С. А. Степанов,

кандидат физико-математических наук

СРАВНЕНИЯ

ИЗДАТЕЛЬСТВО «ЗНАНИЕ»
Москва 1975

51
С79

Степанов С. А.
С79 Сравнения. М., «Знание», 1975
64 с. (Новое в жизни, науке, технике. Серия «Математика, кибернетика», 11. Издается ежемесячно с 1967 г.)

Брошюра знакомит читателя с основами теории сравнений, одной из интересных и важных областей математического знания. Доступное изложение современного состояния теории сравнений стало возможно благодаря работам автора брошюры, создавшего новый арифметический метод доказательства всех ее результатов. Ранее это было под силу лишь сложному аппарату алгебраической геометрии.

20200 51

ПРЕДИСЛОВИЕ

Теория сравнений — наука о целых числах, рассматриваемых в их связи с остатками от деления на фиксированное натуральное число, называемое модулем. Созданная трудами Ферма, Эйлера, Лежандра, Лагранжа, К. Гаусса и Дирихле теория сравнений обогатила математику многими новыми понятиями; ее идеи и методы давно вышли за пределы теории чисел и проникли в алгебру, алгебраическую геометрию, теорию кодирования, кибернетику, вычислительную технику.

Возникновение теории сравнений связано с изучением диофантовых уравнений. Ясно, что для разрешимости диофантова уравнения необходима разрешимость соответствующего сравнения по любому модулю. Во многих случаях оказывается, что локальная разрешимость, т. е. разрешимость соответствующего сравнения по всем модулям, является также и достаточным условием для разрешимости диофантова уравнения. Например, справедлива следующая теорема, доказанная Лежандром.

Теорема. *Если a, b, c — попарно взаимно простые целые числа, свободные от квадратов и не все одного знака, то уравнение*

$$ax^2 + by^2 + cz^2 = 0$$

разрешимо в целых числах тогда и только тогда, когда разрешимы сравнения

$$x^2 \equiv -bc \pmod{a}$$
$$y^2 \equiv -ca \pmod{b}$$
$$z^2 \equiv -ab \pmod{c}$$

Разрешимость указанных в теореме сравнений для каждого конкретного набора чисел a, b, c можно установить хотя бы простым перебором. Следовательно, теорема Лежандра

дает простой и эффективный критерий разрешимости диофантова уравнения $ax^2 + by^2 + cz^2 = 0$.

Другим примером может служит такое утверждение: *целое число вида $4k + 3$ нельзя представить суммой двух квадратов целых чисел.* Действительно, если бы это было возможно, то было бы разрешимо сравнение

$$x^2 + y^2 \equiv 3 \pmod{4}.$$

Но простая проверка показывает, что последнее сравнение не имеет решений, и мы приходим к противоречию.

Рассмотрение задач подобного рода в дальнейшем привело Гензеля к введению нового типа чисел, названных им p-адическими числами. В настоящее время p-адические числа являются одним из основных инструментов теории чисел и смежных с ней разделов математики.

Другим важным понятием, появлением которого мы обязаны теории сравнений, являются конечные поля (поля Галуа). Сфера их применения с каждым днем расширяется и охватывает не только математику, но и физику, кибернетику, радио и вычислительную технику.

Как самостоятельная наука теория сравнений имеет свои собственные трудные и интересные проблемы. К таким проблемам относится, например, знаменитая гипотеза И. М. Виноградова о распределении квадратичных вычетов и невычетов в натуральном ряде, гипотеза Артина о первообразных корнях и др.

В настоящей брошюре популярно и достаточно полно изложены все основные вопросы теории сравнений, начиная с простейших понятий и определений и кончая самыми последними достижениями. Доступное широкому кругу читателей изложение современного состояния теории сравнений стало возможно благодаря трудам автора С. А. Степанова, создавшего новый арифметический метод, с помощью которого элементарно доказаны все результаты, которые ранее были под силу лишь сложному аппарату алгебраической геометрии.

Книга будет интересна всем, кто любит математику, пытается узнавать новое и размышлять над нерешенными задачами.

Проф. *А. А. Карацуба.*

Глава 1

ОСНОВНЫЕ ПОНЯТИЯ

1. Мы будем рассматривать целые числа в связи с их остатками от деления на данное положительное число m, которое назовем *модулем*. Каждому целому числу a отвечает определенный остаток $r = a - mq$, $0 \leqslant r \leqslant m-1$ от деления его на m; если двум целым числам a и b отвечает один и тот же остаток r, то они называются *равноостаточными по модулю m*, или *сравнимыми по модулю m*. Для обозначения сравнимости чисел a и b употребляется символ $a \equiv b \pmod m$. Ясно, что $a \equiv b \pmod m$ тогда и только тогда, когда разность $a - b$ делится на m. Если $a - b$ не делится на m, то мы говорим, что a и b *несравнимы* по модулю m, и записываем это следующим образом: $a \not\equiv b \pmod m$.

Отношение сравнимости по модулю m является отношением эквивалентности; оно рефлексивно, так как $a \equiv a \pmod m$ симметрично, поскольку из $a \equiv b \pmod m$ следует $b \equiv a \pmod m$, транзитивно, так как из $a \equiv b \pmod m$ и $b \equiv c \pmod m$ следует $a \equiv c \pmod m$. Тем самым отношение «$\equiv \pmod m$» разбивает множество всех целых чисел на непересекающиеся классы эквивалентности $A, B, C, \ldots$, причем два целых числа сравнимы между собой по модулю m тогда и только тогда, когда они лежат в одном и том же классе. Эти классы называются *классами вычетов по модулю m*.

Очевидно, что целые числа $0, 1, \ldots, m-1$ лежат в разных классах вычетов, и так как каждое целое число сравнимо по модулю m с одним из этих чисел, то имеется точно m классов вычетов по модулю m.

Подобно обычным равенствам сравнения можно складывать, вычитать и перемножать. Если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то $a \pm c \equiv b \pm d \pmod m$ и $ac \equiv bd \pmod m$. Действительно, если $a - b = mq$, $c - d = mt$, то $(a-b) \pm (c-d) = (q \pm t)m$. Далее, $(a-b)c = mqc$, так что $ac \equiv bc \pmod m$ и $(c-d)b = mtb$, так что $bc \equiv bd \pmod m$, откуда по свойству транзитивности $ac \equiv bd \pmod m$.

В общем случае делить сравнения нельзя. Мы имеем $36 \equiv 16 \pmod{10}$, $12 \equiv 2 \pmod{10}$, но $3 \not\equiv 8 \pmod{10}$. Однако обе части сравнения можно сократить на множитель, взаимно простой с модулем.

Операции сложения, вычитания и умножения сравнеиий индуцируют аналогичные операции на множестве классов вычетов. Пусть A и B — два класса вычетов по модулю m. Каковы бы ни были числа $a \in A$ и $b \in B$ (запись $a \in A$ означает, что a является элементом множества A), их сумма $a + b$ всегда лежит в одиом и том же классе вычетов C, который мы иазовем *суммой* $C = A + B$ классов A и B. Аналогичным образом определяются *разность* $A - B$ и *произведение* AB двух классов вычетов по модулю m. Для дальнейшего нам потребуются некоторые алгебраические понятия.

Множество G с заданной на нем бинарной операцией xy, ставящей в соответствие каждой паре элементов x, y этого множества некоторый вполне определенный третий элемент $z = xy$ из G, называется *группой*, если:

1) операция ассоциативна, т. е. $(ab)c = a(bc)$ для любых $a, b, c \in G$;

2) в G существует такой элемент e, называемый *единицей*, что $ae = ea = a$ для любого $a \in G$;

3) для любого элемента $a \in G$ существует такой элемент $x \in G$, называемый *обратным* к a, что $ax = xa = e$.

Наряду с указанной выше мультипликативной записью ab групповой операции, называемой умножением, употребляется также аддитивная запись $a + b$, которая называется сложением. В этом случае роль единичного элемента играет нулевой элемент 0 группы G.

Группа G называется *абелевой*, если имеет место коммутативный закон $ab = ba$ для любых элементов $a, b \in G$.

Произведение n элементов, равных a, называется n-й степенью элемента a и обозначается a^n. Наименьшее натуральное число n такое, что $a^n = e$ называется *порядком элемента a*.

Группа G называется циклической, если она состоит из степеней a^n, $n = 0, \pm 1, \pm 2, \ldots$ одного и того же элемента a.

Группа G называется *конечной*, если она состоит из конечного числа элементов. Число элементов конечной группы называется *порядком* этой группы.

Пример 1. Множество целых чисел образует группу относительно сложения.

Пример 2. Множество рациональных чисел образует группу относительно сложения, а множество отличных от нуля рациональных чисел образует группу относительно умножения. Аналогичные утверждения справедливы для вещественных и комплексных чисел.

Множество R с заданными на нем двумя бинарными операциями сложения и умножения называется *кольцом*, если:

1) R является абелевой группой относительно сложения;

2) умножение ассоциативно и имеет единичный элемент e;

3) операции сложения и умножения связаны дистрибутивным законом $(x + y)z = xz + yz$, $z(x + y) = zx + zy$ для любых $x, y, z \in R$.

Кольцо R называется *коммутативным*, если $xy = yx$ для всех $x, y, \in R$.

Коммутативное кольцо, в котором $e \neq 0$ и в котором ненулевые элементы образуют группу по умножению, называется *полем*. Поле называется *конечным*, если оно состоит из конечного числа элементов.

Пример 3. Множество целых чисел образует коммутативное кольцо. Множество рациональных чисел является полем.

Легко проверить, что классы вычетов по модулю m образуют относительно сложения абелеву группу. Нулевым элементом этой группы является класс вычетов, состоящий из всех целых чисел кратных m, а обратным к классу A является класс — A, состоящий из всех элементов класса A, взятых со знаком минус. Более того, классы вычетов по модулю m образуют коммутативное кольцо. Единичным элементом служит класс E, содержащий целое число 1, а дистрибутивный закон $A(B + C) = AB + AC$ непосредственно следует из дистрибутивного закона для целых чисел.

Любое число класса вычетов по модулю m называется *вычетом* по модулю m. Вычет r, $0 \leqslant r \leqslant m - 1$, равный остатку от его деления на модуль m, называется *наименьшим неотрицательным вычетом*. Вычет ρ, наименьший по

абсолютной величине, называется *абсолютно наименьшим вычетом*. При $r < \frac{m}{2}$ имеем $\rho = r$; при $r > \frac{m}{2}$ имеем $\rho < r - m$; наконец, если m четное и $r = \frac{m}{2}$, то за ρ можно взять любое из двух чисел $\frac{m}{2}$ и $-\frac{m}{2}$.

Взяв из каждого класса вычетов по одному представителю, получим *полную систему вычетов по модулю m*. Таким образом, множество из m целых чисел образует полную систему вычетов по модулю m тогда и только тогда, когда его элементы несравнимы друг с другом по модулю m. Чаще всего в качестве полной системы вычетов употребляются наименьшие неотрицательные вычеты $0, 1, \ldots, m - 1$ или абслютно наименьшие вычеты, состоящие из чисел $0, \pm 1, \ldots, \pm \frac{m-1}{2}$ в случае нечетного m и чисел $0, \pm 1, \ldots, \pm \frac{m-2}{2}, \frac{m}{2}$ или $0, \pm 1, \ldots, \pm \frac{m-2}{2}, -\frac{m}{2}$ в случаях четного m.

Классы вычетов по модулю m, элементы которых взаимно просты с m, назовем *приведенными классами вычетов*. Взяв из каждого такого класса по одному вычету, получим *приведенную систему вычетов по модулю m*. Приведенную систему вычетов можно составить из чисел полной системы вычетов $0, 1, \ldots, m - 1$, взаимно простых с модулем m. Следовательно, приведенная система вычетов по модулю m состоит из $\varphi(m)$ элементов, где $\varphi(m)$ — *функция Эйлера*, равная количеству неотрицательных целых чисел, меньших m и взаимно простых с m.

Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ — многочлен с целыми коэффициентами. *Решением* сравнения $f(x) \equiv 0 \pmod m$ назовем всякий класс вычетов $x \equiv x_1 \pmod m$ такой, что $f(x_1) \equiv 0 \pmod m$ для целого числа x_1.

Обозначим через (a, b) наибольший общий делитель a и b. Если $(a, m) = 1$ и x пробегает приведенную систему вычетов по модулю m, то ax также пробегает приведенную систему вычетов по модулю m. Действительно, чисел ax столько же, сколько и чисел x, т. е. $\varphi(m)$. Далее, числа ax несравнимы между собой по модулю m и взаимно просты с m. Следовательно, сравнение $ax \equiv 1 \pmod m$ имеет единственное решение $x \equiv x_1 \pmod m$ такое, что $(x_1, m) = 1$. Другими словами, если A, X — приведенные классы вы-

четов и E — класс вычетов, содержащий число 1, то уравнение $AX = E$ разрешимо и тем самым приведенные классы вычетов по модулю m образуют по умножению абелеву группу порядка $\varphi(m)$, единичным элементом которой является класс E.

Далее, если $(a, m) = 1$ и x пробегает приведенную систему вычетов, состоящую из наименьших неотрицательных вычетов $r_1, r_2, \ldots, r_{\varphi(m)}$, то наименьшие неотрицательные вычеты ax состоят из тех же чисел $r_1, r_2, \ldots, r_{\varphi(m)}$. Следовательно,

$$r_1 r_2 \ldots r_{\varphi(m)} \equiv a r_2 \ldots a r_{\varphi(m)} \pmod{m}$$

или

$$(a^{\varphi(m)} - 1) r_1 r_2 \ldots r_{\varphi(m)} \equiv 0 \pmod{m}.$$

Но $r_1, r_2, \ldots, r_{\varphi(m)}$ взаимно просты с модулем m, тогда $a^{\varphi(m)} \equiv 1 \pmod{m}$. Тем самым нами установлен следующий результат.

Теорема Эйлера. *Если a взаимно просто с m, то* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Рассмотрим теперь кольцо классов вычетов по простому модулю p. В этом случае все классы вычетов, за исключением нулевого, будут приведенными и, следовательно, образуют по умножению абелеву группу. Таким образом, *классы вычетов по простому модулю p образуют конечное поле из p элементов.* В дальнейшем мы будем обозначать это поле через F_p и его единичный элемент через 1.

В случае простого модуля p имеет место следующее утверждение, являющееся частным случаем теоремы Эйлера.

Малая теорема Ферма. *Если a не делится на простое число p,* то $a^{p-1} \equiv 1 \pmod{p}$.

Из этой теоремы следует, что $a^p \equiv a \pmod{p}$ для любого целого a. Другими словами, каждый элемент поля классов вычетов по простому модулю p удовлетворяет уравнению $x^p - x = 0$.

Для дальнейшего выяснения структуры поля классов вычетов по простому модулю p нам потребуется понятие первообразного корня. *Первообразным корнем по модулю m* называется такое целое число g, что $g^{\varphi(m)} \equiv 1 \pmod{m}$ и $g^\delta \not\equiv 1 \pmod{m}$ при $1 \leqslant \delta \leqslant \varphi(m) - 1$. Существование первообразных корней для всех простых модулей p устанавливает следующая теорема, принадлежащая Гауссу.

Теорема. *Имеется $\varphi(p-1)$ первообразных корней по простому модулю p.*

Доказательство этой теоремы мы приведем в следующем параграфе для более общего случая произвольных конечных полей.

Из теоремы Гаусса следует, что *мультипликативная группа поля классов вычетов по простому модулю p является циклической группой порядка $p - 1$.*

2. В заключение главы остановимся на вопросе о количестве решений алгебраических сравнений $f(x) \equiv 0 \pmod{p}$ по простому модулю p, где $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ — многочлен с целыми коэффициентами и $a_0 \not\equiv 0 \pmod{p}$.

Два целочисленных многочлена $f(x)$ и $g(x)$ назовем сравнимыми по модулю p (точнее, их следовало бы называть тождественно сравнимыми), если все коэффициенты их разности $f(x) - g(x)$ делятся на p. Для обозначения сравнимости многочленов $f(x)$ и $g(x)$ мы будем использовать тот же символ $f(x) \equiv g(x) \pmod{p}$, что и для обозначения сравнимости чисел.

Мы скажем, что класс вычетов $x \equiv x_1 \pmod{p}$ является *s-кратным решением* сравнения $f(x) \equiv 0 \pmod{p}$, если имеет место разложение $f(x) \equiv (x - x_1)^s g(x) \pmod{p}$, где $s \geqslant 1$ и $g(x)$ — многочлен с целыми коэффициентами, такой, что $g(x_1) \not\equiv 0 \pmod{p}$.

В качестве общего результата о количестве решений сравнения $f(x) \equiv 0 \pmod{p}$ укажем следующую теорему.

