Э. Гекке

Лекции по теории алгебраических чисел

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Э1

Э. Гекке
Э1 Лекции по теории алгебраических чисел / Э. Гекке – М.: Книга по Требованию, 2024. – 262 с.

ISBN 978-5-458-26212-5

Предлагаемая книга имеет своей целью, не предполагая у читателя никаких предварительных сведений из теории чисел, подвести его к пониманию вопросов, стоящих в центре внимания современной теории алгебраических числовых полей. Первые семь глав по материалу не содержат ничего нового. Что же касается формы изложения, то при выборе ее я исходил из современного развития математики и особенно арифметики и прежде всего всюду использовал способы выражения и методы теории групп, что дало возможность получить существенные формальные и идейные упрощения. Последняя, восьмая, глава ведет читателя к вершинам современной теории. В ней дается новое доказательство самых общих квадратичных законов взаимности в произвольных алгебраических числовых полях, проводимое с помощью тэта-функций и значительно более короткое, чем все известные до сих пор доказательства. Книга заканчивается доказательством существования поля классов относительной степени 2, получающимся здесь как следствие законов взаимности. В качестве предварительных сведений от читателя требуется лишь знание элементов дифференциального и интегрального исчислений и алгебры, а для последней главы - также элементов теории аналитических функций комплексного переменного.

ISBN 978-5-458-26212-5

ГЛАВА I

ЭЛЕМЕНТЫ ТЕОРИИ ЦЕЛЫХ РАЦИОНАЛЬНЫХ ЧИСЕЛ

§ 1. Делимость. Наибольший общий делитель. Модули. Простые числа. Основная теорема теории чисел

Предметом арифметики являются в первую очередь целые числа: $0, \pm 1, \pm 2, \ldots$; применение к ним операций сложения, вычитания, умножения и (в некоторых случаях) деления снова приводит к целым числам. Высшая арифметика подвергает подобному же исследованию также и другие классы вещественных или комплексных чисел, причем для получения своих предложений она употребляет аналитические средства, принадлежащие другим областям математики, как исчисление бесконечно малых и теория функций комплексного переменного. Так как в последних частях этой книги будет итти речь также и об этих отделах арифметики, то мы здесь предполагаем известной совокупность вещественных и (обыкновенных) комплексных чисел — числовую область, в которой четыре действия (за исключением деления на 0) неограниченно выполнимы, как это подробно устанавливается обычно в элементах алгебры или диференциального исчисления. В этой широкой области чисел выделяется одно число — единица, 1, — обладающее тем свойством, что уравнение

$$1 \cdot a = a$$

удовлетворяется при каждом a. Из числа 1 с помощью процессов сложения и вычитания получаются последовательно все *целые числа*, а если затем выполнить над ними процесс деления, то получится множество *рациональных чисел* как совокупность частных от деления целых чисел. Лишь далее, начиная с § 21, понятие „целое число“ подвергается существенному обобщению.

В этой вводной части мы кратко изложим основные предложения арифметики, касающиеся свойств делимости обыкновенных целых чисел.

В то время как при целых рациональных a, b выражения $a+b$, $a-b$, ab всегда дают опять целые числа, число $\frac{a}{b}$ — не обязательно целое. Если же оно целое, то мы имеем дело с особым свойством чисел a и b, которое мы выразим знаком

$$b \mid a$$

или словами: b делит a, или: b содержится в a, или: b есть *делитель* a, или: a есть *кратное* b. Каждое целое число $a\,(\neq 0)$ имеет тривиальные делители $\pm a$, ± 1; a и $-a$ имеют одни и те же делители; единственными числами, являющимися делителями каждого числа, являются обе „единицы": 1 и -1. Отличное от нуля целое число a имеет всегда только конечное число делителей, так как эти последние по абсолютной величине не могут превосходить $|a|$; число же 0 делится на каждое другое целое число.

