Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Удмуртский государственный университет»
Институт математики, информационных технологий и физики

А. С. Мерзляков

ТЕОРИЯ ЧИСЕЛ. ТЕОРЕМА ЭЙЛЕРА – ФЕРМА

Учебно-методическое пособие

Ижевск
2025

УДК 511(075.8)
ББК 22.13я73
М521

Рекомендовано к изданию Учебно-методическим советом УдГУ

Рецензент: ведущий научный сотрудник НЦ УдмФНЦ УрО РАН **В. Г. Лебедев**

Мерзляков А. С.

М521 Теория чисел. Теорема Эйлера – Ферма : учеб.-метод. пособие / А. С. Мерзляков. – Ижевск : Удмуртский университет, 2025. – 1,7 Мб. – Текст : электронный.

Данное методическое пособие предназначено для самостоятельной работы студентов-бакалавров направления 02.03.01 «Математика и компьютерные науки», 01.03.01 «Математика», 01.03.02 «Прикладная математика и информатика». В пособии рассматриваются основные понятия теории чисел и их свойства, а также рассматривается один известный результат классической теории чисел по представлению чисел в виде суммы двух квадратов целых чисел.

Пособие знакомит студентов с математическим аппаратом, который используется в теории чисел, а также показывает идеи, которые приводят к решению основного результата данного пособия.

Пособие предназначается для всех студентов, обучающихся по математическим специальностям очной и заочной форм обучения.

Минимальные системные требования:
Celeron 1600 Mhz; 128 Мб RAM; Windows XP/7/8 и выше, 8x DVD-ROM
разрешение экрана 1024×768 или выше; программа для просмотра pdf.

Подписано к использованию 30.12.2025
Объем электронного издания 1,7 Мб
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел. : +7(3412)263-751 E-mail: editorial@udsu.ru

СОДЕРЖАНИЕ

ТЕОРИЯ ЧИСЕЛ. ТЕОРЕМА ЭЙЛЕРА-ФЕРМА

В данном учебно-методическом пособии рассматривается один известному результат классической теории чисел, связанный с представлением натуральных чисел в виде суммы двух квадратов целых чисел, который рассматривался достаточно давно, однако и по сей день не утратил своей актуальности.

Рассмотрение этой задачи такими известными математиками как П. Ферма, Л. Эйлер, уже говорит о том, что в своё время это была достаточно важная математическая проблема, которую они успешно решили. Однако, математический язык решения этой задачи на настоящем этапе уже заметно изменился. Поэтому одной из целей автора данного пособия является попытка связать решение данной задачи с тем математическим аппаратом и материалом, который изучался студентами на предыдущих курсах, такими, например, как «Фундаментальная и компьютерная алгебра», «Математический анализ» и рядом других, а с другой, со знакомством с новыми понятиями и идеями, которые и привели к решению данной задачи.

Пособие разбито на параграфы, и нумерация всех результатов двойная: первое число обозначает номер параграфа, а второе – это номер утверждения, который рассматривается в данном параграфе.

Нужно отметить, что это пособие будет интересно не только студентам, изучающим основы теории чисел, но также и тем, кто будет в дальнейшем пропагандировать данный предмет.

§ 1. ЦЕЛОЧИСЛЕННАЯ ДЕЛИМОСТЬ В Z В ЕЁ СВОЙСТВА

Заметим, что мы будем везде далее иметь дело в основном с натуральными делителями, так как понятно для каждого целого числа, что если число нацело делится на a, то оно надело делится и на (- a).

ОПР. Целое число **a делится (НАЦЕЛО) на целое число b**, если найдется целое число c, такое, что a = b·c. Число a называется **делимым**, число b называется **делителем**, а число c – **частным (Записывается так: b|a)**.

ОПР. Натуральное число называется **простым**, если оно имеет ровно два различных натуральных делителя. Если натуральное число не является единицей и не является простым, тогда оно составное.

ПРИМЕР: числа, 2, 3, 5, 7,… – это всё простые числа, а числа 6, 8 – это составные числа. Будем считать, что число 1, не относится ни к той, ни к другой категории.

Сразу сделаем замечание, что потом мы рассмотрим понятие простого элемента уже в более общем форме, а сейчас начинаем со вполне «школьного» определения.

ОПР. **Собственным делителем натурального числа n** называется натуральный делитель n, отличный от 1 и от него самого. Делители 1 и n называются **несобственными** или **тривиальными** делителями натурального числа n.

ТЕОРЕМА 1.1. (Основная теорема арифметики). Любое натуральное число большее 1, однозначно с точностью до перестановки сомножителей раскладывается в виде произведения степеней простых чисел.

Эту теорему мы докажем позднее, а пока мы примем её без доказательства. Однако, заметим, что данная теорема очень важна при рассмотрении данного вопроса представления числа как суммы квадратов.

В качестве примера, что не во всяком числовом кольце разложение на неприводимые множители однозначно, приведем пример кольца $Z[\sqrt{-5}]$.

ПРИМЕР. Пусть $Z[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a,b$ целые числа$\}$. Это также кольцо целых алгебраических чисел. Число 21 раскладывается двумя различными способами в произведение неприводимых множителей.

$$21 = 3\times7 = (1+2\sqrt{-5})(1-2\sqrt{-5}).$$

В силу более общего (об этом поговорим позднее) определения простого элемента, если 3 делит $(1+2\sqrt{-5})$ $(1-2\sqrt{-5})$, то 3 должно делить либо $(1+2\sqrt{-5})$ либо $(1-2\sqrt{-5})$. Но, как несложно показать, что 3 не делит ни $(1+2\sqrt{-5})$ ни $(1-2\sqrt{-5})$. Значит, есть два различных представления числа 21.

СВОЙСТВА ЦЕЛОЧИСЛЕННОЙ ДЕЛИМОСТИ

Положим, что значок a|b, где a и b целые числа, обозначает, что a есть делитель числа b.

Ряд несложных свойств мы сформулируем в виде лемм, которые будем считать верными без доказательства, так как их формулировки достаточно просты.

ЛЕММА 1.2 d|0, для любого целого $d\neq0$, и $\pm1|a$ для любого целого числа a.