Теорема Лагранжа. *Количество решений сравнения $f(x) = 0 \pmod{p}$ по простому модулю p, взятых с их кратностями, не превосходит степени n многочлена* $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$, $a_0 \not\equiv 0 \pmod{p}$.

Теорему легко доказать индукцией по степени n многочлена $f(x)$. Для $n = 1$ утверждение теоремы очевидно, поскольку $(a_0, p) = 1$. Если сравнение $f(x) \equiv 0 \pmod{p}$ степени $n > 1$ имеет s-кратное решение $x \equiv x_1 \pmod{p}$, то $f(x) \equiv (x - x_1)^s g(x) \pmod{p}$, где $g(x)$ — многочлен степени $n - s$. Следовательно, каждое решение сравнения $f(x) \equiv 0 \pmod{p}$ удовлетворяет или сравнению $x - x_1 \equiv 0 \pmod{p}$, которое дает исходное решение $x \equiv x_1 \pmod{p}$, или сравнению $g(x) \equiv 0 \pmod{p}$, которое по индуктивному предположению имеет не более $n - s$ решений. Тем самым сравнение $f(x) \equiv 0 \pmod{p}$ имеет самое большее n решений.

Заметим, что сравнение $f(x) \equiv 0 \pmod{p}$ мы можем трактовать как уравнение $f(x) = 0$ над полем классов вычетов по простому модулю p. При такой интерпретации

теорема Лагранжа выражает широко известный факт, что число корней не равного нулю многочлена $f(x)$ с коэффициентами из произвольного поля не превосходит степени n многочлена $f(x)$.

Далее, из теорем Лагранжа и Ферма следует, что $x^p - x \equiv x(x-1)\ldots(x-p+1) \pmod p$. Действительно, сравнение $x^p - x - x(x-1)\ldots(x-p+1) \equiv 0 \pmod p$ имеет по теореме Ферма p решений, в то время как степень многочлена $x^p - x - x(x-1)\ldots(x-p+1)$ не выше $p-1$. Значит, все коэффициенты этого многочлена должны делиться на p. В частности, сравнивая коэффициенты при первой степени x, мы получаем *теорему Вильсона*: $(p-1)! \equiv -1 \pmod p$.

Рассмотрим теперь *двучленные сравнения* $x^n \equiv a \pmod p$, где $a \not\equiv 0 \pmod p$. Пусть g — первообразный корень по модулю p и пусть $x \equiv g^y \pmod p$, $a \equiv g^l \pmod p$. Тогда сравнение $x^n \equiv a \pmod p$ эквивалентно линейному сравнению $ny \equiv l \pmod{p-1}$.

Покажем, что линейное сравнение $ax \equiv b \pmod m$ не имеет решений, если b не делится на $d = (a, m)$, и имеет d решений, если b делится на d. Предположим сначала, что $d = 1$. В этом случае, когда x пробегает полную систему вычетов по модулю m, произведение ax также пробегает полную систему вычетов и, следовательно, сравнение $ax \equiv b \pmod m$ имеет единственное решение. Пусть $d > 1$. Из равенства $ax - b = mq$ следует, что сравнение $ax \equiv b \pmod m$ разрешимо лишь тогда, когда b делится на d. При выполнении этого условия мы имеем $\frac{a}{d}x - \frac{b}{d} = \frac{m}{d}q$, причем $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$. Значит, сравнение $\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right)$ имеет единственное решение $x \equiv x_1 \left(\mathrm{mod}\ \frac{m}{d}\right)$, которое дает d решений $x \equiv x_1 \pmod m$, $x \equiv x_1 + \frac{m}{d} \pmod m$, . . . , $x \equiv x_1 + \frac{(d-1)m}{d} \pmod m$. Отсюда следует справедливость следующего утверждения.

Критерий Эйлера. *Пусть p — простое число и $q = (n, p-1)$. Сравнение $x^n \equiv a \pmod p$ разрешимо тогда и только тогда, когда $a^{\frac{p-1}{q}} \equiv 1 \pmod p$ и в случае разрешимости имеет q различных решений.*

Если сравнение $x^n \equiv a \pmod p$, где $a \not\equiv 0 \pmod p$, разрешимо, то a *называется вычетом степени* n по модулю p. В противном случае a называется *невычетом степени* n по модулю p. В частности, при $n = 2$ вычеты и невычеты называются *квадратичными*, при $n = 3$ — *кубическими*, при $n = 4$ — *биквадратичными*.

Заметим, что если a — квадратичный вычет, то сравнение $x^2 \equiv a \pmod p$ имеет два решения: $x \equiv x_0 \pmod p$ и $x \equiv -x_0 \pmod p$; если же a делится на p, то сравнение $x^2 \equiv a \pmod p$ имеет единственное решение: $x \equiv 0 \pmod p$.

Введем, наконец, в рассмотрение *символ Лежандра* $\left(\frac{a}{p}\right)$, который определяется для всех целых a следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \text{ является квадратичным вычетом по модулю } p; \\ -1, & \text{если } a \text{ является квадратичным невычетом по модулю } p; \\ 0, & \text{если } a \text{ делится на } p. \end{cases}$$

Если p — нечетное простое число, то для каждого $a \not\equiv 0 \pmod p$ мы имеем по теореме Ферма $a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p$, причем $a^{\frac{p-1}{2}} - 1$ и $a^{\frac{p-1}{2}} + 1$ не делятся одновременно на p (иначе их разность 2 делилась бы на p). Это замечание позволяет, в случае $n = 2$, следующим образом переформулировать критерий Эйлера:

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

Отсюда мы легко выводим, что $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ для любых двух целых a, b и что $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ при $a \equiv b \pmod p$. Кроме того, из критерия Эйлера следует, что если g — первообразный корень по модулю p, то $\left(\frac{g}{p}\right) = -1$ и, следовательно, $g^y \equiv a^2 \pmod p$ тогда и только тогда, когда y является четным числом. Отсюда следует, что среди чисел $x = 1, 2, \ldots, p-1$ имеется в точности $\frac{p-1}{2}$ квадра-

тичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов по простому модулю $p > 2$.

Более полное изложение основных понятий теории сравнений читатель может найти в книге И. М. Виноградова [1].

Глава 2

СРАВНЕНИЯ ПО ДВОЙНОМУ МОДУЛЮ И КОНЕЧНЫЕ ПОЛЯ

1. Пусть F_p — поле классов вычетов по простому модулю p. Рассмотрим кольцо $F_p[x]$ многочленов от переменного x с коэффициентами из поля F_p. Элементы поля F_p назовем константами кольца $F_p[x]$ и единичный элемент F_p обозначим через 1.

Мы скажем, что многочлен $g(x)$ делится на многочлен $f(x)$ в кольце $F_p[x]$, если существует многочлен $h(x)$ с коэффициентами из F_p, такой, что $g(x) = f(x)\,h(x)$. Если многочлен $f(x)$ не имеет других делителей, кроме $\alpha f(x)$ и α, где $\alpha \in F_p$, то $f(x)$ называется *неприводимым многочленом* в $F_p[x]$. Далее, *наибольшим общим делителем* двух многочленов $f(x)$ и $g(x)$ называется такой многочлен $d(x)$, который является их общим делителем и вместе с тем делится на любой другой общий делитель этих многочленов. Заметим, что наибольший общий делитель определен с точностью до постоянного множителя $\alpha \in F_p$, $\alpha \neq 0$. Если многочлены $f(x)$ и $g(x)$ не имеют общих делителей, отличных от констант, то они называются *взаимно простыми*.

С помощью алгоритма Эвклида легко показать, что если $d(x)$ есть наибольший общий делитель многочленов $f(x)$ и $g(x)$, то в кольце $F_p[x]$ можно найти такие многочлены $u(x)$ и $v(x)$, что $f(x)u(x) + g(x)v(x) = d(x)$, причем если степени многочленов $f(x)$ и $g(x)$ больше нуля, многочлены $u(x)$ и $v(x)$ можно выбрать такими, что степень $u(x)$ меньше степени $g(x)$, а степень $v(x)$ меньше степени $f(x)$. Отсюда следует, в частности, что если произведение $g(x)h(x)$ многочленов $g(x)$ и $h(x)$ делится в кольце $F_p[x]$ на неприводимый многочлен $f(x)$, то либо $g(x)$, либо $h(x)$ делится на $f(x)$. Действительно, если, например, $f(x)$ не делит $g(x)$, то $f(x)u(x) + g(x)v(x) = 1$.

В таком случае $h(x)f(x)u(x) + h(x)g(x)v(x) = h(x)$, тогда $f(x)$ делит $h(x)$. Как следствие мы получаем отсюда следующий результат: *для каждого многочлена $a(x)$ кольца $F_p[x]$ имеет место разложение $a(x) = f_1(x)^{\alpha_1} \ldots f_s(x)^{\alpha_s}$ на неприводимые сомножители $f_1(x), \ldots, f_s(x)$, причем такое разложение с точностью до констант кольца $F_p[x]$ и порядка следования сомножителей единственно.*

Назовем два многочлена $a(x)$ и $b(x)$ из кольца $F_p[x]$ сравнимыми по модулю $f(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$, $\alpha_i \in F_p$, если их разность $a(x) - b(x)$ делится на $f(x)$ в кольце $F_p[x]$. Сравнения такого рода будем называть, следуя Дедекинду, *сравнениями по двойному модулю* и для обозначения сравнимости $a(x)$ и $b(x)$ по модулю $f(x)$ использовать символ: $a(x) \equiv b(x) \pmod{f(x)}$.

Отношение сравнимости по двойному модулю рефлексивно, симметрично, транзитивно и поэтому разбивает множество всех многочленов с коэффициентами из F_p на непересекающиеся классы $A, B, C, \ldots$, называемые классами вычетов по модулю $f(x)$. Поскольку каждый многочлен $a(x)$ сравним по модулю $f(x)$ с одним и только одним многочленом $r(x)$ вида $r(x) = \beta_1 x^{n-1} + \beta_2 x^{n-2} + \ldots + \beta_n$, где $\beta_1, \beta_2, \ldots, \beta_n$ независимо друг от друга пробегают элементы поля F_p, то имеется в точности $q = p^n$ классов вычетов по модулю $f(x)$.

Сравнения по двойному модулю можно складывать, вычитать и перемножать подобно обычным сравнениям. Эти операции индуцируют аналогичные операции на классах вычетов по модулю $f(x)$, превращая множество классов вычетов по двойному модулю в коммутативное кольцо, нулевым элементом которого служит класс, состоящий из всех кратных многочлена $f(x)$, а единицей — класс вычетов E, содержащий единичный элемент 1 поля F_p.

Пусть теперь $f(x) = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$ — неприводимый многочлен из кольца $F_p[x]$. Если многочлен $g(x)$ не делится на $f(x)$, то $f(x)$ и $g(x)$ взаимно просты и, следовательно, в кольце $F_p[x]$ найдутся такие многочлены $u(x)$ и $v(x)$, причем степень $v(x)$ меньше n, что $f(x)u(x) + g(x)v(x) = 1$. В таком случае $g(x)v(x) \equiv 1 \pmod{f(x)}$ и, стало быть, уравнение $AX = E$, где A — класс вычетов по модулю $f(x)$, состоящий из многочленов, не делящихся на $f(x)$, а E — единичный элемент кольца вычетов по модулю $f(x)$ имеет единственное решение $X = A^{-1}$. Следовательно, в случае неприводимого многочлена $f(x)$ классы вычетов по модулю $f(x)$, отличные от

нулевого, образуют по умножению абелеву группу порядка $q-1$.

Таким образом, *классы вычетов по модулю $f(x)$, где $f(x)$ — неприводимый многочлен степени n с коэффициентами из F_p, образуют конечное поле F_q, состоящее из $q=p^n$ элементов.*

В дальнейшем единицу поля F_q будем обозначать через 1.

Пусть снова многочлен $g(x)$ взаимно прост с $f(x)$. Если $r(x)$ пробегает множество R, состоящее из $q-1$ отличных от нуля многочленов вида $\beta_1 x^{n-1}+\beta_2 x^{n-2}+\ldots+\beta_n$, то остатки от деления $g(x)r(x)$ на $f(x)$ пробегают то же самое множество. Следовательно,

$$\prod_{r(x)\in R} g(x)r(x) \equiv \prod_{r(x)\in R} r(x) \pmod{f(x)},$$

или то же самое

$$((g(x))^{q-1}-1)\prod_{r(x)\in R} r(x) \equiv 0 \pmod{f(x)}.$$

Отсюда, поскольку все $r(x)$ не делятся на $f(x)$, мы получаем следующий аналог малой теоремы Ферма: *если $f(x)$ — неприводимый многочлен степени n с коэффициентами из поля F_p и $q=p^n$, то $(g(x))^q \equiv g(x) \pmod{f(x)}$ для любого многочлена $g(x)$ из кольца $F_p[x]$.* Другими словами, каждый элемент поля классов вычетов кольца $F_p[x]$ по модулю $f(x)$, где $f(x)$ — неприводимый многочлен с коэффициентами из F_p удовлетворяет уравнению $z^q-z=0$.

Далее, имеет место следующее обобщение теоремы Лагранжа: *количество решений, взятых с их кратностями, уравнения $F(z)=0$ в элементах поля F_q, где $F(z)$ — не равный нулю многочлен с коэффициентами из F_q, не превосходит степени m многочлена $F(z)$.*

Из этих теорем следует, в частности, что

$$z^q-z \equiv \prod_{r(x)\in R}(z-r(x)) \pmod{f(x)},$$

и тем самым имеет место следующий аналог теоремы Вильсона:

$$\prod_{r(x)\in R} r(x) \equiv -1 \pmod{f(x)}.$$

2. Покажем теперь, что для каждого целого $n\geqslant 1$ и любого простого числа p существуют конечные поля, состоящие из $q=p^n$ элементов. По сказанному выше для этого достаточно установить существование в кольце $F_p[x]$ неприводимых многочленов произвольной степени $n\geqslant 1$.

Пусть $g(x)$ — отличный от нуля нормированный (со старшим коэффициентом 1) многочлен степени n из кольца $F_p[x]$. Положим $N(g)=p^n$ ($N(0)=-\infty$) и назовем эту величину нормой многочлена $g(x)$. Понятие нормы многочлена $g(x)$ кольца $F_p[x]$ аналогично понятию абсолютной величины $|a|$ целого числа a; в частности, мы имеем $N(fg)=N(f)N(g)$ для любых двух многочленов $f(x)$ и $g(x)$ кольца $F_p[x]$.

Рассмотрим *дзета-функцию*

$$\zeta_p(s)=\prod_f\left(1-\frac{1}{N(f)^s}\right)^{-1}$$

кольца $F_p[x]$, где $s=\sigma+it$ — комплексное переменное, $\sigma>1$, и произведение распространено на все нормированные неприводимые многочлены $f(x)$ кольца $F_p[x]$ степени $\geqslant 1$.

По теореме об однозначности разложения на неприводимые сомножители в кольце $F_p[x]$ мы имеем

$$\zeta_p(s)=\prod_f\left(1+\sum_{m=1}^{\infty}\frac{1}{N(f)^{ms}}\right)=1+\sum_g\frac{1}{N(g)^s},$$

где последняя сумма берется по всем нормированным многочленам кольца $F_p[x]$ положительной степени.

Поскольку имеется точно p^n нормированных многочленов степени n, то из последнего равенства следует, что

$$\zeta_p(s)=1+\sum_{n=1}^{\infty}\frac{p^n}{p^{ns}}=\left(1-\frac{p}{p^s}\right)^{-1}.$$

Обозначим через (n) количество нормированных неприводимых многочленов степени n. Тогда, исходя из определения $\zeta_p(s)$, мы имеем:

$$\prod_{n=1}^{\infty}\left(1-\frac{1}{p^{ns}}\right)^{-(n)}=\left(1-\frac{p}{p^s}\right)^{-1}.$$

Отсюда, логарифмируя, получаем

$$\sum_{n=1}^{\infty} (n) \log\left(1 - \frac{1}{p^{ns}}\right) = \log\left(1 - \frac{p}{p^s}\right),$$

или

$$\sum_{n=1}^{\infty} (n) \sum_{m=1}^{\infty} \frac{1}{m p^{mns}} = \sum_{k=1}^{\infty} \frac{p^k}{k p^{ks}}.$$

Сравнивая теперь коэффициенты при p^{-ks}, выводим, что

$$\sum_{d|k} d\,(d) = p^k,$$

откуда по формуле обращения Мебиуса

$$(n) = \frac{1}{n} \sum_{d|n} \mu\,(d)\, p^{\frac{\kappa}{d}}.$$

Выражение $\sum_{d/n} \mu\,(d)\, p^{\frac{n}{d}}$ представляет собой сумму различных степеней простого числа p, взятых со знаками плюс и минус, а следовательно, не может быть равным нулю. В таком случае поскольку (n) — неотрицательное целое число, мы имеем $(n) \geqslant 1$, и, стало быть, для всякого $n \geqslant 1$ существуют неприводимые в кольце $F_p\,[x]$ многочлены степени n.

