} < 1. \tag{5}$$

Следствием (3) и (5) является неравенство $X - Y\sqrt{m} < X + Y\sqrt{m}$, из которого получаем, что $Y > 0$. Теперь из неравенства $X - Y\sqrt{m} > 0$ вытекает, что и $X > 0$. Таким образом, $(X; Y)$ — натуральное решение уравнения Пелля, причём

$$X + Y\sqrt{m} < x_1 + y_1\sqrt{m}.$$

Это противоречит фундаментальности решения $(x_1; y_1)$. □

Явные формулы для решений уравнения Пелля

Пример. Рассмотрим уравнение $x^2 - 2y^2 = 1$. Фундаментальное решение — пара $(3;2)$. Выведем рекуррентные соотношения для последовательностей (x_n) и (y_n). Из равенств

$$x_{k+1} + y_{k+1}\sqrt{2} = (3 + 2\sqrt{2})^{k+1} = (x_k + y_k\sqrt{2})(3 + 2\sqrt{2})$$

следует, что

$$x_{k+1} = 3x_k + 4y_k; \quad y_{k+1} = 2x_k + 3y_k. \tag{6}$$

По формулам (6) последовательно находим решения: $(3;2)$, $(17;12)$, $(99;70)$, $(577;408)$, ... Из соотношений (6), связывающих две последовательности, несложно получить рекуррентные соотношения для каждой из них в отдельности. Например, выразив y_k через x_k и x_{k+1}

$$y_k = \frac{x_{k+1} - 3x_k}{4},$$

получим $y_{k+1} = \frac{x_{k+2} - 3x_{k+1}}{4}$ и подставим во второе соотношение (6):

$$\frac{x_{k+2} - 3x_{k+1}}{4} = 2x_k + 3 \cdot \frac{x_{k+1} - 3x_k}{4},$$

откуда

$$x_{k+2} = 6x_{k+1} - x_k. \tag{7}$$

Аналогично получается соотношение

$$y_{k+2} = 6y_{k+1} - y_k. \tag{8}$$

Решив рекуррентные соотношения (7) и (8), получим явные формулы для (x_n) и (y_n):

$$x_n = \frac{1}{2}\left((3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n\right);$$

$$y_n = \frac{1}{2\sqrt{2}}\left((3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n\right).$$

Явные формулы для последовательностей (x_n) и (y_n) можно получить и не составляя рекуррентных соотношений! Покажем, как это делается в общем случае.

По свойству операции сопряжения, из тождества

$$x_n + \sqrt{m}y_n = (x_1 + \sqrt{m}y_1)^n$$

следует

$$x_n - \sqrt{m}y_n = (x_1 - \sqrt{m}y_1)^n.$$

В результате сложения и вычитания данных тождеств получим

$$x_n = \frac{1}{2}\left((x_1 + \sqrt{m}y_1)^n + (x_1 - \sqrt{m}y_1)^n\right);$$

$$y_n = \frac{1}{2\sqrt{m}}\left((x_1 + \sqrt{m}y_1)^n - (x_1 - \sqrt{m}y_1)^n\right).$$

А теперь из явных формул легко получить рекуррентные соотношения для наших последовательностей. Действительно, каждая из них представляет сумму двух геометричесих прогрессий. Воспользуемся таким (легко проверяемым) фактом: если $a_n = c_1\lambda_1^n + c_2\lambda_2^n$, то $a_{n+2} = (\lambda_1 + \lambda_2)a_{n+1} - \lambda_1\lambda_2 a_n$. Отсюда

$$x_{n+2} = 2x_1x_{n+1} - x_n; \quad y_{n+2} = 2x_1y_{n+1} - y_n.$$

Существование нетривиального решения

Теорема 12.2. *Уравнение (1) имеет нетривиальные решения.*

Доказательство. Опишем алгоритм нахождения некоторого нетривиального решения, придуманный в 2008 г. австралийским математиком Н. Вайлдбергером [18, 25]. Этот способ доказательства теоремы 12.2 значительно проще ранее известных.

Рассмотрим квадратичную форму

$$Q(x,y) = (x\ y)\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = ax^2 + 2bxy + cy^2.$$

Матрицу $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ назовём *подходящей*, если $a > 0, c < 0$.

Уравнение Пелля $x^2 - my^2 = 1$ можно записать в виде $Q(x,y) = 1$ с матрицей квадратичной формы $A_0 = \begin{pmatrix} 1 & 0 \\ 0 & -m \end{pmatrix}$. Заметим, что эта матрица является подходящей, а число $-|A_0|$ не является полным квадратом.

Итог матрицы — сумма её элементов.

Введём в рассмотрение две матрицы: $L = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ и $R = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Будем строить последовательность матриц $A_i = \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix}$, где $i = 0, 1, 2, \ldots$, в которой очередная матрица получается из предыдущей с помощью одного из следующих преобразований.

Левый шаг — замена матрицы $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ на матрицу $L'AL = \begin{pmatrix} a+2b+c & b+c \\ b+c & c \end{pmatrix}$. *Правый шаг* — замена матрицы A на матрицу $R'AR = \begin{pmatrix} a & a+b \\ a+b & a+2b+c \end{pmatrix}$.

Если у матрицы положительный итог, будем делать левый шаг, а если отрицательный, то правый. Легко видеть, что из подходящей матрицы всегда получится подходящая.

Убедимся в том, что итог любой матрицы из нашей последовательности отличен от нуля. Поскольку $|L| = |R| = 1$, левый и правый шаги не меняют определителя матрицы. Значит, определитель каждой матрицы равен $|A_0| = -m$. С другой стороны, матрица с нулевым итогом имеет вид $\begin{pmatrix} a & b \\ b & -a-2b \end{pmatrix}$, где a и b — целые числа, и её определитель равен $-(b-a)^2$. Получаем, что $m = (b-a)^2$, в то время как число m, по условию, не является полным квадратом.

Итак, мы имеем бесконечную последовательность матриц $A_i = \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix}$ таких, что $a_i > 0, c_i < 0, a_i c_i - b_i^2 = -m$. Числа $a_i, -c_i$ и b_i образуют решение в натуральных числах уравнения $xy + z^2 = m$. Очевидно, что это уравнение в натуральных числах имеет имеет конечное множество решений. Значит, в последовательности (A_i) не все матрицы различны. Покажем, что первой повторится матрица A_0.

Для этого сначала убедимся в том, что по матрице A_i можно однозначно определить ей предшествующую матрицу A_{i-1}.

Если $A_i = L'A_{i-1}L$, то $A_{i-1} = (L')^{-1}A_iL^{-1} =$

$$= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} a_i - 2b_i + c_i & b_i - c_i \\ b_i - c_i & c_i \end{pmatrix}.$$

Если $A_i = R'A_{i-1}R$, то $A_{i-1} = (R')^{-1}A_iR^{-1} =$

$$= \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a_i & b_i \\ b_i & c_i \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_i & b_i - a_i \\ b_i - a_i & a_i - 2b_i + c_i \end{pmatrix}.$$

Значит, всё определяется величиной $t = a_i - 2b_i + c_i$. Если $t > 0$, то матрица A_i получена из A_{i-1} левым шагом; если же $t < 0$, то правым. Равенство $t = 0$ невозможно из-за того, что матрица A_{i-1} — подходящая (на её главной диагонали нет нулей).

Таким образом, если некоторая матрица A_i, отличная от A_0, в нашей последовательности встретилась второй раз, то тем же свойством обладает и матрица A_{i-1}. Поэтому первой повторится матрица A_0.

Примеры. Выпишем последовательности матриц (A_i) между двумя вхождениями начальной матрицы A_0 для $m = 2$ и $m = 7$. Над стрелкой перехода указан итог матрицы, а под стрелкой вид шага: R или L.

$$\begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix} \xrightarrow[R]{-1} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \xrightarrow[L]{2} \begin{pmatrix} 2 & 0 \\ 0 & -1 \end{pmatrix} \xrightarrow[L]{1}$$

$$\longrightarrow \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \xrightarrow[R]{-2} \begin{pmatrix} 1 & 0 \\ 0 & -2 \end{pmatrix}.$$

Результирующее преобразование при $m = 2$ задаётся матрицей $N = RL^2R$.

$$\begin{pmatrix} 1 & 0 \\ 0 & -7 \end{pmatrix} \xrightarrow[R]{-6} \begin{pmatrix} 1 & 1 \\ 1 & -6 \end{pmatrix} \xrightarrow[R]{-3} \begin{pmatrix} 1 & 2 \\ 2 & -3 \end{pmatrix} \xrightarrow[L]{2} \begin{pmatrix} 2 & -1 \\ -1 & -3 \end{pmatrix} \xrightarrow[R]{-3}$$

$$\longrightarrow \begin{pmatrix} 2 & 1 \\ 1 & -3 \end{pmatrix} \xrightarrow[L]{1} \begin{pmatrix} 1 & -2 \\ -2 & -3 \end{pmatrix} \xrightarrow[R]{-6} \begin{pmatrix} 1 & -1 \\ -1 & -6 \end{pmatrix} \xrightarrow[R]{-7} \begin{pmatrix} 1 & 0 \\ 0 & -7 \end{pmatrix}.$$

Результирующее преобразование при $m = 7$ задаётся матрицей $N = R^2LRLR^2$.

Заметим, что первый шаг в последовательности преобразований всегда правый (поскольку итог начальной матрицы $1 - m < 0$). Но все шаги правыми быть не могут. Действительно, если матрица A_i получена правым шагом, то $b_i = a_{i-1} + b_{i-1} > b_{i-1}$, а числовая последовательность (b_i) не может быть возрастающей в силу своей периодичности.

Поэтому матрица $N = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, задающая результирующее преобразование, всегда состоит из натуральных чисел.

Итак, предъявлен алгоритм, позволяющий найти матрицу N, для которой выполнено матричное равенство

$$N'A_0N = A_0.$$

Пусть теперь $Q(x,y) = (x\ y)A_0\begin{pmatrix} x \\ y \end{pmatrix} = 1$ и $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = N\begin{pmatrix} x \\ y \end{pmatrix}$. Тогда

$$Q(x_1,y_1) = (x_1\ y_1)A_0\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = (x\ y)N'A_0N\begin{pmatrix} x \\ y \end{pmatrix} =$$

$$= (x\ y)A_0\begin{pmatrix} x \\ y \end{pmatrix} = Q(x,y) = 1.$$

Другими словами, если (x,y) — решение уравнения Пелля, то (x_1,y_1) тоже является решением. В частности, по тривиальному решению $(1,0)$ находим решение (α,γ), которое уже не является тривиальным, поскольку $\alpha,\gamma > 0$. □

Примеры. Для $m = 2$ имеем $N = RL^2R = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$ и решение $(3,2)$. Для $m = 7$ имеем $N = R^2LRLR^2 = \begin{pmatrix} 8 & 21 \\ 3 & 8 \end{pmatrix}$ и решение $(8,3)$.

И явные, и рекуррентные формулы для решений уравнения Пелля требуют знания фундаментального решения.

В таблице приведены соотношения для фундаментальных решений уравнения Пелля при малых m.

m	x	y	m	x	y	m	x	y
2	3	2	20	9	2	37	73	12
3	2	1	21	55	12	38	37	6
5	9	4	22	197	42	39	25	4
6	5	2	23	24	5	40	19	3
7	8	3	24	5	1	41	2 049	320
8	3	1	26	51	10	42	13	2
10	19	6	27	26	5	43	3 482	531
11	10	3	28	127	24	44	199	30
12	7	2	29	9 801	1 820	45	161	24
13	649	180	30	11	2	46	24 335	3 588
14	15	4	31	1 520	273	47	48	7
15	4	1	32	17	3	48	7	1
17	33	8	33	23	4	50	99	14
18	17	4	34	35	6	51	50	7
19	170	39	35	6	1	52	649	90

Приведём ещё несколько примеров: $48\,842^2 - 67 \cdot 5\,967^2 = 1$;

$$1\,766\,319\,049^2 - 61 \cdot 226\,153\,980^2 = 1; \quad 1\,151^2 - 92 \cdot 120^2 = 1.$$

Как видим, даже при небольших m значения x и y могут быть весьма велики. Поэтому примитивным перебором здесь не обойтись. В следующих параграфах будет рассмотрен один из наиболее эффективных методов нахождения решений уравнения Пелля. В его основе лежит понятие цепной дроби.

13. Цепные дроби

Пусть $\dfrac{a}{b}$ — несократимая дробь. Применим алгоритм Евклида к паре чисел $\langle a; b\rangle$:

$$a = ba_0 + r_1; \quad b = r_1a_1 + r_2; \quad r_1 = r_2a_2 + r_3; \quad \ldots;$$

$$r_{n-3} = r_{n-2}a_{n-2} + r_{n-1}; \quad r_{n-2} = r_{n-1}a_{n-1} + 1; \quad r_{n-1} = 1 \cdot a_n.$$

Отсюда возникают следующие выражения для дроби $\dfrac{a}{b}$:

$$\frac{a}{b} = a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\dfrac{b}{r_1}} = a_0 + \frac{1}{a_1 + \dfrac{r_2}{r_1}} = a_0 + \frac{1}{a_1 + \dfrac{1}{\dfrac{r_1}{r_2}}} =$$

$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{r_3}{r_2}}} = \ldots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}. \qquad (1)$$

Последнее выражение в формуле (1) называют цепной дробью и обозначают $[a_0; a_1, a_2, \ldots, a_n]$.

Итак, любое рациональное число представимо в виде цепной дроби.

Пусть теперь α — иррациональное число. Положим

$$a_0 = [\alpha], \quad \alpha_1 = \frac{1}{\{\alpha\}}.$$

Имеет место равенство $\alpha = [\alpha] + \{\alpha\} = a_0 + \dfrac{1}{\alpha_1}$. Построим последовательности (α_k) и (a_k) с помощью рекуррентных соотношений:

$$a_k = [\alpha_k], \quad \alpha_{k+1} = \frac{1}{\{\alpha_k\}}.$$

При этом $\alpha_k = a_k + \dfrac{1}{\alpha_{k+1}}$. Определим функции

$$f_1(x) = a_0 + \frac{1}{x}, \quad f_2(x) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{x}}, \ldots$$

$$f_n(x) = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{x}}}}.$$

На положительной полуоси функция $f_1(x)$ убывает, функция $f_2(x)$ возрастает, функция $f_3(x)$ — вновь убывающая и т. д. Заметим также, что

$$\alpha = f_1(\alpha_1) = f_2(\alpha_2) = \ldots = f_n(\alpha_n) = \ldots.$$

Число $r_n = f_n(a_n) = [a_0; a_1, a_2, \ldots, a_n]$ называют *n-й подходящей дробью числа α*, или *подходящей дробью n-го порядка.*

Отвлечёмся на некоторое время от того, откуда берутся целое число a_0 и натуральные числа $a_1, a_2, \ldots$, и выясним характер поведения последовательности (r_n).

Представим r_n в виде дроби $r_n = \dfrac{p_n}{q_n}$. Пусть $p_0 = a_0$, $q_0 = 1$. Далее имеем

$$r_1 = \frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}.$$

Положим $p_1 = a_0 a_1 + 1 = p_0 a_1 + 1, \quad q_1 = a_1 = q_0 a_1$. Найдём выражение для второй подходящей дроби:

$$r_2 = p_0 + \frac{1}{q_1 + \frac{1}{a_2}} = p_0 + \frac{a_2}{q_1 a_2 + 1} = \frac{(p_0 q_1 + 1)a_2 + p_0}{q_1 a_2 + 1} = \frac{p_1 a_2 + p_0}{q_1 a_2 + q_0}.$$

Можно положить $p_2 = p_1 a_2 + p_0, \quad q_2 = q_1 a_2 + q_0$. Если в выражении для r_2 заменить a_2 на $a_2 + \dfrac{1}{a_3}$, то возникнет 3-я подходящая дробь

$$r_3 = \frac{p_1\left(a_2 + \dfrac{1}{a_3}\right) + p_0}{q_1\left(a_2 + \dfrac{1}{a_3}\right) + q_0} = \frac{(p_1 a_2 + p_0)a_3 + p_1}{(q_1 a_2 + q_0)a_3 + q_1} = \frac{p_2 a_3 + p_1}{q_2 a_3 + q_1}.$$

Естественно взять $p_3 = p_2 a_3 + p_1, \quad q_3 = q_2 a_3 + p_2$. Точно так же методом математической индукции доказывается, что если для числителей и знаменателей подходящих дробей имеют место рекуррентные соотношения

$$p_{n+1} = p_n a_{n+1} + p_{n-1}, \tag{2}$$

$$q_{n+1} = q_n a_{n+1} + q_{n-1}, \tag{3}$$

то для любого натурального n справедливо $r_n = \dfrac{p_n}{q_n}$.

Исключим из найденных соотношений a_{n+1}. Для этого умножим (2) на q_n, а (3) на p_n, после чего вычтем из второго равенства первое:

$$p_n q_{n+1} - p_{n+1} q_n = -(p_{n-1} q_n - p_n q_{n-1}). \tag{4}$$

Заменяя n раз n на $n-1$ в тождестве (4), получим:

$$p_{n-1} q_n - p_n q_{n-1} = -(p_{n-2} q_{n-1} - p_{n-1} q_{n-2}) = \ldots =$$

$$= (-1)^{n-1}(p_0q_1 - p_1q_0) = (-1)^{n-1}(a_0a_1 - (a_0a_1 + 1)) = (-1)^n.$$

Мы доказали, что для любого натурального n

$$p_{n-1}q_n - p_nq_{n-1} = (-1)^n. \tag{5}$$

Из данного тождества вытекает, что p_n и q_n — взаимно простые числа. Действительно, если число d — их общий натуральный делитель, то и левая часть равенства (5) делится на d. Значит, и число $(-1)^n$ делится на d. Отсюда $d = 1$. Доказано, что $\dfrac{p_n}{q_n}$ — несократимая дробь.