Если b отлично от нуля и целое, то среди кратных b, не превосходящих определенного целого числа a, существует точно одно наибольшее, скажем, qb, и потому $a-qb=r$ есть неотрицательное целое число, меньшее чем $|b|$. Это целое число r, однозначно определенное для чисел a и b условиями

$$a=qb+r,\ q \text{ целое},\ 0\leqslant r<|b|,$$

называется остатком от деления a на b или *вычетом* a *по модулю* b. Утверждение $b\mid a$ равнозначно, таким образом, утверждению $r=0$.

Обращаясь теперь к общим делителям c двух целых чисел a, b, т. е. к числам c, для которых имеет место одновременно $c\mid a$ и $c\mid b$, отметим, прежде всего, что среди них имеется один однозначно определенный *наибольший общий делитель*; мы его обозначим через $(a,b)=d$. Согласно этому определению, всегда $d>1$. Обратимся к нахождению свойств числа $d=(a,b)$. Заметим прежде всего, что для любых целых x и y имеем $d\mid ax+by$. Рассмотрим совокупность чисел $L(x,y)=ax+by$, получающуюся, когда x и y пробегают все целые числа. Очевидно, что d есть также наибольший общий делитель всех $L(x,y)$. В самом деле, d есть делитель всех $L(x,y)$, и не существует никакого большего числа, которое обладало бы этим свойством, так как никакое большее число не может содержаться одновременно в $a=L(1,0)$ и в $b=L(0,1)$. Пусть $d_0=L(x_0,y_0)$ будет наименьшее положительное среди чисел $L(x,y)$, так что

$$\text{из } L(x,y)>0 \text{ следует } L(x,y)\geqslant d_0. \tag{1}$$

Мы покажем теперь, что каждое число $n=L(x,y)$ есть кратное d_0 и что $d=d_0$. В самом деле, рассмотрим вычет r числа n по модулю d_0,

$$r=n-qd_0=L(x-qx_0,\ y-qy_0),\quad 0\leqslant r<d_0.$$

Если бы было $r>0$, то из (1) следовало бы $r\geqslant d_0$, поэтому возможно только $r=0$, т. е. $n=qd_0$. Таким образом совокупность чисел $L(x,y)$ содержит только кратные числа d_0, и она совпадает с совокупностью всех кратных числа d_0, так как каждое такое кратное $qd_0=L(qx_0,qy_0)$ действительно содержится среди чисел $L(x,y)$. Поэтому d_0 также есть наибольший общий делитель всех $L(x,y)$ и, следовательно, совпадает с d. В частности, отсюда получается следующая теорема:

Теорема 1. *Если* $(a, b) = d$, *то уравнение*

$$n = ax + by$$

разрешимо в целых числах x, y *тогда и только тогда, когда* $d \mid n$.

Из этого вытекает, далее, что каждый общий делитель чисел a и b, содержась во всех числах $L(x, y)$, содержится в наибольшем общем делителе чисел a и b.

Для нахождения наибольшего общего делителя пользуются, как известно, приемом, идущим еще от Евклида, — так называемым *алгоритмом Евклида*. Смысл его заключается в сведении вычисления (a, b) к вычислению наибольшего общего делителя двух меньших чисел. Именно, из $a = qb + r$ следует, что общие делители чисел a и b совпадают с общими делителями чисел b и r, а потому и $(a, b) = (b, r)$. Примем для удобства $a > 0$, $b > 0$ и, положив для симметрии $a = a_1$, $b = a_2$, обозначим через a_3 вычет a_1 по модулю a_2 и вообще через a_{i+2} вычет a_i по модулю a_{i+1}, для $i = 1, 2, \ldots$, до тех пор пока этот вычет можно определить, т. е. пока $a_{i+1} > 0$. Пусть при этом

$$a_i = q_i a_{i+1} + a_{i+2}, \quad 0 \leqslant a_{i+2} < a_{i+1}.$$

Так как числа a_i для $i > 2$ образуют монотонно убывающую последовательность целых положительных чисел, то процесс должен закончиться после конечного числа шагов, что возможно только тогда, когда получится остаток, равный нулю. Пусть, например, $a_{k+2} = 0$. В силу соотношений

$$(a_1, a_2) = (a_2, a_3) = \ldots = (a_k, a_{k+1}) = (a_{k+1}, a_{k+2}) = (a_{k+1}, 0) = a_{k+1}$$

последний не равный нулю остаток a_{k+1} есть искомый наибольший общий делитель чисел a и b.