3. Выясним теперь структуру полей F_q. Порядком отличного от нуля элемента a поля F_q назовем наименьшее натуральное число l такое, что $a^l = 1$. Заметим, что если a — элемент порядка l, то $a^k = a^r$ тогда и только тогда, когда $k \equiv r \pmod{l}$.

Покажем, что в каждом поле F_q, состоящем из $q = p^n$ элементов, имеется хотя бы один элемент g порядка $q - 1$. Этим будет установлено, что мультипликативная группа поля F_q является циклической группой порядка $q - 1$. Пусть a и b — элементы поля F_q порядков l и m соответственно, где l и m — взаимно простые натуральные числа. Покажем, что в этом случае их произведение ab имеет порядок lm. Действительно, если $(ab)^k = 1$, то $a^{mk} = b^{-mk} = 1$ и $b^{lk} = a^{-lk} = 1$, откуда ввиду условия $(l,m) = 1$ следует, что k кратно l и m, а стало быть, и их произведению lm. Найдем теперь порядок элемента a^k, где a — элемент порядка l. Положим $(l, k) = d$; тогда $(a^k)^{l/d} = (a^l)^{k/d} = 1$ и тем самым порядок элемента a^k делит число $\frac{l}{d}$. С другой стороны, если $a^{ks} = 1$, то ks кратно $l = \frac{l}{d} d$, так как число $\frac{l}{d}$ взаимно просто с k, то оно должно быть делителем s. Следовательно, порядок элемента a^k равен $\frac{l}{d}$.

Докажем теперь существование в поле F_q элемента g порядка $q - 1$. Пусть m — максимальный порядок ненулевых элементов поля F_q и пусть g — элемент порядка m. Так как m различных степеней элемента g отличны от нуля, то $m \leqslant q - 1$. Пусть, далее, a — некоторый другой элемент поля F_q и l — его порядок. Если l не делит m, то $a^{(l,m)}$ имеет порядок $\frac{l}{(l, m)}$, взаимно простой с m, тогда $ga^{(l,m)}$ есть элемент порядка $m\frac{l}{(l, m)}$, превосходящего m. Это противоречие показывает, что l делит m и, следовательно, каждый отличный от нуля элемент поля F_q является корнем многочлена $x^m - 1$. По теореме Лагранжа число корней многочлена $x^m - 1$ в поле F_q не превосходит его степени m. Стало быть, $q - 1 \leqslant m$ и, следовательно, $m = q - 1$.

Таким образом, справедлива следующая теорема: *в любом поле F_q, состоящем из $q = p^n$ элементов, где p — простое число и $n \geqslant 1$ — целое, существует такой элемент g, что если x пробегает полную систему вычетов по модулю $q - 1$, то g^x пробегает по одному разу все ненулевые элементы поля F_q.*

Этот результат можно усилить и доказать, что поле F_q содержит ровно $\varphi\,(q - 1)$ элементов порядка $q - 1$, где $\varphi\,(m)$ — функция Эйлера. Заметим, что приведенное доказательство существования в поле F_q элемента g порядка $q - 1$, по существу, повторяет доказательство Гаусса существования первообразного корня по модулю p.

Вспомним теперь описанный нами выше процесс построения поля F_q. Элементами этого поля являются классы вычетов кольца $F_p\,[x]$ по модулю $f\,(x)$, где $f\,(x)$ — неприводимый многочлен с коэффициентами из F_p степени n. Обозначим через θ класс вычетов, содержащий многочлен $a\,(x) = x$. Тогда $f\,(\theta) = 0$ и, следовательно, многочлен $f\,(x)$ является минимальным многочленом элемента $\theta \in F_q$. Далее, из алгоритма деления с остатком $g\,(x) = f\,(x)h\,(x) +$

$+ r(x)$, где $r(x) = a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n$ — многочлен с коэффициентами из F_p, следует, что каждый элемент ω поля F_q представляется в виде $\omega = r(\theta) = a_1\theta^{n-1} + a_2\theta^{n-2} + \ldots + a_n$. Отсюда видно, что поле F_q является алгебраическим расширением поля F_p степени n.

Характеристикой поля F_q назовем наименьшее натуральное число k, такое, что $\sum_{i=1}^{k} 1 = 0$, где 1 — единицы поля F_q. Мы имеем $\sum_{i=1}^{p} 1 = 1 \cdot p = 0$ и $\sum_{i=1}^{k} 1 \neq 0$ при $1 \leqslant k < p$. Следовательно, поле F_q, где $q = p^n$ имеет характеристику p.

Покажем, что в поле характеристики p имеет место равенство $(\alpha + \beta)^p = \alpha^p + \beta^p$ для любых элементов α и β этого поля. Действительно, по формуле бинома Ньютона мы имеем $(\alpha+\beta)^p = \sum_{i=0}^{p} \binom{p}{k} \alpha^k \beta^{p-k}$, где $\binom{p}{k} = \frac{p(p-1)\ldots(p-k-1)}{k(k-1)\ldots 2\cdot 1}$, и утверждение следует из того, что $\binom{p}{k} \equiv 0 \pmod p$ для всех $k = 1, 2, \ldots, p-1$.

Пусть снова $f(x)$ — неприводимый многочлен степени n с коэффициентами из поля F_q. В поле F_q, где $q = p^n$ уравнение $f(x) = 0$ имеет корень θ. Тогда $f(\theta) = 0$, и, возвышая последнее равенство в степень p, мы получаем, используя свойство полей характеристики p, что $f(\theta^p) = 0$. Повторяя этот процесс, мы убеждаемся, что наряду с θ корнями уравнения $f(x) = 0$ будут θ, θ^p, ..., $\theta^{p^{n-1}}$. Заметим, что дальнейшее возведение в степень p не имеет смысла, ибо $\theta^q = \theta$.

Докажем, что элементы θ, θ^p, ..., $\theta^{p^{n-1}}$ различны между собой. Пусть g — элемент поля F_q порядка $q-1$ и пусть $g = a_1\theta^{n-1} + a_2\theta^{n-2} + \ldots + a_n$, где $a_i \in F_p$. Если $\theta^{p^i} = \theta^{p^j}$ при $1 \leqslant i < j \leqslant n-1$, то $g^{p^i} = g^{p^j}$ и, стало быть, $g^{p^j - p^i} = 1$. Но $1 \leqslant p^j - p^i < q-1$, и мы приходим в противоречие с определением элемента g.

Таким образом, справедливо разложение

$$f(x) = \prod_{i=0}^{n-1} (x - \theta^{p^i}),$$

где $\theta^{p^i} \in F_p$ для всех $i = 0, 1, \ldots, n-1$.

Далее, назовем *показателем числа a по модулю m* наименьшее положительное число k, такое, что $a^k \equiv 1 \pmod m$, и докажем следующий результат.

Теорема. *Пусть α — элемент порядка m поля F_q, где $q = p^n$, k — показатель числа p по модулю m. Тогда многочлен $f(x) = \prod_{i=0}^{k-1} (x - \alpha^{p^i})$ имеет коэффициенты из поля F_p и $f(x)$ неприводим в кольце $F_p[x]$.*

Покажем сначала, что $\alpha^{p^k} = \alpha$ и что элементы $\alpha, \alpha^p, \ldots, \alpha^{p^{k-1}}$ различны между собой. Равенство $\alpha^{p^i} = \alpha^{p^j}$ выполняется тогда и только тогда, когда $\alpha^{p^i - p^j} = 1$, что справедливо лишь в случае, если $p^i - p^j \equiv 0 \pmod m$. Но последнее сравнение равносильно сравнению $p^{i-j} \equiv 1 \pmod m$, откуда $i \equiv j \pmod k$.

Далее, мы имеем:

$$f(x)^p = \prod_{i=0}^{k-1} (x - \alpha^{p^i})^p = \prod_{i=0}^{k-1} (x^p - \alpha^{p^{i+1}}) =$$

$$= \prod_{i=1}^{k} (x^p - \alpha^{p^i}) = \prod_{i=0}^{k-1} (x^p - \alpha^{p^i})$$

и, следовательно, $f(x)^p = f(x^p)$.

Пусть $f(x) = \sum_{s=0}^{k} a_s x^{k-s}$. Тогда

$$f(x)^p = \sum_{s=0}^{k} a_s^p x^{(k-s)p},$$

$$f(x^p) = \sum_{s=0}^{k} a_s x^{(k-s)p},$$

и, сравнивая коэффициенты многочленов $f(x)^p$ и $f(x^p)$, мы получаем, что $a_s^p = a_s$ при всех $s = 0, 1, \ldots, k$. Но равенство $a^p = a$ имеет место лишь тогда, когда $a \in F_p$ (иначе число корней многочлена $x^p - x$ превышало бы его степень), и в таком случае $f(x) \in F_p[x]$. Предположим теперь, что $f(x) = g(x)h(x)$. Так как $f(\alpha) = 0$, то либо $g(\alpha) = 0$, либо $h(\alpha) = 0$. Если $g(\alpha) = 0$, то $g(\alpha^p) = \ldots = g(\alpha^{p^{k-1}}) = 0$ и тогда степень многочлена $g(x)$ равна k,

откуда $g(x) = f(x)$. Аналогично, если $h(\alpha) = 0$, то $h(x) = f(x)$.
Этим теорема доказана.

Следствие. *Пусть α — элемент порядка m поля F_q, $q = p^n$ и пусть $f(x) = \prod_{i=0}^{k-1} (x - \alpha^{p^i})$, где k—показатель числа p по модулю m. Если $g(\alpha) = 0$ для некоторого многочлена $g(x) \in F_p[x]$, то в кольце $F_p[x]$ имеет место разложение:*

$$g(x) = f(x)\, h(x).$$

Действительно, по алгоритму деления с остатком мы имеем $g(x) = f(x)h(x) + r(x)$, где степень многочлена $r(x)$ меньше k. Но если $g(\alpha) = 0$, то $g(\alpha^p) = \ldots = g(\alpha^{p^{k-1}}) = 0$, тогда по теореме Лагранжа $r(x) = 0$. Следствие доказано.

Более подробное изложение теории конечных полей читатель может найти в книге Э. Берликэмпа «Алгебраическая теория кодирования» (М., 1971). Заметим лишь, что все рассмотренные нами поля F_q с одним и тем же q изоморфны между собой. Более того, все конечные поля, состоящие из любого числа элементов, по существу, исчерпываются этими полями. Именно, справедливо следующее утверждение: *любое конечное поле изоморфно одному из полей F_q для некоторого $q = p^n$.*

4. Рассмотрим в заключение главы важный для теории чисел, теории кодирования и других разделов математики вопрос о разложении данного многочлена $f(x)$ кольца $F_p[x]$ на неприводимые сомножители. Для изучения этого вопроса нам потребуются некоторые новые понятия.

Дискриминантом многочлена $f(x) = a_0 \prod_{i=1}^{n} (x - \alpha_i)$ назовем выражение

$$D(f) = a_0^{2(n-1)} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2.$$

Ясно, что дискриминант $D(f)$ многочлена $f(x)$ равен нулю тогда и только тогда, когда многочлен $f(x)$ имеет хотя бы один кратный корень.

Далее, *результантом* двух многочленов

$$f(x) = a_0 \prod_{i=1}^{n} (x - \alpha_i) \text{ и } g(x) = b_0 \prod_{j=1}^{m} (x - \beta_j)$$

мы назовем выражение:

$$R(f, g) = a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

Из определения результата $R(f, q)$ многочленов $f(x)$ и $q(x)$ непосредственно следует, что

$$R(f, g) = a_0^n \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_0^n \prod_{j=1}^{m} f(\beta_j),$$

что $R(f, g) = 0$ тогда и только тогда, когда многочлены $f(x)$ и $g(x)$ имеют хотя бы один общий корень.

Под *производной* $f'(x)$ многочлена $f(x) \in F_p[x]$ будем понимать формальную производную, равную коэффициенту при y в разложении $f(x + y)$ по степеням переменной y. Мы имеем:

1) $(\alpha f(x))' = \alpha f'(x)$ при $\alpha \in F_p$;
2) $(f(x) \pm g(x))' = f'(x) \pm g'(x)$;
3) $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.

Покажем, что для дискриминанта $D(f)$ нормированного многочлена $f(x)$ степени n имеет место равенство:

$$D(f) = (-1)^{\frac{n(n-1)}{2}} R(f, f').$$

Действительно, если $f(x) = \prod_{i=1}^{n} (x - \alpha_i)$, то

$$f'(x) = \sum_{j=1}^{n} \prod_{\substack{i=1 \\ i \neq j}}^{n} (x - \alpha_i), \text{ тогда}$$

$$f'(\alpha_k) = \prod_{\substack{i=1 \\ i \neq k}}^{n} (\alpha_k - \alpha_i).$$

Отсюда

$$R(f,f') = \prod_{k=1}^{n} f'(\alpha_k) = \prod_{k=1}^{n} \prod_{\substack{i=1 \\ i\neq k}}^{n} (\alpha_k - \alpha_i) =$$

$$= \prod_{1\leqslant k<i\leqslant n} (\alpha_k - \alpha_i) \prod_{1\leqslant i<k\leqslant n} (\alpha_k - \alpha_i) = (-1)^{\frac{n(n-1)}{2}} D(f),$$

и тем самым утверждение доказано..

Для дальнейшего нам потребуется также следующее утверждение.

Лемма. *Если $f(x)$ и $g(x)$ — нормированные многочлены, то*

$$D(fg) = D(f)D(g)[R(f,g)]^2.$$

Обозначим через n и m степени многочленов $f(x)$ и $g(x)$ соответственно. Тогда по доказанному выше мы имеем:

$$(-1)^{\frac{(m+n)(m+n-1)}{2}} D(fg) = R(fg,(fg)') = R(fg, f'g+fg'),$$

и поскольку $R(fg, h) = R(f, h)R(g, h)R(f, h + fr) = R(f, h)$, то

$$(-1)^{\frac{(m+n)(m+n-1)}{2}} D(fg) = R(f,f'g+fg')R(g,f'g+fg') =$$

$$= R(f,f'g)R(g,fg') = R(f,f')R(f,g)R(g,f)R(g,g') =$$

$$= (-1)^{\frac{n(n-1)}{2}} D(f)(-1)^{\frac{m(m-1)}{2}} D(g)(-1)^{mn}[R(f,g)]^2.$$

Утверждение леммы следует теперь из равенства

$$\frac{(m+n)(m+n-1)}{2} = \frac{n(n-1)}{2} = mn + \frac{m(m-1)}{2}.$$

Из этой леммы мы легко получаем, что для любых s нормированных многочленов $f_1(x), \ldots, f_s(x)$ справедливо равенство

$$D\left(\prod_{i=1}^{s} f_i\right) = \prod_{i=1}^{s} D(f_i) \prod_{1\leqslant i<j\leqslant s} [R(f_i, f_j)]^2.$$

Заметим далее, что $R(f, g) \in F_p$ для любых многочленов $f(x)$ и $q(x)$ кольца $F_p[x]$. Так как $R(fh, g) = R(f, g)R(h, g)$, то утверждение достаточно доказать для случая, когда $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ является неприводимым

многочленом в кольце $F_p[x]$. В этом случае $f(x) = \prod_{i=0}^{n-1} (x - \Theta^{p^i})$, где $\Theta \in F_q$, $q = p^n$ и, следовательно,

$$R(f,g)^p = \prod_{i=0}^{n-1} g(\Theta^{p^i})^p = \prod_{i=1}^{n} g(\Theta^{p^i}) = R(f,g).$$

Тогда $R(f, g) \in F_p$, и этим утверждение доказано.

Докажем теперь следующий общий результат.

Теорема Штикельбергера: *Пусть $p > 2$ — простое число, $f(x)$ — нормированный многочлен кольца $F_p[x]$ степени n с отличным от нуля дискриминантом $D = D(f)$ и s — число неприводимых делителей многочлена $f(x)$ в кольце $F_p[x]$. Тогда имеет место равенство*

$$\left(\frac{D(f)}{p}\right) = (-1)^{n-s}$$

Пусть сначала $s = 1$, т. е. многочлен $f(x)$ неприводим в кольце $F_p[x]$. В этом случае $f(x) = \prod_{i=0}^{n-1} (x - \alpha^{p^i})$, где $\alpha \in F_q$, $q = p^n$, тогда $D^{1/2} = \prod_{0<i<j\leqslant n-1} (\alpha^{p^i} - \alpha^{p^j})$ — элемент поля F_q. Далее,

$$(D^{1/2})^p = \prod_{1<i<j<n} (\alpha^{p^i} - \alpha^{p^j}) = \prod_{1<i<j<n-1} (\alpha^{p^i} - \alpha^{p^j}) \prod_{1<k<n-1} (\alpha^{p^k} - \alpha^{p^n}) =$$

$$= (-1)^{n-1} \prod_{0<i<j<n-1} (\alpha^{p^i} - \alpha^{p^j}) = (-1)^{n-1} D^{1/2}$$

и, следовательно, $(D^{1/2})^p = D^{1/2}$, если n нечетно, и $(D^{1/2})^p \neq D^{1/2}$, если n четно. Но равенство $a^p = a$ имеет место тогда и только тогда, когда $a \in F_p$. Стало быть, $D \equiv \omega^2 \pmod p$ тогда и только тогда, когда n нечетно. Этим для $s = 1$ теорема доказана.