Соотношение (5) позволяет получить и другие важные следствия.

Поделив (5) на q_nq_{n-1}, получим

$$r_{n-1} - r_n = \frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_nq_{n-1}}. \tag{6}$$

Теперь можно найти разность r_{n-2} и r_n:

$$r_{n-2} - r_n = (r_{n-2} - r_{n-1}) + (r_{n-1} - r_n) = \frac{(-1)^{n-1}}{q_{n-1}q_{n-2}} + \frac{(-1)^n}{q_nq_{n-1}} =$$

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

Из (3) следует, что $q_n - q_{n-2} = a_nq_{n-1}$. Поэтому

$$r_{n-2} - r_n = \frac{(-1)^{n-1}a_n}{q_{n-2}q_n}. \tag{7}$$

Из равенства (7) вытекает, что подходящие дроби нечётного порядка образуют убывающую последовательность, а чётного порядка — возрастающую:

$$r_1 > r_3 > r_5 > \ldots; \quad r_2 < r_4 < r_6 < \ldots.$$

Соотношение (6) показывает, что подходящая дробь нечётного порядка больше следующей за ней дроби: $r_{2k-1} > r_{2k}$. Учитывая характер монотонности подпоследовательностей (r_{2k}) и (r_{2k-1}), получаем теперь, что для любого k

$$r_{2k-1} > r_2, \quad r_{2k} < r_1.$$

Таким образом, убывающая последовательность r_{2k-1} ограничена снизу, а возрастающая последовательность r_{2k} ограничена сверху. По теореме Больцано – Вейерштрасса эти последовательности имеют предел. Из соотношения (6) следует, что указанные пределы равны.

Мы доказали, что произвольная бесконечная последовательность натуральных чисел (a_n) порождает сходящуюся последовательность несократимых дробей (r_n). Поэтому можно ввести понятие бесконечной цепной дроби как предела последовательности конечных цепных дробей:

$$[a_0; a_1, a_2, \ldots] = \lim_{n\to\infty} [a_0; a_1, a_2, \ldots, a_n].$$

Вспомним теперь, что последовательность (a_n) была порождена иррациональным числом α, при этом для любого n

$$\alpha = f_n(\alpha_n), \quad a_n = [\alpha_n] < \alpha_n.$$

Поскольку f_{2k} — возрастающая функция, имеем

$$r_{2k} = f_{2k}(a_{2k}) < f_{2k}(\alpha_{2k}) = \alpha.$$

Из убывания функции f_{2k-1}, в свою очередь, следует:

$$r_{2k-1} = f_{2k-1}(a_{2k-1}) > f_{2k-1}(\alpha_{2k-1}) = \alpha.$$

Значит, $\lim r_{2k} \leqslant \alpha, \quad \lim r_{2k-1} \geqslant \alpha$. Поскольку, как уже доказано, $\lim r_{2k} = \lim r_{2k-1}$, получаем, что $\lim r_n = \alpha$.

Подытожим наши выкладки формулировкой теоремы.

Теорема 13.1. *Последовательность подходящих дробей, порождённая числом α, сходится к α, при этом дроби чётного порядка меньше α и образуют возрастающую последовательность, а дроби нечётного порядка больше α и образуют убывающую последовательность.*

Примеры. $\sqrt{2} = [1; 2, 2, 2, \ldots], \quad \sqrt{11} = [3; 3, 6, 3, 6, \ldots]$.

Известно [10], что последовательность (a_n) является периодической тогда и только тогда, когда число α является *квадратической иррациональностью* — иррациональным корнем квадратного уравнения с целыми коэффициентами.

Некоторую информацию о длинах периода для чисел вида $\sqrt{m}$ можно найти в [18].

Пусть $l(m)$ — длина периода цепной дроби для числа $\sqrt{m}$. Приведём значения $l(m)$ для малых m.

m	2	3	5	6	7	8	10	11	12	13	14	15	17
$l(m)$	1	2	1	2	4	2	1	2	2	5	4	2	1

m	18	19	20	21	22	23	24	26	27	28	29
$l(m)$	2	6	2	6	6	4	2	1	2	4	5

m	30	31	32	33	34	35	37	38	39	40	41
$\lambda(m)$	2	8	4	4	4	2	1	2	2	2	3

14. Разложение числа e в цепную дробь

Определим числовую последовательность $I_{-1}, I_0, I_1, I_2, \ldots$ следующими формулами:

$$I_{3n-1} = \frac{1}{n!}\int\limits_0^1 e^x x^{n+1}(1-x)^n dx,\ n = 0, 1, 2, \ldots;$$

$$I_{3n} = \frac{1}{n!}\int\limits_0^1 e^x x^n (1-x)^{n+1} dx,\ n = 0, 1, 2, \ldots;$$

$$I_{3n-2} = \frac{1}{n!}\int\limits_0^1 e^x x^n (1-x)^n dx,\ n = 1, 2, \ldots.$$

Заметим, что

$$I_{3n-2} - I_{3n-1} = \frac{1}{n!}\int\limits_0^1 e^x x^n (1-x)^n (1-x) dx = I_{3n}.$$

Интегрируя по частям, имеем

$$I_{3n+1} = \frac{1}{(n+1)!}\int\limits_0^1 (x-x^2)^{n+1} de^x = -\frac{1}{n!}\int\limits_0^1 e^x (x-x^2)^n (1-2x) dx =$$

$$= \frac{1}{n!}\int\limits_0^1 e^x (x-x^2)^n (x-(1-x)) dx = I_{3n-1} - I_{3n};$$

$$I_{3n+2} = \frac{-1}{(n+1)!}\int\limits_0^1 (x-x^2)^{n+1} d(e^x(1-x)) =$$

$$= \frac{1}{n!}\int_0^1 e^x x^n (1-x)^{n+1}(1-2x)dx = I_{3n} - (2n+2)I_{3n+1}.$$

Таким образом, для любого неотрицательного целого k выполнено равенство

$$I_{k-1} = b_k I_k + I_{k+1}, \tag{1}$$

где

$$b_k = \begin{cases} 1, & \text{если } k = 3n-1 \text{ или } k = 3n, \\ 2n+2, & \text{если } k = 3n+1. \end{cases}$$

Обозначим $\alpha_k = \frac{I_{k-1}}{I_k}$, где $k = 0, 1, \ldots$ Поделив обе части равенства (1) на I_k, получим

$$\alpha_k = b_k + \frac{1}{\alpha_{k+1}}. \tag{2}$$

Отсюда видно, что $\alpha_k > 1$ и что $b_k = [\alpha_k]$. Значит соотношение (2) даёт разложение числа α_0 в бесконечную цепную дробь:

$$\alpha_0 = [b_0; b_1, b_2, b_3, \ldots] = [1; 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots].$$

Вычислим α_0.

$$I_{-1} = \int_0^1 e^x x dx = 1; \quad I_0 = \int_0^1 e^x (1-x)dx = e - 2;$$

$$\alpha_0 = \frac{I_{-1}}{I_0} = \frac{1}{e-2}.$$

Отсюда

$$e = 2 + \frac{1}{\alpha_0} = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots].$$

Так что цепная дробь числа e имеет вполне регулярный вид (в отличие от представления числа e в виде бесконечной десятичной дроби).

Кстати, из того, что цепная дробь числа e бесконечная, получаем иррациональность числа e.

15. Подходящие дроби как наилучшие приближения

Пусть фиксировано некоторое число α. Введём на множестве несократимых дробей с натуральными знаменателями следующее отношение порядка.

Будем говорить, что дробь $\frac{a}{b}$ ($a \in \mathbb{Z}$, $b \in \mathbb{N}$) *приближает число* α *лучше дроби* $\frac{c}{d} \neq \frac{a}{b}$ ($c \in \mathbb{Z}$, $d \in \mathbb{N}$), если выполняются неравенства

$$b \leqslant d; \quad |b\alpha - a| < |d\alpha - c|.$$

Наилучшим приближением числа α называется такая дробь $\frac{a}{b}$, что ни одна дробь не является приближением лучшим, чем $\frac{a}{b}$.

Проверьте, к примеру, что числа $\frac{1}{1}$, $\frac{3}{2}$, $\frac{7}{5}$ являются наилучшими приближениями числа $\sqrt{2}$.

Таким образом, нет дроби лучше наилучшей, но это не означает, что наилучшая дробь лучше любой другой! Введённое отношение порядка не является линейным: не любые две дроби сравнимы по данному отношению. Например, несравнимы любые два различных наилучших приближения. Если α — иррациональное число, то для него существует бесконечно много наилучших приближений.

Имеет место следующий замечательный факт.

Теорема 15.1. *Всякое наилучшее приближение иррационального числа* α *есть подходящая дробь этого числа.*

Доказательство. Из результатов предыдущего параграфа мы знаем, что для подходящих дробей (r_n) числа α выполняются неравенства

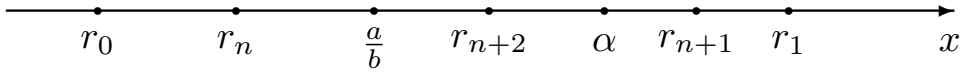
$$r_0 < r_2 < r_4 < r_6 < \ldots < \alpha < \ldots < r_5 < r_3 < r_1.$$

Если наилучшее приближение $\frac{a}{b}$ не является подходящей дробью, то имеет место одна из ситуаций:

- $\frac{a}{b} < r_0$;
- $\frac{a}{b}$ находится между двумя соседними подходящими дробями чётного порядка;

- $\dfrac{a}{b}$ находится между двумя соседними подходящими дробями нечётного порядка;
- $\dfrac{a}{b} > r_1$.

Пусть, например, для некоторого чётного n выполняется неравенство $r_n < \dfrac{a}{b} < r_{n+2}$.



Тогда

$$\left|\frac{a}{b} - r_n\right| = \left|\frac{a}{b} - \frac{p_n}{q_n}\right| = \left|\frac{aq_n - p_n b}{bq_n}\right| \geqslant \frac{1}{bq_n}.$$

С другой стороны,

$$\left|\frac{a}{b} - r_n\right| < r_{n+1} - r_n = \frac{1}{q_n q_{n+1}}.$$

Сопоставление полученных неравенств даёт

$$\frac{1}{bq_n} < \frac{1}{q_n q_{n+1}},$$

откуда $q_{n+1} < b$.

Далее имеем

$$\left|\alpha - \frac{a}{b}\right| > r_{n+2} - \frac{a}{b} = \frac{p_{n+2}}{q_{n+2}} - \frac{a}{b} \geqslant \frac{1}{bq_{n+2}},$$

откуда

$$|b\alpha - a| > \frac{1}{q_{n+2}}.$$

В то же время

$$|\alpha - r_{n+1}| < r_{n+1} - r_{n+2} = \frac{1}{q_{n+1}q_{n+2}}$$

и

$$|q_{n+1}\alpha - p_{n+1}| < \frac{1}{q_{n+2}}.$$

Значит,

$$|q_{n+1}\alpha - p_{n+1}| < |b\alpha - a|.$$

Таким образом, дробь $r_{n+1} = \dfrac{p_{n+1}}{q_{n+1}}$ является лучшим приближением α, нежели дробь $\dfrac{a}{b}$ — последняя не является наилучшим приближением.

Аналогично рассматриваются три других случая. □

Верным является и обратное утверждение.

Теорема 15.2. *Всякая подходящая дробь иррационального числа α является его наилучшим приближением.*

Доказательство этой теоремы можно найти в [17].

Теорема 15.3. *Всякая дробь, удовлетворяющая неравенству*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2},$$

есть наилучшее приближение α.

Доказательство. Пусть дробь $\dfrac{c}{d} \neq \dfrac{a}{b}$ приближает α лучше, чем дробь $\dfrac{a}{b}$. Тогда

$$|d\alpha - c| < |b\alpha - a| < \frac{1}{2b}; \quad \left|\alpha - \frac{c}{d}\right| < \frac{1}{2bd};$$

$$\left|\frac{c}{d} - \frac{a}{b}\right| \leqslant \left|\frac{c}{d} - \alpha\right| + \left|\alpha - \frac{a}{b}\right| < \frac{1}{2bd} + \frac{1}{2b^2} = \frac{b+d}{2b^2d}.$$

В то же время

$$\left|\frac{c}{d} - \frac{a}{b}\right| = \frac{|cb - ad|}{db} \geqslant \frac{1}{bd}.$$

Значит, $\dfrac{1}{bd} < \dfrac{b+d}{2b^2d}$, откуда $d > b$. Противоречие! □

Теперь всё готово для того, чтобы установить связь между решениями уравнения Пелля $x^2 - my^2 = 1$ и подходящими дробями числа $\sqrt{m}$.

16. Уравнение Пелля и подходящие дроби

Теорема 16.1. *Пусть $(x; y)$ — натуральное решение уравнения*

$$x^2 - my^2 = 1. \tag{1}$$

Тогда $\dfrac{x}{y}$ — подходящая дробь числа $\sqrt{m}$.

Доказательство. Поскольку $x > y > 0$ и $\sqrt{m} > 1$, имеем

$$x + y\sqrt{m} > 2y.$$

Поэтому

$$x - y\sqrt{m} = \frac{1}{x + y\sqrt{m}} < \frac{1}{2y}; \quad 0 < \frac{x}{y} - \sqrt{m} < \frac{1}{2y^2}.$$

Согласно теореме 15.3 число $\dfrac{x}{y}$ является наилучшим приближением числа $\sqrt{m}$, следовательно, и подходящей дробью этого числа (по теореме 15.1). □

Итак, фундаментальное решение уравнения Пелля (1) можно найти, перебирая подходящие дроби числа $\sqrt{m}$. Укажем номера соответствующих дробей при $m \leqslant 30$.

1-я подходящая дробь даст фундаментальное решение при $m = 2, 3, 5, 6, 8, 10, 11, 12, 15, 17, 18, 20, 24, 26, 27, 30$;

3-я подходящая дробь даст фундаментальное решение при $m = 7, 14, 23, 28$;

5-я подходящая дробь даст фундаментальное решение при $m = 19, 21, 22$;

9-я подходящая дробь даст фундаментальное решение при $m = 13, 29$.

А при $m = 61$ номер подходящей дроби — 21.

Имеет место следующая теорема, доказательство которой можно найти в [4].

Теорема 16.2. *Пусть $\dfrac{p_n}{q_n}$ — n-я подходящая дробь числа $\sqrt{m}$, а $l(m)$ — длина периода его цепной дроби. Пара $(p_n; q_n)$ является решением уравнения (1) тогда и только тогда, когда $n \equiv -1 (\mathrm{mod}\, l(m))$ и n нечётно.*

Замечание. Известны и другие алгоритмы решения уравнения Пелля. Два из них — *индийский* и *английский* — описаны в [18] и [27].

17. Сравнения n-й степени

Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ — многочлен с целыми коэффициентами. *Решить сравнение*

$$f(x) \equiv 0 (\mathrm{mod}\, m) \tag{1}$$

означает найти все целые значения переменной x, ему удовлетворяющие. Как известно, если $x \equiv x_0 (\mathrm{mod}\, m)$, то и $f(x) \equiv f(x_0) (\mathrm{mod}\, m)$. Поэтому в качестве решений уравнения (1) можно рассматривать классы вычетов по модулю m. Будем говорить, что сравнение (1) имеет столько решений, сколько классов вычетов по модулю m ему удовлетворяют. Степень многочлена $f(x)$ называют *степенью сравнения* (1). Пусть p — простое число. Тогда сравнение

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 (\mathrm{mod}\, p) \qquad (2)$$

с целыми коэффициентами a_i можно свести к некоторому сравнению степени не выше $p-1$. Действительно, поделим многочлен $f(x)$ на многочлен $x^p - x$:

$$f(x) = (x^p - x) q(x) + r(x),$$

где степень остатка $r(x)$ не превосходит $p-1$. Из малой теоремы Ферма следует, что $f(x) \equiv r(x) (\mathrm{mod}\, p)$.

Теорема 17.1. *Если сравнение n-й степени по простому модулю p имеет более n решений, то все коэффициенты многочлена $f(x)$ кратны p.*

Доказательство. Пусть сравнение (2) имеет $n+1$ решений x_1, x_2, $\ldots$, x_{n+1}, где $x_i \not\equiv x_j (\mathrm{mod}\, p)$ при $i \neq j$. Многочлены $g_0 = 1$ и $g_k(x) = \prod_{i=1}^{k} (x - x_i)$, $k = 1, \ldots, n$, образуют базис в пространстве $\mathbb{Z}_n[x]$ многочленов с целыми коэффициентами степени не выше n. Разложим многочлен $f(x)$ по этому базису:

$$f(x) = \sum_{k=0}^{n} b_k g_k(x). \qquad (3)$$

Заметим, что $g_k(x_i) = 0$ при $i \leqslant k$. Поскольку $f(x_1) = b_0$, коэффициент b_0 делится на p. Подставим теперь в многочлен (3) $x = x_2$:

$$f(x_2) = b_1 g_1(x_2) + b_0 = b_1 (x_2 - x_1) + b_0.$$

Теперь видно, что b_1 делится на p. Подставляя далее вместо x последовательно x_2, $\ldots$, x_n, x_{n+1}, приходим к тому, что кратны p также

коэффициенты $b_2,\ldots,\ b_{n-1},\ b_n$. Если раскрыть скобки в разложениях многочленов $g_k(x)$ на множители и привести подобные в тождестве (3), получим, что и все коэффициенты a_k многочлена $f(x)$ кратны p. $\square$

Данная теорема является очевидным аналогом известного (ещё из средней школы) свойства многочленов: если многочлен степени не выше n имеет более n корней, то он тождественно равен нулю. Поскольку нас интересует делимость на p значений многочлена с целыми коэффициентами в целых точках, можно рассматривать коэффициенты многочлена по модулю p. Получилось, что если количество решений (по модулю p) больше степени многочлена, то все его коэффициенты по модулю p равны нулю.