ЛЕММА 1.3. Если d|A, то d|B, то d| (A ± B).

ЛЕММА 1.4. Если b|a и c|b, то c|a.

ЛЕММА 1.5. Если c|a, d|b, то cd|ab.

ЛЕММА 1.6. Если p|ab, то p|a или p|b, где p - простое число.

ЛЕММА 1.7. Если c|s, $c|a_i$, i=1,2,3.., n-1, то $c|a_n$, где $s=a_1+a_2+...+a_n$.

УПР. Доказать, что верны леммы 1.2 – 1.7.

ТЕОРЕМА 1.8. (Теорема Евклида) Простых чисел бесконечно много.

Доказательство. Приведём известное доказательство, основанное на методе от противного. Допустим, что есть только конечное число простых $p_1< p_2 < p_3< \ldots\ldots< p_k$.Тогда рассмотрим число

$$N = p_1\cdot p_2\cdot p_3\cdot \ldots\ldots\cdot p_k + 1. \quad (1)$$

Понятно, что $N > p_k$, значит, оно составное. Ну а раз оно составное, то оно, согласно Т.1.1, имеет разложение в виде произведения простых сомножителей. Отсюда получаем, что

$$N = p_1^{\alpha_1}p_2^{\alpha_2}..p_k^{\alpha_k}.$$

Но среди этих простых делителей могут быть только простые от p_1 до p_k. Значит, в равенстве (1) сумма (т. е. число N) делится на p_1, произведение простых делится на p_1, значит, по свойствам делимости на p_1 делится и 1. Противоречие. Значит, простых чисел бесконечно много.

Также рассмотрим ещё один результат, который впоследствии может пригодиться.

ТЕОРЕМА 1.9. (О количестве натуральных делителей) Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} .. p_k^{\alpha_k}$ – натуральное число, тогда количество его натуральных делителей можно вычислить по формуле:

$$\tau(n) = (\alpha_1+1)\cdot(\alpha_2+1)\cdot\ldots\cdot(\alpha_k+1).$$

Доказательство. Понятно, что произвольным делителем числа n будет выбор степеней для простых делителей. Для каждого простого числа p_i есть ровно α_i+1 кандидат для выбора степени этого простого числа, как делителя, от 0, до α_i. Поэтому по правилу произведения, получаем, что общее число натуральных делителей равно $(\alpha_1+1)\cdot(\alpha_2+1)\cdot\ldots\cdot(\alpha_k+1)$.

Заметим, что несложно понять, что общее количество целых делителей равен удвоенному произведению, т.е. $2(\alpha_1+1)\cdot(\alpha_2+1)\cdot\ldots\cdot(\alpha_k+1)$.

Рассмотрим ещё один достаточно интересный результат.

ТЕОРЕМА 1.10 (Степень вхождения простого в n!) Пусть $\nu_p(n)$ – это степень, с которой данное простое число p входит в разложение n! Тогда

$$\nu_p(n) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

Доказательство. Заметим, что чисел делящихся на p, и не превосходящих n, ровно $\left[\frac{n}{p}\right]$. Чисел, которые делятся на p^2, и не превосходящих n, ровно $\left[\frac{n}{p^2}\right]$. Суммируя все, получаем результат теоремы.

§ 2. ПРИЗНАКИ ДЕЛИМОСТИ

Напомним хорошо известные «школьные» признаки, которые нам также впоследствии помогут.

1. Натуральное число $n=\overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$ чётное, тогда и только тогда, когда его последняя цифра, т. е. a_o, чётна.

2. Если натуральное число $\overline{a_1 a_0}$, составленное из двух последних цифр данного натурального числа $n=\overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$, делится на 4, то и все число n делится на 4.

3. Если число $\overline{a_2 a_1 a_0}$, составленное из трёх последних цифр данного натурального числа

$n = \overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$, делится на 8, то и всё число делится на 8.

Это всё частные случаи признака делимости на 2^k, который мы сейчас и рассмотрим.

ЛЕММА 2.1. (Признак делимости на 2^k). Пусть n = $\overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$ – натуральное число. Если число, составленное из его k последних цифр, т. е. число $\overline{a_{k-1...} a_2 a_1 a_0}$, делится на 2^k, то и само число n делится на 2^k.

Доказательство. Число n можно записать следующим образом

$$n = \overline{a_{m...} a_{m-1} a_{m-2}...a_k} \cdot 10^k + \overline{a_{k-1...} a_2 a_1 a_0} .$$

Заметим, что число 10^k делится на 2^k, поэтому делимость самого числа n на 2^k определяется делимостью числа $\overline{a_{k-1...} a_2 a_1 a_0}$. Если это число делится на 2^k, тогда и само число делится на 2^k . Верно и обратное, если число n делится на 2^k, то отсюда следует, что число $\overline{a_{k-1...} a_2 a_1 a_0}$, т. е. число, составленное из k последних цифр числа, также делится на 2^k.

Аналогичен признак делимости на 5. Понятно, что верны следующие утверждения.

3. Если последняя цифра натурального числа n = $\overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$ делится на 5, то и число n делится на 5.

4. Натуральное число n = $\overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$ делится на 25 $\Leftrightarrow$ когда число, составленное из двух последних цифр числа, т. е. число $\overline{a_1 a_0}$, делится на 25.

5. Верно ли утверждение, если натуральное число $\overline{a_2 a_1 a_0}$, составленное из трёх последних цифр натурального числа n = $\overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$, делится на 125, то и само число n делится на 125?

ЛЕММА 2.2. (Признак делимости на 5^k). Пусть n = $\overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$ – натуральное число. Если число, составленное из его k последних цифр, т. е. число $\overline{a_{k-1...} a_2 a_1 a_0}$, делится на 5^k, то и само число n делится на 5^k.

Доказательство. Число n можно записать следующим образом

$$n = \overline{a_{m...} a_{m-1} a_{m-2}...a_k} \cdot 10^k + \overline{a_{k-1...} a_2 a_1 a_0} .$$

Заметим, что число 10^k делится на 5^k, поэтому делимость самого числа n на 5^k определяется делимостью числа $\overline{a_{k-1...} a_2 a_1 a_0}$. Если это число делится на 5^k, тогда и само число делится на 5^k. Верно и обратное, если число n делится на 5^k , то отсюда следует, что число $\overline{a_{k-1...} a_2 a_1 a_0}$, т. е. число составленное из k последних цифр числа также делится на 5^k.