Пусть теперь $f(x) = \prod_{i=1}^{s} f_i(x)$, где $f_i(x)$ — неприводимые многочлены кольца $F_p[x]$, степени которых равны величинам n_i соответственно, и пусть $D_i = D(f_i)$. Тогда $D = R^2 \prod_{i=1}^{s} D_i$, где $R = \prod_{1<i<j<s} R(f_i, f_j)$ и, следовательно $D^{1/2} =$

$= R\prod_{i=1} D_i^{1/2}$, $(D^{1/2})^p = R^p \prod_{i=1}^{s} (D_i^{1/2})^p$. Но $R \in F_p$ и, стало быть, $(D^{1/2})^p = R\prod_{i=1}^{s}(D_i^{1/2})^p$. По доказанному выше $(D_i^{1/2})^p = (-1)^{n_i-1} D_i^{1/2}$.

В таком случае

$$(D^{1/2})^p = R\prod_{i=1}^{s}(-1)^{n_i-1} D_i^{1/2},$$

и поскольку

$$\sum_{i=1}^{s} n_i = n,$$

мы имеем

$$(D^{1/2})^p = (-1)^{n-s} R\prod_{i=1}^{s} D_i^{1/2} = (-1)^{n-s} D^{1/2}.$$

Следовательно, $D^{1/2} \in F_p$ тогда и только тогда, когда $n \equiv s \pmod 2$. Теорема доказана.

Теорема Штикельбергера позволяет судить о четности или нечетности числа различных простых делителей многочлена по его дискриминанту $D(f)$. При этом величина $\bar{\mu}(f) = (-1)^n \left(\frac{D(f)}{p}\right)$, где n — степень многочлена $f(x)$, является аналогом арифметической функции $\mu(m)$, которая определяется для всех натуральных чисел m равенствами:

$$\mu(m) = \begin{cases} 1, \text{ если } m = 1; \\ 0, \text{ если } m \text{ делится на квадрат простого числа;} \\ (-1)^s, \text{ если } m = p_1 p_2 \ldots p_s. \end{cases}$$

Действительно, если $\alpha \in F_p$ и $\alpha \neq 0$, то $D(\alpha) = 1$ и, следовательно, $\bar{\mu}(\alpha) = 1$ (заметим, что в кольце $F_p[x]$ ненулевые элементы поля F_p играют роль, аналогичную той, которую в кольце целых чисел играют элементы $+1$ и -1). Далее, если многочлен $f(x)$ делится на квадрат неприводимого многочлена, то $D(f) = 0$, и тогда $\bar{\mu}(f) = 0$. Наконец, если $f(x) = f_1(x) \ldots f_s(x)$, то по теореме Штикельбергера $\bar{\mu}(f) = (-1)^s$, тем самым в этом случае зна-

чение $\bar{\mu}(f)$ определяет четность числа различных неприводимых сомножителей многочлена $f(x)$.

В качестве следствия полученных нами выше результатов докажем следующее утверждение, принадлежащее Гауссу:

Квадратичный закон взаимности: *Если p и l — различные нечетные простые числа, то*

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

Доказательство, которое мы приведем, принадлежит Суону.

Рассмотрим над полем F_p многочлен $x^l - 1$. Если в некотором поле F_q содержится элемент α порядка l (такое поле, конечно, существует), то в этом поле имеет место разложение $x^l - 1 = (x-1)\prod_{i=1}^{l-1}(x - \alpha^i)$, где все степени α^i, $i = 1, 2, \ldots, l-1$ являются элементами поля F_q одного и того же порядка l. Положим $g(x) = \prod_{i=1}^{l-1}(x - \alpha^i)$. Каждый неприводимый делитель многочлена $g(x)$ в кольце $F_p[x]$ имеет степень k, где k — показатель числа p по модулю l. Следовательно, число различных неприводимых делителей многочлена $x^l - 1$ в кольце $F_p[x]$ равно $s = 1 + \frac{l-1}{k}$. Далее, по определению символа Лежандра число k делит $\frac{l-1}{2}$ тогда и только тогда, когда $\left(\frac{p}{l}\right) = 1$.

В таком случае $(-1)^{\frac{l-1}{k}} = \left(\frac{p}{l}\right)$, откуда $\left(\frac{p}{l}\right) = -(-1)^s$. (1)

Воспользуемся теперь теоремой Штикельбергера. Пусть D — дискриминант многочлена $x^l - 1$. Тогда мы имеем $\left(\frac{D}{p}\right) = (-1)^{l-s} = -(-1)^s$. Но $D = (-1)^{\frac{l(l-1)}{2}} R(x^l = 1, lx^{l-1}) = (-1)^{\frac{l(l-1)}{2}} l^l = (-1)^{\frac{l-1}{2}} l^l$, и в таком случае

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

По критерию Эйлера мы имеем при $p > 2$ $\left(\frac{-1}{p}\right) \equiv$

$\equiv (-1)^{\frac{p-1}{2}} \pmod p$, откуда $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Следовательно, $-(-1)^s = (-1)^{\frac{p-1}{2}\cdot\frac{l-1}{2}}\left(\frac{l}{p^r}\right)$, (2) и сравнивая (1), (2), мы получаем, что $\left(\frac{p}{l}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{l-1}{2}}\left(\frac{l}{p}\right)$. Но $\left(\frac{l}{p}\right)^2 = 1$, тогда $\left(\frac{p}{l}\right)\left(\frac{l}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{l-1}{2}}$.
Утверждение доказано.

Глава 3

СРАВНЕНИЯ С ДВУМЯ ПЕРЕМЕННЫМИ. РАСПРЕДЕЛЕНИЕ СТЕПЕННЫХ ВЫЧЕТОВ И НЕВЫЧЕТОВ

1. Пусть $f(x_1, \ldots, x_n)$ — многочлен от переменных $x_1, \ldots, x_n$ с целыми коэффициентами. Основным вопросом, который нас будет в дальнейшем интересовать, является вопрос о количестве решений алгебраических сравнений

$$f(x_1, \ldots, x_n) \equiv 0 \pmod m.$$

Под *решением сравнения* $f(x_1, \ldots, x_n) \equiv 0 \pmod m$ мы понимаем всякий набор $x_1 \equiv x_1' \pmod m, \ldots, x_n \equiv x_n' \pmod m$ классов вычетов по модулю m, такой, что $f(x_1', \ldots, x_n') \equiv 0 \pmod m$ для целых $x_1', \ldots, x_n'$.

Обозначим через $N(m)$ количество решений сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod m$ и покажем, что $N(m)$ является *мультипликативной функцией*, т. е.

$$N(m_1m_2) = N(m_1)N(m_2) \text{ при } (m_1, m_2) = 1.$$

Действительно, если $x_i = x_i' + m_1t_i$ и $x_i = y_i' + m_2u_i$, $i = 1, 2, \ldots, n$ являются решениями сравнений $f(x_1, \ldots, x_n) \equiv 0 \pmod{m_1}$ и $f(x_1, \ldots, x_n) \equiv 0 \pmod{m_2}$ соответственно, где $(m_1, m_2) = 1$, то при каждом $i = 1, 2, \ldots, n$ мы имеем $m_1t_i - m_2u_i = x_i' - y_i'$. Далее, поскольку каждое целочисленное решение уравнения

$m_1t_i - m_2u_i = x_i' - y_i'$ представляется в виде $t_i = t_i' + m_2z_i$, $u_i = u_i' + m_1z_i$, где t_i', u_i' — некоторое частное решение этого уравнения, а z_i — пробегают множество целых чисел, то набор $x_i = x_i' + m_1t_i' + m_1m_2z_i = y_i' + m_2u_i' + m_1m_2z_i$, $i = 1, 2, \ldots, n$ является решением сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod{m_1m_2}$. Следовательно, каждой паре $x_i \equiv x_i' \pmod m$, $x_i \equiv y_i' \pmod{m_2}$, $i = 1, 2, \ldots, n$, решений сравнений $f(x_1, \ldots, x_n) \equiv 0 \pmod{m_1}$ и $f(x_1, \ldots, x_n) \equiv 0 \pmod{m_2}$ соответствует единственное решение сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod{m_1m_2}$ и, следовательно, $N(m_1m_2) = N(m_1)N(m_2)$ при $(m_1, m_2) = 1$.

В силу свойства мультипликативности задача о количестве решений сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod m$ по произвольному модулю m сводится к более узкой задаче о количестве решений сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod{p^\alpha}$ по модулю p^α, равному степени простого числа p. Для разрешимости сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod{p^\alpha}$, $\alpha > 1$ необходимо, чтобы было разрешимо сравнение $f(x_1, \ldots, x_n) \equiv 0 \pmod p$. В невырожденных случаях разрешимость последнего сравнения является также и достаточным условием для разрешимости сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod{p^\alpha}$. Именно, пусть $s \geqslant 1$ — целое и $x_1 \equiv x_1^{(s)} \pmod{p^s}, \ldots x_n \equiv x_n^{(s)} \pmod{p^s}$ — решение сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod{p^s}$ такое, что $\frac{\partial f}{\partial x_i}(x_1^{(s)}, \ldots, x_n^{(s)}) \not\equiv 0 \pmod p$ хотя бы для одного номера $i = 1, 2, \ldots, n$ (под частной производной $\frac{\partial f}{\partial x}(x_1, \ldots, x_n)$ многочлена $f(x_1, \ldots, x_n)$ мы понимаем формальную производную, равную коэффициенту при первой степени y_i многочлена $F(y_i) = f(x_1, \ldots, x_{i-1}, x_i + y_i, x_{i+1}, \ldots, x_n)$, при разложении его по степеням переменной y_i). Тогда $x_i = x_i^{(s)} + p^st_i$, $i = 1, 2, \ldots, n$, $f(x_1^{(s)}, \ldots, x_n^{(s)}) = p^st_0$ и по формуле Тейлора сравнение $f(x_1, \ldots, x_n) \equiv 0 \pmod{p^{s+1}}$ можно переписать в виде

$$f(x_1^{(s)}, \ldots, x_n^{(s)}) + p^s\sum_{i=1}^{n}\frac{\partial f}{\partial x_i}t_i \equiv 0 \pmod{p^{s+1}}.$$

Отсюда для определения $t_1, \ldots, t_n$ получаем сравнение

$t_0 + \sum_{i=1}^{n} \frac{\partial f}{\partial x_i} t_i \equiv 0 \pmod p$, которое имеет p^{n-1} различных решений. Тем самым справедливо следующее утверждение:

Теорема. *Каждое решение* $x_1 \equiv x_1^{(1)} \pmod p, \ldots, x_n \equiv x_n^{(1)} \pmod p$ *сравнения* $f(x_1, \ldots, x_n) \equiv 0 \pmod p$ *такое, что* $\frac{\partial f}{\partial x_i}(x_1^{(1)}, \ldots, x_n^{(1)}) \not\equiv 0 \pmod p$ *хотя бы для одного* $i = 1, 2, \ldots, n$ *порождает* $p^{(\alpha-1)(n-1)}$ *различных решений* $x_1 \equiv x_1^{(\alpha)} \pmod{p^\alpha}, \ldots, x_n \equiv x_n^{(\alpha)} \pmod{p^\alpha}$ *сравнения* $f(x_1, \ldots, x_n) \equiv 0 \pmod{p^{(\alpha)}}$.

Следовательно, вопрос о количестве решений алгебраических сравнений $f(x_1, \ldots, x_n) \equiv 0 \pmod m$ по составному модулю m сводится к аналогичному вопросу для сравнений $f(x_1, \ldots, x_n) \equiv 0 \pmod p$ по простому модулю p. Тем самым сравнения по простому модулю p составляют фундамент теории алгебраических сравнений.

2. Первые результаты в задачах о количестве решений сравнений $f(x, y) \equiv 0 \pmod p$ по простому модулю $p > 2$ были получены Лагранжем, доказавшим в 1770 году разрешимость сравнения $x^2 + y^2 + 1 \equiv 0 \pmod p$. В дальнейшем для количества N_p этого сравнения была получена точная формула $N_p = p - (-1)^{\frac{p-1}{2}}$. Более трудным оказался вопрос о количестве решений сравнения $f(x, y) \equiv 0 \pmod p$ в случае, когда $f(x, y)$ является многочленом степени большей 2. Некоторые частные случаи сравнения $y^2 \equiv f(x) \pmod p$ с многочленом $f(x)$ третьей степени были исследованы Якобсталем (см. [7]).

В 1924 году Э. Артин [9] предположил, что для количества N_p решений сравнения $y^2 \equiv f(x) \pmod p$, где $f(x)$ — многочлен степени $n \geqslant 3$, не сравнимый по модулю p с квадратом $g^2(x)$ другого многочлена $g(x)$, справедлива оценка

$$|N_p - p| \leqslant 2\left[\frac{n-1}{2}\right] p^{1/2}, \qquad (1)$$

где символ $[\alpha]$ означает целую часть числа α, т. е. наибольшее целое, не превосходящее α. Оценка может быть выражена в виде

$$\left|\sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right)\right| \leqslant 2\left[\frac{n-1}{2}\right] p^{1/2}.$$

Для оценок сумм символов Лежандра

$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right)$$

Хопфом [13], Давенпортом [11] и Морделлом [14] применялся метод кратных сумм. В этом методе оцениваемая сумма представляется как среднее по некоторому количеству таких же сумм, но с другими параметрами, после чего осреднение распространяется на все многочлены данной степени. Однако методом кратных сумм гипотеза Артина не только не была доказана, но даже не был получен истинный порядок оценки по p.

В 1933 году Хассе [12] доказал гипотезу Артина для сравнений вида $y^2 \equiv x^3 + ax + b \pmod p$. В дальнейшем Вейль [15] распространил метод Хассе на общий случай и для количества N_q решений уравнения $f(x, y) = 0$ в элементах поля F_q, где $f(x, y)$ — абсолютно неприводимый многочлен, получил оценку $|N_q - q| \leqslant c(f)\, q^{1/2}$. Метод Хассе — Вейля требует привлечения современного аппарата абстрактной алгебраической геометрии и очень сложен.

В 1969 году автором [5], [6] был предложен новый, чисто арифметический метод получения оценок Хассе — Вейля, позволивший в дальнейшем доказать также ряд более сильных результатов.

Проиллюстрируем этот метод на примере сравнения

$$y^2 \equiv ax^2 + bx + c \pmod p, \qquad (2)$$

где a и b не делятся одновременно на p. Обозначим через N_p количество решений этого сравнения. Мы имеем:

$$N_p = \sum_{x=0}^{p-1} \left(1 + \left(\frac{ax^2 + bx + c}{p}\right)\right) = p + \sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p}\right).$$

Если $a \equiv 0 \pmod p$, то

$$N_p = p + \sum_{x=0}^{p-1} \left(\frac{bx + c}{p}\right),$$

и поскольку $bx + c$ пробегает вместе с x полную систему вычетов, то в этом случае $N_p = p$.

Предположим далее, что $a\not\equiv 0 \pmod p$ и обозначим через $d=b^2-4ac$ дискриминант многочлена ax^2+bx+c. Если $p>2$ и $d\not\equiv 0 \pmod p$, то мы имеем:

$$\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)=\left(\frac{a}{p}\right)\sum_{x=0}^{p-1}\left(\frac{\left(x+\frac{b}{2a}\right)^2}{p}\right)=$$

$$=\left(\frac{a}{p}\right)\sum_{y=0}^{p-1}\left(\frac{y^2}{p}\right)=\left(\frac{a}{p}\right)(p-1),$$

и, следовательно, в этом случае

$$N_p=\begin{cases}2p-1, & \text{если } \left(\frac{a}{p}\right)=1;\\ 1, & \text{если } \left(\frac{a}{p}\right)=-1.\end{cases}$$

Пусть теперь $a\not\equiv 0 \pmod p$, $d\not\equiv 0 \pmod p$ и $p>3$. Покажем, что в этом случае для числа N_p решений сравнения (2) имеет место формула

$$N_p=p-\left(\frac{a}{p}\right).$$

Нам удобнее будет трактовать сравнение (2) как уравнение

$$y^2=ax^2+bx+c$$

над полем F_p, состоящим из p элементов, а величину N_p — как число элементов поля F_p, удовлетворяющих этому уравнению.