При доказательстве теоремы 1 мы воспользовались только одним свойством числового множества $L(x, y)$, а именно тем, что оно есть модуль.

Определение. Система S целых чисел называется *модулем*, если она содержит хоть одно число, отличное от нуля, и если вместе с числами m, n к S принадлежит всегда также $m - n$.

Таким образом, если m принадлежит к S, то к S принадлежит также $m - m = 0$, далее, $0 - m = -m$, $m - (-m) = 2m$, $2m - (-m) = 3m$ и т. д., а также $-m - m = -2m$, $-2m - m = -3m$ и т. д.; вообще, если m принадлежит к S, то к S принадлежит и mx при любом целом x, а следовательно, вместе с m и n к S принадлежит также $mx + ny$ при любых целых x и y.

Мы можем теперь, отправляясь от доказательства теоремы 1, доказать относительно модулей следующую очень общую теорему:

Теорема 2. *Совокупность чисел каждого модуля* S *совпадает с совокупностью кратных некоторого определенного числа* d. *Модулем* S *число* d *определяется с точностью до множителя* ± 1.

Для доказательства заметим, что S во всяком случае содержит положительные числа. Пусть d — наименьшее из них. Если n при-

надлежит S, то, как уже было прежде указано, S принадлежит также $n - qd$ при любом целом q, в частности, — также остаток от деления n на d; но он неотрицателен и меньше d, а следовательно, должен быть равен нулю. Таким образом каждое n из S есть кратное d, и так как d принадлежит S, то и все кратные d принадлежат S. Если, наконец, d' есть другое число, также обладающее тем свойством, что S состоит из всех его кратных, то d должно быть кратным d', и обратно, т. е. $d' = \pm d$.

Если мы в произвольной линейной форме $a_1x_1 + \ldots + a_nx_n$ с целыми коэфициентами $a_1, \ldots, a_n$ заставим $x_1, \ldots, x_n$ пробегать все целые числа, то полученная таким образом совокупность значений формы, очевидно, составит модуль. Поэтому мы получаем следующую теорему:

Теорема 3. *Совокупность значений линейной формы от n переменных с целыми коэфициентами, которые не все равны нулю, совпадает с совокупностью значений некоторой формы от одной переменной, dx. При этом d есть наибольший общий делитель коэфициентов первоначальной формы.*

Таким образом, для того чтобы уравнение

$$k = a_1x_1 + \ldots + a_nx_n$$

(так называемое диофантово уравнение) было разрешимо в целых числах $x_1, \ldots, x_n$, необходимо и достаточно, чтобы наибольший общий делитель чисел $a_1, \ldots, a_n$ был делителем k.

Если $(a, b) = 1$, то мы называем a и b *взаимно простыми*. По теореме 1, для того чтобы $(a, b) = 1$, необходимо и достаточно, чтобы уравнение

$$ax + by = 1$$

было разрешимо в целых числах x, y.

Важнейшее правило для вычисления символа (a, b) формулируется следующей теоремой:

Теорема 4. *Для любых трех целых чисел a, b, c, где $c > 0$, имеет место соотношение*

$$(a, b)\, c = (ac, bc). \tag{2}$$

Действительно, если $(a, b) = d$, то из равенства $ax + by = d$, которое, согласно теореме 1, наверное выполняется при некоторых целых x, y, следует $acx + bcy = cd$, а потому cd есть кратное (ac, bc), опять-таки по теореме 1; но, с другой стороны, cd, очевидно, есть общий делитель ac и bc, а потому необходимо равно (ac, bc).