18. Квадратичные вычеты и невычеты. Символы Лежандра и Якоби

Пусть p — простое число. Число a, не делящееся на p, называется *квадратичным вычетом* по модулю p, если разрешимо (относительно x) сравнение $x^2 \equiv a (\mathrm{mod}\, p)$, и *квадратичным невычетом* в противном случае.

Теорема 18.1. *Пусть p — нечётное простое число. Тогда среди чисел $1, 2, \ldots, p-1$ квадратичных вычетов ровно половина.*

Доказательство. Сначала заметим, что $x^2 \equiv y^2 (\mathrm{mod}\, p)$ тогда и только тогда, когда хотя бы одно из чисел $x+y$ и $x-y$ делится на p (поскольку p — простое число). Если не равные друг другу числа x и y берутся из множества $A = \{1, 2, \ldots, p-1\}$, то $0 < |x-y| < p$ и

$$x^2 \equiv y^2 (\mathrm{mod}\, p) \iff x + y \vdots p.$$

Поскольку A — приведённая система вычетов, квадрат любого числа из A сравним по модулю p с некоторым числом из того же множества A. Разобьём множество A на пары вида $\{k, p-k\}$. Квадраты любых двух чисел из разных пар не сравнимы по модулю p, а квадраты двух чисел из одной пары сравнимы по модулю p. Таким образом, каждой паре соответствует свой «индивидуальный» квадратичный вычет, а квадратичных вычетов столько же, сколько и указанных пар, то есть $(p-1)/2$. $\square$

Упражнение 9. Пусть $p > 3$ — простое число. Возьмём все квадратичные вычеты из множества $\{1, 2, \ldots, p-1\}$. Докажите, что их сумма кратна p.

Символ Лежандра

Для простого числа p *символ Лежандра* $\left(\frac{a}{p}\right)$ определяется так:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \text{ делится на } p, \\ 1, & \text{если } a \text{ — квадратичный вычет,} \\ -1, & \text{если } a \text{ — квадратичный невычет.} \end{cases}$$

Из определения символа Лежандра непосредственно следует, что при любом целом b справедливо $\left(\frac{b^2}{p}\right) = 1$.

В записи $\left(\frac{a}{p}\right)$ числа a и p называют соответственно числителем и знаменателем символа Лежандра.

Теорема 18.2. (Лемма Эйлера.) *Если p — нечётное простое число, то*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\, p).$$

Доказательство. Рассмотрим три возможных случая.

I. a кратно p. Здесь утверждение тривиально.

II. a — квадратичный вычет. Для некоторого числа b, не кратного p, имеем $a \equiv b^2 (\mathrm{mod}\, p)$. Тогда, используя малую теорему Ферма, получим

$$a^{\frac{p-1}{2}} \equiv b^{2(\frac{p-1}{2})} \equiv b^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

III. a — квадратичный невычет. Поскольку

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

число $a^{\frac{p-1}{2}}$ сравнимо по модулю p с 1 или -1. Мы уже выяснили, что сравнению $x^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\, p)$ удовлетворяет $\frac{p-1}{2}$ квадратичных вычетов. В силу теоремы 17.1 других решений у данного сравнения нет. Значит, для квадратичного невычета остается лишь возможность $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$. $\square$

Простейшие свойства символа Лежандра

- *Если* $a \equiv b (\mathrm{mod}\, p)$, *то* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$; $\quad \left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$;
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Все эти свойства непосредственно вытекают из леммы Эйлера.

Теперь становятся очевидными следующие утверждения: *произведение двух квадратичных вычетов — вычет, произведение вычета и невычета — невычет, произведение двух невычетов — вычет.*

Теорема 18.3. (Лемма Гаусса.) *Пусть* p *— нечётное простое число,* a *не кратно* p, $q = (p-1)/2$, $P = \{1, 2, \ldots, q\}$ *и для каждого* $k \in P$ *число* $\varepsilon_k \in \{-1, 1\}$ *выбрано так, что число* $ak\varepsilon_k$ *сравнимо по модулю* p *с каким-нибудь числом из* P. *Тогда*

$$\left(\frac{a}{p}\right) = \prod_{k=1}^{q} \varepsilon_k.$$

Доказательство. Сначала заметим, что числа $\pm 1, \pm 2, \ldots, \pm q$ образуют приведённую систему вычетов по модулю p. Тем же свойством обладает и множество чисел $\{\pm a, \pm 2a, \ldots, \pm qa\}$. Поэтому, во-первых, числа ε_k существуют, а, во-вторых, числа $a\varepsilon_1, 2a\varepsilon_2, \ldots, ka\varepsilon_k$ попарно несравнимы по модулю p. Стало быть, когда число k пробегает по P, то и число $ak\varepsilon_k$ пробегает по P. Пусть $K = \prod\limits_{k=1}^{q} k$. Тогда

$$K \equiv \prod_{k=1}^{q} ak\varepsilon_k \equiv a^q K \prod_{k=1}^{q} \varepsilon_k \equiv \left(\frac{a}{p}\right) K \prod_{k=1}^{q} \varepsilon_k (\mathrm{mod}\, p).$$

Сократив на K, получим $\left(\frac{a}{p}\right) \prod\limits_{k=1}^{q} \varepsilon_k \equiv 1 (\mathrm{mod}\, p)$, откуда и вытекает требуемое. □

Выведем теперь формулу для вычисления ε_k. Здесь нам поможет равенство

$$\left[\frac{2ak}{p}\right] = \left[2\left[\frac{ak}{p}\right] + 2\left\{\frac{ak}{p}\right\}\right] = 2\left[\frac{ak}{p}\right] + \left[2\left\{\frac{ak}{p}\right\}\right].$$

Если $\varepsilon_k = 1$, то $0 < ak < \frac{p}{2}$, дробная часть числа $\frac{ak}{p}$ меньше $\frac{1}{2}$, а целая часть удвоенной дробной части $2\left\{\frac{ak}{p}\right\}$ равна нулю. Если же $\varepsilon_k = -1$, то $\frac{p}{2} < ak < p$, $\left\{\frac{ak}{p}\right\} > \frac{1}{2}$, $\left[2\left\{\frac{ak}{p}\right\}\right] = 1$. Следовательно,

$$\varepsilon_k = (-1)^{\left[2\left\{\frac{ak}{p}\right\}\right]} = (-1)^{\left[\frac{2ak}{p}\right]}.$$

Таким образом, лемму Гаусса можно переписать в виде

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{k=1}^{q}\left[\frac{2ak}{p}\right]}. \tag{4}$$

Далее сделаем такой трюк. Пусть a — нечётное число. Тогда $a + p$ — чётное, и можно записать

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{2a}{p}\right) = \left(\frac{2a + 2p}{p}\right) = \left(\frac{4 \cdot \frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) =$$

$$= (-1)^{\sum\limits_{k=1}^{q}\left[\frac{(a+p)k}{p}\right]} = (-1)^{\sum\limits_{k=1}^{q}\left[\frac{ak}{p}\right] + \sum\limits_{k=1}^{q} k}.$$

Поскольку

$$\sum_{k=1}^{q} k = \frac{1+q}{2} \cdot q = \frac{1 + \frac{p-1}{2}}{2} \cdot \frac{p-1}{2} = \frac{p+1}{4} \cdot \frac{p-1}{2} = \frac{p^2-1}{8},$$

мы получили тождество

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{k=1}^{q}\left[\frac{ak}{p}\right] + \frac{p^2-1}{8}}. \tag{5}$$

Извлечём из него два полезных следствия. Во-первых, можно получить простое выражение для символа Лежандра $\left(\frac{2}{p}\right)$, положив в (5) $a = 1$:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{6}$$

Во-вторых, теперь из (5) и (6) вытекает (напомним, для нечётного a), что

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{k=1}^{q}\left[\frac{ak}{p}\right]}. \tag{7}$$

Получилось, что если из выражения в правой части формулы (4) убрать двойку, то при нечётном a его значение не изменится!

Свойство (7) лежит в основе наиболее известного доказательства знаменитого закона взаимности квадратичных вычетов[4].

Теорема 18.4. (Квадратичный закон взаимности.) *Если p и q — различные нечётные простые числа, то*

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

Доказательство. Положим $p_1 = \frac{p-1}{2}$ и $q_1 = \frac{q-1}{2}$ и рассмотрим всевозможные пары чисел вида $\langle qx, py\rangle$, где $x = 1, 2, \ldots, p_1$, $y = 1, 2, \ldots, q_1$.

Пусть S_1 — количество пар $\langle qx, py\rangle$, в которых $qx < py$, а S_2 — количество пар, в которых $qx > py$.

Поскольку общее количество рассматриваемых пар есть $p_1 q_1$ и в каждой паре $qx \neq py$, имеем $S_1 + S_2 = p_1 q_1$.

Получим формулу для вычисления S_1. Нам нужно выполнение неравенства $qx < py$, или $x < \frac{p}{q}y$. Ясно, что $\frac{p}{q}y$ — нецелое число и при фиксированном y допустимых значений x в точности $\left[\frac{p}{q}y\right]$. Поэтому

$$S_1 = \sum_{y=1}^{q_1} \left[\frac{p}{q}y\right].$$

Аналогично находим S_2:

$$S_2 = \sum_{x=1}^{p_1} \left[\frac{q}{p}x\right].$$

Видно, что правая часть последней формулы совпадает с выражением для показателя степени (-1) в формуле (7), если положить $a = q$. Поэтому $\left(\frac{q}{p}\right) = (-1)^{S_2}$. Точно так же $\left(\frac{p}{q}\right) = (-1)^{S_1}$. Следовательно,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S_1}\cdot(-1)^{S_2} = (-1)^{S_1+S_2} = (-1)^{p_1 q_1}.$$

[4]Этот закон сформулировал А. Лежандр, но открыл (в некоторой эквивалентной форме) ещё Л. Эйлер. А первое доказательство нашёл в 1796 г. К. Гаусс после года «напряжённейших усилий». Доказательство это было весьма громоздким. Позднее Гаусс нашёл ещё шесть других доказательств (а ныне известное число различных доказательств т. н. «золотой теоремы» достигает пятидесяти). Исторические подробности можно найти а книге [11].

Это и требовалось доказать! □

Покажем, как закон взаимности работает при вычислении символов Лежандра.

Пример. Вычислить $\left(\frac{59}{269}\right)$.

Имеем $\left(\frac{59}{269}\right)\left(\frac{269}{59}\right) = (-1)^{\frac{59-1}{2}\cdot\frac{269-1}{2}} = (-1)^{29\cdot 134} = 1$. Поэтому $\left(\frac{59}{269}\right) = \left(\frac{269}{59}\right)$. Далее:

$$\left(\frac{269}{59}\right) = \left(\frac{59\cdot 4+33}{59}\right) = \left(\frac{33}{59}\right) = \left(\frac{3}{59}\right)\left(\frac{11}{59}\right).$$

Вновь применим закон взаимности:

$$\left(\frac{3}{59}\right)\left(\frac{59}{3}\right) = (-1)^{1\cdot 29} = -1, \quad \left(\frac{11}{59}\right)\left(\frac{59}{11}\right) = (-1)^{5\cdot 29} = -1,$$

откуда $\left(\frac{3}{59}\right) = -\left(\frac{59}{3}\right)$ и $\left(\frac{11}{59}\right) = -\left(\frac{59}{11}\right)$. Наконец,

$$\left(\frac{59}{3}\right) = \left(\frac{2}{3}\right) = -1; \quad \left(\frac{59}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{2^2}{11}\right) = 1.$$

Таким образом, $\left(\frac{59}{269}\right) = \left(\frac{3}{59}\right)\left(\frac{11}{59}\right) = \left(\frac{59}{3}\right)\left(\frac{59}{11}\right) = -1$.

Задачи на символ Лежандра

Упражнение 10. Пусть p — простое число. Докажите, что найдётся такое целое число x, что число $(x^2-2)(x^2-3)(x^2-6)$ делится на p.

Упражнение 11. Пусть p — простое число. Докажите следующие утверждения.

1. $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 (\mathrm{mod}\, 4)$.

2. Если $x^2+1 \vdots p$, где $x \in \mathbb{Z}$, то $p \equiv 1 (\mathrm{mod}\, 4)$.

3. Если $x^2+1 \vdots n$, где $x \in \mathbb{Z}$, а n — нечётное натуральное число, то $n \equiv 1 (\mathrm{mod}\, 4)$.

4. **(Теорема Жирара)** Если $p \equiv 3 (\mathrm{mod}\, 4)$ и $x^2+y^2 \vdots p$ $(x, y \in \mathbb{Z})$, то оба числа x и y кратны p.

Доказательство. Имеем $x^2 \equiv -y^2 (\mathrm{mod}\, p)$. Если x не делится на p, то $\left(\frac{-y^2}{p}\right) = 1$, откуда $\left(\frac{-1}{p}\right) = 1$ и $p = 4k+1$, что противоречит условию теоремы.□

5. Существует бесконечно много простых чисел вида $4k + 1$.

   Доказательство. Пусть $p_1 = 5, p_2 = 13, \ldots, p_n$ — все простые числа вида $4k + 1$. Рассмотрим число $P = (p_1 p_2 \ldots p_n)^2 + 1$. Все его нечётные делители имеют вид $4k + 1$, но среди них нет $p_1, p_2, \ldots, p_n$. Противоречие! □

Упражнение 12. Докажите, что следующие уравнения не имеют решений в натуральных числах:

а) $(x^2 - 1)y = 4z^2 + (2z + 1)^2$;

б) $x^3 + 7 = y^2$.

Упражнение 13. (Л. Эйлер) Докажите, что уравнение

$$4xy - x - y = z^2$$

имеет бесконечно много решений в целых числах, но не имеет решений в натуральных числах.

Упражнение 14. Пусть p — простое число. Докажите, что

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{если } p = 12k \pm 1, \\ -1, & \text{если } p = 12k \pm 5. \end{cases}$$

Упражнение 15. Пусть p — простое число. Докажите, что

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & \text{если } p = 6k + 1, \\ -1, & \text{если } p = 6k - 1. \end{cases}$$

Упражнение 16. Докажите, что существует бесконечно много простых чисел вида $p = 6k + 1$.

Доказательство. Предполагая противное, обозначим через N произведение всех простых чисел указанного вида. Рассмотрим число $m = 4N^2 + 3$. Оно нечётно и не делится на 3 (т. к. N не делится на 3). Пусть p — какой-нибудь простой делитель числа m. Ясно, что $p > 3$. Тогда $(2N)^2 \equiv -3 (\mathrm{mod}\, p)$, откуда $\left(\frac{-3}{p}\right) = 1$. По предыдущей

задаче получаем $p = 6k + 1$. Но тогда N делится на p, и $3 = m - 4N^2$ также делится на p, что невозможно. Противоречие получено! □

Упражнение 17. Пусть $p = 2^n - 1$ — простое число Мерсенна, причём $p > 3$. Докажите, что $\left(\frac{3}{p}\right) = -1$.

Упражнение 18. Пусть $p = 2^n + 1$ — простое число, причём $p > 3$. Докажите, что $\left(\frac{3}{p}\right) = -1$.

Упражнение 19. Докажите, что при любом $n > 1$ число $3^n - 1$ не делится на $2^n - 1$.

Доказательство. Если n чётно, то $2^n - 1 \vdots 3$, и утверждение очевидно.

Пусть $n = 2k + 1$. Убедимся сначала, что число 3 является квадратичным вычетом по любому простому делителю числа $3^n - 1$. Действительно, если $3^n - 1 \vdots p$, то $3^n \equiv 1 (\mathrm{mod}\, p)$, $3^{n+1} \equiv 3 (\mathrm{mod}\, p)$ и $\left(3^{\frac{n+1}{2}}\right)^2 \equiv 3 (\mathrm{mod}\, p)$.

Из упражнения 14 теперь следует, что число p *сравнимо с* 1 *или* -1 *по модулю* 12. Если $2^n - 1$ делит число $3^n - 1$, то все его простые делители являются делителями $3^n - 1$ и обладают отмеченным свойством. Но тогда и $2^n - 1 \equiv \pm 1 (\mathrm{mod}\, 12)$.

Однако, это не так! Поскольку $2^4 \equiv 2^2 (\mathrm{mod}\, 12)$, справедливо $2^{2k} \equiv 2^2 (\mathrm{mod}\, 12)$ и

$$2^{2k+1} - 1 \equiv 2 \cdot 2^2 - 1 \equiv 7 (\mathrm{mod}\, 12).$$

Полученное противоречие доказывает утверждение задачи. □

Упражнение 20. (Н. Н. Осипов) Если x и y — целые числа, причём y не кратно 3, то $3x^2 - 1$ не делится на $8y^2 - 1$. Доказать.

Символ Якоби

Квадратичный закон взаимности позволяет свести вычисление символа Лежандра $\left(\frac{p}{q}\right)$, где $p < q$ — нечётные простые числа, к вычислению символа Лежандра с меньшим знаменателем $\left(\frac{q}{p}\right)$. Если далее заменить числитель на остаток от его деления на знаменатель, выделить в последнем часть, свободную от квадратов, и *разложить её на простые множители*, то мы сведём задачу к такой же, только с меньшим знаменателем. Как это делается, продемонстрировано в решённом выше примере.

