Т.М. Банникова, Н.А. Баранова

Основы теории чисел

Ижевск
2009

Федеральное агентство по образованию
Государственное образовательное учреждение
высшего профессионального образования
"Удмуртский государственный университет"

Т.М. Банникова, Н.А. Баранова

Основы теории чисел

Учебно-методическое пособие

Ижевск 2009

УДК 511(075)
ББК 22.13я7
Б 232

Рецензент: к.ф.-м.н., доцент кафедры прикладной информатики ИжГТУ Ицков А.Г.

Банникова Т.М., Баранова Н.А.
Б 232 Основы теории чисел: учебно-методическое пособие
Ижевск, 2009. 95 с.

Настоящее учебное пособие представляет предназначено для студентов математического факультета и факультета информационных технологий и вычислительной техники. Пособие может быть использовано при организации лабораторных и самостоятельных работ студентов по курсам «Алгебра», «Геометрия и алгебра», «Алгебра и геометрия», Учебное пособие может быть полезно студентам математических специальностей высших учебных заведений при изучении спецкурсов по криптографии

В пособии представлены следующие разделы теории чисел: теория делимости целых чисел, цепные дроби, мультипликативные функции, теория сравнений. Каждая глава пособия снабжена задачами для самостоятельного решения.

Оглавление

Глава 1
Теория делимости

1.1. Делимость целых чисел. Свойства делимости

Говорят, что целое число a делит целое число b, если найдется целое число c такое, что $b = a \cdot c$. И пишут $a|b$. Число a называется *делителем* числа b.

Делитель a называется *собственным* делителем числа b, если $1 < |a| < |b|$, и *несобственным* в противном случае.

Пример 1. $5|35$; число 5 делит число 35, так как $35 = 5 \cdot 7$. При этом число 5 является собственным делителем числа 35.

Положительное, целое число $p \neq 1$ называется *простым*, если оно не имеет собственных делителей, и *составным* в противном случае.

Пример 2.
2, 3, 5, 7, 11, 13, 17, 19, 23, 29 и т. д. — простые числа;
4, 6, 8, 0, -2, 9, 10, 12, -3, -4 и т. д. — составные числа.

Свойства:

1. $a|a$, при $a \neq 0$.
2. Если $a|b$ и $b|a$, то $a = \pm b$.
3. Если $a|b$ и $b|c$, то $a|c$ (транзитивность).
4. Если $a|b$ и $a|c$, то $a|(b + c)$.

Доказательство. Докажем свойства 1 и 3.

1. Если $a \neq 0$, то по определению из равенства $a = a \cdot 1$ следует $a|a$.

3. Если $a|b$ и $b|c$, то найдутся числа x и y, что $b = a \cdot x$, $c = b \cdot y$, тогда $c = a \cdot (x \cdot y)$, где $x \cdot y$ — целое число. Это означает, что $a|c$.

Остальные свойства докажите самостоятельно.

Свойства собственного делителя.

1. Положительный наименьший собственный делитель составного числа n не превосходит $\sqrt{n}$.

2. Положительный наименьший собственный делитель составного числа n есть простое число.

Доказательство.

1. Пусть положительный наименьший собственный делитель составного числа n равен p, тогда $n = p \cdot q$, где q — собственный делитель n не меньший p. Получаем $p^2 \leqslant p \cdot q = n$, таким образом, $p \leqslant \sqrt{n}$.

2. Пусть p положительный наименьший собственный делитель n не простое число. Значит, оно имеет собственный делитель q: $1 < q < p < n$, при этом $q|p$ и $p|n$. По свойству транзитивности получаем, что $q|n$. Таким образом, q — собственный делитель n меньший p — противоречие. Свойства доказаны.

Как можно применить данные свойства?

Пример 3. Рассмотрим задачу: является ли число 287 простым числом?

Решение. Найдем наименьший собственный делитель числа 287. Для этого проверим все простые числа от 2 до $\sqrt{287}$. Или от 2 до 13. Получаем: $2 \nmid 287$, $3 \nmid 287$, $5 \nmid 287$, $7 \nmid 287$, $11 \nmid 287$, $13 \nmid 287$. Таким образом, данное число является простым.

Теорема (основная теорема арифметики). *Любое целое число* $(n > 1)$ *может быть представлено в виде произведения простых чисел и при том единственным образом с точностью до порядка сомножителей.*

Доказательство.

1) пусть $n > 1$ — простое число. Тогда запишем $n = p_1$, и теорема верна.

2) Пусть $n > 1$ — составное. Обозначим через p_1 положительный наименьший собственный делитель числа n. По свойствам p_1 — является простым числом и $n = p_1 \cdot n_1$.

Если n_1 — простое, обозначим его p_2 и запишем $n = p_1 \cdot p_2$. Если n_1 — составное, то поступим с ним также как с n, выделив положительный наименьший собственный делитель. Получим $n = p_1 \cdot p_2 \cdot n_2$. И так далее. Такой процесс конечен, то есть на некотором шаге число n_k будет обязательно простым. Таким образом, получили следующее разложение $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$ и доказали теорему.

Разложение $n = p_1^a \cdot p_2^b \cdot \ldots \cdot p_k^m$, где p_i все различные простые, $a, b, \ldots, m$ — натуральные, называется *каноническим разложением* числа n.

Пример 4. Найти каноническое разложение числа $m = 2\,420$.

Решение.

$m = 2420 = 2 \cdot 1210 = 2 \cdot 2 \cdot 605 = 2 \cdot 2 \cdot 5 \cdot 121 = 2 \cdot 2 \cdot 5 \cdot 11 \cdot 11.$

Ответ. $m = 2^2 \cdot 5 \cdot 11^2$.

Теорема. *Для данного целого отличного от нуля числа* b*, всякое целое число* a *единственным образом представимо в виде* $a = b \cdot q + r$*, где* $0 \leqslant r < |b|$.

Доказательство. Ясно, что одно представление числа равенством $a = b \cdot q + r$ мы получим, если возьмем $b \cdot q$ равным наибольшему кратному числа b, не превосходящему a.

Тогда, очевидно, $0 \leqslant r < |b|$. Докажем единственность такого представления. Пусть $a = b \cdot q + r$ и $a = b \cdot q_1 + r_1$ — два таких представления. Значит $0 = a - a = b(q - q_1) + (r - r_1)$. Здесь 0

делится на b; $b(q-q_1)$ делится на b, следовательно $(r-r_1)$ обязано делиться на b. Так как $0 \leqslant r < b$ и $0 \leqslant r_1 < b$, то $r - r_1 < b$ и $r - r_1$ делится на b, значит $r - r_1$ равно нулю, а, значит и $q - q_1$ равно нулю, т. е. два таких представления совпадают. Доказательство завершено.

Число q называется *неполным частным*, а число r — *остатком* от деления a на b.

Пример 5.
Если $a = 5$, $b = 2$: $5 = 2 \cdot 2 + 1$, $q = 2$, $r = 1$.
Если $a = -5$, $b = 2$: $-5 = 2 \cdot (-3) + 1$, $q = -3$, $r = 1$.
Если $a = -10$, $b = 3$: $-10 = 3 \cdot (-4) + 2$, $q = 4$, $r = 2$.

1.2. НОД и НОК. Их свойства

Пусть a и b — целые положительные числа. Целое число d называется *наибольшим общим делителем* чисел a и b, если d делит одновременно a и b и каждый другой общий делитель a и b делит d. Обозначается НОД(a, b).

Известно, что НОД двух чисел — единственный.

Говорят, что два целых числа a и b *взаимно простые*, если их единственными общими делителями являются единицы ± 1.

Свойства:

1. Если $a|(b \cdot c)$ и НОД$(a, b) = 1$, то $a|c$.

2. Если p — простое число и $p|(b \cdot c)$, то либо $p|b$, либо $p|c$.

3. Для любых целых чисел a и k справедливо: НОД$(a, k \cdot a) = a$; НОД$(1, a) = 1$.

   Докажите эти свойства самостоятельно.

4. Если $a = bq + c$, то совокупность общих делителей a и b совпадает с совокупностью общих делителей b и c, в частности,

$$\text{НОД}(a, b) = \text{НОД}(b, c).$$

Доказательство. Пусть $d|a$, $d|b$, тогда $d|c$. Пусть $d|c$, $d|b$, тогда $d|a$.

5. Если для целых чисел a и b существую целые x и y такие, что $ax + by = 1$, то НОД$(a, b) = 1$.

Доказательство. Пусть НОД$(a, b) = d$, тогда $d|a$, $d|b$, значит $a = a^* \cdot d$, $b = b^* \cdot d$, где a^*, b^* — целые числа. По условию задачи $ax + by = 1$, для некоторых x, y. Следовательно, получаем равенство $(a^* \cdot d)x + (b^* \cdot d)y = 1$ или $d(a^* \cdot x + b^* \cdot y) = 1$. Значит, по определению делимости целых чисел, число d делит 1. Но $d > 0$, следовательно, $d = 1$, то есть НОД$(a, b) = 1$.

Теорема. *В кольце Z имеется бесконечно много простых чисел.*

Доказательство. От противного. Пусть $p_1, p_2, \ldots, p_n$ — все простые, какие только есть.

Рассмотрим число $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$. Число a больше всех p, значит оно составное. Его наименьший отличный от 1 делитель c, будучи простым, не может совпадать ни с одним из $p_1, p_2, \ldots, p_n$, так как иначе $c|(a - p_1 \cdot p_2 \cdot \ldots \cdot p_n) = 1$. Получили противоречие, что доказывает нашу теорему.

Пример 6. Простыми являются числа: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 и т. д. Для составления таблицы простых чисел древний грек Эратосфен придумал процедуру, которая получила название «решето Эратосфена».

Понятие *решета Эратосфена* рассмотрим на примере.

Пример 7. Найти все простые числа из промежутка $[800; 830]$, используя «решето Эратосфена».

Решение. Найдем простые проверочные числа: $\sqrt{830} < 29$. Выпишем все числа из заданного промежутка и вычеркнем среди них последовательно все числа, делящиеся на 2, 3, 5, 7, 11, 13, 17, 19, 23:

800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830.

На 2 делятся: $800, 802, \ldots,$ — каждое второе;

На 3 делятся: $801, 804, \ldots,$ — каждое третье;

На 5 делятся: $800, 805, \ldots,$ — каждое пятое;

На 7 делятся: $805, 812, \ldots,$ — каждое седьмое;

На 11 делятся: $803, 814, \ldots,$ каждое одиннадцатое;

На 13 делятся: $806, 819, \ldots,$ — каждое тринадцатое; и т. д.

Ответ. 809, 811, 821, 823.

Алгоритм Евклида: для целых чисел a и b можно составить алгоритм:

$$\begin{array}{cc}
a = b \cdot q_1 + r_1 & 0 \leqslant r_1 < b \\
b = r_1 \cdot q_2 + r_2 & 0 \leqslant r_2 < r_1 \\
r_1 = r_2 \cdot q_3 + r_3 & 0 \leqslant r_3 < r_2 \\
r_2 = r_3 \cdot q_4 + r_4 & 0 \leqslant r_4 < r_3 \\
\ldots\ldots\ldots & \ldots\ldots\ldots \\
r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1} & 0 \leqslant r_{n-1} < r_{n-2} \\
r_{n-2} = r_{n-1} \cdot q_n + r_n & 0 \leqslant r_n < r_{n-1} \\
r_{n-1} = r_n \cdot q_{n+1} & r_{n+1} = 0.
\end{array}$$

Имеем: $b > r_1 > r_2 > \ldots > r_n > 0$, следовательно процесс оборвется максимум через b шагов. В силу единственности нахождения частного и остатка на каждом шаге деления, алгоритм единственен.

Теорема. *Последний, отличный от нуля, остаток в алгоритме Евклида для чисел a и b есть* НОД(a, b).

Доказательство. Просмотрим последовательно равенства сверху вниз: всякий делитель a и b делит $r_1, r_2, \ldots, r_n$. Если же просматривать эту цепочку равенств от последнего к первому, то видно, что $r_n | r_{n-1}$, $r_n | r_{n-2}$, и так далее, т. е. r_n делит a и b. Поэтому r_n — наибольший общий делитель чисел a и b. Доказательство завершено.

Теорема (свойство линейной представимости НОД). *Если* $\text{НОД}(a, b) = d$*, то найдутся такие целые* u *и* v*, что*

$$d = a \cdot u + b \cdot v.$$

Доказательство. Из цепочки равенств имеем:

$$r_n = r_{n-2} - r_{n-1} \cdot q_n = r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1}) \cdot q_n = \dots$$

(идем по цепочке равенств снизу вверх,
выражая из каждого следующего равенства
остаток и подставляя его в получившееся
уже к этому моменту выражение)

$$\dots = a \cdot u + b \cdot v = \text{НОД}(a, b).$$

Доказательство завершено.

Пример 8. Найти наибольший общий делитель (НОД) чисел и его линейное представление:
а) $\text{НОД}(733, 1998)$; б) $\text{НОД}(2, 5, 8)$.

Решение.
а) НОД конечного набора чисел — есть натуральное наибольшее число, делящее нацело любое число из набора. Известно, что один из способов нахождения НОД двух (а следовательно и любого количества) чисел есть алгоритм Евклида: последний, отличный от нуля, остаток в алгоритме Евклида есть $\text{НОД}(a, b)$.

Итак, решение нашей задачи основывается на алгоритме Евклида:

$1998 = 733 \cdot 2 + 532$
$733 = 532 \cdot 1 + 201$
$532 = 201 \cdot 2 + 130$
$201 = 130 \cdot 1 + 71$
$130 = 71 \cdot 1 + 59$
$71 = 59 \cdot 1 + 12$
$59 = 12 \cdot 4 + 11$

$12 = 11 \cdot 1 + 1$

$11 = 1 \cdot 11 + 0$

Поэтому НОД$(1998, 733) = 1$.

Из данного алгоритма можно получить линейное представление НОД$(1998, 733)$, рассматривая алгоритм «с конца».

Линейное представление:

$1 = 12-11 = 12-(59-12\cdot 4) = 12\cdot 5-59 = (71-59)\cdot 5-59 = 71\cdot 5-$
$-6\cdot 59 = 5\cdot 71-6\cdot(130-71) = 11\cdot 71-6\cdot 130 = 11\cdot(201-130)-6\cdot 130 =$
$= 11 \cdot 201 - 17 \cdot 130 = 11 \cdot 201 - 17 \cdot (532 - 201 \cdot 2) =$
$= 45 \cdot 201 - 17 \cdot 532 = 45 \cdot (733 - 532) - 17 \cdot 532 = 45 \cdot 733 - 62 \cdot 532 =$
$= 45 \cdot 733 - 62 \cdot (1998 - 733 \cdot 2) = 169 \cdot 733 - 62 \cdot 1998.$

Проверка: $169 \cdot 733 - 62 \cdot 1998 = 123877 - 123876 = 1$.

б) чтобы найти НОД нескольких чисел, несложно понять, что достаточно найти НОД двух чисел, потом НОД полученного НОД и следующего числа и т. д.

То есть, если НОД$(b, c) = d$, то НОД$(a, b, c) =$ НОД(a, d).

НОД$(2, 5, 8) =$ НОД$(2,$ НОД$(5, 8)) =$ НОД$(2, 1) = 1$.

Линейное представление в общем случае можно найти так:

если НОД$(b, c) = d = x \cdot b + y \cdot c$, НОД$(a, d) = z \cdot a + t \cdot d$,

то НОД$(a, b, c) = z \cdot a + t \cdot (x \cdot b + y \cdot c)$.

Или подберем ответ сами, что в данном случае совсем не сложно и можно сделать гораздо быстрее, чем искать представление в общем виде, как в п. а): 1=8-5-2.

Ответ.

а) НОД$(733, 1198) = 1$, $\quad 1 = 169 \cdot 733 - 62 \cdot 1998$;

б) НОД$(2, 5, 8) = 1$, $\quad 1 = 8 - 5 - 2$.

Пусть a и b — целые положительные числа. Целое число m называется *наименьшим общим кратным* чисел a и b, если m делится одновременно на a и b и каждое другое общее кратное a и b делится на m. Обозначается НОК$[a, b]$.

Известно, что НОК двух чисел — единственно.

Свойства:

1. Если НОД$(a, b) = 1$, то НОК$[a, b] = a \cdot b$.
2. $a \cdot b =$ НОД$(a, b) \cdot$ НОК$[a, b]$.

Докажите эти свойства самостоятельно.

Пример 9. Найдите наименьшее общее кратное (НОК) чисел $[2, 5, 8]$.

Решение. НОК — есть натуральное наименьшее число, делящееся на все числа из заданного набора. Так как 8 уже делится на 2, то $\text{НОК}[2, 5, 8] = 5 \cdot 8 = 40$.

Ответ. $\text{НОК}[2, 5, 8] = 40$.

1.3. Диофантовы уравнения

Диофантовым уравнением первой степени называется уравнение вида

$$a \cdot x + b \cdot y = c$$

с целыми коэффициентами a, b, c, решаемое на множестве целых чисел.

Один из способов решения такого уравнения основывается на свойствах НОД. Рассмотрим его на примере.

Пример 10. Решите Диофантово уравнение при помощи линейного представления НОД: $47x - 111y = 89$.

Решение. Если $\text{НОД}(a, b) = 1$, то найдутся такие x, y, что $a \cdot x + b \cdot y = 1$. Тогда выполнится: $ax \cdot c + by \cdot c = c$. $\text{НОД}(47, 111) = 1$. Найдем x, y:

$111 = 47 \cdot 2 + 17$

$47 = 17 \cdot 2 + 13$

$17 = 13 \cdot 1 + 4$

$13 = 4 \cdot 3 + 1$

$4 = 1 \cdot 4 + 0$.

Линейное представление: $1 = 13 - 4 \cdot 3 = 13 - (17 - 13 \cdot 1) \cdot 3 = 13 \cdot 4 - 17 \cdot 3 = (47 - 17 \cdot 2) \cdot 4 - 17 \cdot 3 = 47 \cdot 4 - 17 \cdot 11 = 47 \cdot 4 - (111 - 47 \cdot 2) \cdot 11 = 47 \cdot 26 - 111 \cdot 11$.

Тогда выполняется: $89 = 47 \cdot (89 \cdot 26) - 111 \cdot (89 \cdot 11)$.

$x = 89 \cdot 26 + 111t$; $y = 89 \cdot 11 + 47t$, где t — любое целое.

Ответ. $x = 2314 + 111t$, $y = 979 + 47t$, $t = Z$.

В отличие от уравнений первой степени, алгоритмы решения диофантовых уравнений более высоких степеней в общем виде отсутствуют. Более того, существуют различные классы диофантовых уравнений, которые не имеют решений. Остановимся подробнее на частных случаях диофантовых уравнений степени $\geqslant 2$.

Пример 11.
а) $(2x+y)(5x+3y)=7$;
б) $xy=x+y+3$;
в) $x^2=14+y^2$;
г) $x^2+y^2=x+y+2$.

Решение этих задач связано с идеей перебора. После преобразования уравнения (чаще всего разложение на множители) перебор сводится к ограниченному количеству пар. Например, уравнение $xy=x+y+3$ после преобразования имеет вид $(x-1)(y-1)=4$. Рассматривая разложение 4 в произведение двух целых множителей получаем ответ: $(5;2)$, $(2;5)$, $(0;-3)$, $(-3;0)$, $(3;3)$, $(-1;-1)$.

Существует ряд уравнений, не имеющих решений. Доказательство этого чаще всего основано на рассмотрении остатков по какому-либо модулю. Этот же прием подходит и для тех случаев, когда легко подбирается единственное решение и доказывается, что другие решения отсутствуют.

Пример 12. Решить уравнение в целых числах: $3^m+7=2^n$.

Решение. Сразу видно, что пара $m=2$ и $n=4$ является решением данного уравнения. Докажем, что остальные решения отсутствуют.

Перепишем уравнение в следующем виде: $3^m=4^k-7$.

Так как $4^k-7\equiv 1(\mathrm{mod}\ 4)$, а

$3^{2p}\equiv 1(\mathrm{mod}\ 4)$, $3^{2p+1}\equiv 3(\mathrm{mod}\ 4)$, то m — четно, т. е. $m=2p$;

$3^{2p}+7=2^{2k}$, следовательно $7=2^{2k}-3^{2p}=(2^k-3^p)(2^k+3^p)$, следовательно $2^k+3^p=7$; $2^k-3^p=1$, и получается единственное решение $k=2$ и $p=1$.

При решении диофантовых уравнений часто оказывются полезными различные неравенства и оценки, например при решении следующих уравнений:

а) $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=1$;

б) $x^2-y^2=1982$.

в) Докажите, что уравнение $\frac{1}{x}-\frac{1}{y}=\frac{1}{n}$ имеет единственное решение в натуральных числах тогда и только тогда, когда n — простое число.

Существуют диофантовы уравнения, имеющие специальные названия. Например, *уравнением Пелля* называется уравнение вида $x^2-Ny^2=1$, где натуральное число N свободно от квадратов.

Это уравнение имеет бесконечно много решений в целых числах. Кроме того, существует такое решение (x_1,y_1), что каждое другое решение задается соотношением

$$x_k+y_k\sqrt{N}=\pm(x_1+y_1\sqrt{N})^k.$$

Будем говорить, что решение (x,y) больше, чем решение (u,v), если

$$x+y\sqrt{N}>u+v\sqrt{N}.$$

Тогда наименьшее решение (x_1,y_1) с положительными x_1 и y_1 называется *фундаментальными*.

Фундаментальное решение можно найти, раскладывая $\sqrt{N}$ в непрерывную дробь. Этот метод называется *методом Браункера*.

При нечетном n решением будет пара (P_n,Q_n), при четном n — пара (P_{2n+1},Q_{2n+1}).

Рассмотрим пример $x^2-34y^2=1$.

Раскладываем $\sqrt{34}$ в непрерывную дробь

$$\sqrt{34}=5+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{10+\ldots}}}},$$

где $a_0 = 5$, $a_1 = 1$, $a_2 = 4$, $a_3 = 1$, $n = 3$ — нечетное.

$\frac{P_0}{Q_0} = \frac{5}{1}$, $\frac{P_1}{Q_1} = \frac{6}{1}$, $\frac{P_2}{Q_2} = \frac{39}{5}$, $\frac{P_3}{Q_3} = \frac{35}{6}$.

Получим: $x_1 = 35$, $y_1 = 6$.

По формуле $x_k + y_k = \pm(x_1 + y_1\sqrt{N})^k$ можем выписывать и другие пары, являющиеся решением.

1.4. Важнейшие функции в теории чисел

1.4.1. Мультипликативные функции

В этом пункте речь пойдет об одном важном классе функций, которому в теории чисел посвящены целые монографии (см., напр., книжку Г. Дэвенпорта «Мультипликативная теория чисел»).

Функция $\theta : R \to R$ (или, более общо, $\theta : C \to C$) называется *мультипликативной*, если:

1) функция определена всюду на N и существует $a \in N$ такой, что $\theta(a) \neq 0$;

2) для любых взаимно простых натуральных чисел a_1 и a_2 выполняется $\theta(a_1 \cdot a_2) = \theta(a_1) \cdot \theta(a_2)$.

Пример 13. $\theta(a) = a^s$, где s — любое (действительное или комплексное) число. Проверка аксиом 1) и 2) из определения мультипликативной функции не составляет труда, а сам пример показывает, что мультипликативных функций по меньшей мере континуум, т. е. много.

Перечислим, кое-где доказывая, некоторые свойства мультипликативных функций. Пусть всюду ниже $\theta(a)$ — произвольная мультипликативная функция.

Свойства:

1. $\theta(1) = 1$.