Напомним, что элемент $\alpha\in F_p$ является s-кратным корнем многочлена $f(x)$ с коэффициентами из F_p, если $f(x)=(x-\alpha)^s g(x)$ и $g(\alpha)\neq 0$ в поле F_p. Под производной $f'(x)$ многочлена $f(x)$ мы снова понимаем формальную производную.

Лемма. *Если $f(\alpha)=f'(\alpha)=0$, то α является по меньшей мере 2-кратным корнем многочлена $f(x)$.*

Утверждение леммы непосредственно следует из разложения $f(x)=f(\alpha+x-\alpha)=f(\alpha)+f'(\alpha)(x-\alpha)+g(x)(x-\alpha)^2=(x-\alpha)^2 g(x)$.

Положим $r(x)=ax^2+bx+c$ и разобьем элементы поля F_p на три класса: A, B и C. В класс A отнесем те $\alpha\in F_p$,

для которых $1-r(\alpha)^{\frac{p-1}{2}}=0$, в класс B — те элементы $\alpha\in F_p$, для которых $1+r(\alpha)^{\frac{p-1}{2}}=0$, и в класс C — те элементы $\alpha\in F_p$, для котрых $r(\alpha)=0$. Обозначим через $|A|$, $|B|$ и $|C|$ количество элементов в классах A, B и C соответственно. Мы имеем:

$$|A|+|B|+|C|=p$$

и по критерию Эйлера

$$N_p=2|A|+|C|.$$

Рассмотрим многочлен

$$R(x)=2r(x)\left(1+r(x)^{\frac{p-1}{2}}\right)+r'(x)(x^p-x).$$

Так как $x^p-x=0$ для каждого $x\in F_p$, то $R(x)$ имеет корнями все элементы классов B и C. Более того, поскольку

$$R'(x)=2r'(x)\left(1+r(x)^{\frac{p-1}{2}}\right)-r(x)^{\frac{p-1}{2}}r'(x)+$$

$$+r''(x)(x^p-x)-r'(x)=r'(x)\left(1+r(x)^{\frac{p-1}{2}}\right)+r''(x)(x^p-x)$$

(учитывая, что в поле F_p справедливо равенство $p=0$), мы получаем по лемме, что все элементы класса B являются по меньшей мере 2-кратными корнями многочлена $R(x)$.

Далее легко убедиться, что

$$R(x)=2a\left(1+a^{\frac{p-1}{2}}\right)x^{p+1}+b\left(1+a^{\frac{p-1}{2}}\right)x^p-a^{\frac{p-1}{2}}\times$$

$$\times\frac{d}{4a}x^{p-1}+Q(x)=2a\left(1+\left(\frac{a}{p}\right)\right)x^{p+1}+b\left(1+\left(\frac{a}{p}\right)\right)x^p-$$

$$-\left(\frac{a}{p}\right)\frac{d}{4a}x^{p-1}+Q(x),$$

где $Q(x)$ — многочлен степени не выше $p-2$, и так как $a\not\equiv 0 \pmod p$, $d\not\equiv 0 \pmod p$, то $R(x)\neq 0$. Тогда по теореме

Лагранжа, сравнивая количество корней многочлена $R(x)$, взятых с их кратностями, со степенью многочлена $R(x)$, мы получаем:

$$2|B|+|C|\leqslant\begin{cases} p+1, & \text{если } \left(\frac{a}{p}\right)=1; \\ p-1, & \text{если } \left(\frac{a}{p}\right)=-1. \end{cases}$$

Отсюда

$$2(p-|A|-|C|)+|C|\leqslant p+\left(\frac{a}{p}\right)$$

и, стало быть,

$$N_p=2|A|+|C|\geqslant p-\left(\frac{a}{p}\right).$$

Проводя аналогичные рассуждения для многочлена

$$S(x)=2r(x)\left(1-r(x)^{\frac{p-1}{2}}\right)+r'(x)(x^p-x),$$

мы получаем

$$N_p=2|A|+|C|\leqslant p-\left(\frac{a}{p}\right).$$

Тем самым нами установлен следующий результат.

Т е о р е м а: *Пусть $d=b^2-4ac$ — дискриминант многочлена ax^2+bx+c и a, b не делятся одновременно на простое число $p>3$. Тогда*

$$\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)=\begin{cases} \left(\frac{a}{p}\right)(p-1), & \text{если } d\equiv 0 \pmod p; \\ -\left(\frac{a}{p}\right), & \text{если } d\not\equiv 0 \pmod p. \end{cases}$$

3. Рассмотрим теперь сравнение

$$y^2\equiv f(x) \pmod p,$$

где $f(x)$ — многочлен степени $n\geqslant 3$, и докажем таким же методом следующую теорему.

Т е о р е м а. *Пусть $n\geqslant 3$ — нечетное число и $p>9n^2$ —*

простое число. Тогда для количества N_p решений сравнения

$$y^2\equiv f(x) \pmod p, \tag{3}$$

где $f(x)=x^n+a_1x^{n-1}+\ldots+a_n$ — многочлен с целыми коэффициентами, справедлива оценка

$$|N_p-p|\leqslant c(n)\,p^{1/2}.$$

Ради простоты изложения мы не будем вычислять константу $c(n)$. Заметим лишь, что изложенный ниже метод позволяет получить оценку

$$|N_p-p|\leqslant(n-1)\left(p-\frac{(n-3)(n-4)}{n}\right)^{1/2},$$

которая при больших значениях n оказывается сильнее оценки Хассе — Вейля.

Будем трактовать сравнение (3) как уравнение

$$y^2=f(x)$$

над полем классов вычетов F_p по простому модулю p, состоящим из p элементов. Разделим элементы поля F_p на три класса: A, B и C. В класс A отнесем те элементы $\alpha\in F_p$, для которых $1-f(\alpha)^{\frac{p-1}{2}}=0$, в класс B — те элементы $\alpha\in F_p$, для которых $1+f(\alpha)^{\frac{p-1}{2}}=0$ и в класс C — те $\alpha\in F_p$, для которых $f(\alpha)=0$. Обозначим через $|A|$, $|B|$ и $|C|$ число элементов в классах A, B и C соответственно. Мы имеем:

$$|A|+|B|+|C|=p \quad \text{и} \quad N_p=2|A|+|C|.$$

Обозначим, далее, через $D=2\frac{d}{dx}$ оператор дифференцирования в кольце $F_p[x]$ многочленов от переменного x с коэффициентами из F_p. Под производной $\frac{d}{dx}g(x)=g'(x)$ мы снова будем понимать формальную производную многочлена $g(x)\in F[x]$.

Рассмотрим многочлен

$$R_0(x)=\left(1+f(x)^{\frac{p-1}{2}}\right)\sum_{j=1}^{2m} r_j^{(0)}(x)\,(x^p-x)^{j-1}+$$

$$+\sum_{j=1}^{2m} t_j^{(0)}(x)(x^p-x)^j,$$

где $m\leqslant\frac{p-1}{2}$ — натуральное число и $r_j^{(0)}(x)$, $t_j^{(0)}(x)$ — некоторые многочлены из кольца $F_p[x]$. Ясно, что все элементы класса B являются корнями этого многочлена. Положим $Ri(x)=DiR_0(x)$ и

$$R_i^*(x)=\left(1+f(x)^{\frac{p-1}{2}}\right)\sum_{j=1}^{2m} r_j^{(i)}(x)\,(x^p-x)^{j-1}+$$

$$+\sum_{j=1}^{2m} t_j^{(i)}(x)\,(x^p-x)^j,\quad i=1,2,\ldots,$$

где $r_j^{(i)}(x)$, $t_j^{(i)}(x)$ задаются рекурентными соотношениями

$$r_j^{(i)}=Dr_j^{(i-1)}-2jr_{j+1}^{(i-1)}-\frac{f'}{f}r_j^{(i-1)},$$

$$t_j^{(i)}=Dt_j^{(i-1)}-2(j+1)\,t_{j+1}^{(i-1)}+\frac{f'}{f}r_{j+1}^{(i-1)} \qquad (4)$$

с начальными значениями $r_j^{(0)}(x)$, $t_j^{(0)}(x)$, $j=1, 2, \ldots$, такими, что $r_j^{(0)}=t_j^{(0)}=0$ при $j>2m$. Пусть для некоторого i выполнено равенство $R_i(x)=R_i^*(x)$ и пусть $F_k^{(j)}(x)$ определены рекуррентными соотношениями

$$F_1^{(1)}=\frac{f'}{f}, \qquad (5)$$

$$F_k^{(j)}=DF_k^{(j-1)}+2(k-1)F_{k-1}^{(j-1)}+\frac{f'}{f}F_k^{(j-1)},\ k=1,2,\ldots,j-1,$$

$$F_j^{(j)}=2(j-1)F_{j-1}^{(j-1)}+2^{j-1}(j-1)!\,\frac{f'}{f}.$$

Докажем индукцией по s, что если

$$2^j j!\ t_j^i=\sum_{k=1}^{i} F_k^i\ r_k^i,\ j=1,2,\ldots,s;\ s<p-1,$$

то $R_{i+1}(x)=R_{i+l}^*(x)$ при всех $l=1, 2, \ldots, s$. Мы имеем:

$$R_{i+1}(x)=DR_i(x)=DR_i^*(x)=-f^{\frac{p-1}{1}}\frac{f'}{f}\sum_{j=1}^{2m} r_j^{(i)}(x^p-x)^{j-1}+$$

$$+\left(1+f^{\frac{p-1}{2}}\right)\sum_{j=1}^{2m}\left(Dr_j^{(i)}\right)(x^p-x)^{j-1}-\left(1+f^{\frac{p-1}{2}}\right)\times$$

$$\times\sum_{j=1}^{2m} 2(j-1)\,r_j^{(i)}(x^p-x)^{j-2}+\sum_{j=1}^{2m}\left(Dt_j^{(i)}\right)(x^p-x)^j-$$

$$-\sum_{j=1}^{2m} 2jt_j^{(i)}(x^p-x)^{j-1}.$$

Следовательно,

$$R_{i+1}(x)=\left(1+f^{\frac{p-1}{2}}\right)\sum_{j=1}^{2m-1}\left(Dr_j^{(i)}-2jr_{j+1}^i-\frac{f'}{f}r_j^{(i)}\right)\times$$

$$\times(x^p-x)^{j-1}+\left(1+f^{\frac{p-1}{2}}\right)\left(Dr_{2m}^{(i)}-\frac{f'}{f}r_{2m}^{(i)}\right)(x^p-x)^{2m-1}+$$

$$+Dt_{2m}^{(i)}(x^p-x)^{2m}+\sum_{j=1}^{2m-1}\left(Dt_j^{(i)}-2(j+1)\,t_{j+1}^{(i)}+\frac{f'}{f}r_{j+1}^{(i)}\right)\times$$

$$\times(x^p-x)^j+\frac{f'}{f}r_1^{(i)}-2t_1^{(i)}$$

и по формулам (4)

$$R_{i+1}(x)=R_{i+1}^*(x)+\frac{f'}{f}r_1^{(i)}-2t_1^{(i)}.$$

Отсюда следует, что утверждение справедливо для $s=1$. Предположим теперь, что наше утверждение справедливо

для $s \geqslant 1$, и докажем его справедливость для $s+1$. Мы имеем:

$$2^j j! \; t_j^i = \sum_{k=1}^{i} F_k^i \; r_k^i, \qquad j=1, \; 2, \; \ldots, \; s+1 \tag{6}$$

и, следовательно, $R_{i+1}(x)=R_{i+1}^*(x)$. Далее, по формулам (5) мы имеем при $j=2, 3, \ldots, s+1$

$$2^j j! t_j^{(i)} = \sum_{k=1}^{j-1} \left(DF_k^{(j-1)}\right) r_k^{(i)} + 2 \sum_{k=1}^{j-1} k F_k^{(j-1)} r_{k+1}^{(i)} +$$

$$+ \frac{f'}{f} \sum_{k=1}^{j-1} F_k^{(j-1)} r_k^{(i)} + 2^{j-1}(j-1)! \frac{f'}{f} r_j^{(i)}.$$

Отсюда

$$2^j j! t_j^{(i)} = D\left(\sum_{k=1}^{j-1} F_k^{(j-1)} r_k^{(i)}\right) - \sum_{k=1}^{j-1} F_k^{(j-1)} \times$$

$$\times \left(Dr_k^{(i)} - 2kr_{k+1}^{(i)} - \frac{f'}{f} r_k^{(i)}\right) + 2^{j-1}(j-1)! \frac{f'}{f} r_j^{(i)}$$

и по формулам (4) и (6)

$$2^j j! t_j^{(i)} = 2^{j-1}(j-1)! \, Dt_{j-1}^{(i)} - \sum_{k=1}^{j-1} F_k^{(j-1)} r_k^{(i+1)} +$$

$$+ 2^{j-1}(j-1)! \frac{f}{f} r_j^{(i)}.$$

Следовательно,

$$2^{j-1}(j-1)! \; t_{j-1}^{(i+1)} = \sum_{k=1}^{j-1} F_k^{(i-1)} \; r_k^{(j+1)}, \; j=2, \; 3, \; \ldots, \; s+1$$

и по индуктивному предположению $R_{i+l}(x)=R_{i+l}^*(x)$ при $l=2, 3, \ldots, s+1$. Тем самым утверждение справедливо для всех $s<p-1$.

Л е м м а. *Пусть $g(x)$ — не равный нулю многочлен с коэффициентами из поля F_p и $s<p+1$ — натуральное число. Если $g(\alpha)=g'(\alpha)=g''(\alpha)= \ldots =g^{s-1}(\alpha)=0$, то α*

является по меньшей мере s-кратным корнем многочлена $g(x)$.

Утверждение леммы непосредственно следует из разложения

$$g(x) = g(\alpha + x - \alpha) = g(\alpha) + \frac{g'(\alpha)}{1!}(x-\alpha) +$$

$$+ \frac{g''(\alpha)}{2!}(x-\alpha)^2 + \ldots + \frac{g^{(s-1)}(\alpha)}{(s-1)!}(x-\alpha)^{s-1} + h(x)(x-\alpha)^s.$$

Выберем теперь коэффициенты $r_j^{(0)}(x)$, $t_j^{(0)}(x)$ многочлена $R_0(x)$ таким образом, чтобы выполнялись равенства

$$2^j j! t_j^{(0)} = \sum_{k=1}^{s} F_k^{(j)} r_k^{(0)}, \; j=1, \; 2, \; \ldots, \; 2m-1. \tag{7}$$

Тогда $R_i(x)=R_i^*(x)$ при $i=1, 2, \ldots, 2m-1$, и поскольку $r_j^{(i)}$, $t_j^{(i)}$, определенные соотношениями (4), являются рациональными функциями вида $r_j^{(i)}=\frac{R_j^{(i)}}{f^i}$, $t_j^{(i)}=\frac{T_j^{(i)}}{f^i}$, мы имеем по лемме, что все элементы класса B являются по меньшей мере $2m$-кратными корнями многочлена $R_0(x)$. Будем теперь добиваться, чтобы многочлен $R_0(x)$ имел не слишком высокую степень и, кроме того, чтобы $R_0(x) \neq 0$. Положим для этого $r_j^{(0)}(x)=t_j^{(0)}(x)=0$ при $j=m+1, \ldots, 2m-1$. Тогда система (7) перепишется в виде:

$$2^j j! t_j^{(0)} = \sum_{k=1}^{j} F_k^{(j)} r_k^{(0)}, \; j=1, \; 2, \; \ldots, \; m, \tag{8}$$

$$0 = \sum_{k=1}^{m} F_k^{(j)} r_k^{(0)}, \; j=m+1, \; \ldots, \; 2m-1. \tag{9}$$

Индукцией по j легко доказать, что $F_k^{(j)}(x)$ есть рациональные функции вида $F_k^{(j)}=\frac{P_k^{(j)}}{f^{j-k+1}}$, причем степени многочленов $P_k^{(j)}(x)$ не превосходят величин $(n-1)(j-k+1)$ соответственно. Положим $r_k^{(0)}=f^{m-k+1}r_k$. Тогда система (9) перейдет в эквивалентную систему

$$\sum_{k=1}^{m} P_k^{(j)} r_k = 0, \quad j = m+1, \ \ldots, \ 2m-1$$

с полиномиальными коэффициентами $P_k^{(j)}(x)$, которая нетривиальным образом разрешима в многочленах $r_k(x)$, степени которых не превосходят величины $(n-1)\,m^2$. Определим теперь многочлены $t_j^{(0)}(x)$, $j=1, 2, \ldots, m$ равенствами (8). Ясно, что степени δ_j, ω_k многочленов $r_j^{(0)}(x)$, $t_k^{(0)}(x)$ не превосходят величины $nm(m+1)$, и если мы возьмем