Отметим еще понятие *наименьшего общего кратного* двух чисел a, b. Это есть наименьшее положительное число v, которое делится как на a, так и на b. Наименьшее общее кратное v связано с наибольшим общим делителем $d = (a, b)$ соотношением

$$v = \frac{|ab|}{d}. \tag{3}$$

В самом деле, согласно (2), имеем

$$\left(\frac{a}{d}, \frac{b}{d}\right)=1, \quad v=\left(\frac{a}{d}v, \frac{b}{d}v\right).$$

Но $\frac{ab}{d}$ есть общий делитель $\frac{a}{d}v$ и $\frac{b}{d}v$, а следовательно, является делителем v, т. е. $v \geqslant \frac{|ab|}{d}$; с другой стороны, $\frac{ab}{d}$ есть число, делящееся как на a так и на b, а потому по абсолютной величине $\geqslant v$. Поэтому $\frac{ab}{d}=\pm v$.

Так как числа, делящиеся на a и b, образуют модуль и v есть наименьшее положительное встречающееся в нем число, то каждое число, делящееся на a и b, должно быть кратным v.

Мы обратимся теперь к разложению чисел на множители. Если не существует другого разложения числа a на целочисленные множители, кроме тривиального, при котором один из множителей есть ± 1, а другой $\pm a$, то a называется *простым числом*. Такие числа существуют, например ± 2, ± 3, ± 5, ... Единицы ± 1 не причисляются к простым числам. Ограничимся для простоты разложением положительных чисел a на положительные множители. Прежде всего мы заметим, что каждое $a>1$ делится по крайней мере на одно положительное простое число; действительно, наименьший положительный и превосходящий единицу множитель числа a, очевидно, может быть только простым числом. Выделим из положительного числа a при помощи разложения $a=p_1a_1$ простой множитель p_1; далее, в случае если $a_1>1$, выделим из a_1 дальнейший простой множитель p_2, и т. д. Процесс этот должен будет через конечное число шагов закончиться, так как $a_1, a_2, \ldots$ образуют убывающую последовательность целых положительных чисел; иначе говоря, некоторое a_k необходимо должно будет стать равным единице. Этим способом a будет представлено в виде произведения $p_1p_2\ldots p_k$ из простых чисел. Таким образом простые числа являются теми простейшими элементами, из которых можно при помощи умножения построить каждое целое число. При этом имеет место следующая *основная теорема арифметики*:

Теорема 5. *Каждое положительное целое число, превосходящее единицу, можно одним и — отвлекаясь от порядка множителей — только одним способом представить в виде произведения положительных простых множителей.*

Покажем прежде всего, что простое число p только тогда может делить произведение ab двух целых чисел, если оно делит по крайней мере один из сомножителей. Это следует из теоремы 4. В самом деле, если простое число p не есть делитель a, то, как простое число, оно вообще не может иметь общих делителей с a, так что $(a, p)=1$. Тогда, по теореме 4, для каждого положительного целого числа b

$$(ab, pb)=b.$$

Отсюда следует, что если $p \mid ab$, то и $p \mid b$, так что простое число p должно быть делителем второго множителя произведения ab. Эта теорема сразу переносится на произведения нескольких множителей.

Чтобы доказать теперь теорему 5, рассмотрим два представления положительного числа a в виде произведения степеней различных положительных простых чисел p_i, q_i:

$$p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \dots q_k^{b_k}.$$

По только что доказанному, каждое простое число q входит делителем по крайней мере в один простой множитель левой части, а потому совпадает с некоторым p_i. Таким образом числа $q_1, \dots, q_k$ (быть может расположенные в другом порядке) совпадают с числами $p_1, \dots, p_r$, и обратно, так что и $k = r$. Выберем нумерацию так, чтобы $p_i = q_i$. Если бы теперь соответственные показатели степеней не оказались равными, например, $a_1 > b_1$, то после деления обеих частей равенства на $q_1^{b_1}$ мы получили бы, что левая часть имеет еще множитель $p_1 = q_1$, в то время как правая часть его уже не имеет; но это противоречит только что доказанному. Таким образом $a_1 = b_1$ и вообще $a_i = b_i$, $i = 1, \dots, k$.