Доказательство. Пусть a — то самое натуральное число, для которого $\theta(a) \neq 0$. Тогда $\theta(a \cdot 1) = \theta(a) \cdot \theta(1) = \theta(a)$.

2. $\theta(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}) = \theta(p_1^{\alpha_1})\cdot\theta(p_2^{\alpha_2})\cdot\ldots\cdot\theta(p_n^{\alpha_n})$, где $p_1, p_2\ldots, p_n$ — различные простые числа.

   Доказательство очевидно.

3. Обратно, мы всегда построим некоторую мультипликативную функцию $\theta(a)$, если зададим $\theta(1) = 1$ и произвольно определим $\theta(p\alpha)$ для всех простых p и всех натуральных α, а для остальных натуральных чисел доопределим функцию $\theta(a)$, используя равенство

$$\theta(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}) = \theta(p_1^{\alpha_1})\cdot\theta(p_2^{\alpha_2})\cdot\ldots\cdot\theta(p_n^{\alpha_n}).$$

Доказательство сразу следует из основной теоремы арифметики.

Пример 14. Пусть $\theta(1) = 1$ и $\theta(p\cdot\alpha) = 2$ для всех p и α. Тогда, для произвольного числа,

$$\theta(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_n^{\alpha_n}) = 2^n.$$

4. Произведение нескольких мультипликативных функций является мультипликативной функцией.

Доказательство. Сначала докажем для двух сомножителей. Пусть θ_1 и θ_2 — мультипликативные функции $\theta = \theta_1\cdot\theta_2$, тогда (проверяем аксиомы определения):

1. $\theta(1) = \theta_1(1)\cdot\theta_2(1) = 1$ и, кроме того, существует такое a (это $a = 1$), что $\theta(a)\neq 0$.

2. Пусть $(a, b) = 1$ — взаимно просты. Тогда

$$\theta(a\cdot b) = \theta_1(a\cdot b)\cdot\theta_2(a\cdot b) = \theta_1(a)\cdot\theta_1(b)\cdot\theta_2(a)\cdot\theta_2(b) = \\ = \theta_1(a)\cdot\theta_2(a)\cdot\theta_1(b)\cdot\theta_2(b) = \theta(a)\cdot\theta(b).$$

Доказательство для большего числа сомножителей проводится стандартным индуктивным рассуждением.

Введем удобное обозначение. Всюду далее, символом

$$\sum_{d|n}$$

будем обозначать сумму чего-либо, в которой суммирование проведено по всем делителям d числа n.

Теорема 1. *Пусть*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$$

— каноническое разложение числа $a \in N$, θ — любая мультипликативная функция. Тогда:

$$\sum_{d|a} \theta(d) = \left(1 + \theta(p_1) + \theta(p_1^2) + \ldots + \theta(p_1^{\alpha_1})\right) \times \\ \times \left(1 + \theta(p_2) + \theta(p_2^2) + \ldots + \theta(p_2^{\alpha_2})\right) \times \ldots \\ \ldots \times \left(1 + \theta(p_n) + \theta(p_n^2) + \ldots + \theta(p_n^{\alpha_n})\right).$$

Если $a = 1$, то считаем правую часть равной 1.

Доказательство. Раскроем скобки в правой части. Получим сумму всех (без пропусков и повторений) слагаемых вида

$$\theta(p_1^{\beta_1}) \cdot \theta(p_2^{\beta_2}) \cdot \ldots \cdot \theta(p_n^{\beta_n}),$$

где $0 \leqslant \beta_k \leqslant \alpha_k$, для всех $k \leqslant n$. Так как различные простые числа заведомо взаимно просты, то

$$\theta\left(p_1^{\beta_1}\right) \cdot \theta\left(p_2^{\beta_2}\right) \cdot \ldots \cdot \theta\left(p_n^{\beta_n}\right) = \theta\left(p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}\right),$$

а это как раз то, что стоит в доказываемом равенстве слева, поэтому теорема доказана.

Теорема 2. *Пусть $\theta(a)$ — любая мультипликативная функция. Тогда*

$$\chi(a) = \sum_{d|a} \theta(d)$$

— также мультипликативная функция.

Доказательство. Проверим для $\chi(a)$ аксиомы определения мультипликативной функции.

1) $\chi(a) = \sum\limits_{d|1} \theta(d) = \theta(1) = 1$.

2) Пусть НОД$(a, b) = 1$;

$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$; $b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_k^{\beta_k}$, и все p и q различны. Тогда, по предыдущей лемме, имеем: (делители чисел a и b различны)

$$\chi(ab) = \sum_{d|ab} \theta(d) = \prod_i \left(1 + \theta(p_i) + \theta(p_i^2) + \ldots + \theta(p_i^{\alpha_i})\right) \times$$

$$\times \prod_j \left(1 + \theta(q_j) + \theta(q_j^2) + \ldots + \theta(q_j^{\beta_j})\right) = \chi(a) \cdot \chi(b).$$

Доказательство завершено.

Теорема. *Можно доказать обратное утверждение к теореме 2 настоящего пункта, а именно, если*

$$f(a) = \sum_{d|a} \theta(d)$$

— мультипликативная функция и функция $\theta(n)$ всюду определена хотя бы на N, то $\theta(n)$ также обязана быть мультипликативной функцией.

Докажите эту теорему самостоятельно.

1.4.2. Примеры мультипликативных функций

В предыдущем пункте были даны общие понятия о мультипликативных функциях. В этом пункте мы рассмотрим серию примеров полезных мультипликативных функций.

Число делителей данного числа

Пусть $\theta(a) = a^0 \equiv 1$ — тождественная единица (заведомо мультипликативная функция). Тогда, если

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n},$$

то тождество теоремы 1 принимает вид:

$$\tau(a) = \sum_{d|a} \theta(d) = (1+\alpha_1) \cdot (1+\alpha_2) \cdot \ldots \cdot (1+\alpha_n) = \sum_{d|a} 1$$

— это не что иное, как количество делителей числа a. По теореме 2 количество делителей $\tau(a)$ числа a есть мультипликативная функция.

Пример 15. Вычислить значение функции τ при $a = 720$.

$$\tau(720) = \tau(2^4 \cdot 3^2 \cdot 5) = (4+1) \cdot (2+1) \cdot (1+1) = 30.$$

Сумма делителей данного числа

Пусть $\theta(a) = a^1 \equiv a$ — тождественная мультипликативная функция. Тогда, если

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n},$$

то тождество теоремы 1 принимает вид:

$$S(a) = \sum_{d|a} d = \sum_{d|a} \theta(d) =$$

$$\underbrace{(1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1})}\underbrace{(1 + p_2 + p_2^2 + \ldots + p_2^{\alpha_2})} \ldots$$

$$\ldots \underbrace{(1 + p_n + p_n^2 + \ldots + p_n^{\alpha_n})} = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \ldots \frac{p_n^{\alpha_n+1} - 1}{p_n - 1}$$

— сумма всех делителей числа a. По теореме 2, сумма всех делителей есть мультипликативная функция.

Пример 16. Вычислить значение функции S при $a = 720$.

$$S(720) = S(2^4 \cdot 3^2 \cdot 5) = \frac{2^5 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 2418.$$

Функция Мебиуса

Функция Мебиуса $\mu(a)$ — это мультипликативная функция, определяемая следующим образом: если p — простое число, то $\mu(p) = -1$; $\mu(p \cdot \alpha) = 0$, при $\alpha > 1$; на остальных натуральных числах функция доопределяется по мультипликативности.

Таким образом, если число a делится на квадрат натурального числа, отличный от единицы, то $\mu(a) = 0$; если же

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_n,$$

a свободно от квадратов, то $\mu(a) = (-1)^k$, где k — число различных простых делителей a. Понятно, что $\mu(1) = (-1)^0 = 1$, как и должно быть.

Теорема. *Пусть $\theta(a)$ — произвольная мультипликативная функция,*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}.$$

Тогда:

$$\sum_{d|a} \mu(d) \cdot \theta(d) = (1 - \theta(p_1)) \cdot (1 - \theta(p_2)) \cdot \ldots \cdot (1 - \theta(p_n))$$

(*при $a = 1$ считаем правую часть равной* 1).

Доказательство. Рассмотрим функцию $\theta_1(x) = \mu(x) \cdot \theta(x)$. Эта функция мультипликативна, как произведение мультипликативных функций. Для $\theta_1(x)$ имеем (p — простое): $\theta_1(p) = -\theta(x)$;

$\theta_1(p\alpha) = 0$, при $\alpha > 1$. Следовательно, для $\theta_1(x)$ тождество теоремы 1 выглядит так:

$$\sum_{d|a} \mu(d) \cdot \theta(d) = \big(1 - \theta(p_1)\big) \cdot \big(1 - \theta(p_2)\big) \cdot \ldots \cdot \big(1 - \theta(p_n)\big).$$

Доказательство завершено.

Следствие. *Пусть* $\theta(d) = d^{-1} = \frac{1}{d}$ (*это, конечно, мультипликативная функция*),

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}, \quad a > 0.$$

Тогда:

$$\sum_{d|a} \frac{\mu(d)}{d} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right).$$

Следствие доказано.

Физический смысл этой правой части раскрывает пример следующей функции.

Функция Эйлера.

Функция Эйлера $\varphi(a)$ есть количество чисел из ряда

$$0, 1, 2, \ldots, a - 1,$$

взаимно простых с a.

Теорема. *Пусть*

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}.$$

Тогда:
1) $\varphi(a) = \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right)$ (*формула Эйлера*);
2) $\varphi(a) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdot \ldots \cdot \left(p_n^{\alpha_n} - p_n^{\alpha_n - 1}\right)$,
в частности, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, $\varphi(p) = p - 1$.

Доказательство. Пусть x пробегает числа $0, 1, 2, \ldots, a-1$. Положим $\delta_x = \text{НОД}(x, a)$ — наибольший общий делитель. Тогда $\varphi(a)$ есть число значений δ_x, равных 1. Придумаем такую функцию $\chi(\delta_x)$, чтобы она была единицей, когда δ_x единица, и была нулем в остальных случаях. Вот подходящая кандидатура:

$$c(d_x) = \sum_{d|d_x} m(d) = \begin{cases} 0, & \text{если} \quad d_x > 1, \\ 1, & \text{если} \quad d_x = 1. \end{cases}$$

Последнее легко понять, если вспомнить теорему 1, и в ее формулировке взять $\theta(d) \equiv 1$. Далее, можно усмотреть, что:

$$\varphi(a) = \sum_{0 \leqslant x < a} \chi(\delta_x) = \sum_{0 \leqslant x < a} \left(\sum_{d|\delta_x} \mu(d) \right).$$

Поскольку справа сумма в скобках берется по всем делителям d числа $\delta_x = (x, a)$, то d делит x и d делит a. Значит, в первой сумме справа в суммировании участвуют только те x, которые кратны d. Таких x среди чисел $0, 1, 2, \ldots, a-1$ ровно $\frac{a}{d}$ штук.

Получается, что:

$$\varphi(a) = \sum_{d|a} \frac{a}{d} \mu(d) = a \sum_{d|a} \frac{\mu(d)}{d} =$$

$$= a \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right),$$

что и требовалось.

Имеем

$$\varphi(a) = \sum_{0 \leqslant x < a} \left(\sum_{d|\text{НОД}(x,a)} \mu(d) \right).$$

Зафиксируем некоторое d_0 такое, что d_0 делит a, d_0 делит x, $x < a$. Значит в сумме справа в скобках слагаемых $\mu(d_0)$ ров-

но $a|d_0$ штук и $\varphi(a)$ есть просто сумма

$$\sum_{d_0|a} \frac{a}{d_0}.$$

После этого, равенство

$$\sum_{d|a} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right)$$

получается применением следствия из теоремы 1.

Второе утверждение леммы следует из первого внесением впереди стоящего множителя a внутрь скобок.

Следствие. Функция Эйлера вычисляется по следующей формуле:

$$\varphi(a) = \left(\sum_{d|a} \frac{\mu(d)}{d}\right) \cdot a.$$

Доказательство. Пусть

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}.$$

Тогда, по теореме 1, имеем:

$$\sum_{d|a} \varphi(d) = \prod_{k=1}^{n} \left(1 + \varphi(p_k) + \varphi(p_k^2) + \ldots + \varphi(p_k^{\alpha_k})\right) =$$

$$= \prod_{k=1}^{n} \left(1 + (p_k - 1)) + (p_k^2 - 1) + \ldots + (p_k^{\alpha_k} - p_k^{\alpha_k - 1})\right) =$$

$$= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} = a.$$

Следствие доказано.

Следствие. *Функция Эйлера мультипликативна.*

Доказательство. Имеем:

$$\varphi(a) = \left(\sum_{d|a} \frac{\mu(d)}{d}\right) \cdot a$$

— произведение двух мультипликативных функций, первая из которых мультипликативна по теореме 2. Значит, $\varphi(a)$ — мультипликативна и следствие доказано.

В следующих примерах вычислим функцию Эйлера для конкретных значений n:

Пример 17. $\varphi(5) = 5 - 1 = 4$.

Пример 18. $\varphi(60) = 60 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 16$.

Пример 19. $\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = (2-1) \cdot (3-1) \cdot (5-1) = 8$; $\sum\limits_{d|30} = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(15) + \varphi(30) =$
$= 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$.

1.5. Непрерывные и подходящие дроби

Рассмотрим понятие непрерывной дроби.

Для вещественного (не целого) λ, обозначим через q_1 наибольшее целое не превосходящее λ. Тогда λ можно записать в виде $\lambda = q_1 + \frac{1}{\lambda_1}$ при $\lambda_1 > 1$. Аналогично $\lambda_1 = q_2 + \frac{1}{\lambda_2}$ при $\lambda_2 > 1$, тогда $\lambda = q_1 + \cfrac{1}{q_2 + \frac{1}{\lambda_2}}$ и т. д.

Получаем выражение вида:

$$\lambda = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ldots \cfrac{1}{q_m + \ldots}}}}.$$

Оно называется *бесконечной цепной дробью* или *непрерывной дробью.*

Если число рациональное, то процесс построения непрерывной дроби конечен и в этом случае полученную дробь называют конечной цепной дробью.

Теорема. *Любое рациональное число единственным образом представимо в виде конечной цепной дроби.*

Процесс нахождения представления рационального числа в виде конечной цепной дроби основан на алгоритме Евклида. Рассмотрим его на примере. А доказательство в общем виде приведите самостоятельно.

Пример 20. Представьте число $\lambda = \frac{105}{38}$ в виде непрерывной дроби.

Решение. Имеем дробь $\lambda = \frac{105}{38}$. Составим алгоритм Евклида для $(105, 38)$:

$105 = 38 \cdot 2 + 29$

$38 = 29 \cdot 1 + 9$

$29 = 9 \cdot 3 + 2$

$9 = 2 \cdot 4 + 1$

$2 = 1 \cdot 2 + 0$. Тогда $q_1 = 2$, $q_2 = 1$, $q_3 = 3$, $q_4 = 4$, $q_5 = 2$.

Ответ. $\lambda = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{4 + \frac{1}{2}}}}$.

Если представить этот процесс в общем виде, то доказательство теоремы становится очевидным.

Рассмотрим еще одно понятие, связанное с непрерывными дробями.

Дроби $\delta_1 = q_1$, $\delta_2 = q_1 + \frac{1}{q_2}$, $\delta_3 = q_1 + \cfrac{1}{q_2 + \frac{1}{q_3}}$ и т.д. называются *подходящими дробями.*

Подходящие дроби обычно записывают в виде $\delta_i = \dfrac{P_i}{Q_i}$ — i-я подходящая дробь.

Докажем рекуррентные соотношения:

$$P_s = q_s \cdot P_{s-1} + P_{s-2},$$
$$Q_s = q_s \cdot Q_{s-1} + Q_{s-2},$$

где $P_0 = 1$, $P_1 = q_1$, $Q_0 = 0$, $Q_1 = 1$, $s > 1$, целое.

Доказательство.

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1},$$

$$\delta_2 = \frac{q_1 + \frac{1}{q_2}}{1} = \frac{q_2 \cdot q_1 + 1}{q_2 \cdot 1 + 0} = \frac{q_2 \cdot P_1 + P_0}{q_2 \cdot Q_1 + Q_0} = \frac{P_2}{Q_2},$$

$$\delta_3 = \frac{\left(q_1 + \frac{1}{q_2}\right) \cdot P_1 + P_0}{\left(q_2 + \frac{1}{q_3}\right) \cdot Q_1 + Q_0} = \frac{q_3 \cdot P_2 + P_1}{q_3 \cdot Q_2 + Q_1} = \frac{P_3}{Q_3}$$

и т. д., и вообще при $s > 1$

$$\delta_s = \frac{q_s \cdot P_{s-1} + P_{s-2}}{q_s \cdot Q_{s-1} + Q_{s-2}} = \frac{P_s}{Q_s}.$$

Таким образом, числители и знаменатели подходящих дробей мы можем последовательно вычислять по формулам

$$P_s = q_s \cdot P_{s-1} + P_{s-2},$$
$$Q_s = q_s \cdot Q_{s-1} + Q_{s-2}.$$

Пример 21. Для числа $\lambda = \dfrac{5391}{3976}$ найдите шестую подходящую дробь.

Находим q_s по алгоритму Евклида:

$5391 = 3976 \cdot \mathbf{1} + 1415$
$3976 = 1415 \cdot \mathbf{2} + 1146$
$1415 = 1146 \cdot \mathbf{1} + 269$
$1146 = 269 \cdot \mathbf{4} + 70$
$269 = 70 \cdot \mathbf{3} + 59$
$70 = 59 \cdot \mathbf{1} + 11.$
То есть $q_1 = 1$, $q_2 = 2$, $q_3 = 1$, $q_4 = 4$, $q_5 = 3$, $q_6 = 1$.
Из рекуррентных соотношений находим:

$$\begin{aligned} P_1 &= 1, & Q_1 &= 1, \\ P_2 &= 2 \cdot 1 + 1 = 3, & Q_2 &= 2 \cdot 1 + 0 = 2, \\ P_3 &= 1 \cdot 3 + 1 = 4, & Q_3 &= 1 \cdot 2 + 1 = 3, \\ P_4 &= 4 \cdot 4 + 3 = 19, & Q_4 &= 4 \cdot 3 + 2 = 14, \\ P_5 &= 3 \cdot 19 + 4 = 61, & Q_4 &= 3 \cdot 14 + 3 = 45, \\ P_6 &= 1 \cdot 61 + 19 = 80, & Q_6 &= 1 \cdot 45 + 14 = 59. \end{aligned}$$

Ответ. $\delta_6 = \dfrac{80}{59}$.

1.6. Непрерывные дроби в решении задач

Число называется *квадратичной иррациональностью*, если оно является корнем квадратного уравнения $ax^2 + bx + c = 0$ с целыми коэффициентами a, b, c. Это уравнение определено однозначно, если потребовать, чтобы числа a, b, c были взаимно просты в совокупности и $a \geqslant 0$.

Пример 22. Числа $\sqrt{3}$, $3\sqrt{2}+5$, $\dfrac{1+\sqrt{15}}{7-4\sqrt{15}}$ являются квадратичными иррациональностями; числа $\sqrt[3]{5}$, $2\sqrt[5]{7}+3$, e, π не являются квадратичными иррациональностями.

Любая квадратичная иррациональность имеет вид $u + v\sqrt{N}$, где числа u, v рациональные и N не является полным квадратом. Квадратичная иррациональность вида $u - v\sqrt{N}$ называется *сопряженной* к иррациональности $u + v\sqrt{N}$.

Теорема (Лагранжа). *Квадратичные иррациональности и только они могут быть представлены в виде бесконечной периодической обыкновенной непрерывной дроби.*

Доказательство. Сначала докажем достаточность. Рассмотрим бесконечную периодическую обыкновенную непрерывную дробь

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}$$

Назовем число

$$r_k = a_k + \cfrac{1}{a_{k+1} + \cfrac{1}{a_{k+2} + \dots}}$$

остатком непрерывной дроби α, тогда

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots \cfrac{\dots}{a_{k-1}} + \cfrac{1}{r_k}}}.$$

Для остатков периодической непрерывной дроби выполняется соотношение $r_{k+1} = r_k$, где $k \geqslant k_0$ и t — период последовательности $\{a_k\}$. По способу составления подходящих дробей имеем

$$\alpha = \frac{r_k \cdot P_{k-1} + P_{k-2}}{r_k \cdot Q_{k-1} + Q_{k-2}} =$$

$$= \frac{r_{k+t} \cdot P_{k+t-1} + P_{k+t-2}}{r_{k+t} \cdot Q_{k+t-1} + Q_{k+t-2}} = \frac{r_k \cdot P_{k+t-1} + P_{k+t-2}}{r_k \cdot Q_{k+t-1} + Q_{k+t-2}},$$

откуда

$$\frac{r_k \cdot P_{k-1} + P_{k-2}}{r_k \cdot Q_{k-1} + Q_{k-2}} = \frac{r_k \cdot P_{k+t-1} + P_{k+t-2}}{r_k \cdot Q_{k+t-1} + Q_{k+t-2}},$$

то есть r_k является корнем квадратного уравнения

$$\begin{gathered}(P_{k-1}\cdot Q_{k+t-1}-P_{k+t-1}\cdot Q_{k-1})\cdot r^2+\\ +(P_{k-1}\cdot Q_{k+t-2}+P_{k-2}\cdot Q_{k+t-1}-\\ -P_{k+t-1}\cdot Q_{k-2}-P_{k+t-2}\cdot Q_{k-1})\cdot r+\\ +(P_{k-2}\cdot Q_{k+t-2}-P_{k+t-2}\cdot Q_{k-2})=0\end{gathered}$$

с целыми коэффициентами. Значит, r_k — квадратичная иррациональность. Тогда и

$$\frac{r_k\cdot P_{k-1}+P_{k-2}}{r_k\cdot Q_{k-1}+Q_{k-2}}$$

— квадратичная иррациональность.

Теперь докажем необходимость. Пусть число α является корнем квадратного уравнения с целыми коэффициентами

$$a\cdot\alpha^2+b\cdot\alpha+c=0. \tag{1.1}$$

Разожим число α в обыкновенную непрерывную дробь и выразим его некоторый остаток r_k непрерывной дроби:

$$\alpha=\frac{r_k\cdot P_{k-1}+P_{k-2}}{r_k\cdot Q_{k-1}+Q_{k-2}}.$$

Подставляя это выражение в формулу 1.1 и проводя ряд преобразований, снова получаем квадратное уравнение

$$A_k\cdot r_k^2+B_k\cdot r_k+C_k=0 \tag{1.2}$$

относительно r_k с целыми коэффициентами

$$\begin{aligned}A_k&=a\cdot P_{k-1}^2+b\cdot P_{k-1}\cdot Q_{k-1}+c\cdot Q_{k-1}^2,\\ B_k&=2a\cdot P_{k-1}\cdot P_{k-2}+b\cdot(P_{k-1}\cdot Q_{k-2}+P_{k-2}\cdot Q_{k-1})+\\ &\quad+2c\cdot Q_{k-1}\cdot Q_{k-2},\\ C_k&=a\cdot P_{k-2}^2+b\cdot P_{k-2}\cdot Q_{k-2}+c\cdot Q_{k-2}^2.\end{aligned}$$

Заметим, что $C_k = A_{k-1}$ и

$$B_k^2 - 4A_k \cdot C_k = (b^2 - 4ac) \cdot (P_{k-1} \cdot Q_{k-2} + P_{k-2} \cdot Q_{k-1})^2 = \\ = (b^2 - 4ac)(-1)^{2(k-2)} = b^2 - 4ac,$$

то есть дискриминанты уравнений 1.1 и 1.2 совпадают при любом k.