Вспомним ещё один хорошо известный признак делимости на 3 и на 9.

ЛЕММА 2.3. (Признак делимости на 3 и 9). Натуральное число n = $\overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$ делится на 9 $\Leftrightarrow$ когда сумма цифр числа делится на 3 (на 9)

Доказательство. Сначала докажем одно хорошо известное свойство о том, что разность между натуральным числом n и суммой его цифр делится на 9.

Рассмотрим эту разность n – S(n). Число n = $\overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$ может быть записано в виде

$$a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_1 \cdot 10 + a_o - (a_m + a_{m-1} + \ldots + a_1 + a_o) =$$

$$a_m \cdot (10^m - 1) + a_{m-1} \cdot (10^{m-1} - 1) + \ldots + a_1 \cdot (10 - 1) = 9k,$$ где k – натуральное число или 0.

Значит, если сумма цифр делится на 9, то и число делится на 9. Верно и обратное, если число делится на 9, тогда и сумма его цифр также должна делиться на 9. Это всё следует из свойств целочисленной делимости.

Рассмотрим ещё один признак делимости, который иногда рассматривается в школьной математике.

ЛЕММА 2.4. (Признак делимости на 11). Доказать, что натуральное число

n = $\overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$ делится на 11, если разность между суммами цифр, стоящих не чётных местах и суммой цифр, стоящих на нечётных местах, делится на 11, т. е.

$(a_o + a_2 + a_4 + \ldots) - (a_1 + a_3 + a_5 + \ldots)$ делится на 11.

Доказательство. Число n = $\overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0}$ может быть записано в виде

$$n = \overline{a_m a_{m-1}...a_k a_{k-1...} a_2 a_1 a_0} = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_1 \cdot 10 + a_o =$$

$$= \ldots a_4 \cdot (9999 + 1) + a_3 \cdot (1001 - 1) + a_2 \cdot (99 + 1) + a_1 \cdot (11 - 1) + a_o =$$

$$= \ldots a_4 \cdot 9999 + a_3 \cdot 1001 + a_2 \cdot 99 + a_1 \cdot 11 + a_o + (\ldots + a_2 + a_o) - (\ldots + a_3 + a_1).$$

Заметим, что первое выражение делится на 11, значит, делимость числа на 11 в целом определяется разностью между суммами цифр, стоящих на чётных позициях (начиная с нулевой последней цифры числа) и стоящих на нечётных позициях числа. Если эта разность делится на 11, тогда и число делится на 11. Несложно видеть, что верно и обратное, т. е. если число делится на 11, то тогда эта разность будет также делиться на 11.

УПР. Верно ли утверждение, если число, делится на 101 когда разность между суммой двузначных чисел, образованных цифрами, стоящих на 1 и 2; на 5 и 6, и т. д., и суммой двузначных чисел, образованных из цифр, стоящих на 3 и 4, 7 и 8, и т.д. местах, делится на 101? (Нумерация цифр ведётся с последней цифры натурального числа).

§ 3. ДЕЛИМОСТЬ ЦЕЛЫХ ЧИСЕЛ С ОСТАТКОМ

В этом параграфе мы рассмотрим свойства делимости целых чисел с остатком, и будем рассматривать свойства такой делимости. Понятно, что если остаток при делении равен 0, то этот случай мы уже рассмотрели выше – это целочисленная делимость. Таким образом, деление с остатком, это некоторое обобщение целочисленной делимости.

Целое число a может делиться нацело на число b, а может и не делиться. Однако для любых двух целых чисел a и b ($b \neq 0$) справедлива теорема.

ТЕОРЕМА 3.1. Для любых двух целых чисел a и b ($b \neq 0$) существуют два однозначно определенных числа q и r, такие, что $a = b \times q + r$, где $0 \leq r < |b|$. Числа **a** и **b** называются соответственно (точно также, как и в определении целочисленной делимости выше) **делимое** и **делитель**, число **q** называется **неполным частным**, а число **r** – **остатком a при делении на b**. Если r=0, говорят, что целое число a нацело делится на целое число b. (Определение делимости нацело).

Доказательство этого факта связано с тем, что каждому целому числу соответствует некоторая целая точка на числовой прямой. Поэтому если рассмотрим на оси множество всех точек, кратных b, то любая целая точка a попадает в какой-то один полуоткрытый интервал $[q \cdot |b|;(q+1) \cdot |b|)$. Так вот такой интервал (в который попадает число a) для каждого a единственен, и остатком числа a при делении на целое число b будет расстояние от a до левого края интервала (т. е. числа $q|b|$). Понятно, что расстояние будет всегда неотрицательно. А неполное частное будет выбираться в зависимости от знака делителя b.

Введём обозначения: остаток числа A при делении на число m будем обозначать далее таким образом $(A)_m$. Будем в дальнейшем понимать, что число m – это натуральное число.

СВОЙСТВА ДЕЛИМОСТИ С ОСТАТКОМ

Рассмотрим некоторые простейшие свойства делимости с остатком. Первые три свойства очень простые и их можно рассматривать в качестве упражнения для студентов.

ЛЕММА 3.2. Остатков при делении на натуральное число m ровно m штук: а именно, это числа 0, 1, ..., m - 1.

Доказательство этого факта несложно, поэтому не будем его здесь рассматривать.

ЛЕММА 3.3. Остаток от деления суммы a + b на натуральное число m, равно остатку от суммы остатков a и b при делении на m.

Доказательство и этого факта понятно, так как сумма остатков может быть больше делителя, значит, после сложения остатков нужно рассмотреть, чему равен остаток от суммы остатков относительно делителя m.

ЛЕММА 3.4. Остаток от деления произведения ab на натуральное число m, равно остатку от произведения остатков a и b при делении на m.

Доказательство и этого совершенно аналогично тому, о чём говорилось выше, так как произведение остатков может быть больше делителя, значит, после умножения остатков нужно рассмотреть, чему равен остаток от произведения остатков относительно делителя m.