Этой теоремой об *однозначной* разложимости каждого числа на простые множители дан существенно новый метод для разрешения рассмотренных выше вопросов, например, о том, является ли данное число b делителем другого числа a, о том, как найти наибольший общий делитель или наименьшее общее кратное чисел a и b, и т. д. В самом деле, представим себе a и b разложенными на их простые множители:

$$a = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}, \quad b = p_1^{b_1} p_2^{b_2} \dots p_r^{b_r},$$

где в качестве показателей a_i, b_i допускаются также нули. Очевидно, $b \mid a$ тогда и только тогда, если постоянно $a_i \geqslant b_i$. Далее,

$$(a, b) = p_1^{d_1} p_2^{d_2} \dots p_r^{d_r}, \quad \text{где} \quad d_i = \min(a_i, b_i), \quad i = 1, \dots, r,$$

$$v = p_1^{c_1} p_2^{c_2} \dots p_r^{c_r}, \quad \text{где} \quad c_i = \max(a_i, b_i), \quad i = 1, \dots, r.$$

Что *существует бесчисленное множество простых чисел*, доказывается следующим, принадлежащим Евклиду, рассуждением:

$$z = p_1 p_2 \dots p_n + 1$$

есть число, не делящееся ни на одно из простых чисел $p_1, p_2, \dots, p_n$. Поэтому z делится по крайней мере на одно простое число, отличное от $p_1, \dots, p_n$, а следовательно, если существует n простых чисел, то их существует и $n + 1$.

§ 2. Сравнения и классы вычетов

Всяким целым числом $n \neq 0$ определяется распределение всех целых чисел соответственно остаткам, которые они дают при делении на n. Два целых числа a и b, которые при делении на n дают один

и тот же остаток, мы относим к одному *классу вычетов по модулю* n или просто к одному классу $\bmod n$, и пишем $a \equiv b \pmod n$ (читается: a сравнимо с b по модулю n или modulo n); соотношение $a \equiv b \pmod n$ равносильно, таким образом, с $n \mid (a - b)$. Если a не сравнимо с b по модулю n, то мы пишем $a \not\equiv b \pmod n$. $a \equiv 0 \pmod n$ означает, что a делится на n. Каждое целое число называется *представителем* своего класса. Так как различными остатками при делении на n являются числа $0, 1, 2, \ldots, |n| - 1$, то количество всех различных классов по модулю n равно $|n|$.

Для вычислений со сравнениями имеют место следующие легко устанавливаемые правила: Если a, b, c, d, n — целые числа и $n \neq 0$, то

I. $a \equiv a \pmod n$.

II. Из $a \equiv b \pmod n$ следует $b \equiv a \pmod n$.

III. Из $a \equiv b \pmod n$ и $b \equiv c \pmod n$ следует $a \equiv c \pmod n$.

IV. Из $a \equiv b \pmod n$ и $c \equiv d \pmod n$ следует $a \pm c \equiv b \pm d \pmod n$.

V. Из $a \equiv b \pmod n$ следует $ac \equiv bc \pmod n$.

Вообще из $a \equiv b \pmod n$ и $c \equiv d \pmod n$ следует также $ac \equiv bd \pmod n$. В частности, из $a \equiv b \pmod n$ следует $a^k \equiv b^k \pmod n$ при каждом целом и положительном k.

При помощи повторного применения правил IV и V мы получаем: Если $a \equiv b \pmod n$ и $f(x)$ есть целая рациональная функция от x (полином относительно x) с целочисленными коэфициентами, то $f(a) \equiv f(b) \pmod n$.