Из неравенства $\left|\alpha - \dfrac{P_{k-1}}{Q_{k-1}}\right| < \dfrac{1}{Q_{k-1}^2}$ получаем, что

$$P_{k-1} = \alpha \cdot Q_{k-1} + \frac{\varepsilon_{k-1}}{Q_{k-1}}$$

при некотором ε_{k-1}, таком, что $|\varepsilon_{k-1}| < 1$. Тогда

$$A_k = a \cdot P_{k-1}^2 + b \cdot P_{k-1} \cdot Q_{k-1} + c \cdot Q_{k-1}^2 =$$

$$= a\left(\alpha \cdot Q_{k-1} + \frac{\varepsilon_{k-1}}{Q_{k-1}}\right)^2 + b\left(\alpha \cdot Q_{k-1} + \frac{\varepsilon_{k-1}}{Q_{k-1}}\right) \cdot Q_{k-1} + c \cdot Q_{k-1}^2 =$$

$$= (a \cdot \alpha^2 + b \cdot \alpha + c) \cdot Q_{k-1}^2 + 2\alpha \cdot \varepsilon_{k-1} + a \cdot \frac{\varepsilon_{k-1}^2}{Q_{k-1}^2} + b \cdot \varepsilon_{k-1} =$$

$$= 0 \cdot Q_{k-1}^2 + \alpha \cdot \varepsilon_{k-1} + a \cdot \frac{\varepsilon_{k-1}^2}{Q_{k-1}^2} + b \cdot \varepsilon_{k-1} =$$

$$= 2\alpha \cdot \varepsilon_{k-1} + a \cdot \frac{\varepsilon_{k-1}^2}{Q_{k-1}^2} + b \cdot \varepsilon_{k-1}.$$

∎

Значит,

$$|A_k| = \left|2a \cdot \alpha \cdot \varepsilon_{k-1} + a \cdot \frac{\varepsilon_{k-1}^2}{Q_{k-1}^2} + b \cdot \varepsilon_{k-1}\right| < 2|a \cdot \alpha| + |a| + |b|,$$

$$|C_k| = |A_{k-1}| < 2|a \cdot \alpha| + |a| + |b|$$

для любого натурального k. Таким образом, целые коэффициенты A_k и C_k уравнения 1.2 ограничены по абсолютной величине и,

следовательно, при изменении k могут принимать лишь конечное число различных значений. Дискриминанты уравнений 1.1 и 1.2 совпадают, поэтому коэффициент B_k может принимать лишь конечное число различных значений. Значит, при $k = 1, 2, \ldots$ существует лишь конечное число различных уравнений вида 1.2, то есть лишь конечное число различных остатков r_k. Следовательно, найдутся два одинаковых остатка r_k и r_{k-1} с разными номерами, что и означает периодичность непрерывной дроби.

Пример 23. Разложим в непрерывную дробь число $1 + 2\sqrt{3} = [4; \{2, 6\}]$.

Эта непрерывная дробь периодическая, и все a_k равны либо 2, либо 6 при $k > 1$. Действительно, обозначим через x бесконечную непрерывную дробь $[0; 2, 6, 2, 6, \ldots]$. Тогда

$$x = \frac{1}{2 + \dfrac{1}{6 + x}}.$$

Упрощая выражение, получаем, что x является корнем уравнения

$$x^2 + 6x - 3 = 0,$$

откуда $x = -3 + 2\sqrt{3}$ и $4 + x = 1 + 2\sqrt{3}$.

Рассмотрим примеры использования непрерывных дробей для решения простейших диофантовых уравнений и сравнений первой степени.

Предположим, что $\dfrac{P_k}{Q_k}$ — последняя подходящая дробь в представлении непрерывной дробью рационального числа $\dfrac{a}{b}$, где НОД$(a, b) = 1$. Тогда $a = P_k$, $b = Q_k$. Известны рекуррентные соотношения

$$\begin{aligned} P_k &= q_k \cdot P_{k-1} + P_{k-2}, \\ Q_k &= q_k \cdot Q_{k-1} + Q_{k-2}, \\ P_0 &= 1, \quad P_1 = q_1, \\ Q_0 &= 0, \quad Q_1 = 1, \end{aligned}$$

используя которые и находим одно решение диофантова уравнения $ax - by = 1$:

$$x_0 = (-1)^{k-1} \cdot Q_{k-1}, \quad y_0 = (-1)^{k-1} \cdot P_{k-1}.$$

Остальные решения имеют вид

$$x = (-1)^{k-1} \cdot Q_{k-1} + bt, \quad y = (-1)^{k-1} \cdot P_{k-1} + at, \quad t \in \mathbb{Z}.$$

В общем случае диофантово уравнение $ax - by = c$ разрешимо, если число c делится на НОД(a, b).

Пример 24. Решим диофантово уравнение $31x - 23y = 11$.

Решение. Поскольку 11 делится на НОД$(31, 23) = 1$, решение существует. Заполняем таблицу:

k	-1	0	1	2	3
a_k		1	2	1	7
P_k	1	1	3	4	31
Q_k	0	1	2	3	23

Значит, $k = 3$, $\dfrac{P_2}{Q_2} = \dfrac{4}{3}$. Находим решение:
$x = (-1)^2 \cdot 11 \cdot 3 + 23t = 33 + 23t$,
$y = (-1)^2 \cdot 11 \cdot 4 + 31t = 44 + 31t$, где $t \in \mathbb{Z}$.
Проверка:
$31 \cdot (33 + 23t) - 23 \cdot (44 + 31t) =$
$= 31 \cdot 33 + 31 \cdot 23t - 23 \cdot 44 - 23 \cdot 31t = 31 \cdot 33 - 23 \cdot 44 = 11.$

Пример 25. Решим диофантово уравнение $655x - 115y = 700$.

Решение. Поскольку 700 делится на НОД$(655, 115) = 5$, решение существует. Заполняем таблицу:

k	-1	0	1	2	3	4
a_k		5	1	2	3	2
P_k	1	5	6	17	57	131
Q_k	0	1	1	3	10	23

Значит, $k = 4$, $\frac{P_3}{Q_3} = \frac{57}{10}$. Находим решение:
$x = (-1)^3 \cdot 140 \cdot 10 + 115t = -1400 + 115t$,
$y = (-1)^3 \cdot 140 \cdot 57 + 655t = -7980 + 655t$, где $t \in \mathbb{Z}$.

Проверка:
$655 \cdot (-1400 + 115t) - 115 \cdot (-7980 + 655t) =$
$= -655 \cdot 1400 + 655 \cdot 115t + 115 \cdot 7980 - 115 \cdot 655t =$
$= -917\,000 + 917\,700 = 700.$
Аналогично решаются сравнения первой степени вида

$$ax \equiv b (\mathrm{mod}\ m).$$

Для этого достаточно взять обе части диофантова уравнения

$$ax - my = b$$

по модулю m. Это сравнение разрешимо только тогда, когда b делится на НОД(a, m).

Задачи для самостоятельного решения

1. Найдите каноническое разложение числа:

   a) $m = 2\,880$, b) $m = 5\,780$, c) $m = 6\,480$.

2. Найдите наименьшее общее кратное чисел:

   a) НОК$[7, 15, 18]$, b) НОК$[3, 8, 19]$, c) НОК$[3, 2, 26]$.

3. Найдите все простые числа, используя «решето Эратосфена» из промежутка:

   a) $[810; 840]$, b) $[840; 870]$, c) $[870; 900]$.

4. Найдите наибольший общий делитель чисел и его линейное представление:

   a) НОД$(739, 1\,999)$; НОД$(7, 15, 18)$;
   b) НОД$(743, 2\,000)$; НОД$(3, 10, 15)$;
   c) НОД$(751, 2\,001)$; НОД$(3, 8, 19)$.

5. Докажите свойства делимости:

   a) если $a|b$ и $c|d$, то $(ac)|(bd)$;
   b) если НОД$(a, c) = 1$ и $a|(bc)$, то $a|b$;
   c) если $a|(bc)$ и НОД$(a, c) = 1$, то $a|b$;
   d) если $a|b$, $c|b$ и НОД$(a, c) = 1$, то $(ac)|b$;
   e) если $a|b$ и $a|c$, то $a|$НОД(b, c).

6. Докажите свойства НОД:

   a) если НОД$(a, b) = 1$, то НОД$(ac, b) =$ НОД(c, b) для любого целого c;
   b) если НОД$(a, b) = d$, то НОД$(a/d, b/d) = 1$;
   c) если НОД$(a, b) = 1$, $(c, b) = 1$, то НОД$(ac, b) = 1$;
   d) если НОД$(a, b) = d$, то найдутся такие целые числа x и y, что $ax + by = d$;
   e) НОД$(am, bm) = m \cdot$ НОД(a, b) для любого целого m.

7. Решите Диофантово уравнение при помощи линейного представления НОД:

   a) $43x - 111y = 87$; b) $39x - 111y = 89$;
   c) $41x - 111y = 87$; d) $38x - 111y = 89$.

8. Решите Диофантово уравнение при помощи подходящих дробей:

   a) $43x - 111y = 87$; b) $39x - 111y = 89$;
   c) $41x - 111y = 87$; d) $38x - 111y = 89$.

   Сравните результат с предыдущей задачей.

9. Представьте число λ в виде непрерывной дроби:

   a) $\lambda = \frac{105}{29}$; b) $\lambda = \frac{105}{31}$; c) $\lambda = \frac{105}{37}$.

10. Для числа λ найдите:

    a) четвёртую подходящую дробь, если $\lambda = \frac{5\,391}{3\,977}$;

    b) пятую подходящую дробь, если $\lambda = \frac{5\,391}{39\,957}$;

    c) шестую подходящую дробь, если $\lambda = \frac{5\,391}{3\,971}$.

11. Докажите, что при условии $56 \cdot a = 65 \cdot b$ число $a + b$ — составное.

12. Докажите, что число, имеющее нечетное число делителей, есть точный квадрат.

13. Решите уравнения в целых числах.

    a) $x^2 - 7y = 10$;
    b) $x^3 + 21y^2 + 5 = 0$;
    c) $15x^2 - 7y^2 = 9$;
    d) $x^2 + y^2 + z^2 = 8t - 1$;
    e) $3 \cdot 2^m + 1 = n^2$.

14. Докажите, что число вида $11m+1$ (при целом m) не является полным квадратом.

15. Пусть $\theta(p \cdot \alpha) = \alpha$ для всех простых p. Вычислите

    a) $\theta(864)$; b) $\theta(49\,500)$.

16. Пусть $\theta(p \cdot \alpha) = \alpha$ для всех простых p. Вычислите

    а) $\sum\limits_{d|864} \theta(d)$; б) $\sum\limits_{d|49\,500} \theta(d)$.

17. Найдите число делителей и сумму делителей чисел:

    a) 5 600; b) 116 424.

18. Найдите сумму собственных делителей (т. е. делителей, отличных от самого числа) чисел:

    a) 6; b) 28; c) 496; d) 8 128.

19. Составьте таблицу значений функции Мебиуса $\mu(n)$ для всех значений n от 1 до 100.

20. Составьте таблицу значений функции Эйлера $\varphi(n)$ для всех значений n от 1 до 100.

21. Используя формулу Эйлера для $\varphi(n)$, еще раз докажите бесконечность множества простых чисел.

22. Пусть k — натуральное число, d пробегает все делители числа a с условием $\varphi(d) = k$. Докажите, что $\sum\limits_{d} \mu(d) = 0$.

23. Пусть k — четное натуральное число, d пробегает все делители свободного от квадратов числа $a = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ с условием $0 < d < \sqrt{a}$. Докажите, что $\sum\limits_{d} \mu(d) = 0$.

Глава 2
Теория сравнений

2.1. Сравнения и их свойства

Пусть число m целое, больше 1. Говорят, что целые числа a и b *сравнимы* друг с другом *по модулю* m, если $m|(a-b)$ и обозначают

$$a \equiv b(\mathrm{mod}\ m).$$

Пример 26. $8 \equiv 3(\mathrm{mod}\ 5)$; $-3 \equiv 1(\mathrm{mod}\ 4)$.

Теорема. *Два числа сравнимы друг с другом по модулю m тогда и только тогда, когда они дают одинаковые остатки при делении на m.*

Доказательство. Пусть $a \equiv b(\mathrm{mod}\ m)$, по определению это означает, что $m|(a-b)$. Представим

$$a = mq + r, \quad b = mq_1 + r_1, \quad 0 \leqslant r < m, \quad 0 \leqslant r_1 < m.$$

Рассмотрим разность $a - b = m(q - q_1) + (r - r_1)$.

Из условий $m|(a-b)$, $m|m \cdot (q - q_1)$ получаем, что $m|(r - r_1)$. В связи с ограничениями на r, r_1 выводим $r - r_1 = 0$, т. е. $r = r_1$. Обратно, из $a = mq + r$, $b = mq_1 + r$ получем $a - b = m(q - q_1)$, т. е. $a \equiv b(\mathrm{mod}\ m)$.

Свойства сравнений.

1. Сравнения по общему модулю можно почленно сложить и вычесть:

$$a \equiv b(\mathrm{mod}\ m), \quad c \equiv d(\mathrm{mod}\ m) \Rightarrow$$
$$a + c \equiv b + d(\mathrm{mod}\ m), \quad a - c \equiv b - d(\mathrm{mod}\ m).$$

Доказательство. По определению сравнений получаем, что $m|(a-b), m|(c-d) \Rightarrow$ по свойствам делимости $m|(a-b)\pm(c-d)$, т. е. $m|\,[(a \pm c) - (b \pm d)]$. Возвращаясь к определению сравнения, получаем $a \pm c \equiv b \pm d (\mathrm{mod}\ m)$.

2. Сравнения по общему модулю можно почленно перемножить:

$$a \equiv b(\mathrm{mod}\ m),\quad c \equiv d(\mathrm{mod}\ m)\ \Rightarrow\ ac \equiv bd(\mathrm{mod}\ m).$$

Доказательство.

$$\begin{array}{c} m|(a-b) \\ m(c-d) \end{array} \Rightarrow \begin{array}{c} m|(a-b)*c \\ m(c-d)*b \end{array} \quad \Rightarrow$$

$$m|\,[ac - bc + cb - db] \Rightarrow m|(ac - db) \Rightarrow ac \equiv bd(\mathrm{mod}\ m).$$

3. К обеим частям сравнения можно прибавить (вычесть) одно и тоже число:

$$a \equiv b(\mathrm{mod}\ m),\quad \text{то}\quad \forall c\colon a \pm c \equiv b \pm c(\mathrm{mod}\ m).$$

4. Обе части сравнения можно умножить на любое число:

$$a \equiv b(\mathrm{mod}\ m),\quad \text{то}\quad \forall c\colon ac \equiv bc(\mathrm{mod}\ m).$$

5. Обе части сравнения можно сократить на одно и тоже число, взаимно простое с mod m:

$$a \equiv b(\mathrm{mod}\ m),\ d|a,\ d|b,\ (d,m) = 1\ \Rightarrow\ \frac{a}{d} = \frac{d}{b}(\mathrm{mod}\ m).$$

Пример 27. $8 \equiv 6(\mathrm{mod}\ 2)$, но $4 \neq 3(\mathrm{mod}\ 2)$.

6. Обе части сравнения можно возводить в одну и туже степень:

$$a \equiv b(\mathrm{mod}\ m)\ \Rightarrow\ \forall n \in N,\ a^n \equiv b^n(\mathrm{mod}\ m).$$

7. Обе части сравнения и модуль можно сократить на одно и тоже число:

$$a \equiv b(\mathrm{mod}\ m),\ d|a,\ d|b,\ d|m\ \Rightarrow\ \frac{a}{d} = \frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right).$$

8. Если $a \equiv b(\mathrm{mod}\ m_1)$, $a \equiv b(\mathrm{mod}\ m_2)$, то $a \equiv b\,(\mathrm{mod}\ [m_1, m_2])$.

9. Если $a \equiv b(\mathrm{mod}\ m)$, $d|m$, то $a \equiv b(\mathrm{mod}\ d)$.

Свойства 3–9 докажите самостоятельно.

10. Если $a \equiv b(\mathrm{mod}\ m)$, то $\mathrm{НОД}(a, m) = \mathrm{НОД}(b, m)$.

Доказательство. $\mathrm{НОД}(a, m) = d$. По определению НОД $d|a$, $d|m \Rightarrow a = d \cdot k$, $m = d \cdot n$, но $a \equiv b(\mathrm{mod}\ m) \Rightarrow a - b|m$, т. е. $a - b = m - q$. Заменим $dk - b = d \cdot n \cdot q$, или $d(k - nq) = b \Rightarrow d|b, d|m \Rightarrow d|\mathrm{НОД}(b, m)$, и наоборот.

Пример 28. Докажите, что число вида $3m+2$ (при целом m) не является полным квадратом.

Доказательство. Проведем от противного.

Пусть $3m + 2 = n^2$ при некотором натуральном n. Рассмотрим остатки от деления n на 3: $n \equiv 0(\mathrm{mod}\ 3)$, или $n \equiv 1(\mathrm{mod}\ 3)$, или $n \equiv 2(\mathrm{mod}\ 3)$. Тогда, соответственно, $n^2 \equiv 0(\mathrm{mod}\ 3)$, или $n^2 \equiv 1(\mathrm{mod}\ 3)$, или $n^2 \equiv 4(\mathrm{mod}\ 3) \equiv 1(\mathrm{mod}\ 3)$. Но по условию $n^2 = 3m + 2 \equiv 2(\mathrm{mod}\ 3)$ — противоречие.

Утверждение. *Отношение сравнимости по модулю m на множестве целых чисел является отношением эквивалентности и разбивает множество Z на классы эквивалентных элементов, которые обозначаются $\overline{1}, \overline{2}, \overline{3}, \overline{4}, \ldots, \overline{m-1}$. Множество всех классов эквивалентности по модулю m обозначаются Z_m.*

Попытайтесь доказать это утверждение самостоятельно.

Пример 29. $Z_6 = \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}$.

2.1.1. Классы вычетов

Бинарным отношением эквивалентности называется такое бинарное отношение на множестве M, что для любых $x, y, z \in M$:

1. $x \sim x$ — рефлексивность;
2. Если $x \sim y$, то $y \sim x$ — симметричность;
3. Если $x \sim y$, $y \sim z$, то $x \sim z$ — транзитивность.

Пример 30. $M = Z$ бинарное отношение: $x \sim y \Leftrightarrow x - y \in Z$. Это отношение — отношение эквивалентности.

Множество всех элементов множества M, эквивалентных элементу a, называется *классом эквивалентности*:

$$c_a = \{x \in M | x \sim a\}.$$

Пример 31. $M = Z$, $x \sim y \Leftrightarrow x + y \in$ чётным числам,тогда

$$c_2 = \{\text{все чётные}\}, \quad c_3 = \{\text{все нечётные}\}.$$

Теорема. *Отношение сравнимости является отношением эквивалентности, т. е. для любых* $a, b, c \in \mathbb{Z}$

1. $a \equiv a (\mathrm{mod}\ m)$;
2. *Если* $a \equiv b (\mathrm{mod}\ m)$, *то* $b \equiv a (\mathrm{mod}\ m)$;
3. *Если* $a \equiv b (\mathrm{mod}\ m)$, $b \equiv c (\mathrm{mod}\ m)$, *то* $a \equiv c (\mathrm{mod}\ m)$.

Доказательство.

1. $m|(a - a)$;
2. $m|(a - b)$, то $b - a = -(a - b)$ кратно m;
3. $m|(a - b)$, $m|(b - c)$, то $m|\big[(a - b) + (b - c)\big] = a - c$.

$\overline{a} = \{x \in Z,\ x \equiv a (\mathrm{mod}\ m)\}$ — класс вычетов по $\mathrm{mod}\ m$, а любое число $\in \overline{a}$ называется *вычетом*.

Пример 32. Что есть класс $\overline{5} \bmod 8$ — ?
$\overline{5} = \{5, 13, -3, \ldots\} = \{8k + 5\}$.
По mod 8 существует 8 различных классов
$\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$.

Теорема.

1. *Существует точно m классов вычетов по* mod m*;*
2. *Никакие* 2 *класса вычетов по* mod m *не пересекаются;*
3. *Объединение всех классов вычетов по* mod m *дает все множество Z.*

Доказательство.

1. Существует ровно m различных остатков от деления на m.
2. Одно число не может давать 2 различных остатка при делении на m.
3. Любое целое число лежит в одном из классов.

Обозначим Z_m — множество классов вычетов по модулю m называется *кольцом классов вычетов* mod m.

Пример 33. $Z_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Если от каждого класса вычетов по mod m взять по одному представителю, то мы получим *полную систему вычетов.*

Пример 34.

1) $0, 1, 2, 3, 4$ — полная система вычетов по mod 5;
2) $5, 1, 2, -2, 4$ — полная система вычетов по mod 5;
3) $5, 1, 2, 4, 9,\ 5, 1, 2, 4$ — не полная система вычетов по mod 5.

Если в полной системе вычетов взяты все вычеты, взаимнопростые с модулем, то система называется *приведенной.*

Теорема. 1) *Любые* $\varphi(m)$ *чисел, попарно не сравнимые по модулю* m *и взаимно простые с модулем, образуют приведенную систему вычетов по модулю* m. 2) *Если* НОД$(a, m) = 1$ *и* x *пробегает приведенную систему вычетов по модулю* m, *то* ax *так же пробегает приведенную систему вычетов по модулю* m.

Доказательство. Утверждение 1) — очевидно. Докажем утверждение 2). Числа ax попарно несравнимы и их ровно $\varphi(m)$ штук. Все они взаимно просты с модулем, т.к. НОД$(x, m) = 1$, НОД$(a, m) = 1$, следовательно НОД$(ax, m) = 1$. Значит, числа ax образуют приведенную систему вычетов.

Пример 35.
1) $1, 2, 3, 4$ — приведенная система вычетов по mod 5.
2) $1, 5$ — приведенная система вычетов по mod 6.
Элемент $a \in A$ называется *обратимым*, если существует

$$b \in A\colon a \cdot b = 1.$$

Пример 36. $5 \in Z_8$ — обратим?
$5 \cdot b \equiv 1 (\mathrm{mod}\ 8)$, $b = 5$, тогда $25 \equiv 1 (\mathrm{mod}\ 7)$, следовательно 5 — обратим.

Теорема (Эйлера). *Пусть* $m > 1$, НОД$(a, m) = 1$, $\varphi(m)$ — *функция Эйлера. Тогда:*

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

Доказательство. Пусть x пробегает приведенную систему вычетов по mod m: $x = r_1, r_2, \ldots, r_c$, где $c = \varphi(m)$ их число, $r_1, r_2, \ldots, r_c$ — наименьшие неотрицательные вычеты по mod m. Следовательно, наименьшие неотрицательные вычеты, соответствующие числам $a \cdot x$ суть соответственно: $\rho_1, \rho_2, \ldots, \rho_c$ тоже пробегают приведенную систему вычетов, но в другом порядке.

Тогда:

$$a \cdot r_1 \equiv \rho_1 (\mathrm{mod}\ m)$$
$$a \cdot r_2 \equiv \rho_2 (\mathrm{mod}\ m)$$
$$\dots$$
$$a \cdot r_c \equiv \rho_c (\mathrm{mod}\ m).$$

Перемножим эти c штук сравнений. Получится:

$$a^c \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_c \equiv \rho_1 \cdot \rho_2 \cdot \ldots \cdot \rho_c (\mathrm{mod}\ m).$$

Так как $r_1 \cdot r_2 \cdot \ldots \cdot r_c = \rho_1 \cdot \rho_2 \cdot \ldots \cdot \rho_c \neq 0$ и *взаимно просто с модулем* m, то, поделив последнее сравнение на $r_1 \cdot r_2 \cdot \ldots \cdot r_c$, получим $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m)$.