$(m+1)^2 \leqslant \frac{p}{2n}$, то

$$\delta_j + \frac{n}{2} < n(m+1)^2 \leqslant \frac{p}{2} \text{ и } \omega_k + \frac{n}{2} < n(m+1)^2 \leqslant \frac{p}{2} \quad (10)$$

(степень нулевого многочлена условимся считать равной $-\infty$). Обозначим через Δ_j и Ω_k степени многочленов $\left(1+f^{\frac{p-1}{2}}\right) r_j^{(0)}(x^p-x)^{j-1}$ и $t_k^{(0)}(x^p-x)^k$. Мы имеем $\Delta_j = \frac{n}{2}\,p - \frac{n}{2} + \delta_j + p(j-1)$ и $\Omega_k = \omega_k + pk$. Так как n нечетно, то из (10) следует, что $\Delta_j \neq \Omega_k$ при всех j, $k = 1, 2, \ldots, m$, для которых $r_j^{(0)}(x) \not\equiv 0$, $t_k^{(0)}(x) \not\equiv 0$, и что $\Delta_j > \Delta_k$, $\Omega_j > \Omega_k$ при всех $j > k$, для которых $r_j^{(0)}(x) \not\equiv 0$, $t_j^{(0)}(x) \not\equiv 0$. Далее, поскольку не все $r_j^{(0)}(x)$ равны нулю, отсюда следует, что члены

$$\left(1+f^{\frac{p-1}{2}}\right) r_j^{(0)}(x^p-x)^{j-1}, \quad t_k^{(0)}(x^p - x^k), \quad j, \ k = 1,2, \ \ldots, \ m$$

не смогут уничтожиться и, следовательно, $R_0(x) \not\equiv 0$. Кроме того, степень многочлена $R_0(x)$ не превосходит величины

$$mp + \frac{n(p-1)}{2} + nm(m+1).$$

Сравнивая число корней многочлена $R_0(x)$ с его степенью, мы получаем по теореме Лагранжа

$$2m|B| \leqslant mp + \frac{n(p-1)}{2} + nm(m+1).$$

Следовательно,

$$2m(p - |A| - |C|) \leqslant mp + \frac{n(p-1)}{2} + nm(m+1),$$

и поскольку $|C| \leqslant n$, то

$$mN_p = m(2|A| + |C|) \geqslant mp - \frac{n(p-1)}{2} - nm(m+2).$$

Взяв теперь $m = \left[\left(\frac{p}{2n}\right)^{1/2}\right] - 1$, мы получаем

$$N_p \geqslant p - c(n)\,p^{1/2}.$$

Аналогичные рассуждения, проведенные для многочлена

$$S_0(x) = \left(1 - f(x)^{\frac{p-1}{2}}\right) \sum_{j=1}^{2m} r_j^{(0)}(x)(x^p-x)^{j-1} + \sum_{j=1}^{2m} t_j^{(0)}(x)(x^p-x)^j$$

дают

$$N_p \leqslant p - c(n)\,p^{1/2}.$$

Следовательно,

$$|N_p - p| \leqslant c(n)\,p^{1/2},$$

и тем самым теорема доказана.

Заметим, что полученная нами оценка для величины N_p может быть выражена в виде:

$$\left| \sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right) \right| \leqslant c(n)\,p^{1/2}.$$

4. Воспользуемся теперь полученными нами результатами для изучения законов распределения степенных вычетов и невычетов по простому модулю p. В главе 1 мы показали, что при $p>2$ имеется в точности $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов по модулю p. Однако

мы ничего не говорили о том, каким образом они расположены среди чисел 1, 2, ..., $p-1$.

Обозначим через $d(p)$ максимальное расстояние между соседними невычетами, через $n(p)$ — наименьший квадратичный невычет и через $r(p)$ — наименьший простой вычет по модулю p среди чисел 1, 2, ..., $p-1$.

Первые результаты в вопросе о распределении квадратичных вычетов и невычетов были получены И. М. Виноградовым [2]. В частности, для наименьшего квадратичного невычета в 1914 году им была доказана оценка

$$n(p) \leqslant c p^{\frac{1}{2e^{1/2}}} (\ln p)^2,$$

где e — неперово число (основание натурального логарифма, $e=2.718281\ldots$).

И. М. Виноградов высказал также ряд гипотез о поведении величин $d(p)$, $n(p)$ и $r(p)$, а именно: *для любого фиксированного* $\varepsilon>0$

$$\text{I. } \frac{d(p)}{p^\varepsilon} \longrightarrow 0, \quad \text{II. } \frac{n(p)}{p^\varepsilon} \longrightarrow 0, \quad \text{III. } \frac{r(p)}{p^\varepsilon} \longrightarrow 0$$

при $p \to \infty$.

В настоящее время мы далеки от доказательства этих гипотез. Особенно трудной представляется гипотеза I, которая в отличие от гипотез II и III не следует даже из расширенной гипотезы Римана для L-рядов Дирихле.

Наиболее сильный результат о поведении величин $d(p)$ и $n(p)$ дает следующая теорема, принадлежащая Д. Берджессу [10].

Теорема. *Для любого* $\varepsilon>0$ *существуют* $\delta=\delta(\varepsilon)>0$ *и* $p_0=p_0(\varepsilon)$, *такие, что при* $H > p^{\frac{1}{4}+\varepsilon}$, $p>p_0$ *и любом* N *справедлива оценка*

$$\left|\sum_{x=N+1}^{N+H} \left(\frac{x}{p}\right)\right| < Hp^{-\delta}.$$

Следствие. *Для любого* $\delta>0$ *существует константа* $p_1=p_1(\delta)$, *такая, что при* $p>p_1$ *имеет место неравенство*

$$n(p) < p^{\frac{1}{4e^{1/2}}+\delta}.$$

Основой для доказательства теоремы Берджесса является полученная нами выше оценка

$$\left|\sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right)\right| \leqslant c(n)\, p^{1/2}. \tag{11}$$

Вывод теоремы Берджесса из этой оценки, который мы здесь приведем, принадлежит А. А. Карацубе [4].

Докажем предварительно три леммы.

Лемма 1. (неравенство Гёльдера). *Пусть* a_i, b_i, $i=1, 2, \ldots, N$ *и* α, β — *неотрицательные действительные числа, причем* $\frac{1}{\alpha}+\frac{1}{\beta}=1$. *Тогда*

$$\sum_{i=1}^{N} a_i b_i \leqslant \left(\sum_{i=1}^{N} a_i^\alpha\right)^{1/\alpha} \left(\sum_{i=1}^{N} b_i^\beta\right)^{1/\beta}.$$

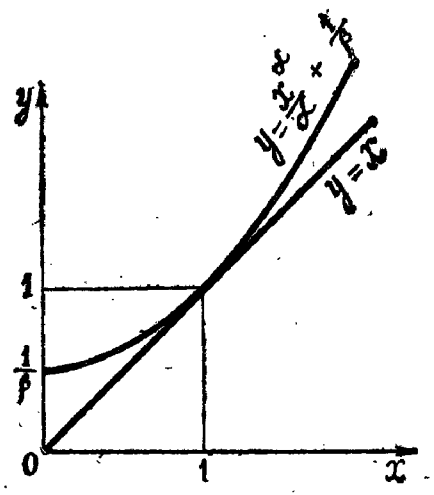
Будем предполагать, что a_i и b_i не все равны нулю (в противном случае нечего было бы доказывать). Рассмотрим при $x>0$ функции $f(x)=x$ и $g(x)=\frac{x^\alpha}{\alpha}+\frac{1}{\beta}$. Мы имеем $f(1)=g(1)=1$ и $f'(1)=g'(1)=1$. Следовательно, прямая $y=x$ является касательной к кривой $y=\frac{x^\alpha}{\alpha}+\frac{1}{\beta}$, и поскольку производная $g'(x)=x^{\alpha-1}$ ($\alpha>1$) функции $g(x)$ монотонно возрастает с ростом x, то график функции $y=\frac{x^\alpha}{\alpha}+\frac{1}{\beta}$ при $x>0$ расположен выше графика функции $y=x$ (см. рисунок.) Отсюда мы получаем:

$$x \leqslant \frac{x^\alpha}{\alpha}+\frac{1}{\beta},$$

и если мы положим $x=uv^{1-\beta}$, где u, $v>0$, то

$$uv^{1-\beta} \leqslant \frac{u^\alpha v^{(1-\beta)\alpha}}{\alpha}+\frac{1}{\beta}.$$

$$uv = (uv^{1-\beta})\, v^{\beta} \leqslant \frac{u^{\alpha}\, v^{\alpha+\beta-\alpha\beta}}{\alpha} + \frac{v^{\beta}}{\beta},$$



Следовательно,

и из равенства $\frac{1}{\alpha} + \frac{1}{\beta} = 1$ мы имеем:

$$uv \leqslant \frac{u^{\alpha}}{\alpha} + \frac{v^{\beta}}{\beta}.$$

Положим

$$u_i = \frac{a_i}{\left(\sum\limits_{i=1}^{N} a_i^{\alpha}\right)^{1/\alpha}}, \quad v_i = \frac{b_i}{\left(\sum\limits_{i=1}^{N} b_i^{\beta}\right)^{1/\beta}}.$$

Тогда из последнего неравенства следует:

$$\sum_{i=1}^{N} a_i b_i \leqslant \left(\frac{1}{\alpha} + \frac{1}{\beta}\right) \left(\sum_{i=1}^{N} a_i^{\alpha}\right)^{1/\alpha} \left(\sum_{i=1}^{N} b_i^{\beta}\right)^{1/\beta} =$$

$$= \left(\sum_{i=1}^{N} a_i^{\alpha}\right)^{1/\alpha} \left(\sum_{i=1}^{N} b_i^{\beta}\right)^{1/\beta},$$

и тем самым лемма I доказана.

Л е м м а 2. *Пусть N — количество решений сравнения $xy \equiv x'y' \pmod p$, где $1 \leqslant x, x' \leqslant H$, $1 \leqslant y, y' \leqslant H_1$, $1 \leqslant HH_1 < p$. Тогда при любом $\omega > 0$ справедлива оценка $N \leqslant c(HH_1)^{1+\omega}$, где $c > 0$ — некоторая константа.*

Поскольку $HH_1 < p$, то N равно числу решений в целых x, y, x', y', $1 \leqslant x, x' \leqslant H$, $1 \leqslant y, y' \leqslant H_1$ уравнения $xy = x'y'$. Обозначим через $d(n)$ количество решений в x', y' уравнения $x'y' = n$ и заметим, что если $n = p^{\alpha_1} \dots p_s^{\alpha_s}$, то $d(n) = (\alpha_1 + 1) \dots (\alpha_s + 1)$. Отсюда следует, что $d(mn) \leqslant d(m)\, d(n)$, и тогда

$$N = \sum_{x=1}^{H} \sum_{y=1}^{H_1} d(xy) \leqslant \left(\sum_{x=1}^{H} d(x)\right)\left(\sum_{y=1}^{H_1} d(y)\right).$$

Далее, мы имеем:

$$\sum_{n=1}^{t} d(n) = \sum_{1 \leqslant xy \leqslant t} 1 = \sum_{x=1}^{t} \left[\frac{t}{x}\right] \leqslant c_0 t \log t$$

и, следовательно,

$$N \leqslant c\,(HH_1)^{1+\omega}.$$

Лемма доказана.

Следующая лемма принадлежит Давенпорту и Эрдешу:

Л е м м а 3. *Пусть r — натуральное число, p — простое число и $1 \leqslant h \leqslant p-1$ — целое число. Тогда*

$$\sum_{x=0}^{p-1} \left(\sum_{\lambda=1}^{h} \left(\frac{x+\lambda}{p}\right)\right)^{2r} \leqslant (2r)^r p h^r + c\,(r)\, p^{1/2} h^{2r},$$

где $c(r)$ — некоторая константа, зависящая лишь от r.

Мы имеем:

$$\sum_{x=0}^{p-1} \left(\sum_{\lambda=1}^{h} \left(\frac{x+\lambda}{p}\right)\right)^{2r} = \sum_{\lambda_1=1}^{h} \dots \sum_{\lambda_{2r}=1}^{h} \sum_{x=0}^{p-1} \left(\frac{(x+\lambda_1)\dots(x+\lambda_{2r})}{p}\right).$$

Разобьем наборы $(\lambda_1, \dots, \lambda_{2r})$ на два класса: A и B. В класс A отнесем те $(\lambda_1, \dots, \lambda_{2r})$, в которых λ_i имеют не более r различных значений, и каждое такое значение встречается четное число раз; остальные наборы $(\lambda_1, \dots, \lambda_{2r})$ отнесем в класс B. Число наборов первого класса не превосходит величины $(2r)^r h^r$, и так как

$$\left|\sum_{x=0}^{p-1}\left(\frac{(x+\lambda_1)\ldots(x+\lambda_{2r})}{p}\right)\right|\leqslant p,$$

то

$$\sum_{\substack{\lambda_1=1\\(\lambda_1,\ldots,\lambda_{2r})\in A}}^{h}\cdots\sum_{\lambda_{2r}=1}^{h}\sum_{x=0}^{p-1}\left(\frac{(x+\lambda_1)\ldots(x+\lambda_{2r})}{p}\right)\leqslant$$

$$\leqslant\sum_{\substack{\lambda_1=1\\(\lambda_1,\ldots,\lambda_{2r})\in A}}^{h}\cdots\sum_{\lambda_{2r}=1}^{h}\left|\sum_{x=0}^{p-1}\left(\frac{(x+\lambda_1)\ldots(x+\lambda_{2r})}{p}\right)\right|\leqslant(2r)^r ph^r.$$

Число наборов класса B не превосходит величины h^{2r}, и для каждого набора $(\lambda_1, \ldots, \lambda_{2r})\in B$ мы имеем:

$$\sum_{x=0}^{p-1}\left(\frac{(x+\lambda_1)\ldots(x+\lambda_{2r})}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{(x+\tau_1)^{e_1}\ldots(x+\tau_s)^{e_s}}{p}\right),$$

где $s\leqslant 2r$, $\tau_1, \ldots, \tau_s$ попарно несравнимы между собой по модулю p и $e_1, \ldots, e_s$ не все четные. Выбросим теперь в последней сумме те множители $(x+\tau_i)^{e_i}$, в которых e_i четно. Тогда она запишется в виде

$$S=\sum_{x=0}^{p-1}\left(\frac{(x+\alpha_1)\ldots(x+\alpha_n)}{p}\right),$$

где $1\leqslant n\leqslant 2r$ и $\alpha_1, \ldots, \alpha_n$ попарно несравнимы по модулю p. Если n нечетно, то мы имеем по (11)

$$S\leqslant c'(n)\,p^{1/2}.$$

Если же n четное число, то, положив $x+\alpha_1=y^{-1}$, мы получим

$$S=\sum_{x=0}^{p-1}\left(\frac{(x+\alpha_1)\ldots(x+\alpha_n)}{p}\right)=\sum_{y=1}^{p-1}\left(\frac{(1+\beta_1 y)\ldots(1-\beta_{n-1}y)}{p}\right),$$

и тогда снова по (11)

$$|S|\leqslant c^*(n)\,p^{1/2}.$$

Следовательно,

$$\sum_{x=0}^{p-1}\left(\sum_{\lambda=1}^{h}\left(\frac{x+\lambda}{p}\right)\right)^2\leqslant(2r)^r ph^r+c\,(r)\,p^{1/2}h^{2r}$$

и этим лемма 3 доказана.