Таким образом, поскольку это касается целых рациональных операций (сложения, вычитания, умножения), можно, коротко говоря, производить вычисления со сравнениями по одному и тому же модулю точно так же, как и с уравнениями. Иначе обстоит дело с делением. Из $ca \equiv cb \pmod n$ не следует $a \equiv b \pmod n$. В самом деле, $ca \equiv cb \pmod n$ означает, что $n \mid c(a - b)$. Если теперь $(n, c) = d$, то имеем далее

$$\left(\frac{n}{d}, \frac{c}{d}\right) = 1, \quad \frac{n}{d} \mid \frac{c}{d}(a - b),$$

а следовательно, по теореме 4, мы можем лишь утверждать, что

$$\frac{n}{d} \mid (a - b), \quad \text{т. е.} \quad a \equiv b \pmod{\frac{n}{d}}.$$

Например, из $5 \cdot 4 \equiv 5 \cdot 1 \pmod{15}$ не следует, что $4 \equiv 1 \pmod{15}$, а следует только, что $4 \equiv 1 \pmod{\frac{15}{5} = 3}$. Таким образом имеет место следующая теорема:

Теорема 6. *Если* $(c, n) = d$, *то из* $ca \equiv cb \pmod n$ *следует* $a \equiv b \pmod{\frac{n}{d}}$, *и обратно.*

Именно этим обусловливается то обстоятельство, что *произведение двух целых чисел может быть сравнимо с нулем даже тогда, когда*

ни один из сомножителей этим свойством не обладает. Например, $2 \cdot 3 \equiv 0 \pmod 6$, но ни 2, ни 3 не сравнимы с нулем по модулю 6.

Что касается связи между сравнениями *по различным модулям*, то мы видим непосредственно из определения, что если некоторое сравнение выполняется по модулю n, то оно справедливо также и для каждого делителя n, в частности, и для $-n$. Далее если

$$a \equiv b \pmod{n_1} \text{ и } a \equiv b \pmod{n_2},$$

то

$$a \equiv b \pmod{v},$$

где v есть наименьшее общее кратное n_1 и n_2.

Так как классы вычетов по модулям n и $-n$ совпадают, то достаточно исследовать классы вычетов по положительному модулю n.

Систему целых чисел мы называем *полной системой вычетов по модулю n*, если она содержит точно по одному представителю от каждого класса вычетов по модулю n. Так как такая система состоит из $|n|$ различных чисел, то $|n|$ попарно несравнимых по модулю n чисел всегда образуют полную систему вычетов mod n. Такими являются, например, числа $0, 1, 2, \ldots, |n|-1$.

Теорема 7. *Если числа $x_1, \ldots, x_n$ образуют полную систему вычетов по модулю n $(n > 0)$, то и числа $ax_1 + b, \ldots, ax_n + b$ образуют такую систему, если только a, b — целые числа и $(a, n) = 1$.*

В самом деле, n чисел $ax_i + b$ $(i = 1, \ldots, n)$, согласно теореме 6, также все не сравнимы между собой по модулю n.

Нижеследующая теорема дает полезное часто представление системы вычетов по составному модулю.

Теорема 8. *Пусть $a_1, a_2, \ldots, a_n$ — целые попарно взаимно простые числа и $A = a_1 a_2 \ldots a_n$. Если в выражении*

$$L(x_1, \ldots, x_n) = \frac{A}{a_1} c_1 x_1 + \ldots + \frac{A}{a_n} c_n x_n,$$

где c_i — любые числа, взаимно простые соответственно с a_i $(i = 1, \ldots, n)$, заставить числа x_i пробегать независимо друг от друга соответственно полные системы вычетов по модулям a_i $(i = 1, \ldots, n)$, то полученная система чисел будет составлять полную систему вычетов по модулю A.

В самом деле, количество получаемых чисел L равно $|A|$, так что нужно лишь доказать, что все они не сравнимы между собой по модулю A. Но из справедливости сравнения

$$L(x_1, \ldots, x_n) \equiv L(x_1', \ldots, x_n') \pmod A$$

следует справедливость каждого из сравнений

$$L(x_1, \ldots, x_n) \equiv L(x_1', \ldots, x_n') \pmod{a_i}$$