Следующая теорема — теорема Ферма — является непосредственным следствием теоремы Эйлера.

Теорема (Ферма). *Пусть p — простое число, p не делит a. Тогда:*

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p).$$

Доказательство. Положим в условии теоремы Эйлера $m = p$, тогда $\varphi(m) = p - 1$. Получаем $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

Необходимо отметить важность условия взаимной простоты модуля и числа a в формулировках теорем Эйлера и Ферма. Простой пример: сравнение $6^2 \equiv 1 \mathrm{mod}\ 3$ очевидно не выполняется. Однако можно легко подправить формулировку теоремы Ферма, чтобы снять ограничение взаимной простоты.

Следствие. *Без всяких ограничений на $a \in Z$,*

$$a^p \equiv a (\mathrm{mod}\ p).$$

Доказательство. Умножим обе части сравнения

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p)$$

на a. Ясно, что получится сравнение, справедливое и при a, кратном p.

Применение сравнений рассмотрим на примерах.

Пример 37. Найти остаток от деления 2^{1037} на 19.

Решение. При нахождении остатка от деления 2^{1037} на 19, воспользуемся теоремой Эйлера. Так как НОД$(2, 19) = 1$, то

$2^{\varphi(19)} \equiv 1(\text{mod } 19)$,

$2^{18} \equiv 1(\text{mod } 19)$.

$1037 \equiv 11(\text{mod } 18)$, то

$1037 = 18 \cdot k + 11$, где k — целое число.

Имеем

$2^{1037} \equiv 2^{18 \cdot k+11}(\text{mod } 19) \equiv 2^{18 \cdot k} \cdot 2^{11}(\text{mod } 19) \equiv$

$\equiv (2^{18})k \cdot 2^{11}(\text{mod } 19) \equiv 1^k \cdot 2^{11}(\text{mod } 19) \equiv$

$\equiv 2048(\text{mod } 19) \equiv 15(\text{mod } 19)$.

Ответ. Остаток равен 15.

Пример 38. Доказать, что при любом натуральном n число $37^{n+2} + 16^{n+1} + 23^n$ делится на 7.

Решение. Очевидно, что

$37 \equiv 2(\text{mod } 7)$, $16 \equiv 2(\text{mod } 7)$, $23 \equiv 2(\text{mod } 7)$.

Возведем первое сравнение в степень $n + 2$, второе — в степень $n + 1$, третье — в степень n и сложим:

$$\begin{aligned} &37^{n+2} \equiv 2^{n+2}(\text{mod } 7) \\ &16^{n+1} \equiv 2^{n+1}(\text{mod } 7) \qquad + \\ &23^n \equiv 2^n(\text{mod } 7) \\ &\overline{\qquad\qquad\qquad\qquad\qquad\qquad} \\ &37^{n+2} + 16^{n+1} + 23^n \equiv 2^n \cdot 7(\text{mod } 7), \end{aligned}$$

т. е. $37^{n+2} + 16^{n+1} + 23^n$ делится на 7.

2.2. Решение сравнений первой степени

Говорят, что $x \equiv x_0(\text{mod } m)$ является *решением сравнения*

$$a \cdot x \equiv b(\text{mod } m),$$

если верно $a \cdot x_0 \equiv b(\text{mod } m)$.

Теорема. *Сравнение*

$$a \cdot x \equiv 1(\text{mod } m)$$

разрешимо тогда и только тогда, когда НОД$(a, m) = 1$. *Если сравнение разрешимо, то оно имеет единственное решение по модулю* m.

Попытайтесь доказать эту теорему самостоятельно.

Способы решений сравнений рассмотрим на примерах.

Пример 39. Решить сравнение по определению:

a) $8x \equiv 11(\text{mod } 14)$; b) $3x \equiv 5(\text{mod } 7)$.

Решение.

a) Задано $8x \equiv 11(\text{mod } 14)$, по определению сравнения получаем $14|(8x - 11)$, но $(8x - 11)$ число нечетное при любом x. Значит, 14 не может делить $(8x - 11)$. Следовательно, сравнение не разрешимо.

b) Задано $3x \equiv 5(\text{mod } 7)$, по определению имеем: $7|(3x - 5)$, т. е. $3x - 5 = 7k$, где k — целое число.

Выразим $x = \dfrac{5 + 7k}{3} = 1 + 2k + \dfrac{2 + k}{3}$, x — целое число, значит $(2 + k)$ должно делится на 3. Возьмем в качестве $k = 1$, тогда $x = \dfrac{5 + 7}{3} = 4$. НОД$(3, 7) = 1$, то система имеет единственное решение по модулю 7.

Ответ. a) решения нет; b) $x \equiv 4(\text{mod } 7)$.

Пример 40. Решить сравнение, используя линейное представление НОД: $3x \equiv 5(\text{mod } 7)$.

Решение. Задано $3x \equiv 5(\text{mod } 7)$, НОД$(3, 7) = 1$, то система имеет единственное решение по модулю 7.

Найдем линейное представление НОД$(3, 7) = 1$.

$7 = 3 \cdot 2 + 1$;

$3 = 1 \cdot 3$.

Линейное представление НОД:

$1 = 7 + 3 \cdot (-2)$, тогда $3 \cdot (-2) \equiv 1(\text{mod } 7)$;

умножая на 5 обе части сравнения, получаем
$3 \cdot \big((-2) \cdot 5\big) \equiv 5 (\mathrm{mod}\ 7)$, тогда
$x \equiv (-2) \cdot 5 (\mathrm{mod}\ 7) \equiv -10 (\mathrm{mod}\ 7) \equiv 4 (\mathrm{mod}\ 7)$.

Ответ. $x \equiv 4 (\mathrm{mod}\ 7)$.

Пример 41. Решить сравнение, используя теорему Эйлера: $3x \equiv 5 (\mathrm{mod}\ 7)$.

Решение. НОД$(3, 7) = 1$, то система имеет единственное решение по модулю 7.

Для нашего сравнения имеем: НОД$(3, 7) = 1$, значит, теорема выполняется:
$x \equiv 3^{\varphi(7)-1} \cdot 5 (\mathrm{mod}\ 7) \equiv 3^{6-1} \cdot 5 (\mathrm{mod}\ 7) \equiv 3^5 \cdot 5 (\mathrm{mod}\ 7) \equiv$
$\equiv 9 \cdot 9 \cdot 3 \cdot 5 (\mathrm{mod}\ 7) \equiv 2 \cdot 2 \cdot 3 \cdot 5 (\mathrm{mod}\ 7) \equiv 12 \cdot 5 (\mathrm{mod}\ 7)$,
$x \equiv 5 \cdot 5 (\mathrm{mod}\ 7) \equiv 25 (\mathrm{mod}\ 7) \equiv 4 (\mathrm{mod}\ 7)$.
Ответ. $x \equiv 4 (\mathrm{mod}\ 7)$.

Пример 42. Решить сравнение $8x \equiv 12 (\mathrm{mod}\ 14)$ (случай не единственности решения).

Решение. $8x \equiv 12 (\mathrm{mod}\ 14)$. По свойствам сравнений разделим все три части сравнения на 2. Получим $4x \equiv 6 (\mathrm{mod}\ 7)$.

Упростим сравнение: $2x \equiv 3 (\mathrm{mod}\ 7)$. Решим любым способом (например подбором): $x \equiv 5 (\mathrm{mod}\ 7)$. Так как НОД$(2, 7) = 1$, то решение единственно по mod 7. Теперь найдем решение по модулю 14: положим $x = 5 + 7t$, где t — целое число, тогда при $t = 0$, $x_1 \equiv 5 (\mathrm{mod}\ 14)$, при $t = 1$, $x_2 \equiv 5 + 7 (\mathrm{mod}\ 14) \equiv 12 (\mathrm{mod}\ 14)$.

При больших t получаем $5 + 7t > 14$, т. е. решения повторяются.

Ответ. $x_1 \equiv 5 (\mathrm{mod}\ 14)$, $x_2 \equiv 12 (\mathrm{mod}\ 14)$.

Теорема. *Если* $ax \equiv b (\mathrm{mod}\ m)$, *то*

$$x \equiv (-1)^{n-1} \cdot P_{n-1} \cdot b (\mathrm{mod}\ m),$$

где $\frac{m}{a} = \frac{P_n}{Q_n}$ — *n-ая подходящая дробь.*

Доказательство. Разлагая в непрерывную дробь отношение $m : a$,

$$\frac{m}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_n}}}.$$

и рассматривая две последние подходящие дроби:

$$\frac{P_{n-1}}{Q_{n-1}}, \quad \frac{P_n}{Q_n} = \frac{m}{a},$$

согласно свойствам непрерывных дробей имеем

$$mQ_{n-1} - aP_{n-1} = (-1)^n,$$
$$aP_{n-1} \equiv (-1)^{n-1} (\mathrm{mod}\ m),$$
$$a \cdot (-1)^{n-1} P_{n-1} b \equiv b (\mathrm{mod}\ m).$$

Итак, наше сравнение имеет решение

$$x \equiv (-1)^{n-1} P_{n-1} b (\mathrm{mod}\ m),$$

для разыскания которого достаточно вычислить P_{n-1}.

Пример 43. Решить сравнение $11x \equiv -192 (\mathrm{mod}\ 401)$, используя подходящие дроби.

Решение. Найдем необходимые P_n, Q_n.

$401 = 11 \cdot 36 + 5$;

$11 = 5 \cdot 2 + 1$;

$5 = 1 \cdot 5$.

Значит $n = 3$, $q_1 = 36$, $q_2 = 2$, $q_3 = 5$; $P_0 = 1$, $P_1 = 36$, $P_2 = 2 \cdot 36 + 1 = 73$. Тогда

$x \equiv (-1)^2 \cdot 73 \cdot (-192) (\mathrm{mod}\ 401) \equiv -382 (\mathrm{mod}\ 401) \equiv 19 (\mathrm{mod}\ 401)$. ∎

Ответ. $x \equiv 19 (\mathrm{mod}\ 401)$.

Сравнения можно так же применять в решении диофантовых уравнений.

Пример 44. Решить уравнение $47x - 111y = 89$.

Решение. Условие уравнения можно переписать в следующем виде: $47 \equiv 89 (\mathrm{mod}\ 111)$.

Решим сравнение любым способом $x \equiv 94 (\mathrm{mod}\ 111)$, тогда $x = 94 + 111 \cdot t$. Подставим в уравнение:

$94 \cdot 47 + 111 \cdot t \cdot 47 - 111 \cdot y = 89$,

$111 \cdot t - 111 \cdot y = -111 \cdot 39$,

$y = 39 + 47 \cdot t$.

Ответ. $x = 94 + 111 \cdot t$, $y = 39 + 47 \cdot t$, где $t = Z$.

2.3. Системы сравнений

Теорема (китайская теорема об остатках). *Для натуральных чисел m_1 и m_2 таких что* НОД$(m_1, m_2) = 1$ *система сравнений*

$$\begin{cases} x \equiv a (\mathrm{mod}\ m_1) \\ x \equiv b (\mathrm{mod}\ m_2) \end{cases}$$

разрешима и имеет единственное решение по модулю $(m_1 \cdot m_2)$.

Доказательство. По условию НОД$(m_1, m_2) = 1$. Значит, существует линейное представление с целыми u и v такими, что $m_1 \cdot u + m_2 \cdot v = 1$. Рассмотрим $x = b \cdot m_1 \cdot u + a \cdot m_2 \cdot v$. Легко увидеть, что $x \equiv a (\mathrm{mod}\ m_1)$ и $x \equiv b (\mathrm{mod}\ m_2)$. Таким образом, решение системы существует. Пусть найдется другое решение $x = x_0$ этой системы: $x_0 \equiv a (\mathrm{mod}\ m_1)$ и $x_0 \equiv b (\mathrm{mod}\ m_2)$.

Тогда $x - x_0 \equiv 0 (\mathrm{mod}\ m_1)$ и $x - x_0 \equiv 0 (\mathrm{mod}\ m_2)$, следовательно $m_1 | x - x_0$, $m_2 | x - x_0$. При условии НОД$(m_1, m_2) = 1$, $m_1 \cdot m_2 | x - x_0$, значит $x_0 \equiv x (\mathrm{mod}\ m_1 \cdot m_2)$.

Теорема. *В условиях теоремы, решением системы является $x \equiv b \cdot m_1 \cdot u + a \cdot m_2 \cdot v (\mathrm{mod}\ m_1 \cdot m_2)$, где $m_1 \cdot u + m_2 \cdot v = 1$ — линейное представление* НОД$(m_1, m_2) = 1$.

Пример 45. Решить систему сравнений $\begin{cases} x \equiv 2(\mathrm{mod}\ 5) \\ x \equiv 8(\mathrm{mod}\ 11) \end{cases}$ любым способом.

Решение. Из первого сравнения системы получаем, что $x = 2 + 5t$, где $t = Z$.

Подставим во второе сравнение системы $2 + 5t \equiv 8(\mathrm{mod}\ 11)$. Решим его: $5t \equiv 6(\mathrm{mod}\ 11) \equiv -5(\mathrm{mod}\ 11)$, $t \equiv 10(\mathrm{mod}\ 11)$ или $t = 10 + 11k$, тогда $x = 2 + 5 \cdot (10 + 11k) = 52 + 55k$.

Ответ. $x \equiv 52(\mathrm{mod}\ 55)$.

Пример 46. Решить систему сравнений:

$$a)\ \begin{cases} x \equiv 2(\mathrm{mod}\ 5), \\ x \equiv 8(\mathrm{mod}\ 11); \end{cases} \qquad b)\ \begin{cases} 4x \equiv 3(\mathrm{mod}\ 15), \\ 3x \equiv 1(\mathrm{mod}\ 10). \end{cases}$$

Решение.

а) Рассмотрим систему $\begin{cases} x \equiv 2(\mathrm{mod}\ 5), \\ x \equiv 8(\mathrm{mod}\ 11). \end{cases}$

Модули обладают свойством НОД$(5, 11) = 1$, то решить систему можно по следствию китайской теоремы об остатках. Для этого найдем линейное представление НОД$(5, 11)$:

$1 = 5 \cdot (-2) + 11 \cdot 1$. Тогда по известным формулам имеем

$x = 2 \cdot (11 \cdot 1) + 8 \cdot (5 \cdot (-2))$, или

$x = 22 - 80 = -58$; $x \equiv -58(\mathrm{mod}\ 55) \equiv 52(\mathrm{mod}\ 55)$.

b) $\begin{cases} 4x \equiv 3(\mathrm{mod}\ 15), \\ 3x \equiv 1(\mathrm{mod}\ 10). \end{cases}$

Решим независимо каждое сравнение любым способом:

$$\begin{cases} x \equiv 12(\mathrm{mod}\ 15), \\ x \equiv 7(\mathrm{mod}\ 10). \end{cases}$$

Так как модули не взаимно простые, то решение находим по модулю НОК$[10, 15] = 30$. Из первого сравнения получаем:

$x = 12 + 15 \cdot k$, подставим во второе сравнение системы

$12 + 15 \cdot k \equiv (\mathrm{mod}\ 10)$; упростим
$15 \cdot k \equiv (\mathrm{mod}\ 10)$; $3k \equiv -1(\mathrm{mod}\ 2)$; $k \equiv 1(\mathrm{mod}\ 2)$, тогда
$k = 1 + 2n$, где n — целое число;
подставим k в формулу для x:
$x = 12 + 15 \cdot (1 + 2n) = 27 + 30n \equiv 27(\mathrm{mod}\ 30)$.

Ответ. a) $x \equiv 52(\mathrm{mod}\ 55)$; b) $x \equiv 27(\mathrm{mod}\ 30)$.

Пример 47. Решите систему сравнений:

$$\begin{cases} 3x + 4y \equiv 29(\mathrm{mod}\ 143), \\ 2x - 9y \equiv -847(\mathrm{mod}\ 143). \end{cases}$$

Решение. Решение основывается на свойствах сравнений.

Обратим внимание на то, что число 143 — простое. Умножим первое сравнение на 9, а второе на 4 и сложим их. Умножим первое сравнение на 2, а второе на (-3) и сложим их. Получим систему сравнений с двумя переменными:

$$\begin{cases} 35x \equiv -75(\mathrm{mod}\ 143), \\ 35y \equiv 310(\mathrm{mod}\ 143). \end{cases}$$

Решаем каждое сравнение по отдельности:

$$\begin{cases} 7x \equiv -15(\mathrm{mod}\ 143) \\ 35y \equiv 310(\mathrm{mod}\ 143) \end{cases}, \ldots, \quad \begin{cases} x \equiv 100(\mathrm{mod}\ 143) \\ y \equiv 111(\mathrm{mod}\ 143). \end{cases}$$

Ответ. $x \equiv 100(\mathrm{mod}\ 143)$, $y \equiv 111(\mathrm{mod}\ 143)$.

Задачи для самостоятельного решения

1. Найти остаток от деления:
   a) 2^{1050} на 17; b) 5^{1995} на 9; c) 7^{1018} на 19.
2. Найти остаток от деления:
   a) $(125^{91} + 21)^{50}$ на 18; b) 6^{8^7} на 11; c) $50^{50^{50}}$ на 63.

3. Решить сравнение по определению:
   a) $6x \equiv 11 (\mathrm{mod}\ 16)$; b) $2x \equiv 3 (\mathrm{mod}\ 5)$; c) $3x \equiv 2 (\mathrm{mod}\ 7)$.

4. Решить сравнение, используя линейное представление НОД:
   a) $2x \equiv 3 (\mathrm{mod}\ 11)$; b) $17x \equiv 7 (\mathrm{mod}\ 19)$; c) $5x \equiv 4 (\mathrm{mod}\ 6)$.

5. Решить сравнение, используя теорему Эйлера:
   a) $3x \equiv 7 (\mathrm{mod}\ 11)$; b) $4x \equiv 3 (\mathrm{mod}\ 7)$; c) $4x \equiv 3 (\mathrm{mod}\ 5)$.

6. Решить сравнение, используя подходящие дроби:
   a) $3x \equiv -151 (\mathrm{mod}\ 907)$; b) $3x \equiv -193 (\mathrm{mod}\ 401)$;
   c) $5x \equiv -192 (\mathrm{mod}\ 907)$.

7. Решить сравнение (случай не единственности решения):
   a) $6x \equiv 12 (\mathrm{mod}\ 16)$; b) $12x \equiv 18 (\mathrm{mod}\ 21)$; c) $9x \equiv 15 (\mathrm{mod}\ 24)$.

8. Решите в натуральных числах уравнение:
   a) $x^2 - y^2 = 31$; b) $x^2 - y^2 = 303$.

9. Докажите, что число вида $5m+2$ (при целом m) не является полным квадратом.

10. Каково наименьшее натуральное n, такое, что $n!$ делится на 990?

11. Натуральные числа x, y, z таковы, что $x^2 + y^2 = z^2$. Докажите, что хотя бы одно из этих чисел делится на 3.

12. Докажите, что ни одно из чисел вида 10^{3n+1} нельзя представить в виде суммы двух кубов натуральных чисел.

13. Может ли $n!$ оканчиваться ровно на 5 нулей?

14. Решить систему сравнений:

a) $\begin{cases} x \equiv 6 (\mathrm{mod}\ 7), \\ x \equiv 2 (\mathrm{mod}\ 5); \end{cases}$

b) $\begin{cases} x \equiv 2 (\mathrm{mod}\ 9), \\ x \equiv 5 (\mathrm{mod}\ 11); \end{cases}$

c) $\begin{cases} x \equiv 2 (\mathrm{mod}\ 7), \\ x \equiv 3 (\mathrm{mod}\ 5). \end{cases}$

15. Решить систему сравнений:

a) $\begin{cases} 4x \equiv 3 (\mathrm{mod}\ 25), \\ 7x \equiv 1 (\mathrm{mod}\ 10); \end{cases}$

b) $\begin{cases} 2x \equiv 14 (\mathrm{mod}\ 15), \\ 5x \equiv 1 (\mathrm{mod}\ 21); \end{cases}$

c) $\begin{cases} 4x \equiv 1 (\mathrm{mod}\ 10), \\ 3x \equiv 5 (\mathrm{mod}\ 8). \end{cases}$

16. Решите систему сравнений с двумя переменными:

a) $\begin{cases} 3x + 5y \equiv 2 (\mathrm{mod}\ 7), \\ 4x \equiv 1 (\mathrm{mod}\ 7); \end{cases}$

b) $\begin{cases} x + 3y \equiv 3 (\mathrm{mod}\ 5), \\ 3x + 2y \equiv 2 (\mathrm{mod}\ 5); \end{cases}$

c) $\begin{cases} 9x + 3y \equiv -3 (\mathrm{mod}\ 12), \\ 2x + 2y \equiv 10 (\mathrm{mod}\ 12). \end{cases}$

Глава 3

Сравнение степеней $n \geqslant 2$

3.1. Сравнения по mod p^m

Пусть p — простое число, $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ — многочлен с целыми коэффициентами. Рассмотрим сравнения вида $f(x) \equiv 0(\text{mod } p)$ и $f(x) \equiv 0(\text{mod } p^m)$.

Теорема 1. *Сравнение $f(x) \equiv 0(\text{mod } p)$ имеет более чем n решений (где n — степень многочлена $f(x)$) тогда и только тогда, когда все коэффициенты многочлена $f(x)$ кратны p.*

Доказательство. Пусть сравнение $f(x) \equiv 0(\text{mod } p)$ имеет более чем n решений. Это означает, что многочлен $f(x)$ имеет в поле $\mathbb{Z}_p$ более чем n корней, что возможно только при условии, что $f(x) \equiv 0$ в $\mathbb{Z}_p$, т. е. коэффициенты $f(x)$ кратны p.

Обратно, если коэффициенты $f(x)$ кратны p, то $f(x) \equiv 0$ в $\mathbb{Z}_p$, следовательно $f(x) \equiv 0(\text{mod } p)$ для любого $x \in \mathbb{Z}_p$. Доказательство завершено.

Пример 48. Решите сравнение

$$x^3 - 6x^2 - 12x - 6 \equiv 0(\text{mod } 23).$$

Решение. Так как 23 — простое число, то многочлен $f(x)$ имеет не более трех корней в $\mathbb{Z}_{23}$, так как его коэффициенты не кратны 23. Легко подбором находим три решения сравнения $f(x) \equiv 0(\text{mod } 23)$.

Ответ. $x_1 = \overline{1}$, $x_2 = \overline{2}$, $x_3 = \overline{3}$ по mod 23.

Следствие (теорема Вильсона).

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) + 1 \equiv 0 (\mathrm{mod}\ p).$$

Доказательство. Наше сравнение можно записать в более лаконичной форме, а именно

$$(p-1)! \equiv -1 (\mathrm{mod}\ p).$$

Положим для начала $p = 2$. Тогда $(p-1)! = 1$, а значит верно $1 \equiv -1 (\mathrm{mod}\ 2)$.

Пусть теперь $p \neq 2$. Рассмотрим многочлен

$$f(x) = (x-1) \cdot (x-2) \cdot (x-3) \cdot \ldots \cdot \big(x - (p-1)\big) - (x^{p-1} - 1).$$

Степень этого многочлена не превосходит $p-2$. При этом по теореме Ферма $x^{p-1} \equiv 1 (\mathrm{mod}\ p)$. Значит, сравнение $f(x) \equiv 0 (\mathrm{mod}\ p)$ имеет корни $x = 1, 2, 3, \ldots, (p-1) (\mathrm{mod}\ p)$. По теореме 1 все коэффициенты $f(x)$ кратны p. Найдем свободный коэффициент $f(x)$ (т. е. найдем $f(0)$):

$$(-1)^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) + 1 = (p-1)! + 1 \equiv 0 (\mathrm{mod}\ p).$$

Доказательство завершено.