Следующее утверждение уже более интересно, поэтому рассмотрим его доказательство.

ЛЕММА 3.5. Если A - B делится на m, тогда и только тогда, когда A и B имеют одинаковые остатки при делении на m.

Доказательство. Итак, пусть $A = mq_1 + r_1$, где $0 \le r_1 < m$, и $r=(A)_m$; $B = mq_2 + r_2$, где $0 \le r_2 < m$, и $r_2 = (B)_m$. Тогда $A - B = m(q_1 - q_2) + (r_1 - r_2)$.

Заметим, что если $r_1 = r_2$, тогда A – B делится на m.

Если же $A - B = m(q_1 - q_2) + r_1 - r_2$ делится на m, тогда в силу свойств делимости число $(r_1 - r_2)$ также делится на m. Но $(-m) < (1 - m) \le (r_1 - r_2) \le (m - 1) < m$. На данном интервале есть только одно число, которое делится на m, и это число равно 0. А это и означает, что $r_1 = r_2$.

Рассмотрим ещё одно интересное свойство.

ЛЕММА 3.6. Из любых k последовательных целых чисел найдется ровно одно число, которое делится на k.

Доказательство. Пусть n, n+1, …, n + (k - 1) – k последовательных целых чисел, и допустим среди них есть два разных числа a и b (a>b), которые делятся

на k. Тогда их разность (a – b) также делится на k. Но $0 < (a – b) \leq k-1$. Но среди этих чисел нет таких, которые делятся на k. Противоречие. Значит, каждое из этих чисел имеет свой отличный от всех других остаток при делении на k. Но чисел k и остатков от деления на k также ровно k. Значит, каждый из остатков есть ровно в одном экземпляре. Следовательно, найдётся число, которое имеет остаток 0 при делении на k, т. е. оно делится на k.

И рассмотрим ещё одно интересное свойство делимости с остатком при делении квадратов целых чисел, которое нам потребуется далее.

ЛЕММА 3.7. а) При делении квадрата любого целого числа на 3 или на 4 остатки могут быть только 0 или 1.

б) При делении куба любого целого числа на 7 остатки могут быть только 0, 1 или 6.

Доказательство. Если число n имеет остаток a при делении на 3, тогда $n = 3t + a$, но тогда квадрат этого числа можно записать в виде $(3t + a)^2 = 9t^2 + 6at + a^2$. Замечаем, что первые два слагаемых делятся на 3, значит, остаток квадрата определяется остатком от деления квадрата остатка на 3. А это несложно проверить, так как остатков всего 3. И они равны только 0 или 1.

Если же число n имеет остаток a при делении на 4, тогда $n = 4t + a$, но тогда квадрат этого числа можно записать в виде $(4t + a)^2 = 16t^2 + 8at + a^2$. Замечаем, что первые два слагаемых делятся на 4, значит, остаток квадрата определяется остатком от деления квадрата остатка на 4. А это несложно проверить, так как остатков всего четыре. И они снова равны только 0 или 1.

§ 4. НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ. АЛГОРИТМ ЕВКЛИДА

Рассмотрим ещё одно понятие, которое известно ещё из школьных учебников.

ОПР. **Наибольшим общим делителем двух целых чисел a и b** (в дальнейшем будем обозначать просто **НОД** или **(a, b)**) будем называть натуральное число d:

1) d|a и d|b;

2) если d’|a и d’|b, то d’|d, для любого другого делителя d’ чисел a и b.

ЗАМЕЧАНИЕ. Вообще говоря, мы могли рассматривать наибольший общий делитель в кольце целых чисел Z, с более общих позиций, и в дальнейшем об этом ещё поговорим.

ОПР. Два целых числа a и b называются **взаимно простыми**, если их НОД равен 1, т. е. (a,b)=1.

ПРИМЕРЫ: (7,15) = 1, т. е. числа 7 и 15 взаимно просты, (16,25) = 1, также взаимно просты, хотя оба числа не простые, но (7,14) = 7, т. е. числа не взаимно просты.

Как найти наибольший общий делитель двух целых чисел, т.е. (a, b), какой алгоритм можно предложить для его нахождения? Понятно, что, во-первых, можно найти все натуральные делители числа a, затем найти все натуральные делители числа b, а затем найти наибольший общий делитель.

Рассмотрим это более подробно. Например, если

$n = \prod_{p_i | n} p_i^{a_i}$; $m = \prod_{p_i | n} p_i^{\beta_i}$.

Тогда $(n, m) = \prod_{p_i | n} p_i^{\gamma_i}$, где $\gamma_i = \min(\alpha_i, \beta_i)$.

Заметим, кстати, что $[n, m] = \prod_{p_i | n} p_i^{\delta_i}$, где $\delta_i = \max(\alpha_i, \beta_i)$.

Здесь [a,b] – это наименьшее общее кратное двух натуральных чисел a и b.

Этот алгоритм прост, однако очень неэффективен! Если числа a и b достаточно велики, тогда найти все простые делители этих двух натуральных чисел найти просто невозможно: времени работы любого компьютера не хватит!

Однако, можно подсчитать НОД и другим, куда более эффективным методом, который и называется АЛГОРИТМ ЕВКЛИДА и который Вы хорошо знаете (или, точнее, должны хорошо знать). Евклид приводит его в предложениях 1 и 2 книги VII своих «Элементов». О нём говорилось на II курсе, когда рассматривали многочлены и их свойства. Итак, вновь мы будем искать наибольший общий делитель у двух натуральных чисел.

Рассмотрим процесс нахождения НОД двух целых чисел с помощью алгоритма Евклида.

Рассмотрим сам Алгоритм Евклида для двух произвольных целых чисел, в котором будем считать, что b>0.