Проблема здесь состоит в том, что разложение на простые множители — нетривиальная (по трудоёмкости) операция. В связи с этим вводят символ Якоби $\left(\frac{a}{P}\right)$, являющийся обобщением символа Лежандра и обладающий полезными для вычислений свойствами, при этом отказываются от требования, чтобы знаменатель P был простым числом.

Пусть $P = p_1 p_2 \dots p_r$ — произведение нечётных простых чисел, среди которых могут быть повторяющиеся. Для числа a, взаимно простого с P, символ Якоби $\left(\frac{a}{P}\right)$ определяется равенством

$$\left(\frac{a}{P}\right) = \prod_{k=1}^{r} \left(\frac{a}{p_k}\right).$$

Если $r = 1$, т. е. P — нечётное простое число, то символ Якоби превращается в символ Лежандра.

Замечание. Если $\left(\frac{a}{P}\right) = -1$, то для какого-то простого делителя p_k числа P имеем $\left(\frac{a}{p_k}\right) = -1$, в силу чего нет решений у сравнения $x^2 \equiv a (\mathrm{mod}\, p_k)$, тем более и у сравнения $x^2 \equiv a (\mathrm{mod}\, P)$.

Если же $\left(\frac{a}{P}\right) = 1$, то в случае составного P это не не даёт информации о том, разрешимо ли сравнение $x^2 \equiv a (\mathrm{mod}\, P)$. Например, $\left(\frac{-1}{21}\right) = \left(\frac{-1}{3}\right) \cdot \left(\frac{-1}{7}\right) = (-1) \cdot (-1) = 1$, хотя сравнение $x^2 \equiv -1 (\mathrm{mod}\, 21)$ не имеет решений (скажем, из-за того, что $x^2 + 1$ не делится на 3). Символ Якоби используют в промежуточных выкладках при вычислении символа Лежандра.

Простейшие свойства символа Якоби

- *Если* $a \equiv b (\mathrm{mod}\, P)$, *то* $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$.
- $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right); \quad \left(\frac{ab^2}{P}\right) = \left(\frac{a}{P}\right).$

Доказательство перечисленных выше свойств опирается только на определение символа Якоби и соответствующие свойства символа Лежандра.

Доказательства других свойств менее очевидно, и мы их приведём.

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

Доказательство. Преобразуем показатель степени минус единицы:

$$\frac{P-1}{2} = \frac{\left(1+2\cdot\frac{p_1-1}{2}\right)\ldots\left(1+2\cdot\frac{p_r-1}{2}\right)-1}{2} = \sum_{k=1}^{r}\frac{p_k-1}{2} + 2N,$$

где N — некоторое натуральное число. Отсюда

$$(-1)^{\frac{P-1}{2}} = (-1)^{\sum\limits_{k=1}^{r}\frac{p_k-1}{2}} = \prod_{k=1}^{r}(-1)^{\frac{p_k-1}{2}} = \prod_{k=1}^{r}\left(\frac{-1}{p_k}\right) = \left(\frac{-1}{P}\right).$$

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

Доказательство. Преобразуем показатель степени минус единицы:

$$\frac{P^2-1}{8} = \frac{p_1^2\ldots p_r^2-1}{8} = \frac{\left(1+8\cdot\frac{p_1^2-1}{8}\right)\ldots\left(1+8\cdot\frac{p_r^2-1}{8}\right)-1}{8} =$$

$$= \sum_{k=1}^{r}\frac{p_k^2-1}{8} + 2N,$$

где N — некоторое натуральное число. Отсюда

$$(-1)^{\frac{P^2-1}{8}} = (-1)^{\sum\limits_{k=1}^{r}\frac{p_k^2-1}{8}} = \prod_{k=1}^{r}(-1)^{\frac{p_k^2-1}{8}} = \prod_{k=1}^{r}\left(\frac{2}{p_k}\right) = \left(\frac{2}{P}\right).$$

Имеет место и **квадратичный закон взаимности для символа Якоби.**

- Если P и Q — взаимно простые нечётные числа, отличные от единицы, то

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Доказательство. Разложим числа P и Q на простые множители: $P = p_1p_2\ldots p_r$, $Q = q_1q_2\ldots q_s$. Из условия взаимной простоты P и Q следует, что $\forall i,j \quad p_i \neq q_j$. Пользуясь определением символа Якоби и уже известными свойствами символов Лежандра и Якоби, получаем

$$\left(\frac{Q}{P}\right) = \prod_{i=1}^{r}\left(\frac{Q}{p_i}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right) =$$

$$= (-1)^{\sum\limits_{i=1}^{r}\sum\limits_{j=1}^{s}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right) = (-1)^{\sum\limits_{i=1}^{r}\frac{p_i-1}{2}\cdot\sum\limits_{j=1}^{s}\frac{q_j-1}{2}}\left(\frac{P}{Q}\right).$$

Как было показано выше, для некоторого натурального N справедливо равенство $\dfrac{P-1}{2} = \sum\limits_{i=1}^{r}\dfrac{p_i-1}{2} + 2N$, т. е. число $\dfrac{P-1}{2}$ имеет одинаковую чётность с числом $\sum\limits_{i=1}^{r}\dfrac{p_i-1}{2}$. То же верно для чисел $\dfrac{Q-1}{2}$ и $\sum\limits_{j=1}^{s}\dfrac{q_j-1}{2}$. Поэтому

$$(-1)^{\sum\limits_{i=1}^{r}\frac{p_i-1}{2}\cdot\sum\limits_{j=1}^{s}\frac{q_j-1}{2}} = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Теперь всё доказано. □

Пример. Имеет ли решение сравнение $x^2 \equiv 327 (\mathrm{mod}\, 601)$?

Решение. Для ответа на поставленный вопрос нужно вычислить символ Лежандра $\left(\frac{327}{601}\right)$. Вычислять его будем как символ Якоби, пользуясь доказанными выше свойствами.

$$\left(\frac{327}{601}\right) = \left(\frac{601}{327}\right) = \left(\frac{274}{327}\right) = \left(\frac{2}{327}\right)\left(\frac{137}{327}\right) = \left(\frac{137}{327}\right) =$$

$$= \left(\frac{327}{137}\right) = \left(\frac{53}{137}\right) = \left(\frac{137}{53}\right) = \left(\frac{31}{53}\right) = \left(\frac{53}{31}\right) = \left(\frac{22}{31}\right) =$$

$$= \left(\frac{11}{31}\right) = -\left(\frac{31}{11}\right) = -\left(\frac{9}{11}\right) = -1.$$

Таким образом, число 327 является квадратичным невычетом по модулю 601; сравнение решений не имеет.

19. Показатели и первообразные корни

Как известно, если a и m — взаимно простые числа, то для некоторого натурального x выполнено сравнение

$$a^x \equiv 1 (\mathrm{mod}\, m). \qquad (1)$$

Например, в силу теоремы Эйлера, годится $x = \varphi(m)$. Наименьшее число x со свойством (1) называют *показателем*, которому принадлежит число a по модулю m. Обозначение: $\operatorname{ord}_m a$.

Алгебраический смысл показателя очень простой. Рассмотрим циклическую подгруппу с образующим элементом a в мультипликативной группе $\mathbb{Z}_m^*$ (напомним, что $\mathbb{Z}_m^*$ образована обратимыми по умножению классами вычетов по модулю m). Порядок этой подгруппы (или, что то же самое, порядок элемента a) и есть $\operatorname{ord}_m a$.

Простейшие свойства показателя

Положим $\delta = \operatorname{ord}_m a$.

- Числа $1, a, a^2, \ldots, a^{\delta-1}$ попарно несравнимы по модулю m.
  Действительно, если, $a^k \equiv a^n (\operatorname{mod} m)$, где $\delta > k > n \geqslant 0$, то $a^n(a^{k-n} - 1) \vdots m$, откуда $a^{k-n} \equiv 1 (\operatorname{mod} m)$, причём $k - n < \delta$, что противоречит минимальности δ.

- $a^x \equiv a^y (\operatorname{mod} m) \iff x \equiv y (\operatorname{mod} \delta)$.
  Поделим x на δ: $x = \delta q + r$, где $0 \leqslant r < \delta$. Тогда $a^x = (a^\delta)^q a^r \equiv \equiv a^r (\operatorname{mod} m)$. Стало быть, остаток от деления a^x на m однозначно определяется остатком от деления x на δ.

- $a^x \equiv 1 (\operatorname{mod} m) \iff x \vdots \delta$.
  Это непосредственное следствие двух предыдущих свойств.

- $\varphi(m) \vdots \delta$.
  Вытекает из предыдущего свойства и теоремы Эйлера.

- $\operatorname{ord}_m(a^k) = \frac{\delta}{(k,\delta)}$. В частности, если k и δ — взаимно простые числа, то $\operatorname{ord}_m(a^k) = \delta$.
  Действительно, пусть $k = k_1 d, \delta = \delta_1 d$, где $d = (k, \delta)$. Тогда $(k_1, \delta_1) = 1$ и $\delta_1 = \frac{\delta}{(k,d)}$. Имеем

  $$(a^k)^x - 1 \vdots m \iff kx \vdots \delta \iff k_1 dx \vdots \delta_1 d \iff k_1 x \vdots \delta_1 \iff x \vdots \delta_1.$$

Если $\operatorname{ord}_m g = \varphi(m)$, то число g называют **первообразным корнем по модулю** m.

Легко проверить, что для чисел 2, 3, 4, 5 в качестве первообразных корней можно взять соответственно числа 1, 2, 3, 2.

Однако первообразные корни существуют не для любого m.

Показатели по модулю 2^n

Считаем, что $n \geqslant 3$.

Пусть a — произвольное нечётное число, большее единицы. Число $a^2 - 1 = (a-1)(a+1)$ делится на 8 как произведение двух соседних чётных чисел (ровно одно из них кратно четырём). Выделим наибольшую степень двойки, на которую делится число $a^2 - 1$:

$$a^2 - 1 = 2^k c_1.$$

Здесь c_1 — нечётное число, а $k \geqslant 3$. Тогда

$$a^4 - 1 = (a^2-1)(a^2+1) = 2^k c_1(2^k c_1 + 2) = 2^{k+1} c_1(2^{k-1} c_1 + 1).$$

Значит, $a^4 - 1 = 2^{k+1} c_2$, где c_2 — нечётное число.

Пусть для некоторого i справедливо $a^{2^i} = 2^{k+i-1} c_i$, где c_i нечётно. Тогда

$$a^{2^{i+1}} - 1 = \left(a^{2^i} - 1\right)\left(a^{2^i} + 1\right) = 2^{k+i-1} c_i(2^{k+i-1} c_i + 2) =$$

$$= 2^{k+i} c_i(2^{k+i-2} c_i + 1) = 2^{k+i} c_{i+1},$$

где c_{i+1} нечётно.

Мы по индукции доказали, что $\forall i \quad a^{2^i} - 1 = 2^{k+i-1} c_i$. В частности, $a^{2^{n-k+1}} - 1 = 2^n c_{n-k+1}$, а при $j < n-k+1$ число $a^{2^j} - 1$ не делится на 2^n. Значит, с одной стороны, показатель, которому принадлежит число a по модулю 2^n, является делителем числа 2^{n-k+1} и имеет вид 2^j, но при этом $j \geqslant n-k+1$. Следовательно,

$$\operatorname{ord}_{2^n}(a) = 2^{n-k+1} \leqslant 2^{n-2} < 2^{n-1} = \varphi(2^n).$$

Мы воспользовались тем, что $k \geqslant 3$.

Таким образом, не существует первообразных корней по модулю 2^n, где $n \geqslant 3$.

Наибольшему показателю 2^{n-2} по модулю 2^n принадлежат, в частности, числа 3 и 5, поскольку $3^2 - 1 = 2^3$ и $5^2 - 1 = 2^3 \cdot 3$ (т. е. для тройки и пятёрки имеем в выкладках, проведённых выше, $k = 3$).

Если добавить к набору чисел

$$1, 5, 5^2, \ldots, 5^{2^{n-2}-1} \tag{2}$$

числа, отличающиеся от них знаком:

$$-1, -5, -5^2, \ldots, -5^{2^{n-2}-1}, \tag{3}$$

то получим приведённую систему вычетов по модулю 2^n. Действительно, как в наборе (2), так и в наборе (3), числа попарно несравнимы по модулю 2^n (это следует из свойства показателя). Кроме того, числа из первого набора при делении на 4 дают остаток 1, а из второго соответственно 3. Поэтому числа

$$\pm 1, \pm 5, \pm 5^2, \ldots, \pm 5^{2^{n-2}-1} \tag{4}$$

попарно несравнимы по указанному модулю. А всего в наборе (4), как легко подсчитать, $2 \cdot 2^{n-2} = 2^{n-1} = \varphi(2^n)$ чисел. Значит, они образуют приведённую систему вычетов по модулю 2^n (напомним, $n \geqslant 3$).

Упражнение 21. Докажите, что числа $\pm 1, \pm 3, \pm 3^2, \ldots, \pm 3^{2^{n-2}-1}$ также образуют приведённую систему вычетов по модулю 2^n ($n \geqslant 3$).

Упражнение 22. Найдите все целые a, для которых $\pm 1, \pm a, \pm a^2, \ldots, \pm a^{2^{n-2}-1}$ — приведённая система вычетов по модулю 2^n, где $n \geqslant 3$.

Ответ: $a \equiv \pm 3 (\mathrm{mod}\, 8)$.

Показатели по простому модулю

Теорема 19.1. *Пусть p — простое нечётное число, а δ — произвольный делитель числа $p-1$. Тогда δ — показатель, и ему принадлежит ровно $\varphi(\delta)$ остатков от деления на p.*

Доказательство. Зафиксируем показатель δ (мы знаем, что δ делит $\varphi(p) = p-1$). Пусть этому показателю принадлежит число a, т. е. $\mathrm{ord}_p a = \delta$. Тогда числа $1, a, a^2, \ldots, a^{\delta-1}$ попарно несравнимы по модулю p и удовлетворяют сравнению $x^\delta \equiv 1 (\mathrm{mod}\, p)$. Количество этих чисел равно степени сравнения. Поэтому для любого числа b, принадлежащего показателю δ, найдётся число k такое, что $0 \leqslant k \leqslant \delta - 1$ и $b \equiv a^k (\mathrm{mod}\, p)$. Как было отмечено выше,

$$\mathrm{ord}_p(a^k) = \delta \iff (k, \delta) = 1.$$

Стало быть, число k можно выбрать $\varphi(\delta)$ способами.

Таким образом, если есть хотя бы один остаток от деления на p, принадлежащий показателю δ, то таких остатков ровно $\varphi(\delta)$, а для любого числа $d \leqslant p-1$ количество остатков, принадлежащих показателю d, равно либо нулю, либо $\varphi(d)$. Если d не делит $p-1$, то заведомо

d не может быть показателем. Суммируя количество остатков по всем возможным показателям, получаем

$$p-1 \leqslant \sum_{\delta \mid p-1} \varphi(\delta). \tag{5}$$

Однако, на самом деле в соотношении (5) должно быть равенство (см. сумматорную функцию для функции Эйлера; §11). Поэтому и каждый делитель δ числа $p-1$ является показателем, которому принадлежит ровно $\varphi(\delta)$ остатков. $\square$

В частности, показателю $p-1=\varphi(p)$ принадлежит ровно $\varphi(p-1)$ остатков. Значит, первообразные корни по модулю p существуют, и среди чисел $1,2,\ldots,p-1$ их ровно $\varphi(p-1)$.

Первообразные корни по модулям p^n и $2p^n$

Теорема 19.2. *Существует первообразный корень по модулю p^n.*

Доказательство. Пусть g — первообразный корень по модулю p. Существует число t, для которого

$$(g+pt)^{p-1} = 1+pu, \quad u \not\vdots p.$$

Действительно, поскольку $g^{p-1} \equiv 1 (\mathrm{mod}\, p)$, имеем $g^{p-1} = 1+pT_0$ для некоторого T_0. Тогда

$$(g+pt)^{p-1} = g^{p-1} + (p-1)g^{p-2}\cdot pt + p^2T = 1 + pT_0 - g^{p-2}tp + p^2T' =$$

$$= 1 + p(T_0 - g^{p-2}t + pT') = 1+pu.$$

Поскольку $(g^{p-2}, p) = 1$, число u пробегает вместе с t полную систему вычетов по модулю p. В частности, для некоторого t число u не будет кратно p. Зафиксируем такое t и обозначим

$$x = g+pt, \quad y = x^{p-1} = 1+pu.$$

Теперь докажем, что число x является первообразным корнем по модулю p^n для любого $n>1$.

Пусть $\mathrm{ord}_{p^n} x = c$. Тогда $x^c \equiv 1 (\mathrm{mod}\, p^n)$, откуда $x^c \equiv 1 (\mathrm{mod}\, p)$. Поскольку $x \equiv g (\mathrm{mod}\, p)$, получаем, что $g^c \equiv 1 (\mathrm{mod}\, p)$. Число g — первообразный корень по модулю p. Поэтому $\mathrm{ord}_p g = p-1$ и $c \vdots p-1$.