Теорема. *Пусть* $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n \in Z[x]$, $p > 1$ — *простое. Если сравнения*

$$f(x) \equiv 0 (\mathrm{mod}\ p), \quad f'(x) \equiv 0 (\mathrm{mod}\ p)$$

не имеют общих решений, тогда функция $f(x) \equiv 0 (\mathrm{mod}\ p)$ *и* $f(x) \equiv 0 (\mathrm{mod}\ p^m)$ *для любых* $m \geqslant 1$ *имеют одинаковое число решений.*

Доказательство проведем по индукции для степени m.

1. Если $m = 1$, $f(x) \equiv 0 (\mathrm{mod}\ p)$ и $f(x) \equiv 0 (\mathrm{mod}\ p)$ — имеют одинаковое число решений.

2. Пусть $f(x) \equiv 0(\mathrm{mod}\ p^m)$ и $f(x) \equiv 0(\mathrm{mod}\ p)$ — имеют одинаковое число решений.

3. Рассмотрим $f(x) \equiv 0(\mathrm{mod}\ p^{m+1})$.

Пусть $x \equiv x_0(\mathrm{mod}\ p^m)$ — решение сравнения

$$f(x) \equiv 0(\mathrm{mod}\ p^m).$$

Докажем, что x_0 индуцирует решение сравнения

$$f(x) \equiv 0(\mathrm{mod}\ p^{m+1}).$$

Формула Тейлора для $f(x)$ в окрестности точки x_0:

$$f(x) = f(x_0) + \frac{f'(x_0)}{1!}(x - x_0) + \frac{f''(x_0)}{2!}(x - x_0)^2 + \ldots + \\ + \frac{f(n)(x_0)}{n!}(x - x_0)^n + \ldots$$

Так как $x \equiv x_0(\mathrm{mod}\ p^n)$, то $x = x_0 + t \cdot p^m$, следовательно, $x - x_0 = t \cdot p^m$, значит,

$$f(x) = f(x_0) + \frac{f'(x_0)}{1!}tp^m + \frac{f''(x_0)}{2!}t^2p^{2m} + \ldots + \frac{f(n)(x_0)}{n!}t^np^{nm} + \ldots$$

Откуда

$$f(x) \equiv f(x_0) + f'(x_0)tp^m(\mathrm{mod}\ p^{m+1}),$$

$f(x) \equiv 0(\mathrm{mod}\ p^{m+1})$ — по условию задачи, следовательно

$$\frac{f(x_0)}{p^m} + f'(x_0)t \equiv 0(\mathrm{mod}\ p)$$

или

$$f'(x_0)t = -\frac{f(x_0)}{p^m} \equiv 0(\mathrm{mod}\ p). \qquad (*)$$

Так как $f(x_0) \equiv 0(\mathrm{mod}\ p^m)$, то

$$f(x_0) \equiv 0(\mathrm{mod}\ p), \quad f'(x_0) \not\equiv 0(\mathrm{mod}\ p),$$

в силу НОД$(f'(x_0), p) = 1$, следовательно сравнение $(*)$ относительно t имеет единственное решение $t \equiv t_0(\mathrm{mod}\ p)$, $t = t_0 + pt_1$, значит $x = x_0 + tp^m = x_0 + t_0p^m + t_1p^{m+1} \equiv x_0 + t_0p^m(\mathrm{mod}\ p^{m+1})$ — решение сравнения $f(x_0) \equiv 0(\mathrm{mod}\ p^{m+1})$. Доказательство завершено.

При решении задач получаем следующую схему действий.

Решить: $f(x) \equiv 0(\mathrm{mod}\ p^m)$.

Пусть $f(x) \equiv 0(\mathrm{mod}\ p)$ и $f'(x) \equiv 0(\mathrm{mod}\ p)$ — не имеют общего решения.

Тогда:

1) решить $f(x) \equiv 0(\mathrm{mod}\ p)$, следовательно, $x \equiv x_0(\mathrm{mod}\ p^m)$ — решение, тогда рассмотрим $f'(x_0)t \equiv -\dfrac{f(x_0)}{p}(\mathrm{mod}\ p)$, получим $t \equiv t_0(\mathrm{mod}\ p)$, следовательно $x \equiv x_0 + t_0p(\mathrm{mod}\ p^2)$ — решение $f(x) \equiv 0(\mathrm{mod}\ p^2)$, $x_1 = x_0 + t_0p$.

2) Рассмотрим $f'(x_1)t \equiv -\dfrac{f(x_1)}{p^2}(\mathrm{mod}\ p)$, получим $t \equiv t_1(\mathrm{mod}\ p)$, следовательно $x \equiv x_1 + t_1p(\mathrm{mod}\ p^3)$ — решение, $x_2 = x_0 + t_0p + t_1p^2$, и т. д.

Пример 49. Решить $f(x) \equiv 0(\mathrm{mod}\ 27)$, если

$$f(x) = x^4 + 7x + 4.$$

Решение. Рассмотрим

$$\begin{array}{ll} f(x) \equiv 0(\mathrm{mod}\ 3) & f'(x) \equiv 0(\mathrm{mod}\ 27) \\ x^4 + 7x + 4 \equiv 0(\mathrm{mod}\ 3) & 4x^3 + 7 \equiv 0(\mathrm{mod}\ 3) \\ x^4 + x + 1 \equiv 0(\mathrm{mod}\ 3) & x^3 + 1 \equiv 0(\mathrm{mod}\ 3) \\ x_0 \equiv 1(\mathrm{mod}\ 3) & x \equiv 2(\mathrm{mod}\ 3). \end{array}$$

Рассмотрим $f'(x_0)t \equiv -\dfrac{f(x_0)}{p}(\mathrm{mod}\ p) \Leftrightarrow 11t \equiv -4(\mathrm{mod}\ 3)$

$2t \equiv 2(\mathrm{mod}\ 3)$
$t_0 \equiv 1(\mathrm{mod}\ 3)$
$t_0 = 1,\ x_1 = 1 + 1 \cdot 3 = 4(\mathrm{mod}\ 9)$
$t_0 \equiv 1(\mathrm{mod}\ 3)$
Рассмотрим $f'(x_1)t \equiv -\dfrac{f(x_1)}{p^2}(\mathrm{mod}\ p) \Leftrightarrow 263t \equiv -\dfrac{288}{9}(\mathrm{mod}\ 3)$
$2t \equiv -32(\mathrm{mod}\ 3) \equiv 1(\mathrm{mod}\ 3)$
$t \equiv 2(\mathrm{mod}\ 3)$
$t_1 = 2,\ x_2 = x_1 + t_1 p^2 = 4 + 2 \cdot 9 = 22(\mathrm{mod}\ 27)$
Ответ. $x \equiv 22(\mathrm{mod}\ 3)$ — решение.

Следствие. Пусть p — простое, a, n — целые, НОД$(p, a) = 1$, НОД$(p, n) = 1$. Тогда сравнения $x^n \equiv a(\mathrm{mod}\ p)$ и $x^n \equiv a(\mathrm{mod}\ p^m)$ имеют одинаковое число решений для любых $m \geqslant 1$.

Доказательство. Рассмотрим $f(x) = x^n - a$.
$f'(x) = nx^{n-1}$, $f'(x) \equiv 0(\mathrm{mod}\ p)$ тогда и только тогда, когда $nx^{n-1} \equiv 0(\mathrm{mod}\ p)$, НОД$(p, n) = 1$, $x^{n-1} \equiv 0(\mathrm{mod}\ p)$, следовательно, $x \equiv 0(\mathrm{mod}\ p)$ — единственное решение — не решение $f(x) \equiv 0(\mathrm{mod}\ p)$, т. к. НОД$(p, a) = 1$, тогда x_0 — решение $f(x) \equiv 0(\mathrm{mod}\ p)$, то x_0 — не решение $f'(x) \equiv 0(\mathrm{mod}\ p)$, и наоборот, следовательно, выполнена теорема.

Пример 50. Решить сравнение $x^2 \equiv -1(\mathrm{mod}\ 5^3)$.

Решение. Если $x^2 \equiv -1(\mathrm{mod}\ 5) \Leftrightarrow x^2 \equiv 4(\mathrm{mod}\ 5)$
$$x \equiv \pm 2(\mathrm{mod}\ 5) \equiv \begin{cases} 2(\mathrm{mod}\ 5) \\ 3(\mathrm{mod}\ 5), \end{cases}$$
следовательно 2 решения $(\mathrm{mod}\ 5^3)$, значит $x = 2 + 5t$.
$x^2 = 4 + 20t + 25t^2 \equiv -1(\mathrm{mod}\ 25)$,
$5 + 20t \equiv 0(\mathrm{mod}\ 25)$,
$20t \equiv 20(\mathrm{mod}\ 25)$,
$4t \equiv 4(\mathrm{mod}\ 5)$,
$t \equiv 1(\mathrm{mod}\ 25)$,
$t = 1 + 5k$, где $k \in Z$, тогда $x = 7 + 25k$,
$x^2 = 49 + 350k + 25^2 k^2 \equiv 49 + 350k(\mathrm{mod}\ 125) \equiv$

$\equiv 49 + 100k (\mathrm{mod}\ 125)$, так как $x^2 \equiv -1 (\mathrm{mod}\ 125)$, получаем
$49 + 100k \equiv -1 (\mathrm{mod}\ 125)$,
$100k \equiv -50 (\mathrm{mod}\ 125)$,
$4k \equiv -2 (\mathrm{mod}\ 5)$,
$2k \equiv -1 (\mathrm{mod}\ 5)$,
$2k \equiv 4 (\mathrm{mod}\ 5)$
или
$x \equiv 7 + 25k \equiv 7 + 50 (\mathrm{mod}\ 125)$, на основании этого получаем
$x_1 \equiv 57 (\mathrm{mod}\ 125)$,
$x_2 \equiv -57 (\mathrm{mod}\ 125) \equiv 68 (\mathrm{mod}\ 125)$.
Ответ. $x_1 \equiv 57 (\mathrm{mod}\ 125)$, $x_2 \equiv 68 (\mathrm{mod}\ 125)$.

Теорема. *Многочлен $f(x)$, $\deg f(x) = n$ имеет ровно n корней по* mod p *($p \geqslant n$), тогда и только тогда, когда многочлен $R(x)$ имеет все коэффициенты, кратные p, где*

$$x^p - x = f(x) \cdot Q(x) + R(x).$$

Доказательство. Разделим $x^p - 1$ на $f(x)$ с остатком:

$$x^p - x = f(x) \cdot Q(x) + R(x).$$

Пусть $f(x) \equiv 0 (\mathrm{mod}\ p)$ имеет n решений. $x^p \equiv x (\mathrm{mod}\ p)$ для всех $x \in Z_p$, следовательно для всех решений $f(x) \equiv 0 (\mathrm{mod}\ p)$ выполнено $x^p \equiv x (\mathrm{mod}\ p)$.

Пусть x_0 — решение сравнения $f(x) \equiv 0 (\mathrm{mod}\ p)$, тогда $x_0^p - x_0 \equiv 0 (\mathrm{mod}\ p)$, следовательно $R(x) \equiv 0 (\mathrm{mod}\ p)$ для всех x_0, т. е. имеет n решений, но $\deg R(x) < n$, т. е. по теореме 1 все коэффициенты $R(x)$ кратны p.

Обратно:

$x^p - x = f(x) \cdot Q(x) + R(x)$, $\quad \deg f(x) = n$, $\deg Q(x) = p - n$.

Пусть все коэффициенты $R(x)$ кратны p.

Тогда $f(x) \cdot Q(x) = x^p - x - R(x) \equiv 0 (\mathrm{mod}\ p)$ для всех $x \in Z_p$, следовательно $f(x) \cdot Q(x) = 0$ имеет p решений в $\mathbb{Z}_p$, значит $f(x)$ имеет ровно n корней, $Q(x)$ имеет ровно $p - n$ корней. Доказательство завершено.

Пример 51. Решить сравнение

$$f(x) = x^3 + 2x^2 + x + 1 \equiv 0(\mathrm{mod}\ 5).$$

Решение. Рассмотрим разложение

$$x^5 - x = f(x) \cdot (x^2 - 2x + 3) + (-5x^2 - 2x - 3).$$

Таким образом, $R(x) = -5x^2 - 2x - 3$, следовательно, не все коэффициенты кратны 5, значит $f(x)$ имеет $\leqslant 2$ решений.
$x = 1$ — решение, т. к. $f(x) = (x-1)(x^2 + 3x - 1) \equiv 0(\mathrm{mod}\ 5)$. Для сравнения $x^2 + 3x - 1 \equiv 0(\mathrm{mod}\ 5)$, $x \neq 2$, $x \neq 3$, $x \neq 4$, следовательно других решений нет.

Ответ. $x \equiv 1(\mathrm{mod}\ 5)$.

3.2. Сравнение любой степени по составному модулю

Обратимся теперь к решению сравнений по составному модулю.

Теорема. *Если $m_1, m_2, \ldots, m_k$ — попарно простые числа, то сравнение*

$$f(x) \equiv 0(\mathrm{mod}\ m_1 \cdot m_2 \cdot \ldots \cdot m_k)$$

равносильно системе

$$\begin{cases} f(x) \equiv 0(\mathrm{mod}\ m_1), \\ \vdots \\ f(x) \equiv 0(\mathrm{mod}\ m_k). \end{cases}$$

При этом, если $t_1, t_2, \ldots, t_k$ — число решения сравнения

$$f(x) \equiv (\mathrm{mod}\ m_i),$$

соответственно, то $t = t_1 \cdot t_2 \cdot \ldots \cdot t_k$ — число решений системы.

Доказательство. 1) Равносильность докажем последовательно в каждую сторону. Пусть $f(x) \equiv 0(\mathrm{mod}\ m_1 \cdot m_2 \cdot \ldots \cdot m_k)$, следовательно, по свойству сравнений, $f(x) \equiv 0(\mathrm{mod}\ m_i)$ для всех $i = \overline{1 \ldots k}$, что можно записать в виде системы

$$\begin{cases} f(x) \equiv 0(\mathrm{mod}\ m_1), \\ \vdots \\ f(x) \equiv 0(\mathrm{mod}\ m_k). \end{cases} \qquad (*)$$

Обратно, если выполняется $(*)$, то выполняется

$$\begin{cases} \begin{cases} f(x) \equiv 0(\mathrm{mod}\ m_1), \\ f(x) \equiv 0(\mathrm{mod}\ m_2), \end{cases} \\ f(x) \equiv 0(\mathrm{mod}\ m_3), \\ \vdots \\ f(x) \equiv 0(\mathrm{mod}\ m_k). \end{cases}$$

Из системы

$$\begin{cases} f(x) \equiv 0(\mathrm{mod}\ m_1), \\ f(x) \equiv 0(\mathrm{mod}\ m_2) \end{cases}$$

получаем $f(x) \equiv 0\big(\mathrm{НОК}[m_1, m_2]\big) \equiv 0(\mathrm{mod}\ m_1 \cdot m_2)$, значит

$$\begin{cases} f(x) \equiv 0(\mathrm{mod}\ m_1 \cdot m_2), \\ f(x) \equiv 0(\mathrm{mod}\ m_3), \\ \vdots \\ f(x) \equiv 0(\mathrm{mod}\ m_k) \end{cases}$$

и т. д. В итоге приходим к сравнению

$$f(x) \equiv 0(\mathrm{mod}\ m_1 \cdot m_2 \cdot \ldots \cdot m_k).$$

2) Рассмотрим вопрос о числе решений.

Пусть $f(x) \equiv 0(\text{mod } m_i)$ имеет t_i число решений, следовательно, система

$$\begin{cases} f(x) \equiv 0(\text{mod } m_1), \\ f(x) \equiv 0(\text{mod } m_2) \end{cases}$$

имеет $t = t_1 \cdot t_2$ число решений. Продолжая рассуждения для системы $(*)$, получаем $t = t_1 \cdot t_2 \cdot \ldots \cdot t_k$ решений. Доказательство завершено.

Следствие. Пусть $m = 2^\alpha \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Тогда сравнение $f(x) \equiv 0(\text{mod } m)$ — разрешимо тогда и только тогда, когда разрешимы сравнения $f(x) \equiv 0(\text{mod } 2^\alpha)$, $f(x) \equiv 0(\text{mod } p_i^{\alpha_i})$, где $i = \overline{1 \ldots k}$, и число решений равно $d_0 \cdot d_1 \cdot \ldots \cdot d_k$, где d_i — число решений сравнений $f(x) \equiv 0(\text{mod } p_i^{\alpha_i})$, а d_0 — число решений сравнения $f(x) \equiv 0(\text{mod } 2^\alpha)$.

Пример 52. Решите сравнение $x^4+2x^3+8x+9 \equiv 0(\text{mod } 35)$.

Решение.

$$x^4+2x^3+8x+9 \equiv 0(\text{mod } 35) \Leftrightarrow \begin{cases} x^4 + 2x^3 + 8x + 9 \equiv 0(\text{mod } 5), \\ x^4 + 2x^3 + 8x + 9 \equiv 0(\text{mod } 7). \end{cases}$$

Рассмотрим первое сравнение системы. Так как

$$x^4 + 2x^3 - 2x - 1 \equiv 0(\text{mod } 5),$$

то $(x^2 - 1)(x^2 + 2x - 1) \equiv 0(\text{mod } 5)$. Получаем решение

$$\begin{cases} x \equiv 1(\text{mod } 5), \\ x \equiv 4(\text{mod } 5). \end{cases}$$

Рассмотрим второе сравнение системы.
$x^4 + 2x^3 + x + 2 \equiv 0(\text{mod } 7)$; $(x + 2)(x^3 + 1) \equiv 0(\text{mod } 7)$;
$(x + 2)(x + 1)(x^2 - x + 1) \equiv 0(\text{mod } 7)$, откуда

$$\begin{cases} x \equiv 3(\text{mod } 7), \\ x \equiv 5(\text{mod } 7), \\ x \equiv 6(\text{mod } 7). \end{cases}$$

Получаем шесть вариантов для решения системы:

$$\begin{cases} x \equiv 1(\mathrm{mod}\ 5), \\ x \equiv 3(\mathrm{mod}\ 7); \end{cases} \quad \begin{cases} x \equiv 4(\mathrm{mod}\ 5), \\ x \equiv 3(\mathrm{mod}\ 7); \end{cases} \quad \begin{cases} x \equiv 4(\mathrm{mod}\ 5), \\ x \equiv 6(\mathrm{mod}\ 7). \end{cases}$$

$$\begin{cases} x \equiv 1(\mathrm{mod}\ 5), \\ x \equiv 6(\mathrm{mod}\ 7); \end{cases} \quad \begin{cases} x \equiv 4(\mathrm{mod}\ 5), \\ x \equiv 5(\mathrm{mod}\ 7); \end{cases}$$

$$\begin{cases} x \equiv 1(\mathrm{mod}\ 5), \\ x \equiv 6(\mathrm{mod}\ 7); \end{cases}$$

Ответ.

$x \equiv 6(\mathrm{mod}\ 35)$; $x \equiv 19(\mathrm{mod}\ 35)$;
$x \equiv 26(\mathrm{mod}\ 35)$; $x \equiv 24(\mathrm{mod}\ 35)$;
$x \equiv 31(\mathrm{mod}\ 35)$; $x \equiv 34(\mathrm{mod}\ 35)$.

Теорема. *Пусть* НОД$(a_n, m) = 1$. *Тогда найдется унитарный многочлен* $h(x)$ (*со старшим коэффициентом* 1) *степени* n, *такой что сравнение*

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \equiv 0(\mathrm{mod}\ m)$$

равносильно сравнению $h(x) \equiv 0(\mathrm{mod}\ m)$.

Доказательство. Рассмотрим сравнение $a_n \cdot h \equiv 1(\mathrm{mod}\ m)$, т. к. НОД$(a_n, m) = 1$, то существует решение h. Рассмотрим многочлен $h(x) = h \cdot f(x) \equiv x^n + a_{n-1} \cdot h \cdot x^{n-1} + \ldots + a_0 \cdot h(\mathrm{mod}\ m)$. При этом $h(x)$ — унитарный и $h(x) \equiv p(\mathrm{mod}\ m)$. Доказательство завершено.

Пример 53. Найти унитарный многочлен, равносильный данному:

$$70x^6 + 78x^5 + 25x^4 + 68x^3 + 52x^2 + 4x + 3 \equiv 0(\mathrm{mod}\ 101).$$

Решение. НОД$(70, 101) = 1$. Решим сравнение
$70h \equiv 1(\mathrm{mod}\ 101)$,
$h \equiv 13(\mathrm{mod}\ 101)$,
откуда $h(x) = x^6 + 4x^5 + 22x^4 + 76x^3 + 70x^2 + 52x + 39 \equiv 0(\mathrm{mod}\ 101)$.
Ответ. $x^6 + 4x^5 + 22x^4 + 76x^3 + 70x^2 + 52x + 39 \equiv 0(\mathrm{mod}\ 101)$.

Теорема. *Пусть* $x \equiv x_0 (\mathrm{mod}\ m)$ *— решение сравнения*

$$x^n \equiv a (\mathrm{mod}\ m),$$

где НОД$(a, m) = 1$. *Тогда остальные решения находятся как* $x_i \equiv x_0 \cdot y_i (m)$, *где* y_i *— все решения сравнения* $y^n \equiv 1 (\mathrm{mod}\ m)$.

Попытайтесь доказать эту теорему самостоятельно.

Пример 54. Решите сравнение $x^4 \equiv 3 (\mathrm{mod}\ 13)$.

Решение. Очевидно, что $x \equiv 2 (\mathrm{mod}\ 13)$ является решением сравнения $x^4 \equiv 3 (\mathrm{mod}\ 13)$.

Решим сравнение $y^4 \equiv 1 (\mathrm{mod}\ 13)$. $y^4 - 1 \equiv 0 (\mathrm{mod}\ 13)$, разложим на множители левую часть $(y-1)(y+1)(y^2+1) \equiv 0 (\mathrm{mod}\ 13)$, преобразуем $(y-1)(y+1)(y^2-25) \equiv 0 (\mathrm{mod}\ 13)$. Получим решение $y \equiv 1 (\mathrm{mod}\ 13)$, $y \equiv 12 (\mathrm{mod}\ 13)$, $y \equiv 5 (\mathrm{mod}\ 13)$, $y \equiv 8 (\mathrm{mod}\ 13)$. Найдем решения сравнения $x^4 \equiv 3 (\mathrm{mod}\ 13)$:

$$x \equiv 2 \cdot 1 (\mathrm{mod}\ 13), \qquad x \equiv 2 \cdot 12 (\mathrm{mod}\ 13),$$
$$x \equiv 2 \cdot 5 (\mathrm{mod}\ 13), \qquad x \equiv 2 \cdot 8 (\mathrm{mod}\ 13).$$

Ответ.
$x \equiv 2 (\mathrm{mod}\ 13)$, $x \equiv 11 (\mathrm{mod}\ 13)$,
$x \equiv 10 (\mathrm{mod}\ 13)$, $x \equiv 3 (\mathrm{mod}\ 13)$.

3.3. Примитивные корни. Индекс числа

Пусть $m > 1$ — целое. Говорят, что число m обладает *примитивным* корнем, если существует целое g, что $Z_m^* = \langle \overline{g} \rangle$, то есть Z_m^* — циклическая группа, а число g называется *примитивным корнем по* mod m.

Замечание. Если g — примитивный корень по mod m, то

1. $g \in Z_m^* \Leftrightarrow$ НОД$(g, m) = 1$.
2. $\langle \overline{g} \rangle = Z_m^* \Leftrightarrow |\overline{g}| = |Z_m^*| = \varphi(m)$.