Сначала разделим a на b.

$$a = bq_1 + r_1, \text{ где } 0 \le r_1 < b \qquad (1)$$

Затем, будем делить b на ненулевой остаток r_1 (если $r_1=0$, тогда понятно, что НОД (a, b)=b).

$$b = r_1q_2 + r_2, \text{ где } 0 \le r_2 < r_1 \qquad (2)$$

Затем, будем делить первый ненулевой остаток r_1 на ненулевой остаток r_2

$$r_1 = r_2q_3 + r_3, \text{ где } 0 \le r_3 < r_2 \qquad (3)$$

И так будем продолжать

$$r_2 = r_3q_4 + r_4 \qquad \text{где } 0 \le r_4 < r_3 \qquad (4)$$

В силу того, что последовательность остатков от деления $\{r_i\}$ строго убывающая последовательность неотрицательных целых чисел, то в силу принципа наименьшего натурального числа, в ней не может быть бесконечного набора элементов, поэтому в какой-то момент произойдет деление без остатка, т. е. будет справедливы равенства:

$$r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}, \text{ где } 0 \le r_k < 0 \qquad (k-1)$$

$$r_{k-2} = r_{k-1}q_k + r_k, \text{ где } 0 \le r_k < 0 \qquad (k)$$

$$r_{k-1} = r_kq_{k+1} \qquad (k+1)$$

Оказывается, справедлива следующая теорема.

ТЕОРЕМА 4.1 (Алгоритм Евклида). Если мы рассмотрим алгоритм Евклида для нахождения НОД двух натуральных чисел (a, b), то последний ненулевой остаток в этом алгоритме и будет равен d = (a, b). (В рассматриваемом выше случае это r_k).

Доказательство. Покажем, что $(a, b)=r_k$, которое является последним ненулевым остатком в алгоритме Евклида для нахождения НОД. Проверим, что для rk, что для него выполняются оба свойства НОД-а.

Во-первых, покажем, что если d произвольный общий делитель a и b, тогда он делит r_1 (по равенству (1) и свойствам делимости). Следовательно, из (2) получаем, что $d \mid r_2$. Из равенства (3) следует, что $d|r_3$,и т. д.... $d \mid r_k$. Таким образом, любой общий делитель чисел a и b делит r_k.

Покажем сейчас, что r_k делит a и b.

Из равенства (k+1) следует, что $r_k|r_{k-1}$. Из равенства (k) следует, что $r_k|r_{k-2}$, и т. д., из равенств (2) следует, что $r_k|b$ и из равенства (1) следует, что $r_k|a$.

Следовательно, согласно определению, $r_k = (a, b)$.

Рассмотрим действие алгоритма Евклида на примере.

ПРИМЕР: Найти (6188,4709).

Решим задачу с помощью алгоритма Евклида.

$$6188 = 4709 \cdot 1 + 1479;$$
$$4709 = 1479 \cdot 3 + 382;$$
$$1479 = 382 \cdot 3 + 333;$$
$$382 = 333 \cdot 1 + 49;$$
$$333 = 49 \cdot 6 + 37;$$
$$49 = 37 \cdot 1 + 12.$$
$$37 = 12 \cdot 3 + 1.$$

Понятно, что отсюда, согласно теореме 4.1, доказанной выше, следует, что (6188, 4708) = 1.

ПРЕДСТАВЛЕНИЕ Н.О.Д.

Ещё раз отметим, что если мы рассмотрим алгоритм Евклида (т. е. процесс последовательного деления) для нахождения НОД двух натуральных чисел (a, b), то последний ненулевой остаток в этом алгоритме и будет равен d = (a, b). Это замечание нам понадобится в доказательстве следующей теоремы.

ТЕОРЕМА 4.2 (Представление d=(a, b)). Пусть d=(a, b), тогда d – есть наименьшее по модулю ненулевое число, которое представимо в виде ax + by = d, где x, y – целые числа.

Доказательство. Заметим, что представление d в виде ax+by следует прямо из алгоритма Евклида. Нужно проделывать всё в обратном порядке, т. е. сначала рассмотреть равенство (k), где явно присутствует d=Н.О.Д. и начинать выражать d из этого равенства через остатки:

$$d = r_k = r_{k-2} - r_{k-1}q_k. \qquad (*)$$

Из (к-1) равенства можно выразить r_{k-1} через r_{k-2} и r_{k-3}, а именно $r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$, и подставить в (*). Получим, что

$$r_k = r_{k-2} - r_{k-1}q_k = r_{k-2} - (r_{k-3} - r_{k-2}q_{k-1})q_k = r_{k-2}(1 + q_{k-1}q_k) - r_{k-3}q_k \qquad (**)$$

Сейчас из (k-2) равенства выражаем r_{k-2} через r_{k-3} и подставляем в (**) и т. д. В итоге мы придем к выражению r_k в виде $r_k = ax + by$, для некоторых целых x и y.

Заметим, что в настоящее время есть немало более эффективных алгоритмов для нахождения d=(a,b), которые используются в практических целых нахождения наибольшего общего делителя двух целых чисел.

Возникает другой вопрос: найдётся ли целое число, которое по модулю меньше, чем d и не равно 0, и которое также выражается через линейную комбинацию чисел a и b?

Заметим, что любая линейная комбинация чисел a и b будет делиться на d, так как это их НОД. Значит, и предполагаемое число также должно делиться на d, что противоречит предположению. Значит, d – наименьшее по модулю ненулевое число, которое можно представить в виде ax + by = d, для любых целых чисел a и b.

Из результатов, полученных выше, можно показать, что справедлива ещё одна интересная теорема.

ТЕОРЕМА 4.3 (Критерий взаимной простоты чисел a и b). Два целых числа a и b взаимно просты тогда и только тогда, когда существуют два целых числа u и v, таких, что разрешимо уравнение au + bv = 1.

Доказательство. Непосредственно из алгоритма Евклида. Замечаем, что если (a, b)=1, то согласно теореме 4.2. есть линейное представление этого НОД-а в виде ax + by = 1, т. е. уравнение au + bv = 1 разрешимо в целых числах.

Обратно, если есть решение у уравнения au + bv = 1, и пусть d = (a, b). Тогда, согласно свойству делимости, d|1. Значит, d=1, т. е. числа a и b взаимно просты.

СВОЙСТВА Н.О.Д.

У наибольшего общего делителя двух целых чисел a и b, т. е. у (a, b), есть ряд свойств, сформулированных в виде лемм, которые мы последовательно рассмотрим и докажем.