По свойству показателя, $\varphi(p^n) = p^{n-1}(p-1) \vdots c$. Учитывая, что c делится на $p-1$, приходим к выводу, что число c представимо в виде $c = (p-1)p^{r-1}$, где $r \leqslant n$. Осталось убедиться в том, что $r = n$. Имеем

$$y^p = (1+pu)^p = 1 + p^2 u_2, \quad u_2 \not\vdots p;$$

$$y^{p^2} = (1+p^2 u_2)^p = 1 + p^3 u_3, \quad u_3 \not\vdots p;$$

$$y^{p^{r-1}} = (1+p^{r-1} u_{r-1})^p = 1 + p^r u_r, \quad u_r \not\vdots p.$$

Поскольку

$$x^c = x^{(p-1)p^{r-1}} = y^{p^{r-1}} = 1 + p^r u_r \equiv 1 (\mathrm{mod}\, p^n),$$

где u_r не кратно p, получаем, что p^r кратно p^n, откуда $r \geqslant n$. Стало быть, $r = n$. $\square$

Теперь несложно найти первообразный корень и по модулю $2p^n$, учитывая, что $\varphi(2p^n) = \varphi(p^n)$. Заметим, что при нечётном x сравнения $x^t \equiv 1 (\mathrm{mod}\, p^n)$ и $x^t \equiv 1 (\mathrm{mod}\, 2p^n)$ равносильны. Поэтому если первообразный корень g_1 по модулю p^n — нечётное число, то g_1 будет и первообразным корнем по модулю $2p^n$. Если же g_1 чётное число, первообразным корнем по модулю $2p^n$ будет число $g_1 + p^n$.

Для практического нахождения первообразных корней применяют следующий критерий.

Теорема 19.3. *Пусть $m = p^n$ или $m = 2p^n$, где p — простое нечётное число, $n \geqslant 1$. Пусть также $q_1, q_2, \ldots, q_k$ — все различные простые делители числа $d = \varphi(m)$. Число g, взаимно простое с m, — первообразный корень по модулю m тогда и только тогда, когда не выполняется ни одно из сравнений*

$$g^{\frac{d}{q_1}} \equiv 1 (\mathrm{mod}\, m), g^{\frac{d}{q_2}} \equiv 1 (\mathrm{mod}\, m), \ldots, g^{\frac{d}{q_k}} \equiv 1 (\mathrm{mod}\, m).$$

Доказательство. *Необходимость.* Пусть g — первообразный корень по модулю m. Тогда $\mathrm{ord}_m g = d$. Поскольку $\frac{d}{q_i} < d$, сравнение $g^{\frac{d}{q_i}} \equiv 1 (\mathrm{mod}\, m)$ не может иметь места!

Достаточность. От противного: пусть $\mathrm{ord}_m g = \delta < d$. По свойству показателя $d \vdots \delta$. Пусть q — произвольный простой делитель числа $\frac{d}{\delta}$. Тогда $\frac{d}{\delta} = qu$ для некоторого натурального u. При этом $\frac{d}{q} = \delta u$ и

$$g^{\frac{d}{q}} = g^{\delta u} \equiv 1 (\mathrm{mod}\, m),$$

что противоречит условию теоремы.

Пример 1. Найдём первообразный корень по модулю $m = 41$. Число $\varphi(41) = 40$ имеет два простых делителя: 2 и 5. Нам нужно найти число g, не кратное 41 и не удовлетворяющее ни одному из сравнений $g^{20} \equiv 1 (\mathrm{mod}\, 41)$ и $g^8 \equiv 1 (\mathrm{mod}\, 41)$. Последовательно вычисляем (по модулю 41):

$$2^8 \equiv 10,\ 2^{20} \equiv 1,\ 3^8 \equiv 1,\ 4^{20} \equiv 1,\ 5^{20} \equiv 1,\ 6^8 \equiv 10,\ 6^{20} \equiv -1.$$

Значит, 6 — первообразный корень по модулю 41.

Пример 2. Найдём первообразный корень по модулю $m = 41^2$. Будем действовать, как в доказательстве теоремы 19.2. Предварительно заметим, что $6^{40} - 1 = 41 \cdot 3 + 41^2 l$. Поэтому

$$(6 + 41t)^{40} = 6^{40} + 40 \cdot 6^{39} \cdot 41t + 41^2 T =$$

$$= 1 + 41(3 + 41l + 41 \cdot 6^{39} t - 6^{39} t + 41T) = 1 + 41u.$$

Нужно подобрать такое t, при котором $u \not\vdots 41$. Подойдёт $t = 0$. Значит, 6 — первообразный корень по модулю 41^2.

Пример 3. Найдём первообразный корень по модулю $m = 2 \cdot 41^2$. По описанной выше процедуре подойдёт число $6 + 41^2$.

По каким модулям есть первообразные корни?

Мы уже выяснили, что для любого нечётного числа p и любого натурального n существуют первообразные корни по модулю p^n и $2p^n$. Среди степеней двойки первообразные корни имеют только 2 и 4. Оказывается, указанными числами полностью исчерпывается ответ на вопрос из заголовка параграфа!

Теорема 19.4. *Если число m отлично от 2, 4, не имеет вида $m = p^n$ или $m = 2p^n$, где p — нечётное простое число, $n \in \mathbb{N}$, то не существует первообразного корня по модулю m.*

Доказательство. Определим для числа с известным разложением на простые множители $m = \prod\limits_i p_i^{k_i}$ *функцию Кармайкла* $\lambda(m)$ как наименьшее общее кратное всех чисел $\varphi\left(p_i^{k_i}\right) = p_i^{k_i - 1}(p_i - 1)$.

Если $(a, m) = 1$, то для каждого i по теореме Эйлера $a^{\varphi(p_i^{k_i})} - 1 \vdots p_i^{k_i}$. Из определения функции Кармайкла отсюда следует, что для любого i число $a^{\lambda(m)} - 1 \vdots p_i^{k_i}$. Поэтому $a^{\lambda(m)} \equiv 1 (\mathrm{mod}\, m)$.

Если число m имеет два разных простые нечётных делителя p и q, то $(p-1, q-1) \geqslant 2$, $[p-1, q-1] < (p-1)(q-1)$ и $\lambda(m) < \varphi(m)$.

Случай $m = 2^n$ полностью рассмотрен выше.

Осталось рассмотреть случай $m = 2^n p^k$, где $n \geqslant 2$, $k \geqslant 1$, а p — нечётное простое число. Имеем:

$$\varphi(m) = 2^{n-1} p^{k-1}(p-1); \quad \lambda(m) = [2^{n-1}, p^{k-1}(p-1)] < \varphi(m),$$

так как $(2^{n-1}, p-1) \geqslant 2$. □

Задачи на применение первообразного корня

Ниже всюду p — простое нечётное число.

Упражнение 23. Пусть g — первообразный корень по модулю p. Докажите, что число g^k является квадратичным вычетом по модулю p лишь при чётном k.

Упражнение 24. Докажите, что числа $1, 2, \ldots, p-1$ можно расставить по кругу так, что для любых трёх последовательных чисел a, b и c разность $b^2 - ac$ делится на p.

Упражнение 25. При каких k сумма $S = \sum_{j=1}^{p-1} j^k$ кратна p?

Решение. Пусть g — первообразный корень по модулю p. Числа $1, 2, \ldots, p-1$ образуют приведённую систему вычетов по модулю p. Таким же свойством обладают числа $g, 2g, \ldots, (p-1)g$, поскольку g взаимно просто с p. Поэтому

$$S = \sum_{j=1}^{p-1} j^k \equiv \sum_{j=1}^{p-1} (gj)^k \equiv g^k \sum_{j=1}^{p-1} j^k \pmod{p},$$

откуда $S(g^k - 1) \vdots p$. Если k не делится на $p-1$, то $g^k \not\equiv 1 \pmod{p}$, и, следовательно, S делится на p. Если же k кратно $p-1$, то $j^k \equiv 1 \pmod{p}$ $(j = 1, 2, \ldots, p-1)$ и $S \equiv p - 1 \pmod{p}$.

20. Дискретное логарифмирование

Пусть p — нечётное простое число, n — натуральное число, $m = p^n$ или $m = 2p^n$. Пусть также $c = \varphi(m)$, а g — первообразный корень по модулю m. Как показано в предыдущих параграфах, когда число x

пробегает по множеству $\{0, 1, \ldots, c-1\}$, число g^x пробегает приведённую систему вычетов по модулю m. Поэтому для любого числа a, взаимно простого с m, существует единственное число $x \in \{0, 1, \ldots, c-1\}$ такое, что

$$a \equiv g^x (\mathrm{mod}\, m). \tag{1}$$

Если выполнено сравнение (1), то число x называют *индексом числа a по модулю m при основании g* и при этом используют обозначение $x = \mathrm{ind}_g a$ (если в каком-то контекста основание g фиксировано, то его обозначение опускают и записывают просто $x = \mathrm{ind}\, a$). Здесь мы имеем вполне прозрачную аналогию с понятием логарифма. Поэтому нахождение индекса и называют дискретным логарифмированием.

Заметим, что если $x' \in \{0, 1, \ldots, c-1\}$ и число x' обладает свойством (1), то все остальные числа x со свойством (1) сравнимы с x' по модулю c. Это следует из свойств показателя и определения первообразного корня. Индексы числа a (при фиксированном g) образуют класс вычетов по модулю $c = \varphi(m)$, а числа с заданным индексом x образуют класс вычетов по модулю m.

Свойства индекса

Благодаря своему определению, индекс имеет свойства, аналогичные свойствам логарифма.

- $\mathrm{ind}(ab) \equiv \mathrm{ind}\, a + \mathrm{ind}\, b (\mathrm{mod}\, c)$.

Действительно, из сравнений $a \equiv g^{\mathrm{ind}\, a} (\mathrm{mod}\, m)$ и $b \equiv g^{\mathrm{ind}\, b} (\mathrm{mod}\, m)$ следует, что $ab \equiv g^{\mathrm{ind}\, a + \mathrm{ind}\, b} (\mathrm{mod}\, m)$.

- $\mathrm{ind}(a^n) \equiv n\, \mathrm{ind}\, a (\mathrm{mod}\, c)$.

Это — непосредственное следствие предыдущего свойства.

Для простого числа p можно составить две таблицы индексов: в одной по числу a можно найти $\mathrm{ind}\, a$ (для наименьшего первообразного корня g); в другой по значению $\mathrm{ind}\, a$ ищут само число a. В [6] приводятся такие таблицы для всех простых чисел, меньших 100. В той же книге имеется таблица наименьших первообразных корней для всех простых чисел, меньших 4 070.

В общем случае задача дискретного логарифмирования является весьма трудоёмкой. И этот факт лежит в основе применения дискретного логарифмирования в криптографии. Покажем, следуя [13], как

двое лиц, общаясь только через сеть Интернет, могут построить *общий секретный ключ*. При этом, даже зная всю переписку этих лиц, нельзя за приемлемое время восстановить этот ключ.

Пусть лица A и B в процессе переписки выбрали некоторое простое число p и первообразный корень g по модулю p. Далее A и B выбирают (в тайне от врагов) соответственно числа x и y из промежутка чисел от 1 до $p-1$, а сообщают дру другу числа g^x и g^y (по модулю p). Теперь в качестве общего секретного ключа они могут взять число

$$k \equiv g^{xy} (\mathrm{mod}\, p).$$

Действительно, A найдёт k, возведя в степень x число g^y, а B будет возводить в степень y число g^x. А враги A и B, даже зная p, g, g^x и g^y, не смогут за реальное время вычислить k из-за трудоёмкости нахождения индекса.

Числовой пример. Пусть $p = 1\,000\,003$. При этом число $c = p - 1 = 2 \cdot 3 \cdot 166\,167$ является произведением трёх простых чисел. Проверьте, что в качестве первообразного корня по модулю p можно взять число 2. Если A и B возьмут $x = 394\,792$ и $y = 851\,982$, то их общий ключ $k = 958\,970$.

Индексы по составному модулю

Пусть $m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

Если $\alpha = 0$ или $\alpha = 1$ положим $d = 1$; в остальных случаях $d = 2$. Число d_0 определим равенством $dd_0 = \varphi(2^\alpha)$. Для $i = 1, \dots, k$ положим $d_i = \varphi(p_i^{\alpha_i})$ и зафиксируем какой-нибудь первообразный корень g_i по модулю $p_i^{\alpha_i}$. Из мультипликативности функции Эйлера следует, что $\varphi(m) = dd_0 d_1 \dots d_k$.

Для любого числа a, взаимно простого с m, существуют такие числа γ, γ_0, γ_1, …, γ_k, что

$$a \equiv (-1)^\gamma 5^{\gamma_0} (\mathrm{mod}\, 2^\alpha); \qquad \forall i \quad a \equiv g_i^{\gamma_i} (\mathrm{mod}\, p_i^{\alpha_i}). \tag{2}$$

Набор чисел $\gamma, \gamma_0, \gamma_1, \dots \gamma_k$ будет определён однозначно, если дополнительно потребовать выполнение неравенств

$$0 \leqslant \gamma < d, \quad 0 \leqslant \gamma_0 < d_0, \quad \dots, \quad 0 \leqslant \gamma_k < d_k. \tag{3}$$

При выполнении условий (2) и (3) упорядоченный набор чисел $(\gamma, \gamma_0, \dots, \gamma_k)$ называют *системой индексов числа a по модулю m*.

Ясно, что числа, сравнимые между собой по модулю m и взаимно простые с m, имеют одинаковые системы индексов по этому модулю.

Всего разных систем индексов $dd_0d_1 \dots d_k = \varphi(m)$. Для каждой системы индексов система сравнений (2) имеет единственное решение (относительно a) по модулю m.

Если $\gamma = \gamma_0 = \ldots = \gamma_k = 0$, то $a \equiv 1 (\mathrm{mod}\, m)$. Несложно видеть, что если a и b взаимно просты с m, то индексы произведения этих чисел связаны с индексами самих чисел так:

$$\gamma(ab) \equiv \gamma(a) + \gamma(b) (\mathrm{mod}\, d), \quad \forall i\ \gamma_i(ab) \equiv \gamma_i(a) + \gamma_i(b) (\mathrm{mod}\, d_i).$$

На языке алгебры полученный результат можно выразить так: отображение $a \to (\gamma, \gamma_0, \dots, \gamma_k)$ изоморфно отображает мультипликативную группу $\mathbb{Z}_m^*$ на прямую сумму аддитивных групп $\mathbb{Z}_d \oplus \mathbb{Z}_{d_0} \oplus \oplus \ldots \oplus \mathbb{Z}_{d_k}$. Говорят также, что мультипликативная группа $\mathbb{Z}_m^*$ раскладывается в произведение соответствующих циклических аддитивных групп.

Подробно вопросы, связанные с дискретным логарифмированием, рассматриваются в монографии [13].

21. Суммы двух квадратов

Теорема 21.1. *Если $p = 4k + 1$, где $k \in \mathbb{N}$, — простое число, то уравнение*

$$x^2 + y^2 = p \tag{1}$$

разрешимо в целых числах.

Доказательство. Число -1 является квадратичным вычетом по модулю $p = 4k + 1$. Действительно,

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

Поэтому существует такое целое число a, что $a^2 \equiv -1 (\mathrm{mod}\, p)$. Для такого a справедливы соотношения

$$x^2 + y^2 \equiv x^2 - a^2y^2 \equiv (x - ay)(x + ay) (\mathrm{mod}\, p). \tag{2}$$

Можно считать, что $x, y \geqslant 0$. Поскольку мы ищем решения уравнения (1), будем рассматривать целые числа x и y, попадающие в промежуток $\left[0; [\sqrt{p}]\right]$. При этом каждая из переменных x и y принимает

$[\sqrt{p}]+1$ значений, и всего получится $([\sqrt{p}]+1)^2 > \sqrt{p}^2 = p$ упорядоченных пар (x, y). В то же время различных остатков от деления на p числа $x + ay$ ровно p. По принципу Дирихле, найдутся две пары целых чисел (x_1, y_1) и (x_2, y_2), такие что в обеих парах $0 \leqslant x_i \leqslant \sqrt{p}$, $0 \leqslant y_i \leqslant \sqrt{p}$ и

$$x_1 + ay_1 \equiv x_2 + ay_2 (\mathrm{mod}\, p),$$

или

$$(x_1 - x_2) + a(y_1 - y_2) \equiv 0 (\mathrm{mod}\, p).$$

Обозначим $x_0 = x_1 - x_2$ и $y_0 = y_1 - y_2$. Поскольку $(x_1, y_1) \neq (x_2, y_2)$, числа x_0 и y_0 не могут быть одновременно равны нулю. Стало быть, $x_0^2 + y_0^2 > 0$.

Итак, число $x_0 + ay_0$ кратно p. В силу (2), число $x_0^2 + y_0^2$ также делится на p. Покажем, что на самом деле $x_0^2 + y_0^2 = p$. Действительно, $|x_0| = |x_1 - x_2| \leqslant [\sqrt{p}]$, $|y_0| = |y_1 - y_2| \leqslant [\sqrt{p}]$, откуда $|x_0| < \sqrt{p}$ и $|y_0| < \sqrt{p}$. Значит, $0 < x_0^2 + y_0^2 < p + p = 2p$. Единственным числом из интервала $(0; 2p)$, кратным p, является само число p. Это и требовалось доказать.□

Теорема 21.2. *Если уравнения $x^2 + y^2 = a$ и $x^2 + y^2 = b$, где $a, b \in \mathbb{Z}$, разрешимы в целых числах относительно x и y, то разрешимо и уравнение $x^2 + y^2 = ab$.*

Доказательство. Представим сумму квадратов двух чисел в виде определителя второго порядка: $x^2 + y^2 = \begin{vmatrix} x & -y \\ y & x \end{vmatrix}$ и воспользуемся тем, что определитель произведения квадратных матриц равен произведению их определителей.

Итак, для некоторых целых чисел x_1, y_1, x_2, y_2 имеем

$$x_1^2 + y_1^2 = \begin{vmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{vmatrix} = a, \quad x_2^2 + y_2^2 = \begin{vmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{vmatrix} = b.$$

Отсюда

$$\begin{vmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{vmatrix} \cdot \begin{vmatrix} x_2 & -y_2 \\ y_2 & x_2 \end{vmatrix} = \begin{vmatrix} x_1x_2 - y_1y_2 & -(x_1y_2 + x_2y_1) \\ x_1y_2 + x_2y_1 & x_1x_2 - y_1y_2 \end{vmatrix} =$$

$$= (x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2 = ab.$$

Мы получили представление числа ab в виде суммы двух квадратов.