Таким образом, примитивный корень по $\bmod m$ взаимно прост с m и его порядок равен $\varphi(m)$.

Пример 55. Найдем примитивные корни по $\bmod 7$: группа $Z_7^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$, $|Z_7| = \varphi(7) = 6$. $|\overline{1}| = 1$, $|\overline{2}| = 3$, $|\overline{3}| = 6$, $|\overline{4}| = 3$, $|\overline{5}| = 6$, $|\overline{6}| = 2$, следовательно, 3,4 — примитивные корни $\bmod 7$.

Пусть $m > 1$ — целое, обладает примитивным корнем g.

Пусть $a \geqslant 1$ — целое, НОД$(a, m) = 1$.

Целое число $0 \leqslant k \leqslant \varphi(m)$ называется *индексом числа a при основании g по* $\bmod m$, если $a \equiv g^k (\bmod m)$, и обозначается

$$k = \operatorname{ind}_g f (\bmod m).$$

Следует обратить внимание на следующее.

Если m — обладает примитивным корнем, то

$$Z_m^* = \langle \overline{g} \rangle = \left\{ \overline{1}, \overline{g}, \overline{g}^2, \ldots, \overline{g}^{\varphi(m)-1} \right\},$$

при этом, если НОД$(a, m) = 1$, следовательно $\overline{a} \in Z_m^*$, значит существует $0 \leqslant k < \varphi(m) - 1$, что $\overline{a} = \overline{g}^k$, или $a \equiv g^k (\bmod m)$, т. е. для любого a существует $\operatorname{ind}_g a (\bmod m)$.

Пример 56. Найти $\operatorname{ind}_3 25 (\bmod 7)$.

Решение.
$Z_7^* = \langle \overline{3} \rangle = \{\overline{1}, \overline{3}, \overline{3}^2, \overline{3}^3, \overline{3}^4, \overline{3}^5\}$, $a = 25$,
$25 \equiv 4 (\bmod 7) \equiv 3^4 (\bmod 7)$, таким образом, $\operatorname{ind}_3 25 (\bmod 7) = 4$.
Ответ. $\operatorname{ind}_3 25 (\bmod 7) = 4$.

3.4. Свойства индексов при основании $g \bmod m$

Свойства индексов при основании $g \bmod m$:

1) $\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \big(\bmod \varphi(m)\big)$;

2) $\operatorname{ind} a^n \equiv n \operatorname{ind} a \big(\bmod \varphi(m)\big)$;

3) $\operatorname{ind}_g g = 1$.

Свойства 1–2 называются *свойствами аналитического логарифма.*

Доказательство.
1) Пусть $\operatorname{ind} a = k$, $\operatorname{ind} b = n$, тогда
$a \equiv g^k (\mathrm{mod}\ m)$, $\quad b \equiv g^n (\mathrm{mod}\ m)$, $\quad ab \equiv g^{k+n} (\mathrm{mod}\ m)$.
Пусть $\operatorname{ind}(ab) = l$, $ab \equiv g^l (\mathrm{mod}\ m)$,
$g^l \equiv g^{k+n} (\mathrm{mod}\ m) \Leftrightarrow l \equiv k + n (\mathrm{mod}\ \varphi(m))$.
2) следует из 1) (по индукции).
3) $g \equiv g^l (\mathrm{mod}\ m) \Leftrightarrow \operatorname{ind}_g g = 1$.
Свойства доказаны.
Пусть $m > 1$, $n > 1$ — целые; НОД$(a, m) = 1$.

Число a называется *n-степенным вычетом по* mod m, если сравнение $x^n \equiv a (\mathrm{mod}\ m)$ — разрешимо и n-степенным невычетом, в противном случае.

Если $n = 2$, a — квадратичный вычет (невычет);
Если $n = 3$, a — кубический вычет (невычет);
Если $n = 4$, a — биквадратичный вычет (невычет).

Пример 57.

1. $x^2 \equiv -1 (\mathrm{mod}\ 125)$ — разрешимо, следовательно, -1 — квадратичный вычет mod 125;

2. $x^2 \equiv 2 (\mathrm{mod}\ 5)$ — не разрешимо, следовательно 2 — квадратичный невычет mod 5.

3.4.1. Сравнения вида $x^n \equiv a (\mathrm{mod}\ m)$

Теорема. *Пусть $m > 1$, обладает примитивным корнем g,* НОД$(a, m) = 1$*; $n > 1$ — целое,* НОД$\big(n, \varphi(m)\big) = d$*. Тогда сравнение $x^n \equiv a (\mathrm{mod}\ m)$ разрешимо тогда и только тогда, когда*

$$(d | \operatorname{ind}_g a) \overset{(*)}{\Longleftrightarrow} \left(a^{\frac{\varphi(m)}{d}} \equiv 1 (\mathrm{mod}\ m) \right).$$

При этом, если сравнение разрешимо, то оно имеет ровно d решений.

Доказательство. Пусть m обладает примитивным корнем, тогда существует целое число g, что НОД$(g, m) = 1$, $Z_m^* = \langle g \rangle$. Пусть $\operatorname{ind}_g a = k$, т. е. $a \equiv g^k (\bmod\ m)$; $x^n \equiv a (\bmod\ m)$ — сравнение в множестве Z_m^*, т. е. $x \in Z_m^*$ (т. к. НОД$(a, m) = 1$, следовательно x обладает индексом).

Пусть $\operatorname{ind}_g x = t$, т. е. $x \equiv g^t (\bmod\ m)$, $x^n \equiv g^{nt} (\bmod\ m)$. Тогда $x^n \equiv a (\bmod\ m)$, $g^{nt} \equiv g^k (\bmod\ m)$, значит $nt \equiv k \big(\bmod\ \varphi(m)\big)$. Так как НОД$\big(n, \varphi(m)\big) = d$, то сравнение $nt \equiv k \big(\bmod\ \varphi(m)\big)$ разрешимо тогда и только тогда, когда $d | k$, в случае разрешимости имеет d решений. Последнее означает, что $d | \operatorname{ind} a$ и существует d решений сравнения $x^n \equiv a (\bmod\ m)$.

Теперь докажем переход $(*)$.

Необходимость. Пусть $d | k$, где $k = \operatorname{ind}_g a$, тогда получаем $a^{\frac{\varphi(m)}{d}} \equiv g^{\frac{k \cdot \varphi(m)}{d}} \equiv (g^{\varphi(m)})^{\frac{k}{d}} \equiv 1 (\bmod\ m)$, т. к. НОД$(g, m) = 1$.

Достаточность. Пусть $a^{\frac{\varphi(m)}{d}} \equiv 1 (\bmod\ m)$; $\operatorname{ind}_g a = k$, $a \equiv g^k (\bmod\ m)$, следовательно $g^{\frac{k\varphi(m)}{d}} \equiv 1 (\bmod\ m)$, $\dfrac{k\varphi(m)}{d}$ — аннулятор g, откуда $\operatorname{ord} g = \varphi(m)$, т. к. $|g| = |Z_m^*|$, следовательно $\dfrac{k}{p}$ — целое, откуда $d | k$.

Доказательство завершено.

Следствие. В условиях теоремы число a является n-степенным вычетом по mod m тогда и только тогда, когда

$$(d | \operatorname{ind} a) \Leftrightarrow \left(a^{\frac{\varphi(m)}{d}} \equiv 1 (\bmod\ m) \right).$$

Пример 58. Найти все 15-степенные вычеты по mod 27.

Решение. При каких a разрешимо сравнение $x^{15} \equiv a (\bmod\ 27)$?
$m = 27 = 3^3$; $\varphi(27) = 18$. Найдем g, что $|g| = 18$;
НОД$(g, 27) = 1$; $Z_{27}^* = \langle \overline{g} \rangle = \{\overline{g}^0, \overline{g}^1, \ldots, \overline{g}^{17}\}$.

$Z_{27}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}, \overline{10}, \overline{11}, \overline{13}, \overline{14}, \overline{1617}, \overline{19}, \overline{20}, \overline{22}, \overline{23}, \overline{25}, \overline{26}\} = \langle\overline{2}\rangle = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{16}, \overline{5}, \overline{10}, \overline{20}, \overline{13}, \overline{26}, \overline{25}, \overline{23}, \overline{19}, \overline{11}, \overline{22}, \overline{17}, \overline{7}, \overline{14}\}$. По следствию, a — вычет тогда и только тогда, когда $a^{\frac{\varphi(m)}{d}} \equiv 1(\mathrm{mod}\ m)$; $d = \mathrm{НОД}\,(15, \varphi(27)) = 3$, $a^{\frac{18}{3}} \equiv 1(\mathrm{mod}\ 27)$; $a^6 \equiv 1(\mathrm{mod}\ 27)$. Решением этого сравнения являются числа $a = \{\overline{g}^0, \overline{g}^3, \overline{g}^6, \overline{g}^9, \overline{g}^{12}\overline{g}^{15}\}$, $a = \{\overline{1}, \overline{8}, \overline{10}, \overline{26}, \overline{19}, \overline{17}\}$.

Ответ. $a = \{\overline{1}, \overline{8}, \overline{10}, \overline{26}, \overline{19}, \overline{17}\}$.

Следствие. Пусть p не делит a, $p > 2$. Тогда $x^2 \equiv a(\mathrm{mod}\ p)$ разрешимо тогда и только тогда, когда $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$ и имеет 2 решения в случае разрешимости.

Доказательство. Так как p — простое, то Z_p^* — циклическая, т. е. p — обладает примитивным корнем, следовательно по теореме сравнение $x^2 \equiv a(\mathrm{mod}\ p)$ разрешимо тогда и только тогда, когда $a^{\frac{\varphi(m)}{d}} \equiv 1(\mathrm{mod}\ m)$, где $d = \mathrm{НОД}\big(2; (p-1)\big) = 2$; $\varphi(m) = p - 1$. Получаем $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$. Доказательство завершено.

3.4.2. Структура группы обратимых элементов

Кратко остановимся на структуре группы $\mathbb{Z}_m^*$.

Теорема.

1) *Группа $Z_{p^\alpha}^*$ — циклическая, для любого $p > 0$ — простого, для любого $\alpha > 1$.*

2) *Пусть $p = 2$, тогда $Z_{p^\alpha}^*$ имеет строение:*

   а) *если $\alpha = 1$, то Z_2^* — циклическая 1-го порядка;*

   б) *если $\alpha = 2$, то Z_4^* — циклическая 2-го порядка;*

в) *если* $\alpha \geqslant 3$, *то* $Z^*_{2^\alpha}$ — *не циклическая группа:*
$Z^*_{2^\alpha} = H \times F$, *где* $H = \langle -\overline{1} \rangle$ — *циклическая 2-го порядка;*
$F = \langle \overline{5} \rangle$ — *циклическая порядка* $2^{\alpha-2}$. *Таким образом*

$$Z^*_{2^\alpha} = \left\{ (-1)^\alpha 5^b \,\middle|\, \begin{array}{l} a = 0, 1 \\ b = 0, 1, 2, \ldots, 2^{\alpha-1} - 1 \end{array} \right\}.$$

3) *Если* $m = 2^\alpha \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, *тогда* $Z^*_m = Z^*_{2^\alpha} \times Z^*_{p_1^{\alpha_1}} \times \ldots \times Z^*_{p_k^{\alpha_k}}$.

Пример 59. $Z^*_{36} = Z^*_{2^2} \times Z^*_9 \approx 2 \oplus Z_6$.
$Z^*_{2^2}$ — циклическая 2-го порядка, следовательно $\approx Z_2$;
Z^*_9 — циклическая 6-го порядка, следовательно $\approx Z_6$.

Для нас оказывается полезным следствие данной теоремы.

Следствие. Целое, положительное m обладает примитивным корнем $\Leftrightarrow m = 2, 4, p^\alpha, 2p^\alpha$.

Докажите его самостоятельно.

Пример 60. Обладает ли 50 примитивным корнем?

Решение. Струкутра группы $Z^*_{50} = Z^*_2 \times Z^*_{5^2} \approx Z^*_{5^2}$, т. е. Z^*_{50} — циклическая, следовательно, 50 обладает примитивным корнем.

3.4.3. Система индексов числа $a \bmod m$

Рассмотрим отдельно два случая для числа m.

1) Пусть $m = 2^\alpha$, $\alpha \geqslant 3$, следовательно Z^*_m — не циклическая, т. е. m — не обладает примитивным корнем.
$Z^*_m = H \times F = \langle -\overline{1} \rangle \times \langle \overline{5} \rangle$, тогда для любого a, НОД$(a, m) = 1$, следует, что НОД$(a, 2) = 1$. Таким образом, существует пара (x, y), такая, что $a \equiv (-1)^x 5^y (\bmod\, 2^\alpha)$. Пара чисел $\{x, y\}$ называется *системой индексов числа* $a \bmod m$:

$$x \in \{0, 1\}, \quad y \in \{0, 1, 2, 3, \ldots, 2^{\alpha-2} - 1\}.$$

Пример 61. Найти систему индексов для числа 115 по mod 8.

Решение. По условию задачи $m = 8$.

$Z_8^* = \langle -\overline{1}\rangle \times \langle \overline{5}\rangle = \left\{\overline{(-1)^0 5^0}, \overline{(-1)^1 5^0}, \overline{(-1)^0 5^1}, \overline{(-1)^1 5^1}\right\} =$

$= \{\overline{1}, \overline{7}, \overline{5}, \overline{3}\}$, получаем $\alpha = 3$, $x = \{0; 1\}$, $y = \{0, 1\}$;

$a \equiv 115 \equiv 3 (\mathrm{mod}\ 8)$, следовательно $\mathrm{ind}\, 115 \bmod 8 = \{1, 1\}$.

Ответ. $\{1, 1\}$.

2) Рассмотрим общий случай m.

$m = 2^\alpha \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, тогда $Z_m^* = Z_{2^\alpha}^* \times Z_{p_1^{\alpha_1}}^* \times \ldots Z_{p_k^{\alpha_k}}^*$. Если $\alpha \geqslant 3$, то для любого $a \in Z_m^*$ существует набор чисел

$\{x, y, \nu_1, \nu_2, \ldots, \nu_k\}$, $x \in \{0, 1\}$,

$y \in \{0, 1, \ldots, 2^{\alpha-2} - 1\}$, $\nu_i \in \{0, 1, \ldots, \varphi(p_1^{\alpha_1}) - 1\}$, таких, что

$a \equiv (-1)^x \cdot 5^y \cdot g_1^{\nu_1} \cdot \ldots \cdot g_k^{\nu_k} (\mathrm{mod}\ m)$, где $Z_{p_1^{\alpha_1}}^* = \langle \overline{g}_1 \rangle$.

Набор чисел $\{x, y, \nu_1, \ldots, \nu_k\}$ называется *системой индексов числа* $a \bmod m$.

Если $\alpha = 2$, $Z_4^* \approx \{\pm\overline{1}\}$, т. е. $Z_4^* = \langle -\overline{1}\rangle$, $x = \{0, 1\}$, y=$\{0\}$.

Если $\alpha = 1$, $Z_2^* \approx \{1\}$, следовательно $x = 0$, $y = 0$.

Пример 62. Найти систему индексов числа 11 по mod 60.

Решение. По условию задачи $m = 60$.

Рассмотрим группу $Z_{60}^* = Z_4^* \times Z_3^* \times Z_5^* = \langle -\overline{1}\rangle \times \langle \overline{2}\rangle \times \langle \overline{3}\rangle$.

Тогда $a = 11$, $\varphi(60) = 16$,

$11 \equiv (-1)^x (\mathrm{mod}\ 4)$, $\quad x = 1$.

$11 \equiv 2^{\nu_1} (\mathrm{mod}\ 3)$, $\quad \nu_1 = 1$,

$11 \equiv 3^{\nu_2} (\mathrm{mod}\ 5)$, $\quad \nu_2 = 0$,

$\{1, 1, 0\}$ — система индексов для 11.

Ответ. $\{1, 1, 0\}$

3.4.4. Разрешимость сравнений

Теорема. *Пусть* $m = 2^\alpha$, $\alpha \geqslant 2$, $a \equiv 1(\mathrm{mod}\ 2)$, $n > 1$, *целое. Тогда*

1) *Если* $n \equiv 1(\mathrm{mod}\ 2)$, *то сравнение* $x^n \equiv a(\mathrm{mod}\ 2^\alpha)$ *имеет единственное решение.*

2) *Если* $n \equiv 0(\mathrm{mod}\ 2)$, $\text{НОД}(n, 2^{\alpha-2}) = d$, *то сравнение* $x^n \equiv a(\mathrm{mod}\ 2^\alpha)$ — *разрешимо*

$$\overset{(1)}{\iff} \begin{pmatrix} \operatorname{ind} a = \{z, y\} \\ z \equiv 0(\mathrm{mod}\ 2) \\ y \text{ кратно } d \end{pmatrix} \overset{(2)}{\iff} \left(\begin{cases} a \equiv 1(\mathrm{mod}\ 4) \\ a^{\frac{2^{\alpha-2}}{d}} \equiv 1(\mathrm{mod}\ 2^\alpha) \end{cases} \right).$$

В случае разрешимости существует точно $2d$ решений.

Доказательство.

1) Если $n \equiv 1(\mathrm{mod}\ 2)$, следовательно 2 делит a и не делит n, т. е. $x^n \equiv a(\mathrm{mod}\ 2)$ и $x^n \equiv a(\mathrm{mod}\ 2^\alpha)$ имеют одинаковое число решений, но $a \equiv 1(\mathrm{mod}\ 2)$, значит $x^n \equiv 1(\mathrm{mod}\ 2)$, тогда $x \equiv 1(\mathrm{mod}\ 2)$ — единственное решение, следовательно $x^n \equiv a(\mathrm{mod}\ 2^\alpha)$ — имеет единственное решение.

2) Рассмотим $n \equiv 0(\mathrm{mod}\ 2)$. Пусть $d = \text{НОД}(n, 2^{\alpha-2})$.

Докажем переход (1). По условию $a \equiv 1(\mathrm{mod}\ 2)$, следовательно a — нечетное, $a \in Z_{2^\alpha}^*$, значит, существует $\{z, y\} = \operatorname{ind} a$, что $a \equiv (-1)^z \cdot 5^y(\mathrm{mod}\ 2^\alpha)$. Если x — решение, тогда $x \in Z_{2^\alpha}^*$, то $x \equiv (-1)^i \cdot 5^j(\mathrm{mod}\ 2^\alpha)$, откуда

$$(-1)^{in} \cdot 5^{jn} \equiv (-1)^z \cdot 5^y(\mathrm{mod}\ 2^\alpha) \iff$$

$$\iff \begin{cases} i \cdot n \equiv z(\mathrm{mod}\ 2) \\ j \cdot n \equiv y(\mathrm{mod}\ 2^{\alpha-2}) \end{cases} \text{ — разрешимая система} \iff$$

$$\iff \begin{cases} n \equiv 0(\mathrm{mod}\ 2) \text{ — по условию, тогда } z \equiv 0(\mathrm{mod}\ 2), \\ d|n,\ d|2^{\alpha-2}, \text{тогда } d|y. \end{cases}$$

Если сравнение разрешимо, то $i = 0, 1$, тогда сравнение $j \cdot n \equiv y(\mathrm{mod}\ 2^{\alpha-2})$ — имеет d решений, следовательно систе-

ма имеет $2d$ решений, значит, существует $2d$ решений сравнения $x^n \equiv a(\mathrm{mod}\ 2^\alpha)$, и переход (1) доказан.

Докажем переход (2). Условие $\mathrm{ind}\, a = \{z; y\}$ равносильно условию $a \equiv (-1)^z \cdot 5^y (\mathrm{mod}\ 2^\alpha) \equiv (-1)^z (\mathrm{mod}\ 4)$.

Таким образом, $a \equiv 1(\mathrm{mod}\ 4) \Longleftrightarrow z \equiv 0(\mathrm{mod}\ 2)$.

Из условия $d|y$ следует, что

$$a^{\frac{2^{\alpha-2}}{d}} \equiv \left((-1)^z\right)^{\frac{2^{\alpha-2}}{d}} \cdot (5^y)^{\frac{2^{\alpha-2}}{d}} (\mathrm{mod}\ 2^\alpha) \equiv (5^{2^{\alpha-2}})^{\frac{y}{d}} (\mathrm{mod}\ 2^\alpha).$$

Так как $|\overline{5}| = 2^{\alpha-2}$ в $Z^*_{2^\alpha}$, то $a^{\frac{2^{\alpha-2}}{d}} \equiv 1(\mathrm{mod}\ 2^\alpha)$.

Обратно, $a^{\frac{2^{\alpha-2}}{d}} \equiv (5^y)^{\frac{2^{\alpha-2}}{d}} (\mathrm{mod}\ 2^\alpha) \equiv 1(\mathrm{mod}\ 2^\alpha)$, следовательно $\mathrm{ord}\, 5$ делит $\left(y \cdot \dfrac{2^{\alpha-2}}{d}\right)$, но $\mathrm{ord}\, 5 = 2^{\alpha-2}$, следовательно $\dfrac{y}{d}$ — целое, $d|y$, и переход (2) доказан.

Доказательство завершено.

Следствие. Пусть 2 не делит a. Тогда, в зависимости от условий, сравнение $x^2 \equiv a(\mathrm{mod}\ 2^\alpha)$ имеет следующее число решений:

1) при $\alpha = 1$, имеет единственное решение $x \equiv 1(\mathrm{mod}\ 2)$;

2) при $\alpha = 2$, разрешимо $\Leftrightarrow a \equiv 1(\mathrm{mod}\ 4)$ и имеет в случае разрешимости 2 решения $x \equiv \pm 1(\mathrm{mod}\ 4)$;

3) при $\alpha \geqslant 3$, разрешимо $\Leftrightarrow a \equiv 1(\mathrm{mod}\ 4)$ и имеет в случае разрешимости 4 решения.

Доказательство. Имеем: $n = 2 \equiv 0(\mathrm{mod}\ 2)$, и 2 не делит a, откуда $a \equiv 1(\mathrm{mod}\ 2)$.

1) $\alpha = 1$, $x^2 \equiv a(\mathrm{mod}\ 2)$, следовательно $x \equiv 1(\mathrm{mod}\ 2)$ — решение единственное.

2) $\alpha = 2$, $x^2 \equiv a(\mathrm{mod}\ 4)$, $d = \mathrm{НОД}(2; 2^0) = 1$, следовательно разрешимо $\overset{(2)}{\Longleftrightarrow} \begin{cases} a \equiv 1(\mathrm{mod}\ 4) \\ a^{2^0} \equiv 1(\mathrm{mod}\ 4) \end{cases} \Longleftrightarrow a \equiv 1(\mathrm{mod}\ 4)$ и имеет 2 решения: $x^2 \equiv 1(\mathrm{mod}\ 4)$ и $x \equiv \pm 1(\mathrm{mod}\ 4)$.

3) $\alpha \geqslant 3$, $x \equiv a(\mathrm{mod}\ 2^\alpha)$, $d = \mathrm{НОД}(2; 2^{\alpha-2}) = 2$, т. к. $\alpha - 2 \geqslant 1$, следовательно $x^2 \equiv a(\mathrm{mod}\ 2^\alpha)$ — разрешимо.

Тогда по теореме получаем:

$$\begin{cases} z \equiv 0(\text{mod } 2) \\ d|y, \Rightarrow 2|y \end{cases} \iff a = \{5^0; 5^2; 5^4; \ldots; 5^{2^{\alpha-2}-2}\},$$

т. е. $a = 5^{2k} = (5^2)^k \equiv 1^k(\text{mod } 8) \equiv 1(\text{mod } 8)$. Задача имеет $2d$ решений.