ЛЕММА 4.4. (am, bm) = (a, b)·m

Док-во следует из алгоритма Евклида, так как мы просто умножаем все равенства на m.

ЛЕММА 4.5. Если (a,b) = d, то $(\frac{a}{d};\frac{b}{d}) = 1$

Доказательство. Если $(\frac{a}{d};\frac{b}{d})$ = k>1. Тогда a = d·k·a_1; b = d·k·b_1. Но тогда (a, b)=d·k, а не d. Противоречие. Значит, k=1. Понятно, что все общие делители лежат в (a,b).

ЛЕММА 4.6. Если (a, b) = 1, то (ac, b) = (c, b).

Доказательство. Заметим, что (ac, b) делит ac и bc. Отсюда

$$(a\cdot c, b)|(a\cdot c, b\cdot c) = (a, b)\cdot c = c.$$

Но, понятно, что (ac,b)|b. Отсюда требуемое.

ЛЕММА 4.7. Если (a,b) = 1 и b|(a·c). Тогда b|c.

Доказательство. Заметим, что если (a, b) = 1, и b|(ac), значит, все делители числа b – есть делители у числа c. Значит, b|c.

ЛЕММА 4.8. Если числа $a_1,...a_m$ взаимно просты с $b_1,b_2,...b_s$. Тогда

$$(a_1a_2 .a_m,b_1b_2 ...b_s) = 1.$$

Доказательство можно провести методом математической индукции по числу сомножителей m и s. По 3) $(a_1a_2 ...a_m, b_k) = (a_1....a_m,b_k) =...= 1$ для любого $k\leq s$. Положим $A = a_1a_2 ...a_m$. Поэтому $(b_1b_2 ...b_s, A) = (b_2b_3 ..b_s,A) =.... = (b_s,A) = 1$.

ЛЕММА 4.9. Для любых двух натуральных чисел справедливо следующее соотношение. (a, b)·[a, b] = ab.

Доказательство. Заметим, что [a,b] = $\frac{a \cdot b}{(a,b)}$, так как в наименьшем общем кратном только общие делители не будут повторяться. А из этого равенства и следует искомое равенство.

ПРИМЕР: (Мет. реш. олим. задач 8 кл.). Доказать, что числа 27x+4 и 18x+3 взаимно просты для любого натурального x.

Доказательство. Эту задачу можно решать и с помощью алгоритма Евклида и с помощью теоремы 4.3. Давайте решим её с помощью использования теоремы 4.3.

Заметим, что если мы возьмем u = - 2, v = 3, то получим, что (18x+3)·3 - (27x+4)·2=1.

Тогда согласно теореме 4.3, числовые выражения (18x+3) и (27x+4) взаимно просты при любом значении переменной x.

§ 5. РЕШЕНИЕ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ, ЧЕРЕЗ АЛГОРИТМ ЕВКЛИДА

ОПР. Рассмотрим вопрос решения **линейных диофантовых уравнений** (в дальнейшем мы иногда будем обозначить их через ЛДУ), т. е. уравнений в целых числах **вида ax+by=c,** где a, b, c – целые числа.

ОПР. **Решением линейного диофантового уравнения ax+by=c** (*), называется пара целых чисел (x_o, y_o), при подстановке которых уравнение (*) обратится в равенство.

Заметим, что решение у данного уравнения не может быть только одно: либо таких решений не будет, либо их будет бесконечно много. Мы это обоснуем ниже. Однако, если нам нужен только какая-то часть этих решений, например, решения только в натуральных числах, тогда такое решение может быть и одно. Рассмотрим общий вопрос нахождения всех решений данного ЛДУ ax+by = c, если нам известно одно какое-то решение.

Сначала мы будем рассматривать один класс ЛДУ, в котором c = (a, b) = 1, т. е. a и b взаимно просты, и будем искать решение этого класса ЛДУ. Мы уже видели в Т. 4.2, что такое ЛДУ разрешимо, у него должно быть хотя бы одно решение в целых числах.

Оказывается, если мы нашли одно, частное решение такого уравнения (x_o, y_o), то тогда можно найти и общее решение данного уравнения. Для этого докажем следующую лемму.

ЛЕММА 5.1. Пусть (x_o, y_o) и (x_1, y_1) – это частные решения ЛДУ $ax+by=1$, где $(a, b) = 1$, тогда $x_1 = x_o – bt$, а $y_1 = y_o+at$, для некоторого целого t.

Доказательство. Заметим, что если есть два различных решения ЛДУ (x_o, y_o) и (x_1, y_1), то

$$ax_o + by_o = 1 \ (1)$$

и

$$ax_1 + by_1 = 1 \ (2).$$

Если сейчас рассмотреть разность (1) – (2), то получим, что $a(x_o - x_1) + b(y_o - y_1) = 0$. Отсюда получаем, что в силу того, что (a,b)=1, то получаем, что $(x_o - x_1) = bt$ и $(y_o - y_1) = at$, для некоторого фиксированного t (которое, впрочем, может принимать любое целое значение). Значит, получаем соотношения, про которые и говорится в условии следствия. Из этой леммы следует такой результат:

СЛЕДСТВИЕ. Пусть (x_o,y_o) – это частное решение ЛДУ $ax+by=1$, где $(a,b) = 1$. Тогда все решения этого уравнения – это множество пар вида $(x_o – bt, y_o + at)$, где t – произвольное целое число.

Доказательство. В силу леммы 5.1 любые два решения связаны соотношениями, указанными в лемме. Осталось показать, что для любого целого t пара целых чисел $(x_o - bt, y_o + at)$ – также являются решением ЛДУ $ax + by = 1$, при условии, $(a, b) = 1$. А это несложно сделать. Нужно просто подставить их в уравнение.

А вот для нахождения частного решения ЛДУ можно использовать несколько методов, в частности, можно также использовать алгоритм Евклида.

Рассмотрим пример решения одного такого уравнения:

$$31x + 11y = 1$$

с использованием обычного алгоритма Евклида.