Перейдем теперь к доказательству теоремы Берджесса. Докажем сначала оценку

$$\left|\sum_{x=N+1}^{N+1-1}\left(\frac{x}{p}\right)\right|\leqslant cp^{1/2}\ln p,$$

полученную И. М. Виноградовым в 1914 году. Для простоты будем считать, что $N=0$. Введем в рассмотрение сумму Гаусса.

$$S=\sum_{y=1}^{p-1}\left(\frac{y}{p}\right)e^{2\pi i\frac{y}{p}},$$

где e — неперово число, $i=(-1)^{1/2}$, $\pi=3{,}14\ldots$, и воспользуемся равенством $|S|=p^{1/2}$, которое мы докажем в следующей главе. При $x\not\equiv 0 \pmod p$ мы имеем:

$$\left(\frac{x}{p}\right)S=\left(\frac{x^{-1}}{p}\right)S=\sum_{y=1}^{p-1}\left(\frac{x^{-1}y}{p}\right)e^{2\pi i\frac{y}{p}}=\sum_{t=1}^{p-1}\left(\frac{t}{p}\right)e^{2\pi i\frac{xt}{p}}$$

и, следовательно,

$$S\sum_{x=1}^{H}\left(\frac{x}{p}\right)=\sum_{t=1}^{p-1}\left(\frac{t}{p}\right)\sum_{x=1}^{H}e^{2\pi i\frac{xt}{p}}.$$

Отсюда

$$\left|\sum_{x=1}^{H}\left(\frac{x}{p}\right)\right|\leqslant\frac{1}{p^{1/2}}\sum_{t=1}^{p-1}\left|\sum_{x=1}^{H}e^{2\pi i\frac{xt}{p}}\right|$$

и по формуле для суммы геометрической прогрессии

$$\left|\sum_{x=1}^{H}\left(\frac{x}{p}\right)\right|\leqslant\frac{1}{p^{1/2}}\sum_{t=1}^{p-1}\left|\frac{e^{2\pi i\frac{t}{p}}-e^{2\pi i\frac{(H+1)t}{p}}}{1-e^{2\pi i\frac{t}{p}}}\right|\leqslant$$

$$\leqslant \frac{2}{p^{1/2}} \sum_{t=1}^{p-1} \frac{1}{\left|1 - e^{2\pi i \frac{t}{p}}\right|} = \frac{1}{p^{1/2}} \sum_{t=1}^{p-1} \frac{1}{\left|e^{\pi i \frac{t}{p}} - e^{-\pi i \frac{t}{p}}\right|}.$$

Но $e^{\pi i \frac{t}{p}} - e^{-\pi i \frac{t}{p}} = 2i \sin \frac{\pi t}{p}$, тогда

$$\left|\sum_{x=1}^{H} \left(\frac{x}{p}\right)\right| \leqslant \frac{1}{p^{1/2}} \sum_{t=1}^{p-1} \frac{1}{\sin \frac{\pi t}{p}} = \frac{2}{p^{1/2}} \sum_{t=1}^{\frac{p-1}{2}} \frac{1}{\sin \frac{\pi t}{p}}.$$

Из графика функции $y = \sin \frac{\pi t}{p}$ легко видеть, что $\sin \frac{\pi t}{p} \geqslant \frac{2t}{p}$ и, следовательно,

$$\left|\sum_{x=1}^{H} \left(\frac{y}{p}\right)\right| \leqslant p^{1/2} \sum_{t=1}^{\frac{p-1}{2}} \frac{1}{t} \leqslant cp^{1/2} \ln p.$$

Ввиду этой оценки мы можем предположить, что

$p^{\frac{1}{4}+\varepsilon} \leqslant H \leqslant p^{\frac{1}{2}+\frac{\varepsilon}{8}}$, где $0<\varepsilon<0{,}01$.

Положим

$$r = \left[\frac{1}{\varepsilon}\right] + 1, \quad \delta = \frac{\varepsilon}{4}\left(r + \frac{1}{2}\right)^{-1}, \quad H_1 = Hp^{-\frac{1}{2r}-\delta},$$

$$H_2 = p^{\frac{1}{2r}}$$

и введем в рассмотрение символ $O(\ldots)$. Пусть функции $f(x)$ и $g(x)>0$ определены для всех достаточно больших значений переменного x. Тогда запись $f(x)=O(g(x))$ будет означать, что $|f(x)| \leqslant Ag(x)$ при всех достаточно больших значениях x, где $A>0$ — некоторая константа.

При $1 \leqslant y \leqslant H_1$, $1 \leqslant z \leqslant H_2$ мы имеем

$$\sum_{x=1}^{H} \left(\frac{x}{p}\right) = \sum_{x=1}^{H} \left(\frac{x+yz}{p}\right) + O(Hp^{-\delta}),$$

и, суммируя обе части этого равенства, по всем таким y и z, получаем

$$\sum_{x=1}^{H} \left(\frac{x}{p}\right) = W + O(Hp^{-\delta}),$$

где

$$W = (H_1H_2)^{-1} \sum_{x=1}^{H} \sum_{y=1}^{H_1} \sum_{z=1}^{H_2} \left(\frac{x+yz}{p}\right).$$

Оценим сумму W. Мы имеем:

$$|W| \leqslant (H_1H_2)^{-1} \sum_{\lambda} N(\lambda) \sum_{z=1}^{H_2} \left(\frac{\lambda+z}{p}\right),$$

где $N(\lambda)$ — число решений сравнения $xy^{-1} \equiv \lambda \pmod p$.

Положив, далее, $\alpha = \frac{r}{r-1}$, $\beta = r$, $a_\lambda = N(\lambda)^{\frac{r-1}{r}}$, $b_\lambda = \left|N(\lambda)^{\frac{1}{r}} \sum_{z=1}^{H_2} \left(\frac{\lambda+z}{p}\right)\right|$, мы получаем по лемме 1

$$|W|^r \leqslant (H_1H_2)^{-r} \left(\sum_{\lambda} N(\lambda)\right)^{r-1} \left(\sum_{\lambda} N(\lambda) \left|\sum_{z=1}^{H_2} \left(\frac{\lambda+z}{p}\right)\right|^r\right).$$

В таком случае

$$|W|^{2r} \leqslant (H_1H_2)^{-2r} \left(\sum_{\lambda} N(\lambda)\right)^{2(r-1)} \left(\sum_{\lambda} N(\lambda) \left|\sum_{z=1}^{H_2} \left(\frac{\lambda+z}{p}\right)\right|^r\right)^2,$$

и так как (снова по лемме 1 с $\alpha=\beta=2$)

$$\left(\sum_{\lambda} N(\lambda) \left|\sum_{z=1}^{H_2} \left(\frac{\lambda+z}{p}\right)\right|^r\right)^2 \leqslant \sum_{\lambda} N(\lambda)^2 \sum_{\lambda} \left|\sum_{z=1}^{H_2} \left(\frac{\lambda+z}{p}\right)\right|^{2r},$$

то

$$|W|^{2r} \leqslant (H_1H_2)^{-2r} \left(\sum_{\lambda} N(\lambda)\right)^{2(r-1)} \sum_{\lambda} N(\lambda)^2 \sum_{\lambda} \left|\sum_{z=1}^{H_2} \left(\frac{\lambda+z}{p}\right)\right|^{2r}.$$

Далее, поскольку

$$\sum_{\lambda} N(\lambda) = HH_1 \quad \text{и} \quad \sum_{\lambda} N(\lambda)^2 = N,$$

мы имеем по лемме 2:

$$|W|^{2r} \leqslant c\,(H_1H_2)^{-2r}\,(HH_1)^{2(r-1)}\,(HH_1)^{1+\omega}\sum_{\lambda=0}^{p-1}\left|\sum_{z=1}^{H_2}\left(\frac{\lambda+z}{p}\right)\right|^{2r},$$

и на основании леммы 3

$$|W| \leqslant Hp^{-\delta'}.$$

Следовательно,

$$\left|\sum_{x=1}^{H}\left(\frac{x}{p}\right)\right| < Hp^{-\delta},$$

и этим теорема Берджесса доказана.

Перейдем теперь к доказательству следствия. Возьмем $\varepsilon>0$ и положим $H=\left[p^{\frac{1}{4}+\varepsilon}\right]$. Если $n(p)\leqslant H^{1/2}$, то $n(p)\leqslant p^{\frac{1}{8}+\frac{\varepsilon}{2}} < p^{\frac{1}{4e^{1/2}}+\frac{\varepsilon}{2}}$, и в этом случае следствие доказано. Пусть теперь $n(p)>H^{1/2}$ и $\left(\frac{m}{p}\right)=-1$, при $m\leqslant H$. Поскольку для любого неотрицательного квадратичного невычета r мы имеем $r\geqslant n(p)$, то среди простых делителей числа m может быть лишь один квадратичный невычет, иначе неравенство $n(p)>H^{1/2}$ было бы противоречиво. Таким образом, $m=qt$, где q—простое число, $\left(\frac{q}{p}\right)=-1$, и $n(p)\leqslant q\leqslant H$. Далее, поскольку

$$\sum_{\left(\frac{m}{p}\right)=+1}^{H} 1 + \sum_{\left(\frac{m}{p}\right)=-1} 1 = H,$$

то

$$\sum_{m=1}^{H}\left(\frac{m}{p}\right) = \sum_{\left(\frac{m}{p}\right)=+1} 1 - \sum_{\left(\frac{m}{p}\right)=-1} 1 \geqslant H - 2\sum_{\substack{m=1\\ m=qt\\ n(p)\leqslant q\leqslant H}} 1 =$$

$$= H - 2\sum_{n(p)\leqslant q\leqslant H}\left[\frac{H}{q}\right] \geqslant H\left(1-2\sum_{n(p)\leqslant q\leqslant H} q^{-1}\right),$$

где последняя сумма берется по всем простым q, $n(p)\leqslant q\leqslant H$. По теореме Берджесса мы получаем отсюда, что

$$1-2\sum_{n(p)\leqslant q\leqslant H} q^{-1} < p^{-\delta'},\ \delta>0,$$

так что

$$\sum_{n(p)\leqslant q\leqslant H} q^{-1} > \frac{1}{2}\left(1-p^{-\delta'}\right).$$

Воспользуемся теперь следующим фактом из теории простых чисел (см. [7], гл. VII, § 5):

$$\sum_{1\leqslant q\leqslant H}\frac{1}{q} = \log\log H + C + O\left(\frac{1}{\log H}\right).$$

Тогда

$$\log\frac{\log H}{\log n(p)} \geqslant \frac{1}{2} - \omega(p),$$

где $\omega(p)\to 0$ при $p\to\infty$, и, следовательно,

$$\frac{\log H}{\log n(p)} \geqslant e^{\frac{1}{2}-\omega(p)}.$$

Отсюда

$$n(p) \leqslant H^{\frac{1}{e^{1/2}}+\delta''} = p^{\frac{1}{4e^{1/2}}+\delta},$$

и тем самым следствие доказано.

Глава 4

СРАВНЕНИЯ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

Перейдем к изучению вопроса о количестве N_p решений сравнения

$$f(x_1, \ldots, x_n)\equiv 0 \pmod p, \qquad (1)$$

где $f(x_1, \ldots, x_n)$ — многочлен с целыми коэффициентами

от $n \geqslant 3$ переменных $x_1, \ldots, x_n$, и в качестве первого шага докажем следующий общий результат.

Лемма Шевалле. *Если степень r многочлена $f(x_1, \ldots, x_n)$ по совокупности переменных $x_1, \ldots, x_n$ строго меньше n, то число N_p решений сравнения* (1) *делится на p.*

Действительно, по малой теореме Ферма мы имеем

$$N_p = \sum_{x_1=0}^{p-1} \ldots \sum_{x_n=0}^{p-1} (1 - f^{p-1}(x_1, \ldots, x_n)) \equiv \sum_{i_1} \ldots \sum_{i_n} c(i_1, \ldots, i_n) \sum_{x_1=0}^{p-1} \ldots$$

$$\ldots \sum_{x_n=0}^{p-1} x_1^{i_1}, \ \ldots, \ x_n^{i_n} \pmod p,$$

где $i_1, \ldots, i_n$ — неотрицательные целые числа, такие, что $i_1 + \ldots + i_n \leqslant r(p-1)$. Если $i_s = 0$ хотя бы для одного $s = 1, 2, \ldots, n$, то

$$\sum_{x_1=0}^{p-1} \ldots \sum_{x_n=0}^{p-1} x_1^{i_1} \ldots x_n^{i_n} \equiv 0 \pmod p.$$

Если же все $i_1, \ldots, i_n$ отличны от нуля, то мы имеем

$$\sum_{x_1=0}^{p-1} \ldots \sum_{x_n=0}^{p-1} x_1^{i_1} \ \ldots \ x_n^{i_n} = \sum_{x_1=1}^{p-1} \ldots \sum_{x_n=1}^{p-1} x_1^{i_1} \ldots x_n^{i_n},$$

и положив $x_1 \equiv g^{y_1} \pmod p, \ldots, x_n \equiv g^{y_n} \pmod p$, где g — первообразный корень по модулю p, получаем

$$\sum_{x_1=0}^{p-1} \ldots \sum_{x_n=0}^{p-1} x_1^{i_1} \ldots x_n^{i_n} \equiv \sum_{y_1=1}^{p-1} \ldots \sum_{y_n=1}^{p-1} g^{i_1 y_1} \ldots g^{i_k y_n} \pmod p.$$

Далее, поскольку $i_1 + i_2 + \ldots + i_n < n(p-1)$, то хотя бы для одного $s = 1, 2, \ldots, n$ выполняются неравенства $0 < i_j < p-1$, и по формуле для суммы геометрической прогрессии мы имеем

$$\sum_{y_s=1}^{p-1} g^{i_s y_s} = \frac{g^{i_s} - g^{i_s p}}{1 - g^{i_s}} \equiv 0 \pmod p.$$

Следовательно, $N_p \equiv 0 \pmod p$, и лемма доказана.

2. Теория сравнений от многих переменных к настоящему времени развита довольно слабо, поэтому мы ограничимся изучением лишь некоторых вырожденных случаев. Рассмотрим сравнение

$$a_1 x_1^{l_1} + \ldots + a_n x_n^{l_n} \equiv 0 \pmod p \qquad (2)$$

и докажем следующий результат.

Теорема. *Пусть $\delta_i = (l_i, p-1)$, $i = 1, 2, \ldots, n$. Тогда для количества N_p решений сравнения* (2) *имеет место неравенство*

$$|N_p - p^{n-1}| \leqslant (\delta_1 - 1) \ldots (\delta_n - 1) p^{n/2}.$$

Для доказательства этой теоремы введем в рассмотрение суммы Гаусса

$$S_a = \sum_{x=0}^{p-1} e^{2\pi i \frac{ax^l}{p}}.$$

Лемма 1. *Пусть $p > 2$ — простое число и*

$$S_a = \sum_{x=0}^{p-1} e^{2\pi i \frac{ax^2}{p}}.$$

Тогда при $a \not\equiv 0 \pmod p$ имеет место равенство

$$|S_a| = p^{1/2}.$$

Мы имеем:

$$|S_a|^2 = S_a \cdot \bar{S}_a = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} e^{2\pi i \frac{a(x^2 - y^2)}{p}}$$

($\bar{S}_a$ — комплексно спряженная с S_a величина). Сделаем замену переменного $x = y + t$ и заметим, что когда x и y пробегают полную систему вычетов по модулю p, то y и t также пробегают независимо друг от друга полные системы вычетов по модулю p. В таком случае

$$|S_a|^2 = \sum_{t=0}^{p-1} \sum_{y=0}^{p-1} e^{2\pi i \frac{at^2 + 2aty}{p}} = \sum_{t=0}^{p-1} e^{2\pi i \frac{at^2}{p}} \sum_{y=0}^{p-1} e^{2\pi i \frac{2aty}{p}},$$

и поскольку

$$\sum_{y=0}^{p-1} e^{2\pi i\frac{2aty}{p}} = \begin{cases} p, & \text{если } 2at \equiv 0 \pmod p, \\ 0, & \text{если } 2at \not\equiv 0 \pmod p, \end{cases}$$

то

$$|S_a|^2 = p.$$

Лемма доказана.