Рассмотрим другие варианты a:

$a = 5^{2k+1} \equiv 5(\text{mod } 8)$;

$a = (-1) \cdot 5^{2k+1} \equiv -5(\text{mod } 8) \equiv 3(\text{mod } 8)$;

$a = (-1) \cdot 5^{2k} \equiv -1(\text{mod } 8) \equiv 7(\text{mod } 8)$, т. е. задача имеет 4 решения.

Таким образом, все случаи рассмотрены.

Пример 63. Определить число решений и решить следующее сравнение: $x^2 \equiv 17(\text{mod } 2^5)$.

Решение. По условию задачи: $a = 17 \equiv 1(\text{mod } 2)$, $\alpha = 5 \geqslant 3$, $n = 2$. $a = 17 \equiv 1(\text{mod } 8)$, следовательно решение существует, и их 4 штуки.

Найдем эти решения.

$\{z; y\} = \text{ind}\, a$, но следовательно $a = 5^{2k}$, т. е. $z = 0$.

$17 \equiv 5^{2k}(\text{mod } 32)$, $k \neq 0$, $k \neq 1$, $k = 2$ — удовлетворяет, следовательно $y = 4$.

$17 \equiv 625(\text{mod } 32)$ — верно.

По теореме $x \equiv (-1)^i 5^j(\text{mod } 32)$ — решение тогда и только тогда, когда $\begin{cases} i = 0, 1; \\ j \cdot 2 \equiv 4(\text{mod } 8). \end{cases}$

$j \equiv 2(\text{mod } 4)$, следовательно $j \equiv 2(\text{mod } 8)$, $j \equiv 6(\text{mod } 8)$, и $j = \{2, 6\}$, $x \equiv \pm 5^2(\text{mod } 32)$, $x \equiv \pm 5^6(\text{mod } 32)$,

Ответ.

$x_{1,2} \equiv \pm 25(\text{mod } 32)$, $\quad x_{3,4} \equiv \pm 9(\text{mod } 32)$

или

$x_1 \equiv 7(\text{mod } 32)$, $\quad x_2 \equiv 9(\text{mod } 32)$,

$x_3 \equiv 23(\text{mod } 32)$, $\quad x_4 \equiv 5(\text{mod } 32)$.

Теорема. *Пусь $n = 2^\alpha \cdot n_1$, 2 не делит n_1, 2 не делит a. Тогда, если разрешимо сравнение $x^n \equiv a(\mathrm{mod}\ 2^{2\alpha+1})$, то для любого $m \geqslant 2\alpha+1$ разрешимо сравнение $x^n \equiv a(\mathrm{mod}\ 2^m)$, и в случае разрешимости оба имеют одинаковое число решений:*

1) *если $\alpha = 0$, то существует единственное решение;*

2) *если $\alpha > 0$, то существует $2^{\alpha+1}$ решений.*

Доказательство.

1) Если $\alpha = 0$, тогда $n \equiv 1(\mathrm{mod}\ 2)$, по теореме существует единственное решение $x^n \equiv a(\mathrm{mod}\ 2^m)$ для любого m.

2) Если $\alpha > 0$, $m \geqslant 2\alpha + 1$, то доказательство проведем по индукции по m:

а) $m = 2\alpha + 1$; если $x^n \equiv a(\mathrm{mod}\ 2^{2\alpha+1})$ — разрешимо, следовательно $x^n \equiv a(\mathrm{mod}\ 2^{2\alpha+1})$ — разрешимо.

б) Пусть верно для m: т. е. $x^n \equiv a(\mathrm{mod}\ 2^{2\alpha+1})$ — разрешимо и $x^n \equiv a(\mathrm{mod}\ 2^m)$ — разрешимо, т. е. существует x_0, что $x_0^n \equiv a(\mathrm{mod}\ 2^m)$.

3) Рассмотрим $x^n \equiv a(\mathrm{mod}\ 2^{m+1})$, и $x = x_0 + t \cdot 2^{m-\alpha}$, то

$$x^n = (x_0 + t \cdot 2^{m-\alpha})^n = x_0^n + n \cdot x_0^{n-1} \cdot t \cdot 2^{m-\alpha} +$$
$$+ \sum_{k=2}^{n} C_n^k \cdot x_0^{n-k} \cdot t^k \cdot 2^{(m-\alpha)k} \equiv x_0^n + n \cdot x_0^{n-1} \cdot t \cdot 2^{m-\alpha} (\mathrm{mod}\ 2^{m+1}),$$
$$\Big((m-\alpha) \cdot k \geqslant (m-\alpha) \cdot 2 = (m+1) + \big(m - (2\alpha+1)\big) \geqslant m+1\Big),$$

следовательно $x^n \equiv x_0^n + n_1 \cdot x_0^{n-1} \cdot t \cdot 2^m (\mathrm{mod}\ 2^{m+1})$.

Докажем, что $x^n - a \equiv (x^n - a) + n_1 \cdot x_0^{n-1} \cdot t \cdot 2^m (\mathrm{mod}\ 2^{m+1})$, т. е.

$$\frac{x^n - a}{2^m} \equiv \frac{x_0^n - a}{2^m} + n_1 \cdot x_0^{n-1} \cdot t (\mathrm{mod}\ 2). \qquad (*)$$

Рассмотрим x_0 — решение: $x_0 \not\equiv 0(\mathrm{mod}\ 2)$, так как иначе $x_0^n \equiv 0(\mathrm{mod}\ 2)$, т. е. $a \equiv 0(\mathrm{mod}\ 2)$ — противоречит условию, следовательно $x_0 \equiv 1(\mathrm{mod}\ 2)$, тогда $x_0^{n-1} \equiv 1(\mathrm{mod}\ 2)$, $n_1 \equiv 1(\mathrm{mod}\ 2)$ — по условию, тогда $n_1 \cdot x_0^{n-1} \equiv 1(\mathrm{mod}\ 2)$, следовательно существует единственное решение t: $n_1 \cdot x_0^{n-1} \cdot t \equiv -\dfrac{x_0^n - a}{2^m} (\mathrm{mod}\ 2)$, а именно

$t_0 \equiv -\frac{x_0^n - a}{2^m} (\text{mod } m)$, т. е. $t_0 \equiv \frac{x_0^n - a}{2^m} (\text{mod } 2)$. Получаем

$$\frac{x^n - a}{2^m} \equiv \frac{x_0^n - a}{2^m} + n_1 \cdot x_0^{n-1} \cdot t_0 \equiv (\text{mod } 2), \qquad (*)$$

т. е. $x^n \equiv a (\text{mod } 2^{m+1})$,

$x = x_0 + t_0 \cdot 2^{m-\alpha} = x_0 + \frac{x_0^n - a}{2^\alpha} + 2^{m-\alpha+1} \cdot g$ — решение $(*)$.

При $g = 2^\alpha \cdot g_0 + r$ получили

$x = x_0 + \frac{x_0^n - a}{2^\alpha} + 2^{m+1} \cdot g_0 + 2^{m-\alpha+1} \cdot r \equiv$

$\equiv x_0 + \frac{x_0^n - a}{2^\alpha} + r \cdot 2^{m-\alpha+1} (\text{mod } 2^{m+1})$;

$0 \leqslant r \leqslant 2^\alpha - 1$;

следовательно существует 2^α штук различных решений x, но n — четное число, следовательно

$$x \equiv -x_0 - \frac{x_0^n - a}{2^\alpha} - r \cdot 2^{m-\alpha+1} (\text{mod } 2^{m+1})$$

— тоже решение, тогда всего $2^{\alpha+1}$ решений

$$x \equiv \pm \left(x_0 + \frac{x_0^n - a}{2^\alpha} + r \cdot 2^{m-\alpha} \right) (\text{mod } 2^m),$$

где $0 \leqslant r \leqslant 2^\alpha - 1$. Доказательство завершено.

Пример 64. Провести исследование сравнения $x^6 \equiv 17 (\text{mod } 2^m)$.

Решение. По условию задачи $n = 6 = 3 \cdot 2$, $\alpha = 1$, $n_1 = 3$, $a = 17$, $2\alpha + 1 = 3$.

Если $x^6 \equiv 17 (\text{mod } 2^3)$, $x^6 \equiv 17 (\text{mod } 8) \equiv 1 (\text{mod } 8)$ — разрешимо и по теореме имеет решения:

$x \equiv \pm 1 (\text{mod } 8)$; $\quad x \equiv \pm 3 (\text{mod } 8)$.

1) Если $m = 4$, следовательно, $x_0 = 1$,

$x \equiv \pm \left(1 + \frac{1 - 17}{2} + r \cdot 2^3 \right) (\text{mod } 2^4)$, $\quad r = 0, 1$;

$x \equiv \pm 7 (\mathrm{mod}\ 16), \quad r = 0;$
$x \equiv \pm 15 (\mathrm{mod}\ 16) \equiv 1 (\mathrm{mod}\ 16), \quad r = 1.$
2) Если $m = 5$, следовательно, $x_0 = 1$,
$x \equiv \pm \left(1 + \frac{1-17}{2} + r \cdot 2^4\right) (\mathrm{mod}\ 2^5), \quad r = 0, 1;$
$x \equiv \pm 7 (\mathrm{mod}\ 32), \quad r = 0;$
$x \equiv \pm 9 (\mathrm{mod}\ 32) \equiv 1 (\mathrm{mod}\ 16), \quad r = 1.$
и т. д. Проведите дальнейшее исследование самостоятельно.

Теорема. *Пусть* $m = 2^\alpha \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, НОД$(a, m) = 1$. *Тогда сравнение* $x^2 \equiv a (\mathrm{mod}\ m)$ *разрешимо тогда и только тогда, когда*

1) $\alpha = 0, 1$, *без ограничений;*
2) $\alpha = 2$, $a \equiv 1 (\mathrm{mod}\ 4)$; $\alpha \geqslant 3$, $a \equiv 1 (\mathrm{mod}\ 8)$;
3) $a^{\frac{p_i - 1}{2}} \equiv 1 (\mathrm{mod}\ p_i)$, $i = \overline{1 \ldots k}$,

и в случае разрешимости имеет

1) 2^k, $\alpha = 0, 1$;
2) 2^{k+1}, $\alpha = 2$;
3) 2^{k+2}, $\alpha \geqslant 3$

решений.

Доказательство. Было доказано, что $x^2 \equiv a (\mathrm{mod}\ m)$ — разрешимо тогда и только тогда, когда $\begin{cases} x^2 \equiv a (\mathrm{mod}\ 2^\alpha), \\ x^2 \equiv a (\mathrm{mod}\ p_1^{\alpha_i}). \end{cases}$

1) $x^2 \equiv a (\mathrm{mod}\ 2^\alpha)$ — разрешимо тогда и только тогда, когда

$$\begin{cases} \alpha = 0, 1 & \text{без ограничений и имеет единственное решение;} \\ \alpha = 2 & a \equiv 1 (\mathrm{mod}\ 4) \quad \text{и имеет 2 решения;} \\ \alpha \geqslant 3 & a \equiv 1 (\mathrm{mod}\ 8) \quad \text{и имеет 4 решения.} \end{cases}$$

2) $x^2 \equiv a (\mathrm{mod}\ p_1^{\alpha_i})$ — разрешимо тогда и только тогда, когда $a^{\frac{p_i - 1}{2}} \equiv 1 (\mathrm{mod}\ p_i)$ и имеет 2 решения, следовательно:

1) при $\alpha = 0, 1$ получаем 2^k решений;
2) при $\alpha = 2$, получаем $2 \cdot 2^k$ решений;

3) при $\alpha \geqslant 3$, получаем $2^2 \cdot 2^k$ решений.
Таким образом, все случаи рассмотрены.

Пример 65. Определить количество решений сравнения $x^2 \equiv 8(\text{mod } 34)$.
Решение. $34 = 2 \cdot 17$, $x \equiv \pm 12(\text{mod } 34)$.
$\alpha = 1$, тогда сравнение разрешимо и имеет 2 решения.

3.4.5. Символ Лежандра

Пусть $p > 2$ — простое. Обозначение

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если} \quad p|a, \\ 1, & \text{если} \quad a \ \text{— квадратичный вычет} \quad mod\ p, \\ -1, & \text{если} \quad a \ \text{— не квадратичный вычет} \quad mod\ p. \end{cases}$$

Другими словами:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если} \quad p|a, \\ 1, & \text{если} \quad x^2 \equiv a(\text{mod } p) \ \text{— разрешимо}, \\ -1, & \text{если} \quad x^2 \equiv a(\text{mod } p) \ \text{— не разрешимо}. \end{cases}$$

$\left(\frac{a}{p}\right)$ — называется символом Лежандра.

Пример 66. а) $\left(\frac{6}{3}\right) = 0$; б) $\left(\frac{5}{3}\right) = -1$; с) $\left(\frac{7}{2}\right) =$ — не символ Лежандра.

3.4.6. Свойства символа Лежандра

Рассмотрим свойства символа Лежандра.
Пусть $p > 2$, простое, тогда:

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

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;

(3) *Если* $a \equiv b(\mathrm{mod}\ p)$, *то* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(4) $\left(\frac{1}{p}\right) = 1$.

(5) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$, если p не делит b.

(6) $\left(\frac{a+mp}{p}\right) = \left(\frac{a}{p}\right)$.

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

(8) $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n$.

(9) Произведение двух квадратичных вычетов или двух квадратичных невычетов — есть вычет, а произведение вычета на невычет — есть невычет.

Доказательство.

Докажем свойство (1).

Если $p|a$, то $\left(\frac{a}{p}\right) = 0$ и $a^{\frac{p-1}{2}} \equiv 0(\mathrm{mod}\ p)$.

Если p не делит a, то:

1) при $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$, получаем $\left(\frac{a}{p}\right) = 1$ по определению, и наоборот, что и требовалось доказать;

2) при $a^{\frac{p-1}{2}} \not\equiv 1(\mathrm{mod}\ p)$, получаем $\left(\frac{a}{p}\right) = -1$, следовательно по теореме Ферма

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right) \cdot \left(a^{\frac{p-1}{2}} + 1\right) \equiv 0(\mathrm{mod}\ p),$$

но Z_p — поле, следовательно в нем нет делителей 0, откуда

$a^{\frac{p-1}{2}} + 1 \equiv 0 (\text{mod } p)$, т. е. $a^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$, таким образом, получаем $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\text{mod } p)$.

Докажем свойство (2).

$\left(\frac{ab}{p}\right) \overset{\text{по (1)}}{\equiv} (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) (\text{mod } p)$,

следовательно $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \equiv 0 (\text{mod } p)$, но $p > 2$, тогда $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = 0$.

Докажем свойство (3).

Если $a \equiv b (\text{mod } p)$, тогда:

а) $\left(\frac{a}{p}\right) = 0$, т. е. $p|a$, то $p|b$, $\left(\frac{b}{p}\right) = 0$.

б) $x^2 \equiv a (\text{mod } p)$ — разрешимо тогда и только тогда, когда $x^2 \equiv b (\text{mod } p)$ — разрешимо.

Докажем свойство (4).

$x^2 \equiv 1 (\text{mod } p)$ — разрешимо для любых p, следовательно $\left(\frac{1}{p}\right) = 1$.

Докажем свойство (5).

$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b^2}{p}\right)$, если p не делит b, следовательно $\left(\frac{b^2}{p}\right) \neq 0$, но $x^2 \equiv b^2 (\text{mod } p)$ — разрешимо, $x = \pm b (\text{mod } p)$, тогда $\left(\frac{b^2}{p}\right) = 1$, и $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

Докажем свойство (6).

$a + mp \equiv a (\text{mod } p)$, по свойству (3), получаем

$\left(\frac{a+mp}{p}\right) = \left(\frac{a}{p}\right)$.

Докажем свойство (7).

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} (\text{mod } p)$, т. к. $p > 2$, следовательно

$-1 \neq 1(\mathrm{mod}\ p)$, откуда $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Докажите свойство (8) самостоятельно по индукции, используя свойство (2).

Докажем свойство (9).

По свойству (2), $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \{\pm 1\} \cdot \{\pm 1\} = 1 = \left(\frac{ab}{p}\right)$,

$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = 1 \cdot (-1) = -1$.

Доказательство завершено.

Утверждение. *Число квадратичных вычетов по* mod p *равно числу квадратичных невычетов и равно* $\frac{p-1}{2}$.

Доказательство. Рассмотрим все $a \in \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$ — квадратичные вычеты и невычеты по mod p.

$x^2 \equiv a(\mathrm{mod}\ p)$ — разрешимо тогда и только тогда, когда $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\ p)$ — имеет ровно $\frac{p-1}{2}$ решений, следовательно $\frac{p-1}{2}$ — вычетов, а остальные $\frac{p-1}{2}$ — невычеты. Доказательство завершено.

3.4.7. Лемма Гаусса

Пусть $p > 2$ — простое. Приведенная система вычетов $\left\{\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\right\}$ называется *наименьшей системой вычетов* (по абсолютной величине).

Введем обозначение: пусть a и p такие, что НОД$(a, p) = 1$. Рассмотрим ряд чисел вида $a \cdot k$,

$$\left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$$

где $k \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. Для каждого числа из ряда найдем наименьший вычет (по абсолютной величине) по mod p, обозна-

чим его $\delta_k \cdot m_k$, где $\delta_k = \pm 1$ — знак, $1 \leqslant m_k \leqslant \dfrac{p-1}{2}$ — модуль, т. е. $\delta_k \cdot m_k$ принадлежит приведенной системе вычетов, $a \cdot k \equiv \delta_k \cdot m_k (\bmod\, p)$.

Через μ обозначим число отрицательных знаков в ряду

$$\left\{ \delta_1, \delta_2, \ldots, \delta_{\frac{p-1}{2}} \right\}.$$

Пример 67. Найти μ для $p = 11$, $a = 7$.

Решение. $p = 11$, $a = 7$, тогда

$k \in \{1, 2, 3, 4, 5\}$, $\dfrac{p-1}{2} = 5$, $a \cdot k = 7, 14, 21, 28, 35$, откуда

$\delta_k \cdot m_k = \{-4; 3; -1; -5; 2\}$, $\delta_k = \{-1; 1; -1; -1; 1\}$, $\mu = 3$.

Ответ. $\mu = 3$.

Теорема (Гаусса). $\left(\dfrac{a}{p}\right) = (-1)^{\mu}$, *если* p *не делит* a.

Доказательство. $k \in \left\{ 1, 2, \ldots, \dfrac{p-1}{2} \right\}$, найдем m_k.

1) Докажем $\left\{ m_1, \ldots, m_{\frac{p-1}{2}} \right\} = \left\{ 1, 2, \ldots, \dfrac{p-1}{2} \right\}$; так как $m_k \in \left\{ 1, 2, \ldots, \dfrac{p-1}{2} \right\}$, то докажем $m_k \neq m_r$, $\forall k \neq r$: пусть $k \neq r$, $m_k = m_r$, $ka \equiv \pm ra (\bmod\, p)$, следовательно $k \equiv \pm r (\bmod\, p)$, т. е. $k \pm r \equiv 0 (\bmod\, p)$, но $0 < |k \pm r| \leqslant |k| + |r| \leqslant p - 1$, следовательно получили противоречие, т. е. $m_k \neq m_r$.

2) Рассмотрим систему

$$\begin{cases} 1 \cdot a \equiv \delta_1 \cdot m_1 (\bmod\, p), \\ 2 \cdot a \equiv \delta_2 \cdot m_2 (\bmod\, p), \\ \vdots \\ k \cdot a \equiv \delta_k \cdot m_k (\bmod\, p). \end{cases}$$

Произведение сравнений системы дает нам следующее сравнение: $k!a^k \equiv (-1)^\mu \cdot \left(\frac{p-1}{2}\right)!(\mathrm{mod}\ p)$.

$k! = \left(\frac{p-1}{2}\right)!$ не кратно простому p.

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

$\left(\frac{a}{p}\right) \equiv (-1)^\mu(\mathrm{mod}\ p)$, но $\left(\frac{a}{p}\right) = \pm 1$, т. к. p не делит a,

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

Доказательство завершено.

Пример 68. Определить, разрешимо ли сравнение $x^2 \equiv 7(\mathrm{mod}\ 11)$.

Решение. $p = 11$, $a = 7$, $\mu = 3$, следовательно $\left(\frac{a}{p}\right) = (-1)^3 = -1$, т. е. сравнение не разрешимо.

Ответ. Сравнение не разрешимо.

Пример 69. Вычислить символ Лежандра $\left(\frac{1994}{19}\right)$.

Решение.

$\left(\frac{1994}{19}\right) = \left(\frac{18}{19}\right) = \left(\frac{3^2}{19}\right) \cdot \left(\frac{2}{19}\right) = \left(\frac{3}{19}\right)^2 \cdot \left(\frac{2}{19}\right) = \left(\frac{2}{19}\right)$,

$1994 \equiv 18(\mathrm{mod}\ 19)$. Вычислим $\left(\frac{2}{19}\right)$.

$p = 19$, $a = 2$, $\frac{p-1}{2} = 9$, $a_k = \{2; 4; 6; 8; 10; 12; 14; 16; 18\}$,

$\sigma_k \cdot m_k = \{2; 4; 6; 8; -9; -7; -5, -3; -1\}$, следовательно $\mu = 5$,

$\left(\frac{2}{19}\right) = -1$, следовательно $\left(\frac{1994}{19}\right) = -1$.

Ответ. $\left(\frac{1994}{19}\right) = -1$.

3.4.8. Квадратичный закон взаимности

Предложение. Пусть p — простое. Тогда

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 (\mathrm{mod}\ 8), \\ -1, & p \equiv \pm 3 (\mathrm{mod}\ 8). \end{cases}$$

Доказательство. По свойствам символа Лежандра
$\left(\frac{2}{p}\right) = (-1)^{\mu}$, $k \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$,
$2k \in \{2, 4, \ldots, p-1\}$, $2k \equiv \delta_k \cdot m_k (\mathrm{mod}\ p)$.
Если $2k \leqslant \frac{p-1}{2}$, то $\delta_k = 1$, если $2k > \frac{p-1}{2}$, то $\delta_k = -1$.
Рассмотрим p по mod 8, т. е. $p \equiv 1; 3; 5; 7 (\mathrm{mod}\ 8)$.
1) Если $p \equiv 1 (\mathrm{mod}\ 8)$, то $p = 1 + 8t$, следовательно
$\frac{p-1}{2} = 4t$ — четное число, следовательно для
$\frac{p-1}{2} + 2 \leqslant 2k \leqslant p-1$, т. е. для $\frac{p-1}{4} + 1 \leqslant k \leqslant \frac{p-1}{2}$, $\delta_k = -1$, следовательно количество таких $k = \mu$ равно
$\frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4} = 2t$ — четное число и $\left(\frac{2}{p}\right) = 1$.
2) Если $p \equiv -1 (\mathrm{mod}\ 8)$, то $p = -1 + 8t$, следовательно получаем $\frac{p-1}{2} = 4t - 1$ — нечетное число;
$\frac{p-1}{2} + 1 \leqslant 2k \leqslant p-1$, т. е. для $\frac{p+1}{4} \leqslant k \leqslant \frac{p-1}{2}$, $\delta_k = -1$, следовательно $\mu = \frac{p-1}{2} - \frac{p+1}{4} + 1 = 4t - 1 - 2t + 1$ — четное число и $\left(\frac{2}{p}\right) = 1$.
3) Если $p \equiv 3 (\mathrm{mod}\ 8)$, то $p = 3 + 8t$, следовательно получаем $\frac{p-1}{2} = 4t + 1$ — нечетное число, тогда по пункту 2) имеем:
$\mu = \frac{p-1}{2} - \frac{p+1}{4} + 1 = 4t - 1 - 2t + 1 + 1 = 2t + 1$ — нечетное число и $\left(\frac{2}{p}\right) = -1$.