Найдём, используя алгоритм Евклида (30,11).

$$31 = 11\cdot2 + 9 \ \ (1)$$
$$11 = 9\cdot1 + 2 \ \ \ (2)$$
$$9 = 4\cdot2 + 1 \ \ \ (3)$$

Сейчас, из равенства (3) получаем, что $1 = 9 - 4\cdot2$. Из равенства (2) получаем, что $2 = 11 - 9\cdot1$. Отсюда следует, что $1 = 9 - 4\cdot(11 - 9\cdot1) = 9\cdot5 - 4\cdot11$. Из первого равенства получаем, что $9 = 31 - 11\cdot2$. Из это следует, что $1 = 9 - 4\cdot(11 - 9\cdot1) = 9\cdot5 - 4\cdot11 = (31 - 11\cdot2)\cdot5 - 4\cdot11 = 31\cdot5 - 14\cdot11$.

Отсюда видим, что частным решением рассматриваемого ЛДУ есть пара $(x, y) = (5, -11)$.

Но нам же нужно решать уравнение $ax+by = c$, а не только один случай, когда c=1. Оказывается, что это очень несложно после нахождения общего ре-

шения ax+by = 1, найти решение и для произвольного c. Для этого нужно только умножить частное решение (x_o, y_o) на c. А общее решение этого уравнения будет иметь именно такой случай

Однако мы рассматривали решение только одного типа ЛДУ, а именно, когда (a, b) = 1.

Сейчас рассмотрим уравнение общего вида, т. е. ax+by=c, где (a, b) = d. Что можно сказать, в этом случае о решениях данного уравнения. Очевидно отметить, что если d не делит c, то решений в целых числах у этого уравнения не будет. А если d|c, тогда все коэффициенты ЛДУ будут делиться на d, значит, в этом случае, т. е. когда $a = da_1$; $b = db_1$; $c = dc_1$, ЛДУ будет иметь вид:

$da_1x + db_1y = dc_1$. Отсюда $d(a_1x + b_1y = c_1)$, или после сокращения получаем, что $a_1x + b_1y = c_1$,

(где $(a_1, b_1) = 1$). А это уравнение, которые мы уже решали. Только здесь общее решение будут иметь вид не $(x_o - bt, y_o + at)$, как было выше, а $(x_o - b_1t, y_o + a_1t)$, где t – произвольное целое, и $a_1 = a/d$; $b_1 = b/d$; $c_1 = c/d$.

Отсюда справедлива следующая лемма.

ЛЕММА 5.2. ЛДУ ax+by=c, где (a, b) = d, имеет решение тогда и только тогда, когда d|c.

§ 6. СРАВНЕНИЯ И ИХ СВОЙСТВА

Делимость с остатком тесно связана с другим понятием, понятием сравнения. Но сначала я напомню некоторые общие вещи, с которыми вы уже встречались ранее, в частности, в курсе теории множеств.

ОПР. Пусть на множестве X задано отношение τ. Тогда говорят, что τ

а) **рефлексивное**: т. е. (x τ x)

б) **симметричное**, т. е. если (x τ y), тогда и (y τ x)

в) **транзитивное**, т. е. (x τ y)&(y τ z), тогда x τ z.

ПРИМЕРЫ: a) N: x = y. Оно обладает всеми свойствами.

b) N: $x \le y$. Оно не обладает свойством симметричности, но обладает свойством антисимметричности.

c) R: x < y. Оно не обладает свойствами рефлексивности, симметричности, но обладает свойствами антисимметричности и транзитивности.

ОПР. Отношение τ называется **отношением эквивалентности**, если оно

а) **рефлексивное**: т. е. (x τ x)

б) **симметричное**: если (x τ y), то (y τ x)

г) **транзитивное**, т. е. (x τ y)&(y τ z), тогда (x τ z).

Отношение эквивалентности обычно обозначается через ~.

ОПР. Пусть на множестве A задано отношение эквивалентности ~. Множество элементов, которые связаны между собой отношением ~, называется **классом эквивалентности, по отношению** ~. Будем обозначать классы эквивалентности по отношению эквивалентности через $\bar{a}$, где a – произвольный элемент этого класса.

ПРИМЕРЫ: на R^2 задано отношение: две точки, имеющие одинаковые ординаты. Это отношение эквивалентности. Плоскость разбивается по нему на классы, мощность множества которых равносильна мощности R. Класс эквивалентности – это прямая, параллельная оси абсцисс.

ЛЕММА 6.1. Множество классов эквивалентности по отношению ~ является разбиением множества X, в том смысле, что X является объединением непересекающихся классов эквивалентности.

Доказательство. Пусть $X = \bigcup_{i \in I} \bar{a}_i$, где I – некоторое семейство индексов. Допустим, что есть два различных класса эквивалентности $\bar{a}$ и $\bar{b}$ по отношению ~, которые пересекаются по какому-то элементу c. Тогда в силу определения любое x из $\bar{a}$ связано отношением x~c, и для любого y из $\bar{b}$, также выполняется, что c~y. Но тогда в силу транзитивности отношения ~, будет следовать, что x~y, т. е. классы совпадают. Противоречие. Значит, любые два различных класса эквивалентности не пересекаются.

ПРИМЕР: понятно, что в приведенном выше примере плоскость действительно разбивается на классы эквивалентности по данному отношению, и они не пересекаются, т. е. это действительно разбиение множества.

ОПР. Разбиение X, соответствующее отношению эквивалентности ~ называется **фактор-множеством X относительно отношения эквивалентности ~.**

Сейчас мы вернёмся к теории делимости, и далее будем говорить об одном отношении на множестве целых чисел: **отношении сравнимости по модулю m**. Введём определение этого отношения.

ОПР. Пусть $m \in N$. Говорят, что **два целых числа a и b сравнимы по модулю m**, если m|(a-b), записывается это следующим образом: $a \equiv b \pmod m$, и называется сравнением по модулю m.

ПРИМЕРЫ. а). Сравнимы ли между собой два числа 123 и 5 по модулю 7?

Решение. По определению эти два числа сравнимы, если их разность делится на 7. Делится ли 118 на 7. Нет, значит, числа не сравнимы по модулю 7.

б). Сравнимы ли между собой 5 и -3 по модулю 4?