Теорема 21.3. *Пусть n — натуральное число. Уравнение $x^2 + y^2 = n$ разрешимо в целых числах тогда и только тогда, когда разложение числа n на простые множители содержит каждое простое число вида $4k + 3$ в чётной степени.*

Доказательство. *Достаточность.* Пусть в разложении числа n на простые множители в нечётных степенях могут быть только 2 или числа вида $4k+1$ (если все показатели степеней чётные, то доказывать вообще нечего!), т. е.

$$n = p_1 p_2 \dots p_l m^2,$$

где $p_1, p_2, \dots, p_l$ — различные простые числа, среди которых не более одной двойки, а остальные имеют вид $4k+1$. Уравнения $x^2+y^2 = 2$ и $x^2+y^2 = m^2$ имеют соответственно очевидные решения $(1;1)$ и $(m;0)$. Уравнение $x^2 + y^2 = p_i$, где $p_i = 4k+1$, разрешимо в целых числах по теореме 21.1. Значит, в силу теоремы 21.2, разрешимо и уравнение

$$x^2 + y^2 = p_1 p_2 \dots p_l m^2.$$

Необходимость. Будем через $\nu_p(k)$ обозначать показатель степени, с каким простое число p входит в разложение числа k на простые множители. Пусть n — наименьшее натуральное число, представимое в виде суммы двух квадратов ($n = x_0^2 + y_0^2$) и имеющее в своём разложении на простые множители некоторое простое число $p = 4k + 3$ в нечётной степени $\nu_p(n)$.

Если при этом x_0 делится на p, то делиться на p будет и число y_0. Тогда можно записать:

$$x_0 = pu; \quad y_0 = pv; \quad n = p^2(u^2 + v^2).$$

Обозначим $m = u^2+v^2$. С одной стороны, число m представимо в виде суммы двух квадратов, но меньше n. По определению числа n отсюда следует, что $\nu_p(m)$ чётно. Но, с другой стороны, $\nu_p(n) = 2 + \nu_p(m)$, откуда $\nu_p(m)$ нечётно. Получилось противоречие.

Таким образом, числа x_0 и y_0 не делятся на p, и при этом $x_0^2 + y_0^2$ кратно p. Имеем $x_0^2 + y_0^2 \equiv 0 (\mathrm{mod}\, p)$, или

$$x_0^2 \equiv -y_0^2 (\mathrm{mod}\, p).$$

Возведём обе части этого сравнения в степень $\frac{p-1}{2} = 2k + 1$:

$$x_0^{p-1} \equiv -y_0^{p-1} (\mathrm{mod}\, p).$$

Применив малую теорему Ферма, получим отсюда, что $1 \equiv -1 (\mathrm{mod}\, p)$, т. е. 2 делится на p, а это неверно. Полученное противоречие завершает доказательство теоремы.□

Теорема 21.4. *Простое число $p = 4k+1$ представимо в виде суммы квадратов двух целых чисел единственным образом (если не различать представления, отличающиеся друг от друга перестановкой значений x и y или изменением знака одной или двух переменных).*

Доказательство. Пусть для некоторых целых чисел x, y, a и b

$$p = x^2 + y^2 = a^2 + b^2.$$

Сравнение $z^2 \equiv -1 (\mathrm{mod}\, p)$ имеет ровно два решения по модулю p (поскольку -1 — квадратичный вычет по модулю $p = 4k + 1$):

$$z \equiv \pm h (\mathrm{mod}\, p).$$

Отсюда

$$x^2 + y^2 \equiv x^2 - h^2 y^2 (\mathrm{mod}\, p)$$

и $x \equiv \pm hy (\mathrm{mod}\, p)$. Так же и $a \equiv \pm hb (\mathrm{mod}\, p)$. Выбирая нужные знаки переменных x и a, получим

$$x \equiv hy (\mathrm{mod}\, p), \quad a \equiv hb (\mathrm{mod}\, p), \quad xb \equiv hyb \equiv ya (\mathrm{mod}\, p).$$

Имеем

$$p^2 = (x^2 + y^2)(a^2 + b^2) = (xa + yb)^2 + (xb - ya)^2. \tag{3}$$

Поскольку, как показано, $xb - ya = pu$, где $u \in \mathbb{Z}$, получаем теперь, что и $(xa + yb)^2$ делится на p^2, откуда $xa + yb = pv$ для некоторого целого v. Поделим обе части равенства (3) на p^2:

$$1 = v^2 + u^2.$$

Значит, одно из чисел u или v равно нулю.

Если, например, $u = 0$, то

$$xb = ya. \tag{4}$$

Числа x и y взаимно простые (иначе число $p = x^2 + y^2$ делится на квадрат их общего делителя, большего единицы, что невозможно для простого числа), поэтому b делится на y. Но числа a и b также взаимно простые. Стало быть, из (4) следует, что и y делится на b. Таким образом, $y = \pm b$ и $x = \mp a$.

Если же $v = 0$, то $xa = -yb$ и аналогичными выкладками получаем $x = \pm b$, $y = \mp a$. □

22. Любое целое число — сумма четырёх квадратов

В этом параграфе мы докажем знаменитый результат Ж. Л. Лагранжа, датируемый 1770 г. Доказательство разобьём на несколько этапов.

Теорема 22.1. *Если числа a и b представимы в виде суммы четырёх квадратов целых чисел, то тем же свойством обладает и их произведение ab.*

Доказательство. Как и в доказательстве аналогичной теоремы про сумму двух квадратов, нам пригодятся определители второго порядка.

Пусть

$$\alpha = x_1 + ix_2, \quad \beta = x_3 + ix_4, \quad \gamma = y_1 + iy_2, \quad \delta = y_3 + iy_4,$$

$$A = \begin{pmatrix} \alpha & -\beta \\ \overline{\beta} & \overline{\alpha} \end{pmatrix}, \quad B = \begin{pmatrix} \gamma & -\delta \\ \overline{\delta} & \overline{\gamma} \end{pmatrix}.$$

Тогда $|A| = \alpha\overline{\alpha} + \beta\overline{\beta} = x_1^2 + x_2^2 + x_3^2 + x_4^2$, $|B| = \gamma\overline{\gamma} + \delta\overline{\delta} = y_1^2 + y_2^2 + y_3^2 + y_4^2$ и

$$|A| \cdot |B| = |AB| = \begin{vmatrix} \alpha\gamma - \beta\overline{\delta} & -\alpha\delta - \beta\overline{\gamma} \\ \overline{\alpha}\overline{\delta} + \beta\gamma & \overline{\alpha\gamma} - \overline{\beta}\delta \end{vmatrix}.$$

Если обозначить $u = \alpha\gamma - \beta\overline{\delta}$, $v = \alpha\delta + \beta\overline{\gamma}$, то получим

$$|A| \cdot |B| = \begin{vmatrix} u & -v \\ \overline{v} & \overline{u} \end{vmatrix} = |u|^2 + |v|^2,$$

где каждое из чисел $|u|^2$ и $|v|^2$ есть сумма двух квадратов.

Итак, число ab представимо в виде суммы четырёх квадратов. □

Замечание. Если развернуть все обозначения, то придём к тождеству

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) =$$
$$= (x_1y_1 - x_2y_2 - x_3y_3 + x_4y_4)^2 + (x_1y_2 + x_2y_1 - x_3y_4 - x_4y_3)^2 +$$
$$+ (x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)^2,$$

которое, конечно, можно проверить и непосредственным раскрытием скобок.

Теорема 22.2. *Для любого нечётного простого числа p найдутся такие целые числа a и b, что $a^2 + b^2 + 1$ делится на p.*

Доказательство. Рассмотрим множества

$$X_1 = \left\{0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}, \quad X_2 = \{-1 - t \mid t \in X_1\}.$$

Ясно, что эти множества не пересекаются, и в каждом из них по $1 + \frac{p-1}{2} = \frac{p+1}{2}$ элементов. Значит, объединение этих множеств содержит ровно $p + 1$ элементов. Поэтому в $X_1 \cup X_2$ найдутся два разных числа x и y, сравнимых по модулю p.

Покажем, что оба эти числа не могут одновременно входить в X_1.

Пусть, например, $x = k^2$, $y = m^2$, где $0 \leqslant k < m \leqslant \frac{p-1}{2}$. Тогда $0 < m \pm k < p - 1$ и число $y - x = m^2 - k^2 = (m - k)(m + k)$ не кратно p.

Из попарной несравнимости по модулю p чисел из множества X_1 следует очевидно и такое же свойство чисел из X_2.

Итак, одно из чисел x и y входит в X_1, а другое — в X_2. Скажем, $x = a^2 \in X_1$, $y = -1 - b^2 \in X_2$, при этом

$$a^2 \equiv -1 - b^2 (\mathrm{mod}\, p).$$

Это равносильно тому, что требовалось доказать. □

Теорема 22.3. *Любое простое число есть сумма квадратов четырёх целых чисел.*

Доказательство. Пусть p — простое число. Возьмём целые числа a и b, для которых число $a^2 + b^2 + 1$ кратно p (по предыдущей теореме такие числа существуют). Рассмотрим всевозможные четвёрки (x_1, x_2, x_3, x_4) целых чисел, где $\forall i \quad 0 \leqslant x_i \leqslant [\sqrt{p}]$. Для каждой четвёрки составим упорядоченную пару $(x_3 + ax_1 + bx_2, x_4 - bx_1 + ax_2)$ классов вычетов по модулю p. Заметим, что пар класс вычетов заведомо не более p^2, а упомянутых четвёрок $(1 + [\sqrt{p}])^4 > \sqrt{p}^4 = p^2$. Значит, найдутся две разные четвёрки указанного вида (x_1, x_2, x_3, x_4) и (y_1, y_2, y_3, y_4), такие что

$$x_3 + ax_1 + bx_2 \equiv y_3 + ay_1 + by_2 (\mathrm{mod}\, p);$$

$$x_4 - bx_1 + ax_2 \equiv y_4 - by_1 + ay_2 (\mathrm{mod}\, p).$$

Пусть $\forall i \quad z_i = x_i - y_i$. Тогда предыдущие соотношения можно переписать так:

$$z_3 \equiv -az_1 - bz_2 (\mathrm{mod}\, p); \quad z_4 \equiv -az_2 + bz_1 (\mathrm{mod}\, p).$$

Далее имеем:

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 \equiv z_1^2 + z_2^2 + (az_1 + bz_2)^2 + (az_2 - bz_1)^2 \equiv$$

$$\equiv (z_1^2 + z_2^2)(1 + a^2 + b^2) \equiv 0 (\mathrm{mod}\, p).$$

Обозначим $S = z_1^2 + z_2^2 + z_3^2 + z_4^2$. Мы доказали, что число S делится на p. Оценим теперь число S снизу и сверху.

Поскольку $(x_1, x_2, x_3, x_4) \neq (y_1, y_2, y_3, y_4)$, все числа z_i не могут быть одновременно равны нулю. Поэтому $S > 0$. С другой стороны, $\forall i \quad x_i, y_i \in [0; \sqrt{p})$, откуда для всех i выполняются неравенства $|z_i| < \sqrt{p}$, $z_i^2 < p$. Следовательно, $S < 4p$.

Итак, $S = mp$, где $m = 1, 2$ или 3. Рассмотрим возможные случаи отдельно.

- $m = 1$.

Здесь всё отлично! Представление числа p в виде суммы четырёх квадратов уже найдено: $p = z_1^2 + z_2^2 + z_3^2 + z_4^2$.

- $m = 2$.

Поскольку сумма $z_1^2 + z_2^2 + z_3^2 + z_4^2 = 2p$ чётная, числа z_1, z_2, z_3 и z_4 можно разбить на две пары чисел одинаковой чётности. Пусть, к примеру, одинаковую чётность имеют числа z_1 и z_2, а также z_3 и z_4. Тогда числа $\dfrac{z_1 \pm z_2}{2}$ и $\dfrac{z_3 \pm z_4}{2}$ будут целыми, и при этом

$$\left(\frac{z_1 + z_2}{2}\right)^2 + \left(\frac{z_1 - z_2}{2}\right)^2 + \left(\frac{z_3 + z_4}{2}\right)^2 + \left(\frac{z_3 - z_4}{2}\right)^2 =$$

$$= \frac{1}{2}(z_1^2 + z_2^2 + z_3^2 + z_4^2) = p.$$

Искомое представление найдено!

- $m = 3$.

В этом случае число $S = 3p$. Если $p = 3$, то $S = 9$, и нужное представление легко найти: $9 = 2^2+2^2+1^2+0^2$. Пусть теперь $p > 3$. Тогда число S не кратно 9, и все числа z_i не могут одновременно делиться на 3. Если целое число не кратно 3, то его квадрат сравним с 1 по модулю 3. Поскольку S делится на 3, выводим теперь, что из четырёх чисел z_i ровно одно кратно 3, пусть это число z_1. Поменяв, если нужно, знаки остальных трёх чисел, добьёмся того, что $z_2 \equiv z_3 \equiv z_4 \equiv 1 (\mathrm{mod}\, 3)$. Проверьте тождество

$$\left(\frac{z_2+z_3+z_4}{3}\right)^2+\left(\frac{z_1+z_3-z_4}{3}\right)^2+\left(\frac{z_1+z_4-z_2}{3}\right)^2+$$

$$+\left(\frac{z_1+z_2-z_3}{3}\right)^2=\frac{1}{3}(z_1^2+z_2^2+z_3^2+z_4^2)=p.$$

Несложно видеть, что при сделанных предположениях числа $\dfrac{z_2+z_3+z_4}{3}$, $\dfrac{z_1+z_3-z_4}{3}$, $\dfrac{z_1+z_4-z_2}{3}$ и $\dfrac{z_1+z_2-z_3}{3}$ являются целыми. Поэтому представление числа p в виде суммы четырёх квадратов найдено и в этом (последнем возможном) случае.□

Теорема 22.4. *Любое натуральное число представимо в виде суммы квадратов четырёх целых чисел.*

Доказательство. Пусть n — произвольное натуральное число. При $n = 1$ утверждение теоремы очевидно ($1 = 1^2+0^2+0^2+0^2$). Если n — простое число, то ссылаемся на теорему 22.1, а если составное, то применяем теоремы 22.3 и 22.1.□

Упражнение 26. Докажите, что целое число вида $4^k(8m+7)$, где k и m — неотрицательные целые числа, не представимо в виде суммы квадратов трёх целых чисел.

Замечание. К. Ф. Гаусс доказал, что в виде суммы трёх квадратов представимы все натуральные числа, кроме чисел вида $4^k(8m+7)$. Этот результат был опубликован в 1801 г. в его труде под названием «Арифметические исследования».

23. Система RSA

В этом параграфе будет показано, какое применение нашли некоторые классические результаты теории чисел к решению проблемы

создания надёжных шифров — проблемы чрезвычайно актуальной в эпоху массового распространения телекоммуникаций.

Системой тайнописи с открытым ключом (public key cryptosystem) называют такую систему шифрования и дешифрования информации, которая удовлетворяет следующим двум условиям:

- *получатель информации* публикует алгоритм шифрования для всеобщего сведения;

- алгоритм дешифрования известен только получателю информации (держится им в секрете) и *практически* (с помощью вычислительной техники) не может быть раскрыт.

Шифрующий и дешифрующий алгоритмы называют соответственно *открытым* и *закрытым* ключом.

Идея подобной системы тайнописи была высказана в 1975 г., эффективная реализация идеи была предложена в 1977 г. тремя американскими математиками: Р. Райвестом, А. Шамиром и Л. Адлеманом; первые буквы их фамилий (Rivest, Shamir, Adleman) составили имя придуманной ими системы. Описание RSA-системы предварим некоторыми соображениями, связанными с общей идеей тайнописи с открытым ключом.

Всякое сообщение, передаваемое с помощью компьютера по электронным сетям, может быть представлено в виде элемента некоторого числового множества S. Пусть $x \in S$; результат шифрования x (*шифрограмму*) обозначим $y = f(x)$, где f — функция, задаваемая алгоритмом шифрования. Удобно считать, что y тоже принадлежит S; при этом функция f должна осуществлять взаимно однозначное отображение S на себя (разным сообщениям должны соответствовать разные шифрограммы, и наоборот), таким образом, функция f должна осуществлять некоторую перестановку элементов S (т. е. f — *подстановка*, действующая на множестве S). Дешифрующий алгоритм состоит в применении обратной подстановки f^{-1} к шифрограмме $y \in S$: $x = f^{-1}(y)$. Если множество содержит n элементов, то на нем определено $n!$ различных подстановок. *Теоретически* можно найти обратную подстановку f^{-1}, вычислив $f(x)$ для всех $x \in S$. Если, к примеру, S состоит из всех последовательностей 200 десятичных цифр, то $n = 10^{200}$, и реализовать предложенный алгоритм за обозримое время невозможно; знание открытого ключа не даёт, таким образом, *практической* возможности найти закрытый ключ.