4) Если $p \equiv -3(\mathrm{mod}\ 8)$, то $p = -3 + 8t$, следовательно получаем $\dfrac{p-1}{2} = 4t - 2$ — четное число, тогда по пункту 1) имеем:

$\mu = \dfrac{p-1}{2} - \dfrac{p-1}{4} = 4t - 2 - 2t + 1 = 2t - 1$ — нечетное число и $\left(\dfrac{2}{p}\right) = -1$.

Доказательство завершено.

Теорема 2.

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

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

3. *Если $p \neq q$ — нечетные, простые, то*

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

Формула называется квадратичным законом взаимности.

Теорема 3.

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \textit{если} \quad p \equiv 1(\mathrm{mod}\ 4), \\ -1, & \textit{если} \quad p \equiv 3(\mathrm{mod}\ 4); \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \textit{если} \quad p \equiv \pm 1(\mathrm{mod}\ 8), \\ -1, & \textit{если} \quad p \equiv \pm 3(\mathrm{mod}\ 8); \end{cases}$$

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\dfrac{p}{q}\right), & \textit{если} \quad \left[\begin{array}{l} p \equiv 1(\mathrm{mod}\ 4), \\ q \equiv 1(\mathrm{mod}\ 4); \end{array}\right. \\ -\left(\dfrac{p}{q}\right), & \textit{если} \quad \left[\begin{array}{l} p \equiv 3(\mathrm{mod}\ 4), \\ q \equiv 3(\mathrm{mod}\ 4) \end{array}\right. \end{cases}$$

— квадратичный закон взаимности.

Утверждение. *Сформулированные выше теоремы* 2 *и* 3 *равносильны.*

Доказательство.

1) Если $p \equiv 1(\text{mod } 4)$, то $p = 1 + 4t$, следовательно
$\frac{p-1}{2} = 2t$ — четное, получаем $(-1)^{\frac{p-1}{2}} = 1$.
Если $p \equiv 3(\text{mod } 4)$, то $p = 3 + 4t$, следовательно
$\frac{p-1}{2} = 2t + 1$ — нечетное, получаем
$(-1)^{\frac{p-1}{2}} = -1$.

2) Если $p \equiv \pm 1(\text{mod } 8)$, то $p = \pm 1 + 8t$, следовательно
$\frac{p^2-1}{8} = \frac{64t^2 \pm 16t + 1 - 1}{8} = 8t^2 \pm 2t$ — четное, получаем
$(-1)^{\frac{p^2-1}{8}} = 1$.
Если $p \equiv \pm 3(\text{mod } 4)$, то $p = \pm 3 + 8t$, следовательно
$\frac{p^2-1}{8} = 8t^2 \pm 6t + 1$ — нечетное, получаем
$(-1)^{\frac{p^2-1}{8}} = -1$.

3) Если $\begin{cases} p \equiv 1(\text{mod } 4) \Leftrightarrow \frac{p-1}{2} & \text{четное,} \\ q \equiv 1(\text{mod } 4) \Leftrightarrow \frac{q-1}{2} & \text{четное,} \end{cases} \Leftrightarrow (-1)^{\frac{p-1}{2} \cdot \frac{1-1}{2}} = 1.$

Если $\begin{cases} p \equiv 3(\text{mod } 4), \\ q \equiv 4(\text{mod } 4), \end{cases} \Leftrightarrow (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = -1.$

Доказательство завершено.

Рассмотрим доказательства теорем 2 и 3.

Доказательство.

Докажем теорему 2.

Пусть $p \neq q$ — нечетные, простые.

По лемме Гаусса $\left(\frac{p}{q}\right) = (-1)^{\mu}$, где μ — количество $\sigma_k = -1$ из ряда

$$q \cdot k = \left\{ q; 2q; 3q; \ldots, \frac{p-1}{2} \cdot q \right\}.$$

Пусть k — таково, что $\delta_k = -1$. Тогда $q \cdot k \equiv -m_k (\mathrm{mod}\ p)$, т. е. существует $y \in Z$, что $k \cdot q = -m_k + y \cdot p$, следовательно

$m_k = y \cdot p - k \cdot q$, но $1 \leqslant m_k \leqslant \frac{p-1}{2}$, получаем

$0 < 1 \leqslant y \cdot p - k \cdot q \leqslant \frac{p-1}{2}$, из чего следует, что

$y \cdot p \leqslant \frac{p-1}{2} + k \cdot q \leqslant \frac{p-1}{2} + \frac{p-1}{2} \cdot q = \frac{p-1}{2} \cdot (q+1) < \frac{p(q+1)}{2}$,

значит $y < \frac{q+1}{2}$.

Так как $y \in Z$, то $1 \leqslant y \leqslant \frac{q-1}{2}$, $0 < p \cdot y - k \cdot q \leqslant \frac{p-1}{2}$.

Докажем, что существует единственный $y \in Z$ для каждого k из этого условия.

Пусть существуют y_1, y_2 такие, что

$0 < y_1 \cdot p - k \cdot q \leqslant \frac{p-1}{2}, \quad 0 < y_2 \cdot p - k \cdot q \leqslant \frac{p-1}{2}$.

Обозначим $r_1 = y_1 \cdot p - k \cdot q$, $r_2 = y_2 \cdot p - k \cdot q$.

Тогда $y_1 \neq y_2$ равносильно $r_1 \neq r_2$.

Так как $0 < |r_1 - r_2| < \frac{p-1}{2}$, то $|r_1 - r_2| = |p| \cdot |y_1 - y_2|$ не кратно p. Получили противоречие, следовательно $y_1 = y_2$.

Рассмотрим μ — число пар (k, y), таких что

$$k \in \left\{ 1, 2, \ldots, \frac{p-1}{2} \right\}, \quad y \in \left\{ 1, 2, \ldots, \frac{q-1}{2} \right\}$$

и $0 < p \cdot y - k \cdot q \leqslant \frac{p-1}{2}$.

Аналогично $\left(\frac{p}{q}\right) = (-1)^{\mu'}$, где μ' — количество пар (y, k), таких что

$$k \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}, \quad y \in \left\{1, 2, \ldots, \frac{q-1}{2}\right\}$$

и $0 < k \cdot q - y \cdot p \leqslant \frac{q-1}{2}$, следовательно $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\mu+\mu'}$.

Докажем, что $\mu + \mu' \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} (\text{mod } 2)$.

Рассмотрим ограничения:

$0 < y \cdot p - k \cdot q < \frac{p}{2}$ и $0 < k \cdot q - y \cdot p < \frac{q}{2}$.

Так как $(y \cdot p - k \cdot q) \in Z$ и $y = \frac{kq}{p} - \frac{q}{p^2}$, то

$0 < y < \frac{q}{2}$ и $0 < k < \frac{p}{2}$.

Рассмотрим прямые α, β, γ.

α: $y \cdot p - k \cdot q = \frac{p}{2}$, т.е. $y = \frac{1}{2} + \frac{kq}{p}$;

β: $k \cdot q - y \cdot p = \frac{q}{2}$, т.е. $k = \frac{1}{2} + \frac{yp}{q}$;

γ: $y = \frac{kq}{p}$.

На прямых α, β, γ целых точек нет.

Тогда $\mu + \mu'$ — количество целых точек в заштрихованной области.

Треугольник выше прямой α и треугольник ниже прямой β равны по катетам и содержат одинаковое число целых точек. Во всей области ограничения штрихом (прямоугольнике) содержится $\frac{p-1}{2} \cdot \frac{q-1}{2}$ целых точек, следовательно в области $\mu + \mu'$ — количество целых точек $\equiv \frac{p-1}{2} \cdot \frac{q-1}{2} (\mathrm{mod}\ 2)$, т.е.

$\mu + \mu' \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} (\mathrm{mod}\ 2)$.

Доказательство завершено.

Теорема 3 тождественна теореме 2 по утверждению.

Следствие. Пусть $m = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$ — нечетное, НОД$(a, m) = 1$, тогда разрешимость сравнения $x^2 \equiv a (\mathrm{mod}\ m)$ равносильна условию $\left(\frac{a}{p_i}\right) = 1$ для всех $i = 1 \ldots k$, и в случае разрешимости имеет 2^k решений.

Символ Якоби.

Пусть b — нечетное, целое, $a \in Z$, $b = p_1 \cdot p_2 \cdot \ldots \cdot p_n$ — простые. Тогда

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \ldots \cdot \left(\frac{a}{p_n}\right)$$

называется *символом Якоби.*

Пример 70. $\left(\frac{2}{45}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) \cdot (-1) = -1.$

Утверждение.

1) *Если* $\left(\frac{a}{b}\right) = -1$, *то* a — *квадратичный невычет по* mod b.

2) *Если* $\left(\frac{a}{b}\right) = 1$, *то* a — *может быть квадратичным вычетом, так и квадратичным невычетом по* mod b.

Доказательство.

1) Если $\left(\frac{a}{b}\right) = -1$, следовательно существует такое p_i, что $\left(\frac{a}{p_i}\right) = -1$, $p_i|b$, следовательно $x^2 \equiv a(\text{mod } p_i)$ — не разрешимо, следовательно $x^2 \equiv a(\text{mod } p)$ — не разрешимо.

2) Если $\left(\frac{a}{b}\right) = 1$, то возможны разные варианты.

Приведем примеры для каждого случая.

а) $\left(\frac{2}{15}\right) = \left(\frac{2}{5}\right) \cdot \left(\frac{2}{3}\right) = (-1) \cdot (-1) = 1$, но $x^2 \equiv 2(\text{mod } 5)$, $x^2 \equiv 2(\text{mod } 3)$ — не разрешимо, слеовательно $x^2 \equiv 2(\text{mod } 15)$ — не разрешимо.

б) $\left(\frac{2}{7}\right) = 1$, $x^2 \equiv 2(\text{mod } 7)$ — разрешимо.

Доказательство завершено.

Свойства символа Якоби.

1. $\left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right) \cdot \left(\frac{b}{c}\right)$, при c — нечетном.
2. $\left(\frac{a}{b \cdot c}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a}{c}\right)$, при b, c — нечетном.
3. Если $a \equiv d(\text{mod } b)$, то $\left(\frac{a}{b}\right) = \left(\frac{d}{b}\right)$, при b — нечетном.
4. $\left(\frac{1}{b}\right) = 1$, при b — нечетном.
5. $\left(\frac{a \cdot b^2}{c}\right) = \left(\frac{a}{c}\right)$, если НОД$(b, c) = 1$, c — нечетное.
6. $\left(\frac{a + m \cdot b}{b}\right) = \left(\frac{a}{b}\right)$, b — нечетное.

Доказательство очевидно по определению и свойствам символа Лежандра.

Теорема (квадратичный закон взаимности для символа Якоби).

Пусть a, b *— нечетные,* НОД$(a, b) = 1$. *Тогда*

1) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} = \begin{cases} 1, & \text{если} \quad b \equiv 1 (\text{mod } 4), \\ -1, & \text{если} \quad b \equiv 3 (\text{mod } 4). \end{cases}$

2) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}} = \begin{cases} 1, & \text{если} \quad b \equiv \pm 1 (\text{mod } 8), \\ -1, & \text{если} \quad b \equiv \pm 3 (\text{mod } 8). \end{cases}$

3) $\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}} = \begin{cases} 1, & \text{если} \quad \left[\begin{array}{l} a \equiv 1 (\text{mod } 4), \\ b \equiv 1 (\text{mod } 4); \end{array}\right. \\ -1, & \text{если} \quad \left[\begin{array}{l} a \equiv 3 (\text{mod } 4), \\ b \equiv 3 (\text{mod } 4). \end{array}\right. \end{cases}$

Следствие. Если $\left(\frac{a}{m}\right) = -1$, то сравнение $x^2 \equiv a (\text{mod } m)$ — не разрешимо (где m — нечетное).

Пример 71. Вычислить символ Якоби.

1. $\left(\frac{1995}{1993}\right) = \left(\frac{2}{1993}\right) = 1$, так как $1993 \equiv 1 (\text{mod } 8)$.

2. $\left(\frac{1990}{1993}\right) = \left(\frac{2 \cdot 5 \cdot 199}{1993}\right) = \left(\frac{2}{1993}\right) \cdot \left(\frac{5}{1993}\right) \cdot \left(\frac{199}{1993}\right) =$
$= 1 \cdot \left(\frac{1993}{5}\right)\left(\frac{1993}{199}\right) = \left(\frac{3}{5}\right) \cdot (-1)\left(\frac{199}{3}\right) = \left(\frac{2}{3}\right) \cdot (-1) \cdot \left(\frac{1}{3}\right) =$
$= (-1) \cdot (-1) = 1$, так как
$5 \equiv 1 (\text{mod } 4)$, $1993 \equiv 1 (\text{mod } 4)$,
$3 \equiv 3 (\text{mod } 4)$, $199 \equiv 3 (\text{mod } 4)$.

3. $\left(\frac{1992}{1997}\right) = \left(\frac{2 \cdot 2 \cdot 2 \cdot 3 \cdot 83}{1997}\right) = \left(\frac{2}{1997}\right)^3 \cdot \left(\frac{3}{1997}\right) \cdot \left(\frac{83}{1997}\right) =$
$= (-1) \cdot \left(\frac{1997}{3}\right) \cdot \left(\frac{83}{1997}\right) = (-1) \cdot \left(\frac{2}{3}\right) \cdot \left(\frac{5}{83}\right) = \left(\frac{5}{83}\right) = \left(\frac{83}{5}\right) =$
$= \left(\frac{3}{5}\right) = \left(\frac{2}{3}\right) = -1$, так как
$1997 \equiv 5 (\text{mod } 8)$, $1997 \equiv 1 (\text{mod } 4)$.

Пример 72.
Сколько решений имеют сравнения:

1. $x^2 \equiv 219(\text{mod } 383)$.
   $\left(\frac{219}{383}\right) = 1$, следовательно решение существует, т.к. 383 — простое, следовательно 2 решения.

2. $x^2 \equiv 59(\text{mod } 375)$.
   $\left(\frac{59}{375}\right) = \left(\frac{4}{5}\right) = 1$; $\left(\frac{59}{3}\right) = \left(\frac{1}{3}\right) = 1$, следовательно 4 решения.
   $375 = 5 \cdot 75 = 5 \cdot 5^2 \cdot 3 = 5^3 \cdot 3$.

3. $\left(\frac{3766}{5987}\right) = -1$, следовательно решений нет.

Общий итог для сравнений $f(x) \equiv 0(\text{mod } m)$

1. $x^d \equiv 1(\text{mod } p)$, где p — простое: если $d|(p-1)$, то существует d решений.
   $x^2 \equiv 1(\text{mod } p)$ — всегда имеет 2 решения $x = \pm 1(\text{mod } p)$.

2. $x^2 \equiv a(\text{mod } p) \Leftrightarrow a^{\frac{p-1}{2}}$ и имеет 2 решения.

3. Если $f(x) \equiv 0(\text{mod } p)$ и $f'(x) \equiv 0(\text{mod } p)$ не имеют общих решений, то $f(x) \equiv 0(\text{mod } p)$ и $f(x) \equiv 0(\text{mod } p^m)$ имеют одинаковое число решений x_0: $f'(x_0)t \equiv -\frac{f(x_0)}{p}(\text{mod } p)$.

4. $x^n \equiv a(\text{mod } p^m)$ имеет столько же решений, что и
   $x^n \equiv a(\text{mod } p)$, если p не делит a и p не делит n.

5. $x^n \equiv a(\text{mod } m)$ при $m = 2, 4, p^\alpha, 2p^\alpha$ разрешимо тогда и только тогда, когда $a^{\frac{\varphi(m)}{d}} \equiv 1(\text{mod } m)$, где $d = \text{НОД}(n, \varphi(m))$, в случае разрешимости существует d решений.

6. $x^n \equiv a(\mathrm{mod}\ 2^\alpha)$, $\alpha \geqslant 2$, $d = \mathrm{НОД}(n, 2^{\alpha-2})$.

   a) Если n — нечетное, то существует единственное решение.

   b) Если n — четное, то существует $2d$ решений тогда и только тогда, когда

$$\begin{cases} a \equiv 1(\mathrm{mod}\ m), \\ a^{\frac{2^{\alpha-2}}{d}} \equiv 1(\mathrm{mod}\ 2^\alpha); \end{cases}$$

   При этом, если $n = 2^k \cdot n_1$ и $\mathrm{НОД}(n_1, 2) = 1$, то решения сравнения находятся следующим образом:

$$x \equiv \pm\left(x_0 + \frac{x_0^n - a}{2^k} + r \cdot 2^{\alpha-k}\right)(\mathrm{mod}\ 2^\alpha),$$

   где $r = 0, \ldots, 2^k - 1$, а x_0 — решение сравнения $x^n \equiv a(\mathrm{mod}\ 2^{\alpha-1})$.

7. $x^2 \equiv a(\mathrm{mod}\ 2^\alpha)$, a — нечетное, то

   a) если $\alpha = 1$, существует единственное решение;

   b) если $\alpha = 2$, существует два решения тогда и только тогда, когда $a \equiv 1(\mathrm{mod}\ 4)$;

   c) если $\alpha \geqslant 3$, существует четыре решения тогда и только тогда, когда $a \equiv 1(\mathrm{mod}\ 8)$.

8. $x^2 \equiv a(\mathrm{mod}\ p)$ — разрешимо тогда и только тогда, когда $\left(\frac{a}{p}\right) = 1$.

   $x^2 \equiv a(\mathrm{mod}\ m)$ — не разрешимо тогда и только тогда, когда $\left(\frac{a}{m}\right) = -1$, где m— нечетное.

Задачи для самостоятельного решения.

1. Покажите, что для любого целого $n \geqslant 1$ выполняется:

$$n^6 + 2n^5 - n^2 - 2n \equiv 0(\text{mod } 120).$$

2. Найдите группу Z_{20}^* обратимых элементов кольца Z_{20} и все ее подгруппы. Указать цикличность группы. Найти все образующие.

3. Найти все примитивыне корни по модулю $m = 46$.

4. Найдите сравнение степени ниже p, равносильное данному:

$$x^6 - 4x^4 + x^3 - 2x^2 + 5 \equiv 0(\text{mod } 5),$$

если $p = 5$.

5. Найдите сравнение со старшим коэффициентом равным 1, равносильное данному:

$$2x^5 - 9x^4 + 2x^3 + 37x^2 + 10x - 14 \equiv 0(\text{mod } 7).$$

6. Решите сравнение $f(x) \equiv 0(\text{mod } 125)$, используя решение сравнения $f(x) \equiv 0(\text{mod } 5)$, если $f(x) = x^3 + 2x + 5$.

7. Решите сравнение по составному модулю:

$$x^4 - 2x^3 - 8x^2 + 13x - 24 \equiv 0(\text{mod } 30).$$

8. Найдите индекс числа $a = 528$ при основании $g = 3$ по модулю $m = 5$.

9. Найдите число решений сравнения:

   а) $x^2 \equiv -9(\text{mod } 221)$; b) $x^{10} \equiv 1(\text{mod } 31)$.

10. Решите сравнение второй степени:

    а) $x^2 \equiv 1(\text{mod } 44)$; b) $x^2 \equiv 1(\text{mod } 121)$.

11. Решите сравнение $x^2 \equiv 59 (\mathrm{mod}\ 125)$ тремя различными способами.

12. Вычислите символ Якоби:
a) $\left(\frac{1951}{2549}\right)$; b) $\left(\frac{1092}{1381}\right)$.

13. Найдите систему индексов числа a по модулю m, если $a = 33$, $m = 28$.

Литература

1. Баранова Н. А. Банникова Т. М. Теория чисел : учеб.-метод. пособие / Т. М. Банникова, Н. А. Баранова. — Ижевск, 2007. — 51 с.

2. Боревич З. И., Шафаревич И. Р. Теория чисел. — М.: Наука, 1972. — 510 с.

3. Боро В., Цагир Д., Рольфс Ю., Крафт Ч., Янцен Е. Живые числа. М., Мир, 1985.

4. Василенко О.Н Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003.

5. Виноградов И. М. Основы теории чисел. М., Наука, 1981.

6. Грэхем Р. Начала теории Рамсея. М., Мир, 1984. К. Айерлэнд, М. Роузен Классическое введение в современную теорию чисел = A Classical Introduction to Modern Number Theory. — М.: Мир, 1987.

7. Карацуба А. А. Основы аналитической теории чисел. М., Наука, 1975.

8. Клейн Ф. Элементарная математика с точки зрения высшей. М., Наука, 1987.

9. Коблиц Н. Курс теории чисел и криптографии / Пер. с англ. М. А. Михайловой и В. Е. Тараканова под ред. А. М. Зубкова. — М.: Научное изд-во ТВП, 2001.

10. Кострикин А. И. Введение в алгебру. М., Наука, 1977.

11. Кох Х. Алгебраическая теория чисел. — ВИНИТИ, 1990. - Т. 62. — 301 с. — (Итоги науки и техники. Серия «Современные проблемы математики. Фундаментальные направления»).

12. Манин Ю. И., Панчишкин А. А. Введение в теорию чисел. — ВИНИТИ, 1990. — Т. 49. — 341 с. — (Итоги науки и техники. Серия «Современные проблемы математики. Фундаментальные направления»).

13. Маркушевич А. И. Краткий курс теории аналитических функций. М., Наука, 1978.

14. Мерзляков А. С., Баранова Н. А. Банникова Т. М. Алгебра : учеб.-метод. комплекс для напр. 511200 «Математика. Приклад. математика» / УдГУ, Матем. фак., Каф. алгебры и топологии; сост.: А. С. Мерзляков, Н.А. Баранова, Т. М. Банникова. — Ижевск, 2008. — 48 с.

15. Пойа Д. Математика и правдоподобные рассуждения. М., Наука, 1975.

16. Серр Ж. П. Курс арифметики. М., Мир, 1982.

17. Сизый С. В. Лекции по теории чисел: Учебное пособие для математических специальностей. Екатеринбург: Уральский государственный университет им. А. М. Горького, 1999.

18. Сизый С. В., Савинов В. Б., Сафронович Е. Л., Спевак Л. Ф., Дунаев М. В. Книжка, прочитанная вслух. Екатеринбург, УрГУ, 1995.

19. Стройк Д. Я. Краткий очерк истории математики. М., Наука, 1990.

20. Тронин С. Н. Введение в теорию групп. Задачи и теоремы. Часть 1: Учебное пособие. — Казань: Казанский государственный университет им. В.И. Ульянова-Ленина, 2006. — 100 с.

21. Фаддеев Д. К. Лекции по алгебре. М., Наука, 1984.

22. Фельдман Н. И. Седьмая проблема Гильберта. Изд-во МГУ, 1982.

23. Хинчин А. Я. Три жемчужины теории чисел. — М.: Наука, 1979. — 64 с.

24. Хинчин А. Я. Цепные дроби. М., Гос. Изд-во Физ.-Мат. Лит., 1961.

25. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. — М.: МЦНМО, 2002. Доступно с *http://www.cryptography.ru/*

26. Шклярский Д. О., Ченцов Н. Н., Яглом И. М. Избранные задачи и теоремы элементарной математики. М., Наука, 1976.

Татьяна Михайловна Банникова
Наталья Анатольевна Баранова

Основы теории чисел

Учебно-методическое пособие

Напечатано в авторской редакции
с оригинал-макета заказчика

Подписано в печать _____ Формат $60 \times 84\ 1/16$

Печать офсетная. Уч.-изд. л. 2,9. Усл. п.л. 3,02.
Тираж 100 экз. Заказ № _____.

Редакционно-издательский отдел
ГОУВПО «Удмуртский государственный университет»

Типография ГОУВПО «Удмуртский государственный университет»
426034, г. Ижевск, ул. Университетская, 1, корп. 4.