Заметим, что при $a \not\equiv 0 \pmod p$

$$\sum_{x=0}^{p-1} e^{2\pi i\frac{ax^2}{p}} = \sum_{y=0}^{p-1} n(y)\, e^{2\pi i\frac{ay}{p}},$$

где $n(y)$ равно количеству решений сравнений $x^2 \equiv y \pmod p$. Отсюда по критерию Эйлера

$$\sum_{x=0}^{p-1} e^{2\pi i\frac{ax^2}{p}} = \sum_{y=0}^{p-1} \left(1 - \left(\frac{y}{p}\right)\right) e^{2\pi i\frac{ay}{p}} = \sum_{y=0}^{p-1} \left(\frac{y}{p}\right) e^{2\pi i\frac{ay}{p}}.$$

Л е м м а 2. *Пусть* $\delta = (l, p-1)$. *Тогда при* $a \not\equiv 0 \pmod p$ *имеет место оценка*

$$\left|\sum_{x=0}^{p-1} e^{2\pi i\frac{ax^l}{p}}\right| \leqslant (\delta - 1)\, p^{1/2}.$$

Если $\delta = 1$, то x^l вместе с x пробегает полную систему вычетов по модулю p, тогда

$$\sum_{x=0}^{p-1} e^{2\pi i\frac{axl}{p}} = \sum_{y=0}^{p-1} e^{2\pi i\frac{ay}{p}} = 0.$$

Предположим теперь, что $\delta > 1$. Мы имеем:

$$\sum_{x=0}^{p-1} e^{2\pi i\frac{ax^l}{p}} = \sum_{y=0}^{p-1} n(y)\, e^{2\pi i\frac{ay}{p}},$$

где $n(y)$ равно количеству решений сравнения $x^l \equiv y \pmod p$. Обозначим через g некоторый фиксированный первообразный корень по модулю p и положим $y \equiv g^\tau \pmod p$. Тогда по критерию Эйлера

$$n(y) = \begin{cases} 0, & \text{если } \tau \not\equiv 0 \pmod \delta \\ \delta, & \text{если } \tau \equiv 0 \pmod \delta \end{cases}$$

и, следовательно, $n(y) = \sum_{s=0}^{\delta-1} \chi_s(y)$, где

$$\chi_s(y) = e^{2\pi i\frac{s\tau}{\delta}},$$

Отсюда

$$\sum_{x=0}^{p-1} e^{2\pi i\frac{ax^l}{p}} = 1 + \sum_{y=1}^{p-1} \sum_{s=0}^{\delta-1} \chi_s(y)\, e^{2\pi i\frac{ay}{p}} = \sum_{s=1}^{\delta-1} \sum_{y=1}^{p-1} \chi_s(y)\, e^{2\pi i\frac{ay}{p}}. \tag{3}$$

Положим для $s = 1, \ldots, \delta-1$

$$T_s = \sum_{y=1}^{p-1} \chi_s(y)\, e^{2\pi i\frac{ay}{p}}$$

и покажем, что $|T_s| = p^{1/2}$. Мы имеем:

$$|T_s|^2 = \sum_{y=1}^{p-1} \sum_{t=1}^{p-1} \chi_s(y)\, \overline{\chi}_s(t)\, e^{2\pi i\frac{a(y-t)}{p}}.$$

Сделаем замену переменного $y = tz$ и заметим, что $\chi_s(tz) = \chi_s(t)\, \chi_s(z)$. Тогда

$$|T_s|^2 = \sum_{z=1}^{p-1} \chi_s(z) \sum_{t=1}^{p-1} e^{2\pi i\frac{at(z-1)}{p}},$$

и поскольку при $s \not\equiv 0 \pmod \delta$

$$\sum_{z=1}^{p-1} \chi_s(z) = \sum_{z=1}^{p-1} e^{2\pi i\frac{\omega s}{\delta}} = \sum_{\omega=0}^{p-2} e^{2\pi i\frac{s\frac{p-1}{\delta}\omega}{p-1}} = 0,$$

мы имеем:

$$|T_s|^2 = \sum_{z=1}^{p-1} \chi_s(z) \sum_{t=0}^{p-1} e^{2\pi i \frac{at(z-1)}{p}} =$$

$$= p + \sum_{z=2}^{p-1} \chi_s(z) \sum_{t=0}^{p-1} e^{2\pi i \frac{at(z-1)}{p}} = p.$$

Отсюда по (3)

$$\left| \sum_{x=0}^{p-1} e^{2\pi i \frac{ax^l}{p}} \right| \leqslant \sum_{s=1}^{\delta-1} \left| \sum_{y=1}^{p-1} \chi_s(y)\, e^{2\pi i \frac{ay}{p}} \right| = (\delta-1)\, p^{1/2},$$

и тем самым лемма 2 доказана.

Перейдем к доказательству теоремы. Мы имеем:

$$N_p = \frac{1}{p} \sum_{s=0}^{p-1} \sum_{x_1=0}^{p-1} \cdots \sum_{x_n=0}^{p-1} e^{2\pi i \frac{s\left(a_1 x_1^{l_1} + \ldots + a_n x_n^{l_n}\right)}{p}} =$$

$$= p^{n-1} + \frac{1}{p} \sum_{s=1}^{p-1} \prod_{j=1}^{n} \left(\sum_{x_j=0}^{p-1} e^{2\pi i \frac{s a_j x_j^{l_j}}{p}} \right).$$

Отсюда

$$|N_p - p^{n-1}| \leqslant \frac{1}{p} \sum_{s=1}^{p-1} \prod_{j=1}^{n} \left| \sum_{x_j=0}^{p-1} e^{2\pi i \frac{s a_j x_j^{l_j}}{p}} \right|,$$

и по лемме 2

$$|N_p - p^{n-1}| \leqslant \frac{p-1}{p} (\delta_1 - 1) \ldots (\delta_n - 1) p^{n/2} \leqslant (\delta_1 - 1) \ldots (\delta_n - 1) p^{n/2}.$$

Теорема доказана.

Аналогичным образом можно доказать, что для количества N_p решений сравнения

$$a_1 x_1^{l_1} + \ldots + a_n x_n^{l_n} \equiv a_0 \pmod{p},$$

при $a_0 \not\equiv 0 \pmod{p}$ справедлива оценка

$$|N_p - p^{n-1}| \leqslant A p^{\frac{n-1}{2}},$$

где константа A зависит лишь от $l_1, \ldots, l_n$.

В общем случае имеет место следующее утверждение.

Т е о р е м а. *Пусть многочлен $f(x_1, \ldots, x_n)$ неприводим в любом конечном расширении поля F_p. Тогда для количества N_p решений сравнения*

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p}$$

имеет место оценка

$$|N_p - p^{n-1}| \leqslant c(f)\, p^{n-1-1/2}.$$

Для $n=2$ теорему можно доказать тем же методом, каким мы в главе 2 получили оценку $|N_p - p| \leqslant c(f) p^{1/2}$ для числа N_p решений сравнения $y^2 \equiv f(x) \pmod{p}$. Переход от $n=2$ к случаю произвольного числа переменных совершается совсем просто.

3. В заключение рассмотрим некоторые приложения теории сравнений к диофантовым уравнениям. Прежде всего заметим, что из последней теоремы сравнительно просто выводится следующий результат.

С л е д с т в и е. *Если $f(x_1, \ldots, x_n)$ — абсолютно неприводимый многочлен с целыми коэффициентами, то сравнение*

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p^k} \qquad (4)$$

разрешимо для всех $k \geqslant 1$ и всех простых чисел p, больших некоторой границы, зависящей лишь от многочлена f.

Заметим далее, что разрешимость сравнения (4) для всех простых чисел p и всех натуральных k является необходимым условием для разрешимости соответствующего диофантова уравнения

$$f(x_1, \ldots, x_n) = 0.$$

Важность указанного выше следствия заключается в том, что оно сводит проверку этого условия только к конечному числу простых чисел p.

Для доказательства следствия достаточно показать, что число решений сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod p$ при достаточно больших p больше, чем число решений системы сравнений

$$f(x_1, \ldots, x_n) \equiv 0 \pmod p, \qquad f'_{x_n}(x_1, \ldots, x_n) \equiv 0 \pmod p. \tag{5}$$

В таком случае найдется набор классов вычетов $x_1 \equiv x_1^{(1)} \pmod p$, ..., $x_n \equiv x_n^{(1)} \pmod p$ такой, что $f(x_1^{(1)}, \ldots, x_n^{(1)}) \equiv 0 \pmod p$, $f'_{x_n}(x_1^{(1)}, \ldots, x_n^{(1)}) \not\equiv 0 \pmod p$, тогда, как было показано в начале главы 3, сравнение $f(x_1, \ldots, x_n) \equiv 0 \pmod{p^k}$ будет разрешимо при любом целом $k \geqslant 1$.

Докажем сначала, что если не все коэффициенты многочлена $g(x_1, \ldots, x_n)$ делятся на p, то для числа N_p решений сравнения $g(x_1, \ldots, x_n) \equiv 0 \pmod p$ справедливы оценки

$$N_p \leqslant Cp^{n-1},$$

где C — некоторая постоянная, зависящая лишь от многочлена g. Доказательство этого утверждения проведем индукцией по величине n. Для $n=1$ утверждение следует из теоремы Лагранжа. При $n>1$ рассмотрим многочлен $g(x_1, \ldots, x_n)$ как многочлен от $x_1, \ldots, x_{n-1}$, коэффициенты которого суть многочлены от переменной x_n. Обозначим через $d(x_n)$ наибольший общий делитель этих коэффициентов по модулю p. Тогда

$$f(x_1, \ldots, x_n) \equiv d(x_n) h(x_1, \ldots, x_n) \pmod p,$$

причем многочлен $h(x_1, \ldots, x_n)$ ни при каком значении x_n несравним тождественно с нулем по модулю p. Если $d(x_n) \equiv 0 \pmod p$, то $g(x_1, \ldots, x_n) \equiv 0 \pmod p$ для любых $x_1, \ldots, x_{n-1}$. Следовательно, число решений сравнения $g(x_1, \ldots, x_n) \equiv 0 \pmod p$, для которых $d(x_n) \equiv 0 \pmod p$ не превосходит Ap^{n-1}. Рассмотрим теперь те решения сравнения $g(x_1, \ldots, x_n) \equiv 0 \pmod p$, для которых $d(x_n) \not\equiv 0 \pmod p$. В этом случае для каждого такого $x_n \equiv a_n \pmod p$ многочлен $g(x_1, \ldots, x_{n-1}, a_n)$ несравним тождественно с нулем по модулю p, тогда по индуктивному предположению число $N_p(a_n)$ решений сравнения $g(x_1, \ldots, x_{n-1}, a_n) \equiv 0 \pmod p$ удовлетворяет неравенству $N_p(a_n) \leqslant Bp^{n-2}$. Так

как a_n принимает при этом не более p значений, то общее число решений сравнения $g(x_1, \ldots, x_n) \equiv 0 \pmod p$ не превосходит Cp^{n-1}.

Рассмотрим $f(x_1, \ldots, x_n)$ как многочлен от x_n с коэффициентами, являющимися многочленами от $x_1, \ldots, x_{n-1}$. Из абсолютной неприводимости f следует, что его дискриминант $D(x_1, \ldots, x_{n-1})$ не равен тождественно нулю по модулю p, иначе бы f делился на квадрат некоторого другого многочлена. Пусть простое число p не делит все коэффициенты многочлена $D(x_1, \ldots, x_n)$. Тогда если $x_1 = a_1 \pmod p$, ..., $x_n \equiv a_n \pmod p$ — решение системы (5), то $x_n \equiv a_n \pmod p$ является общим корнем по модулю p многочленов $f(a_1, \ldots, a_{n-1}, x_n)$ и $f'_{x_n}(a_1, \ldots, a_{n-1}, x_n)$, поэтому

$$D(a_1, \ldots, a_{n-1}) \equiv 0 \pmod p.$$

Но число систем $(a_1, \ldots, a_{n-1})$, удовлетворяющих последнему сравнению по доказанному выше, не превосходит величины Cp^{n-2}. Для заданных же $a_1, \ldots, a_{n-1}$ значения a_n определяются из сравнения $f(a_1, \ldots, a_{n-1}, x_n) \equiv 0 \pmod p$, поэтому их число не превосходит степени многочлена f по переменной x_n. Таким образом, количество N'_p решений системы (5) не превосходит величины Cp^{n-2}. Для количества же N_p решений сравнения $f(x_1, \ldots, x_n) \equiv 0 \pmod p$ мы имеем оценку $N_p > p^{n-1} - c(f) p^{n-1-\frac{1}{2}}$. Отсюда $N_p - N'_p > p^{n-2}(p - c(f) p^{1/2} - C)$, значит $N_p > N'_p$ при всех достаточно больших p. Следствие доказано.

Как мы уже отмечали, разрешимость серии сравнений

$$f(x_1, \ldots, x_n) \equiv 0 \pmod{p^k}$$

для всех простых p и всех целых $k \geqslant 1$ является необходимым условием для разрешимости уравнения

$$f(x_1, \ldots, x_n) = 0 \tag{6}$$

в целых $x_1, \ldots, x_n$. По доказанному выше, на самом деле, достаточно ограничиться проверкой этого условия для некоторого конечного множества простых чисел p. Например, уравнения

$$x^2+2y^2+5z^2=0$$

и

$$x^3+2y^3+7z^3=0$$

не разрешимы в отличных от нуля целых числах, поскольку соответствующие сравнения

$$x^2+2y^3+5z^2\equiv 0 \pmod{5^k}$$

и

$$x^3+2y^3+7z^3\equiv 0 \pmod{7^k},$$

$k=1, 2, \ldots$ имеют лишь тривиальное решение $x=y=z=0$.

Однако часто случается, что разрешимость сравнений (4) оказывается также и достаточным условием для разрешимости диофантова уравнения (6) в целых или рациональных числах, т. е. локальная разрешимость ведет к глобальной разрешимости. В качестве примера такой ситуации приведем следующую теорему Минковского — Хассе:

Т е о р е м а. *Уравнение*

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

где $\Phi(x_1, \ldots, x_n)=\sum_{ij} a_{ij}x_ix_j$ *— квадратичная форма с целыми коэффициентами* a_{ij}, *нетривиально разрешимо в целых числах (т. е. когда не все* x_i *равны нулю) тогда и только тогда, когда форма* Φ *является неопределенной (т. е. нетривиально представляет нуль в поле вещественных чисел) и когда для любого модуля вида* p^k *сравнение*

$$\Phi(x_1, \ldots, x_n)\equiv 0 \pmod{p^k} \qquad (7)$$

имеет решение, в котором значение хотя бы одной переменной не делится на p.

В частности, используя лемму Шевалле, легко показать, что при $n\geqslant 5$ сравнение (7) всегда разрешимо, и тем самым справедливо следующее утверждение (в дальнейшем под представлением формой нуля мы всегда будем понимать нетривиальное представление).

С л е д с т в и е. *Для того чтобы целочисленная неособенная квадратичная форма от* $n\geqslant 5$ *переменных представляла нуль в кольце целых чисел, необходимо и достаточно, чтобы она была неопределенной.*

Таким образом, всякая неопределенная квадратичная форма от достаточно большого числа переменных целочисленно представляет нуль, а тем самым и всякое целое число. Существует гипотеза Артина, что всякое уравнение

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

где $\Phi(x_1, \ldots, x_n)$ — целочисленная форма нечетной степени d, нетривиальным образом разрешимо в целых числах, если только $n>d^2$. Берч в 1957 году доказал, что всякая форма нечетной степени представляет нуль в кольце целых чисел, если число ее переменных достаточно велико по сравнению со степенью. Сама же гипотеза Артина доказана к настоящему времени лишь для случая $d=2$.

В заключение заметим, что в общей ситуации рассмотренный нами принцип перехода от локальных решений к глобальным неприменим. Например, как показал Рейхардт, уравнение

$$x^4-17=2y^2$$

не имеет решений в целых числах x, y и в то же время соответствующее сравнение

$$x^4-17\equiv 2y^2 \pmod{p^k}$$

разрешимо при всех $k\geqslant 1$ и для всех простых чисел p.

ЛИТЕРАТУРА

1. Виноградов И. М. Основы теории чисел. М., 1972.
2. Виноградов И. М. Избранные труды. М., 1952.
3. Гаусс К. Ф. Труды по теории чисел. М., 1959.
4. Карацуба А. А. Суммы характеров и первообразные корни в конечных полях. Доклады АН СССР, т. 180, № 6, (1968), 1287.
5. Степанов С. А. О числе точек гиперэллиптической кривой над простым конечным полем. Изв.АН СССР, сер. матем., 33, № 5 (1969), 1171.
6. Степанов С. А. Конструктивный метод в теории уравнений над конечными полями. Труды МИАН СССР, 132 (1973), 237.
7. Хассе Г. Лекции по теории чисел, ИЛ, 1953.
8. Чандрасекхаран К. Введение в аналитическую теорию чисел. М., 1974.
9. Artin E. Quadratische Körper in Gebiete der höheren Kongruenzen, II, Math. Z. 19 (1924), 207.
10. Burgess D. The distribution of quadratic residues and nonresidues, Mathematika, 4, No 8 (1957), 106.
11. Davenport H. On the distribution of quadratic residues (mod p) J. London Math. Soc. 6 (1931), 49.
12. Hasse H. Abstrakte Begründung der komplexen Multiplikation und Riemanushe Vermutung in Funktionenkörpern, Abh. Math. Sem. Hamburg, 10 (1934), 325.
13. Hopf H. Über die Verteilung quadratischen Reste, Math. Zeitschrift, 32 (1930), 222.
14. Mordell L. I. On a sum analogous to a Gauss's sum, Quart. J. Math., 3 (1932), 161.
15. Weil A. Sur les courbes algébriques et les variétés qui s'en déduisent, Act. Sci. Ind. 1041. Paris, 1948.

ОГЛАВЛЕНИЕ

Степанов Сергей Александрович

СРАВНЕНИЯ

Редактор В. И. Ковалев
Обложка Л. П. Ромасенко
Худож. редактор В. Н. Конюхов
Техн. редактор. Т. В. Самсонова
Корректор Т. Ю. Дорогова

А 10888. Индекс заказа 54311
Сдано в набор 13/VIII-1975 г.
Подписано к печати 16/X-1975 г.
Формат бумаги 84×108 1/32. Бумага
типографская № 3. Бум. л. 1. Печ. л. 2.
Усл. л. 3,36. Уч.-изд. л. 2,85 Тираж 46 340 экз.
Издательство «Знание». 101835, Москва
центр, проезд Серова, д. 4. Заказ 1682
Цена 11 коп.

Чеховский полиграфический комбинат
Союзполиграфпрома при Государственном
комитете Совета Министров СССР
по делам издательств, полиграфии
и книжной торговли
г. Чехов Московской области