Покажем, как решается в предложенной системе тайнописи *проблема электронной подписи*. Предположим, что имеется группа бизнесменов, которым требуется сообщать друг другу сведения, составляющие коммерческую тайну. Каждый бизнесмен придумывает свой алгоритм шифрования (*прямой алгоритм*); при этом он знает и *обратный алгоритм*. Участники группы издают специальный справочник, в котором приводят полностью все прямые алгоритмы (обратные алгоритмы держатся в секрете). К справочнику имеет доступ любой желающий. Пользуясь справочником, можно послать сообщение любому члену группы, например, Z, зашифровав сообщение с помощью (прямого) алгоритма f_Z. Понять это сообщение сможет только Z, поскольку только он знает обратный алгоритм f_Z^{-1}. Теперь допустим, что бизнесмен A хочет *подписать* свое сообщение, т. е. добиться того, чтобы у Z не было сомнений в том, кто действительный автор сообщения. Тогда бизнесмен A шифрует свое сообщение x дважды: сначала с помощью своего обратного алгоритма f_A^{-1}, а затем полученная шифрограмма шифруется еще раз с помощью прямого алгоритма f_Z. В результате Z получает шифрограмму $y = f_Z(f_A^{-1}(x))$. Для того, чтобы восстановить исходное сообщение, Z применяет свой обратный алгоритм f_Z^{-1}, а затем (всем известный) прямой алгоритм f_A: $f_A(f_Z^{-1}(y)) = x$. Теперь бизнесмен Z знает, что только A мог послать ему этот дважды зашифрованный текст, так как при шифровании был использован секретный алгоритм бизнесмена A.

Описание системы RSA

Множество S составляют натуральные числа, меньшие некоторого натурального числа m и взаимно простые с ним; таким образом, S — приведённая система вычетов по модулю m. Функция $f(x)$ вычисляет остаток от деления x^k на m; при этом показатель степени k должен быть взаимно простым с $\varphi(m)$ ($\varphi(m)$ — функция Эйлера). Числа k и m составляют открытый ключ. В качестве закрытого ключа используется такое число k', что $k \cdot k' \equiv 1 (\mathrm{mod}\, \varphi(m))$. Пусть $y \equiv x^k (\mathrm{mod}\, m)$ и $0 \leqslant y < m$. Тогда

$$y^{k'} \equiv x^{k \cdot k'} \equiv x^{1+s \cdot \varphi(m)} \equiv x \cdot (x^{\varphi(m)})^s \equiv x (\mathrm{mod}\, m),$$

так как по теореме Эйлера $x^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$ при взаимно простых x и m.

Зная разложение m на множители, легко вычислить $\varphi(m)$. Покажем, как по $\varphi(m)$ найти k'. Рассмотрим диофантово уравнение

$$kx + \varphi(m)y = 1.$$

Коэффициенты при неизвестных x и y по условию взаимно просты, поэтому уравнение разрешимо, а его общее решение имеет вид

$$x = x_0 + \varphi(m)t,\ y = y_0 - kt,$$

где t — произвольное целое число, а $(x_0; y_0)$ — некоторое частное решение уравнения. Ясно, что при некотором t число x будет положительно и может быть выбрано в качестве k', так как

$$kx \equiv 1 (\mathrm{mod}\, \varphi(m)).$$

Как правило, в качестве m берут произведение двух (многозначных) простых чисел: $m = pq$, тогда $\varphi(m) = (p-1)(q-1)$.

В оригинальной публикации (1977 г.) о методе RSA p и q были соответственно 64- и 65-значными числами. Авторы опубликовали зашифрованный текст из 129 цифр и открытый ключ (128-значное число m и k=9007), предложив 100 долларов тому, кто первый расшифрует текст. Существовавшие в то время алгоритмы разложения числа на простые множители (а также быстродействие вычислительной техники) не позволяли найти разложение 129-значного числа m за разумное время.

Лишь спустя 17 лет с помощью метода *квадратичного решета* указанное 129-значное число было разложено на множители, что потребовало девятимесячной работы примерно 1600 компьютеров, объединённых сетью Интернет [5].

Ныне для выбора p и q рекомендуют 200-значные числа.

В заключение остановимся на технике вычисления остатка от деления x^k на m. Эта операция не столь трудоемка, как может показаться на первый взгляд. С помощью двоичного представления числа k

$$k = \sum_{i=0}^{s} b_i 2^i$$

получим, что

$$x^k \equiv \prod_{b_i \neq 0} x^{2^i} (\mathrm{mod}\, m).$$

Количество умножений (по модулю m) при вычислении степеней числа x

$$x, x^2, x^4, x^8, \ldots, x^{2^s}$$

равно s (каждая степень в этой последовательности, начиная со второй, получается из предыдущей возведением в квадрат). При вычислении ранее приведённого произведения понадобится не более s умножений. Таким образом, общее число умножений не превосходит $2s$, где $s \leqslant \log_2 k$. Например, при вычислении 9007-й степени понадобится 20 умножений (двоичное представление 9007: 10001100101111).

24. Вероятностный тест Миллера – Рабина

Пусть $\mathbb{Z}_m^*$ — множество классов вычетов, взаимно простых с числом m. Как хорошо известно, $\langle \mathbb{Z}_m^*, \cdot \rangle$ — группа. В дальнейшем мы будем отождествлять класс вычетов и любой вычет из этого класс, так что запись $s \in \mathbb{Z}_m^*$ будет просто обозначать взаимную простоту чисел s и m.

Если m — нечётное простое число, а s взаимно просто с m, то $s^{m-1} \equiv 1 (\mathrm{mod}\, m)$ (по малой теореме Ферма). Пусть $m - 1 = 2^r t$, где t — нечётное число. Поскольку

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

имеет место одно из сравнений: $s^{\frac{m-1}{2}} \equiv 1 (\mathrm{mod}\, m)$ или $s^{\frac{m-1}{2}} \equiv -1 (\mathrm{mod}\, m)$. Если $r > 1$ и $s^{\frac{m-1}{2}} \equiv 1 (\mathrm{mod}\, m)$, то аналогично $s^{\frac{m-1}{4}} \equiv 1 (\mathrm{mod}\, m)$ или $s^{\frac{m-1}{4}} \equiv -1 (\mathrm{mod}\, m)$. Повторяя данные выкладки, приходим к выводу: *последовательность остатков от деления на число $m = 2^r t + 1$, где $r > 0$, а t нечётно, чисел $s^{\frac{m-1}{2^i}}$ $(i = 0, 1, \ldots, r)$ состоит из одних единиц либо начинается с единиц, а первый остаток, отличный от единицы, есть $m - 1$.* Будем в дальнейшем называть такое свойство числа s по отношению к числу m свойством W.

Если число $s \in \mathbb{Z}_m^*$ обладает свойством W, будем называть его *свидетелем простоты*. Пусть S — множество всех свидетелей простоты числа m. Если m — простое число, то $S = \mathbb{Z}_m^*$.

Число $a \in \mathbb{Z}_m^*$ называют *антисвидетелем простоты* числа m, если $a^{m-1} \not\equiv 1 (\mathrm{mod}\, m)$ либо $\forall k \quad a^k \not\equiv -1 (\mathrm{mod}\, m)$ и $\mathrm{ord}_p\, a = p - 1$ для

некоторого простого делителя p числа m. Через A обозначим множество всех антисвидетелей числа m. Несложно проверить, что если $a \in A$, то и $a^{-1} \in A$.

Очевидно, что 1 — свидетель при любом $m > 1$.

Пусть m нечётно.

Докажем, что если $s \in S$, то и $m - s \in S$. Действительно, если $s^{m-1} \equiv 1 (\mathrm{mod}\, m)$, то в силу чётности числа $m-1$ имеем $(-s)^{m-1} \equiv \equiv 1 (\mathrm{mod}\, m)$. Число $\frac{m-1}{2^i}$ чётно при $i < r$ и нечётно при $i = r$. Поэтому в последовательности остатков от деления на m чисел $(-s)^{\frac{m-1}{2^i}}$ по сравнению с такой же последовательностью для чисел $s^{\frac{m-1}{2^i}}$ меняется только последний элемент (он меняет знак). Значит, свойство W при переходе от s к $m - s$ сохраняется.

Итак, $s \in S \iff m - s \in S$.

Рассмотрим несколько примеров.

Пример 1. $m = 9$. Здесь $\mathbb{Z}_m^* = \{1, 2, 4, 5, 7, 8\}$. Поскольку $2^8 = 64 \cdot 4 \equiv 4 (\mathrm{mod}\, 9)$, а $4^8 \equiv 4^2 \equiv 7 (\mathrm{mod}\, 9)$, числа 2 и 4, а также $5 = 9 - 4$ и $7 = 9 - 2$ — антисвидетели простоты, а свидетелей всего два: 1 и 8.

Пример 2. Пусть $m = 3^k$, где $k \geqslant 2$. Докажем, что $S = \{1, m-1\}$. Положим $m - 1 = 3^k - 1 = 2t$ и $q = s^2$. Если $s^{m-1} = s^{2t} \equiv 1 (\mathrm{mod}\, m)$, то

$$s^{2t} - 1 = q^t - 1 = (q-1)(q^{t-1} + q^{t-2} + \ldots + 1) \vdots m. \qquad (1)$$

Поскольку при этом s не делится на 3, $q = s^2 \equiv 1 (\mathrm{mod}\, 3)$. Поэтому

$$Q = q^{t-1} + q^{t-2} + \ldots + 1 \equiv t (\mathrm{mod}\, 3).$$

Но число t не делится на 3. Значит, $(Q, m) = (Q, 3^k) = 1$ и из (1) следует, что $s^2 - 1 = q - 1 \vdots m$. Получилось, что $s \equiv \pm 1 (\mathrm{mod}\, m)$. $\square$

Пример 3. $m = 15$. Здесь $\mathbb{Z}_m^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Имеем $13^{14} \equiv 2^{14} = (4^2)^3 \cdot 4 \equiv 4 (\mathrm{mod}\, 15)$. Отсюда $2, 13 \in A$. Поскольку $4^{14} \equiv \equiv 4^2 \equiv 1 (\mathrm{mod}\, 15)$, а $4^7 \equiv 4 (\mathrm{mod}\, 15)$, число 4 не входит в S. Выясним, является ли число 4 антисвидетелем. Заметим, что $4^k + 1 \equiv 2 (\mathrm{mod}\, 3)$, в силу чего $4^k \not\equiv -1 (\mathrm{mod}\, 3)$ и $4^k \not\equiv -1 (\mathrm{mod}\, 15)$. Для проверки выполнения определения антисвидетеля переберём все простые делители числа 15. Имеем: $\mathrm{ord}_3\, 4 = 1 \neq 2$; $\mathrm{ord}_5\, 4 = 2 \neq 4$. Стало быть, $4 \notin A$. Далее, $8^{14} \equiv 7^{14} \equiv 49^7 \equiv 4^7 \equiv 4 (\mathrm{mod}\, 15)$. Поэтому $7, 8 \in A$. Наконец, число 11 является антисвидетелем, так как $11^{14} \equiv 4^{14} \equiv 1 (\mathrm{mod}\, 15)$, $11^7 \equiv (-4)^7 \equiv -4 (\mathrm{mod}\, 15)$ и $\mathrm{ord}_3\, 11 = 2$. Итак, для числа 15 множества свидетелей и антисвидетелей таковы: $S = \{1, 14\}$, $A = \{2, 7, 8, 11, 13\}$.

1°. Пусть $m = p^2k$, где p — простое число. Образуем множество

$$G = \{1, 1 + pk, 1 + 2pk, 1 + 3pk, \ldots, 1 + (p-1)pk\}.$$

Оно относительно операции умножения по модулю m образует циклическую группу порядка p. Действительно,

$$(1 + xpk)(1 + ypk) \equiv 1 + (x + y)pk (\mathrm{mod}\, m),$$

что говорит об изоморфизме мультипликативной группы G и аддитивной группы $\mathbb{Z}_p$.

2°. Пусть $a \in A$, $s \in S$. Тогда $as \notin S$.

Доказательство. Случай $a^{m-1} \not\equiv 1 (\mathrm{mod}\, m)$ тривиален: $(as)^{m-1} \equiv \equiv a^{m-1} \not\equiv 1 (\mathrm{mod}\, m)$, откуда $as \notin S$.

Пусть теперь $a^{m-1} \equiv 1 (\mathrm{mod}\, m)$, $\forall k \quad a^k \not\equiv -1 (\mathrm{mod}\, m)$ и $\mathrm{ord}_p a = = p-1$, где p — некоторый простой делитель числа m. Возьмём максимальное i, для которого $a^{\frac{m-1}{2^i}} \equiv 1 (\mathrm{mod}\, m)$. При этом $a^{\frac{m-1}{2^i}} \equiv 1 (\mathrm{mod}\, p)$.

Поскольку $\mathrm{ord}_p a = p - 1$, имеем $\frac{m-1}{2^i} \vdots p - 1$. Отсюда $\frac{m-1}{2^i}$ — чётное число. Стало быть, $i < r$ (напомним, что $m - 1 = 2^r t$, где t — нечётное число) и

$$a^{\frac{m-1}{2^r}} = a^t \not\equiv 1 (\mathrm{mod}\, m).$$

При $j \leqslant i$ число $\dfrac{m-1}{2^j}$ делится на $\dfrac{m-1}{2^i}$, которое, в свою очередь, кратно $p - 1$. В силу малой теоремы Ферма, $s^{\frac{m-1}{2^j}} \equiv 1 (\mathrm{mod}\, p)$. Тогда $s^{\frac{m-1}{2^j}} \not\equiv -1 (\mathrm{mod}\, p)$. Значит,

$$\forall j \leqslant i \quad s^{\frac{m-1}{2^j}} \not\equiv -1 (\mathrm{mod}\, m).$$

Из определения свидетеля отсюда следует, что

$$\forall j \leqslant i \quad s^{\frac{m-1}{2^j}} \equiv 1 (\mathrm{mod}\, m); \quad s^{\frac{m-1}{2^{i+1}}} \equiv \pm 1 (\mathrm{mod}\, m).$$

В то же время, a — антисвидетель и

$$\forall j \leqslant i \quad a^{\frac{m-1}{2^j}} \equiv 1 (\mathrm{mod}\, m); \quad a^{\frac{m-1}{2^{i+1}}} \not\equiv \pm 1 (\mathrm{mod}\, m).$$

Следовательно,

$$\forall j \leqslant i \quad (as)^{\frac{m-1}{2^j}} \equiv s^{\frac{m-1}{2^j}} \equiv 1 (\mathrm{mod}\, m),$$

но

$$(as)^{\frac{m-1}{2^{i+1}}} \equiv \pm a^{\frac{m-1}{2^{i+1}}} \not\equiv \pm 1 (\mathrm{mod}\, m).$$

Доказано, что as — не свидетель.$\square$

3°. Для $x \in \mathbb{Z}_m^*$ обозначим $Sx = \{sx \mid s \in S\}$. Пусть $a, b \in \mathbb{Z}_m^*$ и $a \neq b$. Тогда $Sa \cap Sb = \emptyset \iff S \cap Sab^{-1} = \emptyset$.

Доказательство. Достаточно убедиться в том, что непустота каждого из двух пересечений множеств означает непустоту и другого пересечения. Действительно,

$$sA \cap sB \neq \emptyset \iff \exists c \in Sa \cap Sb \iff \exists s_1, s_2 \quad c = s_1 a = s_2 b \iff$$

$$\iff \exists s_1, s_2 \quad cb^{-1} = s_2 = s_1 ab^{-1} \iff S \cap Sab^{-1} \neq \emptyset.$$

4°. Пусть G — подгруппа мультипликативной группы $\mathbb{Z}_m^*$. Тогда множества Sg по всем $g \in G$ попарно не пересекаются тогда и только тогда, когда $S \cap Sg = \emptyset$ при $g \neq 1$.

Это непосредственное следствие предыдущего утверждения.

5°. $\forall a \in \mathbb{Z}_m^* \quad Sa \subset \mathbb{Z}_m^*, |S| = |Sa|$.

Доказательство. Отображение $x \to xa$ является биекцией между S и Sa, так как равенство $s_i a = s_j a$ влечёт равенство $s_i = s_j$.

6°. Если $m \vdots p^2$, то $|S| \leqslant \dfrac{\varphi(m)}{p}$.

Доказательство. Рассмотрим циклическую группу G из 1°. В ней порядок каждого элемента (кроме единицы) равен p. Поскольку m кратно p, число $m-1$ не делится на p. Поэтому если $1 \neq a \in G$, то $a^{m-1} \not\equiv 1 (\mathrm{mod}\, m)$, значит, a — антисвидетель. Из 2° теперь следует, что $S \cap Sa = \emptyset$. Благодаря 4° получаем, что множества Sg $(g \in G)$ попарно не пересекаются. В силу 5° имеем

$$\left| \bigcup_{g \in G} Sg \right| = |S| \cdot |G| = |S| \cdot p.$$

При этом $\bigcup\limits_{g \in G} Sg \subset \mathbb{Z}_m^*$. Стало быть, $\varphi(m) \geqslant |S| \cdot p$. $\square$

7°. Пусть $m = p_1 p_2$, где $p_1 \neq p_2$ — простые числа. Тогда $|S| \leqslant \frac{\varphi(m)}{4}$.

Доказательство. Убедимся сначала в том, что

$$\exists a_1 \in \mathbb{Z}_m^* \quad a_1 \equiv 1 (\mathrm{mod}\, p_2),\ \mathrm{ord}_{p_1} a_1 = p_1 - 1.$$

Действительно, по теореме о первообразном корне существует такое число x_1, что $\mathrm{ord}_{p_1} x_1 = p_1 - 1$. Для любого целого числа t имеем $(x_1 + tp_1)^{p_1 - 1} \equiv 1 (\mathrm{mod}\, p_1)$. Найдём t из условия $x_1 + tp_1 - sp_2 = 1$.

Благодаря взаимной простоте чисел p_1 и p_2 такое t существует. Теперь можно положить $a_1 = x_1 + tp_1$.

Для любого $k \in \mathbb{N}$ имеем $a_1^k \equiv 1 (\mathrm{mod}\, p_2)$, откуда $a_1^k \not\equiv -1 (\mathrm{mod}\, p_2)$ и $a_1^k \not\equiv -1 (\mathrm{mod}\, m)$. С учётом того, что $\mathrm{ord}_{p_1} a_1 = p_1 - 1$, получаем, что a_1 — антисвидетель простоты числа m. Таким же свойством обладает и число a_2, определяемое условиями

$$a_2 \equiv 1 (\mathrm{mod}\, p_1),\ \mathrm{ord}_{p_2} a_2 = p_2 - 1.$$

Докажем, что антисвидетелем будет и число $a = a_1 a_2$. Действительно,

$$a^k = (a_1 a_2)^k \equiv 1 (\mathrm{mod}\, m) \iff \begin{cases} a_1^k a_2^k - 1 \vdots p_1; \\ a_1^k a_2^k - 1 \vdots p_2 \end{cases} \iff$$

$$\iff \begin{cases} a_1^k \equiv 1 (\mathrm{mod}\, p_1); \\ a_2^k \equiv 1 (\mathrm{mod}\, p_2) \end{cases} \iff \begin{cases} k \vdots p_1 - 1; \\ k \vdots p_2 - 1. \end{cases}$$

Если $a^{m-1} \equiv 1 (\mathrm{mod}\, m)$, то $m - 1 \vdots p_1 - 1$. Но тогда

$$p_2 - 1 = p_1 p_2 - 1 - p_2(p_1 - 1) = m - 1 - p_2(p_1 - 1) \vdots p_1 - 1.$$

Точно так же $p_1 - 1 \vdots p_2 - 1$. Отсюда $p_2 = p_1$, что противоречит условию. Значит, $a^{m-1} \not\equiv 1 (\mathrm{mod}\, m)$. Следовательно, a — антисвидетель. Аналогично доказывается, что $a_1 a_2^{-1} \in A$.

Множества S, Sa_1, Sa_2, Sa_1a_2 попарно не пересекаются в силу 3° и равномощны в силу 5°. Отсюда

$$|S| \leqslant \frac{\varphi(m)}{4}. \tag{1}$$

8°. Пусть число m свободно от квадратов и делится на три разных простых числа p_1, p_2 и p_3.

Аналогично тому, как это было сделано в 7°, найдём числа a_1, a_2 из множества $\mathbb{Z}_m^*$, обладающие следующими свойствами:

$$a_1 \equiv 1 (\mathrm{mod}\, p_2 p_3),\ \mathrm{ord}_{p_1} a_1 = p_1 - 1,$$

$$a_2 \equiv 1 (\mathrm{mod}\, p_1 p_3),\ \mathrm{ord}_{p_2} a_2 = p_2 - 1.$$

При этом числа $a_1, a_2, a = a_1 a_2, b = a_1 a_2^{-1}$ сравнимы с 1 по модулю p_3. Так же, как и в 7°, показывается, что числа a_1, a_2, a, b являются антисвидетелями, откуда следует, что равномощные множества S, Sa_1, Sa_2 и Sa попарно не пересекаются. Вновь получаем неравенство (1).

Из примера 2 и пунктов 1°–8° вытекает следующее утверждение.

Теорема 24.1. (М. Рабин, 1980 г.) *Составное нечётное число m имеет не более $\frac{\varphi(m)}{4}$ свидетелей простоты.*

Данная теорема лежит в основе вероятностного теста Миллера – Рабина, проверяющего простоту числа m. На каждом шаге этого теста в отношении случайного числа, меньшего m, проводится проверка, является ли оно свидетелем простоты числа m. Если нет, то число m составное. Как показывает теорема Рабина, для составного числа m вероятность того, что случайное число входит в множество S, меньше $\frac{1}{4}$. Поэтому, если после n шагов теста не обнаружено, что данное число составное, то вероятность того, что мы ошибёмся, назвав данное число простым, меньше, чем $\frac{1}{4^n}$.

25. Тест Люка – Лемера

Как отмечалось выше, наибольшими известными простыми числами являются числа Мерсенна. Для доказательства их простоты имеется эффективный критерий Люка – Лемера.

Метод, разработанный французом Э. Люка в 1856 г., был пригоден для простых чисел вида $p = 4n + 3$. Результат Люка состоял в следующем.

Рассмотрим последовательность $r_0 = 3$, $r_{n+1} = r_n^2 - 2$. Число M_p, где p — простое число и $p \equiv 3 (\mathrm{mod}\, 4)$, является простым тогда и только тогда, когда число r_{p-2} делится на M_p.

Доказательство этой теоремы и обсуждение технических подробностей реализации критерия Люка можно найти в статье [15].

В 1932 г. американец Д. Лемер усовершенствовал метод Люка, изменив всего лишь начальный член последовательности: вместо 3 он взял 4. Однако теперь критерий заработал для всех простых чисел! Как было установлено позднее, в качестве r_0 подходит также число 10. Полная информация о том, какие числа можно взять в качестве r_0 в тесте Люка – Лемера, содержится в онлайн-энциклопедии целочисленных последовательностей (The On-Line Encyclopedia of Integer Sequences, сокращённо — OEIS),

расположенной на сайте `http://oeis.org`, см. последовательность A018844.

Приведём примеры работы данного критерия.

При $p = 3$ имеем $M_p = 2^3 - 1 = 7$; $r_0 = 4$; $r_{p-2} = r_1 = 4^2 - 2 = 14 \vdots 7$. Поэтому 7 — простое число:).

При $p = 11$ имеем $M_p = 2^{11} - 1 = 2047$. Нас интересует, делится ли число $r_{p-2} = r_9$ на 2047. Выпишем остатки от деления чисел r_n на 2047 для $n = 0, 1, \ldots, 9$:

$$4, 14, 194, 788, 701, 119, 1877, 240, 282, 1736.$$

Как видно, r_9 не делится на 2047. Поэтому 2047 — составное число. Критерий Люка – Лемера позволяет установить, что число Мерсенна составное, не находя при этом его простые делители. Но в данном примере эти делители легко обнаруживаются: $2047 = 23 \cdot 89$.

В этом разделе мы приведём эффектное доказательство корректности теста Люка – Лемера. Это — адаптированное (к предполагаемому уровню знаний читателей данных заметок) изложение рассуждения [29] из блога выдающегося математика современности Теренса Тао (род. в 1975 г. в Австралии).

Теорема 25.1. *Пусть $r_0 = 4$ и $r_{n+1} = r_n^2 - 2$ при $n \in \mathbb{N}$. Число Мерсенна M_p, где p — простое число, является простым тогда и только тогда, когда число r_{p-2} делится на M_p.*

Доказательство. Несложно заметить, что если $r_0 = x + \frac{1}{x}$ и $r_{n+1} = r_n^2 - 2$ при $n \in \mathbb{N}$, то $r_n = x^{2^n} + y^{2^n}$, где $y = \dfrac{1}{x}$. Доказательство — индукцией по n. Действительно, пусть уже известно, что $r_k = x^{2^k} + y^{2^k}$. Поскольку $xy = 1$, имеем

$$r_{k+1} = \left(x^{2^k} + y^{2^k}\right)^2 - 2 = x^{2^{k+1}} + y^{2^{k+1}}.$$

В нашем случае $x = 2 + \sqrt{3}$, $y = 2 - \sqrt{3}$.

Докажем **достаточность.** Пусть r_{p-2} кратно M_p. Тогда для некоторого натурального k

$$x^{2^{p-2}} + y^{2^{p-2}} = kM_p; \quad x^{2^{p-2}} = kM_p - y^{2^{p-2}}.$$

Умножим обе части последнего равенства на $x^{2^{p-2}}$:

$$x^{2^{p-1}} = kM_p x^{2^{p-2}} - 1. \tag{1}$$

Предположим, что число M_p составное, а q — его наименьший простой делитель. Ясно, что $q > 2$ и $q^2 \leqslant M_p$.

Рассмотрим кольцо

$$X = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}_q\}.$$

Здесь $\mathbb{Z}_q$ — множество классов вычетов по модулю q, а операции сложения и умножения вводятся естественным образом. Ясно, что $|X| = q^2$.

Будем далее считать, что в записи $a + b\sqrt{3}$ целые числа a и b заменяют соответствующие классы вычетов по модулю m. В силу данного соглашения можно записать: $x \in X$.

Рассмотрим мультипликативную группу этого кольца $\langle X^*, \cdot \rangle$, которая состоит из элементов, имеющих обратный элемент по умножению. Из-за необратимости нуля $|X^*| < |X|$, т. е. $|X^*| \leqslant q^2 - 1$.

Поскольку M_p делится на q, из (1) следует, что в кольце X справедливо $x^{2^{p-1}} = -1$, откуда $x^{2^p} = 1$. Значит, порядок элемента x в X^* равен 2^p. Но

$$|X^*| \leqslant q^2 - 1 \leqslant M_p - 1 = 2^p - 2.$$

Получилось противоречие: порядок элемента группы оказался больше порядка группы (а по теореме Лагранжа первое число должно быть делителем второго).

Необходимость. Пусть M_p — простое число. При нечётном $p \geqslant 3$ имеют место сравнения

$$M_p \equiv -1 (\mathrm{mod}\, 4); \quad M_p \equiv 1 (\mathrm{mod}\, 3).$$

Далее будем использовать обозначение $q = M_p$.

Для дальнейшего нам понадобятся значения символов Лежандра $\left(\frac{2}{q}\right)$ и $\left(\frac{3}{q}\right)$. Вычислим первый из них:

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = (-1)^{\frac{(2^p-1)^2-1}{8}} = (-1)^{2^{2p-3}-2^{p-2}} = 1.$$

Для вычисления второго применим квадратичный закон взаимности:

$$\left(\frac{3}{q}\right)\left(\frac{q}{3}\right) = (-1)^{\frac{q-1}{2}\cdot\frac{3-1}{2}} = (-1)^{\frac{2^p-2}{2}} = (-1)^{2^{p-1}-1} = -1. \qquad (2)$$

С помощью леммы Эйлера найдём $\left(\frac{q}{3}\right)$:

$$\left(\frac{q}{3}\right) \equiv q^{\frac{3-1}{2}} \equiv q \equiv 1(\mathrm{mod}\, 3).$$

Значит, $\left(\frac{q}{3}\right) = 1$, и с учётом соотношения (2) получаем $\left(\frac{3}{q}\right) = -1$.

Вновь применим лемму Эйлера:

$$2^{\frac{q-1}{2}} \equiv 1(\mathrm{mod}\, q); \quad 3^{\frac{q-1}{2}} \equiv -1(\mathrm{mod}\, q). \tag{3}$$

Далее будем вести вычисления в кольце X.

Применив формулу бинома Ньютона и воспользовавшись тем, что биномиальный коэффициент C_q^k, где $0 < k < q$, кратен простому числу q, получим

$$\forall a, b \in X \quad (a+b)^q = a^q + b^q.$$

Заметим, что $x = 2 + \sqrt{3} = \frac{(6+2\sqrt{3})^2}{24}$. При этом

$$(6 + 2\sqrt{3})^q = 6^q + 2^q(\sqrt{3})^q = 6^q + 2^q \cdot 3^{\frac{q-1}{2}} \cdot \sqrt{3} = 6 - 2\sqrt{3}.$$

Мы применили малую теорему Ферма, согласно которой $6^q \equiv 6(\mathrm{mod}\, q)$ и $2^q \equiv 2(\mathrm{mod}\, q)$, а также второе соотношение из (3).

Дальнейшие выкладки таковы (повторим, что все вычисления ведутся в кольце X):

$$x^{\frac{q+1}{2}} = \left(\frac{(6+2\sqrt{3})^2}{24}\right)^{\frac{q+1}{2}} = \frac{(6+2\sqrt{3})^{q+1}}{24^{\frac{q+1}{2}}} = \frac{(6+2\sqrt{3})^q(6+2\sqrt{3})}{24 \cdot 24^{\frac{q-1}{2}}} =$$

$$= \frac{(6-2\sqrt{3})(6+2\sqrt{3})}{24 \cdot 3^{\frac{q-1}{2}} \cdot \left(2^{\frac{q-1}{2}}\right)^3} = \frac{36-12}{24 \cdot (-1) \cdot 1} = -1.$$

Наконец,

$$r_{p-2} = x^{2^{p-2}} + y^{2^{p-2}} = x^{\frac{q+1}{4}} + y^{\frac{q+1}{4}} = y^{\frac{q+1}{4}}\left(x^{\frac{q+1}{2}} + 1\right) = 0.$$

Доказано, что число r_{p-2} делится на $q = M_p = 2^p - 1$.□

Библиографический список

1. Айерлэнд, К. *Классическое введение в современную теорию чисел* / К. Айерлэнд, М. Роузен. — М.: Мир, 1987. – 415 с.

2. Арнольд, В. И. *Цепные дроби* / В. И. Арнольд. — М.: Изд-во МЦНМО, 2001. – 40 с.

3. Бугаенко, В. О. *Уравнения Пелля* / В. О. Бугаенко. — М.: Изд-во МЦНМО, 2001. – 32 с.

4. Бухштаб, А. А. *Теория чисел* / А. А. Бухштаб. — М.: Просвещение, 1966. – 380 с.

5. *Введение в криптографию* / под ред. В. В. Ященко. – 2-е изд., испр. — М.: МЦНМО-ЧеРо, 1999. – 272 с.

6. Виноградов, И. М. *Основы теории чисел* / И. М. Виноградов. — М.: Наука, 1965. – 172 с.

7. Галочкин, А. И. *Введение в теорию чисел* / А. И. Галочкин, Ю. В. Нестеренко, А. Б. Шидловский. — М.: Изд-во МГУ, 1995. – 160 с.

8. Гарднер, М. *От мозаик Пенроуза к надежным шифрам* / М. Гарднер. — М.: Мир, 1993. – 416 с.

9. Гашков, С. Б. *Арифметика. Алгоритмы. Сложность вычислений* / С. Б. Гашков, В. Н. Чубариков. — М.: Высш. шк., 2000. – 320 с.

10. Гельфонд, А. О. *Решение уравнений в целых числах* / А. О. Гельфонд. — М.: Наука, 1978. – 64 с.

11. Гиндикин, С. Г. *Рассказы о физиках и математиках* / С. Г. Гиндикин. — М.: МЦНМО, 2013. – 5-е изд., доп. – 496 с.

12. Краснов, М. Л. *Вся высшая математика:* учебник. Т.7 / М. Л. Краснов, А. И. Киселёв, Г. И. Макаренко и др. — М.: КомКнига, 2014. – 208 с.

13. Нестеренко, Ю. В. *Теория чисел* / Ю. В. Нестеренко. — М.: Издательский центр «Академия», 2008. – 272 с.

14. Прасолов, В. В. *Задачи по алгебре, арифметике и анализу* / В. В. Прасолов. — М.: МЦНМО, 2007. – 608 с.

15. Рудаков, А. Н. *Числа Фибоначчи и простота числа* $2^{127} - 1$ / А. Н. Рудаков // Математическое просвещение. – 2000. – Сер. 3. – Вып. 4. – С. 127–139.

16. Сизый, С. В. *Лекции по теории чисел* / С. В. Сизый. — М.: ФИЗМАТЛИТ, 2007. – 192 с.

17. Спивак, А. В. *Арифметика* / А. В. Спивак. — М.: Бюро Квантум, 2007. – 160 с. (Б-чка «Квант». Вып. 102.)

18. Спивак, А. В. *Арифметика-2* / А. В. Спивак. — М.: Бюро Квантум, 2008. – 160 с. (Б-чка «Квант». Вып. 109.)

19. Хинчин, А. Я. *Цепные дроби* / А. Я. Хинчин. — М.: Наука, 1978. – 112 с.

20. Шибасов, Л. П. *От единицы до бесконечности* / Л. П. Шибасов. — М.: Дрофа, 2004. – 208 с.

21. Эвнин, А. Ю. *Девятнадцать доказательств теоремы Евклида* / А. Ю. Эвнин. // Квант. – 2001. – № 1. – С. 35–38. Интернет: `http://www.vivovoco.rsl.ru/quantum/2001.01/matkr_1_01.pdf`.

22. Эвнин, А. Ю. *Дискретная математика:* конспект лекций / А. Ю. Эвнин. — Челябинск: Изд-во ЮУрГУ, 1998. – 176 с.

23. Эвнин, А. Ю. *Задачник по дискретной математике* / А. Ю. Эвнин. – 2-е изд., перераб. и доп. — Челябинск: Изд-во ЮУрГУ, 2002. – 164 с.

24. Эвнин, А. Ю. *Задачник по дискретной математике.* 5-е изд. / А. Ю. Эвнин. — М.: Книжный дом «ЛИБРОКОМ», 2012. – 264 с.

25. Эвнин, А. Ю. *Уравнение Пелля* / А. Ю. Эвнин // Математика в высшем образовании. – 2009. – № 7. – С. 79–85.

26. Эвнин, А. Ю. *Элементарная теория чисел:* сборник олимпиадных задач / А. Ю. Эвнин. — Челябинск: ЧГТУ, 1996. – 76 с.

27. Эдвардс, Г. *Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел* / Г. Эдвардс. — М.: Мир, 1980. – 484 с.

28. Tao, T. *The Lucas-Lehmer test for Mersenne primes* / Terence Tao // `https://terrytao.wordpress.com/2008/10/02/the-lucas-lehmer-test-for-mersenne-primes`

Оглавление

Учебное издание

Эвнин Александр Юрьевич

ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Учебное пособие

2-е издание, переработанное и дополненное

Техн. редактор *А. В. Миних*

Издательский центр Южно-Уральского государственного университета

Подписано в печать 23.11.2015. Формат 60×84 1/16. Печать цифровая.
Усл. печ. л. 5,58. Тираж 30 экз. Заказ 621/476.

Отпечатано в типографии Издательского центра ЮУрГУ.
454080, г. Челябинск, пр. им. В. И. Ленина, 76.