Решение. Опять же по определению получаем, что 5 - (-3) = 8, т. е. сравнимы.

Покажем, что это отношение является отношением эквивалентности.

ЛЕММА 6.2. Отношение сравнимости по модулю натурального числа m на множестве Z является отношением эквивалентности.

Доказательство. Заметим, что для любого целого числа a выполняется $a \equiv a \pmod m$, т. е. свойство рефлексивности выполняется. Также заметим, что если $a \equiv b \pmod m$, то и $b \equiv a \pmod m$, т. е. выполняется также и свойство симметричности. И если $a \equiv b \pmod m$, $b \equiv c \pmod m$, тогда

$a - b = mt_1$, $b - c = mt_1$. Если мы сложим два эти равенства, то получим, что $a - c = mT$, где T – целое число. Значит, по определению $a \equiv c \pmod m$. Значит, выполняется и свойство транзитивности. Отсюда данное отношение является отношением эквивалентности.

Рассмотрим, что будет представлять собой класс эквивалентности по отношению сравнимости по модулю m, где m – натуральное число, и что будет представлять из себя фактор-множество на Z?

Заметим, что класс эквивалентности по отношению сравнимости, в силу того, что оно является отношением эквивалентности, будет определяться остатком при делении на m. Этот класс эквивалентности представляет из себя множество целых чисел, которые имеют одинаковый остаток при делении на m. Это следует из леммы 3.5. $m|(A - B) \Leftrightarrow (A)_m = (B)_m$). Поэтому в дальнейшем классы эквивалентности по отношению сравнимости по модулю натурального числа m будем обозначать следующим образом: $\bar{0};\bar{1};\bar{2};$ ….. .

ОПР. Их будем называть **классами вычетов по модулю m**, а сами числа, которые лежат в этих классах – просто **вычетами по модулю m**.

Как несложно понять, классов вычетов по модулю m будет ровно столько, сколько остатков при делении на m, т. е. ровно m штук, а именно это будут классы $\bar{0};\bar{1};\bar{2};\ldots..\overline{m-1}$. Заметим, что мы могли бы обозначить эти классы и по-другому, например, $\overline{m};\overline{m+1};\overline{m+2};\ldots..\overline{2m-1}$. Но использовать остатки обычно удобнее.

Множество всех классов вычетов будем обозначать $Z/\equiv m$.Покажем, что на этом множестве классов $Z/\equiv m$ можно ввести операции, с которыми это мно-

жество будет образовывать кольцо, которое будем называть в дальнейшем **кольцом классов вычетов**, и обозначать через $\mathbf{Z_m}$.

Определим на множестве классов вычетов $Z/\equiv m$ операции сложения и умножения, полагая, что мы работаем с остатками при делении целых чисел на m.

Рассмотрим пример операции сложения и умножения на классах вычетов по модулю 3, т. е. на $Z/\equiv 3$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{2}$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

ОПР. Взяв от каждого класса эквивалентности по одному представителю (вычету), получим систему вычетов, которая называется ***полной системой вычетов.***

ОПР. Если задана произвольная полная система вычетов по модулю m, то выбрав в ней вычеты, которые взаимно просты с модулем m, получим систему вычетов, которая называется ***приведенной системой вычетов по модулю m.***

Число классов вычетов в приведенной системе вычетов равно **значению функции Эйлера**, определённой на множестве натуральных чисел, и которая обозначается через φ (n).

По определению полагаем, что $\varphi(1)=1$.

ПРИМЕР: по модулю 7. Полная система вычетов по модулю 7 это, например, числа 1, 2, 3, 4, 5, 6, 7, а приведенная система вычетов – это числа 1, 2, 3, 4, 5, 6. Значение функции Эйлера $\varphi(7)$, следовательно, равно 6.

Рассмотрим простейшие свойства сравнений $a\equiv b(\mathrm{mod} m)$, помимо тех, которыми обладают по определению (это рефлексивность, симметричность и транзитивность). Все эти свойства легко доказываются, используя известные свойства делимости.

Далее везде числа a, b, c, d это целые числа, если не оговаривается отдельно, и m, m_1, m_2 – это натуральные числа.

ЛЕММА 6.3. Если $a\equiv b$ (modm), то $a\equiv b(\mathrm{mod}\ d)$; где $d|m$, $d\in N$.

Доказательство. Если $a\equiv b$ (modm), то $a - b = mt = dm_1t$, где $t\in Z$ и d – произвольный делитель числа m. Значит, по определению, $a\equiv b$ (mod d).

ЛЕММА 6.4. Если $a\equiv b(\mathrm{mod} m)$, $c\equiv d(\mathrm{mod} m)$, то $a\pm c\equiv b\pm d(\mathrm{mod} m)$.

Доказательство. Если $a \equiv b \pmod m$, то $a - b = mt_1$, где $t_1 \in Z$, и $c - d = mt_2$, где $t_2 \in Z$. Вычитаем (или прибавляем) два равенства, и получаем, что $a \pm c \equiv b \pm d \pmod m$.

ЛЕММА 6.5. Если $a \equiv b \pmod m$, $c \equiv d \pmod m$, то $ac \equiv bd \pmod m$;

Доказательство. Если $a \equiv b \pmod m$, то $a - b = mt_1$, где $t_1 \in Z$, и $a = b + mt_1$ (1).

Если $c \equiv d \pmod m$ (2), отсюда $c = d + mt_2$, где $t_2 \in Z$. Перемножаем равенство (1) на равенство (2), и получаем, что $a \cdot c \equiv b \cdot d \pmod m$.

ЛЕММА 6.6. Если $a \equiv b \pmod m$, то для любого натурального $n \in N$ справедливо $a^n \equiv b^n \pmod m$.

Доказательство. Это можно сказать прямое следствие леммы 6.5. Перемножая сравнение

$a \equiv b \pmod m$ n раз с самим собой, получим нужный результат.

ЛЕММА 6.7. Если $a \equiv b \pmod m$, то $ac \equiv bc \pmod m$, где c – произвольное целое число.

Доказательство. Если $a \equiv b \pmod m$, то $a - b = mt$ (1), где $t \in Z$. Равенство (1) можно умножить на любое целое число c, от этого равенство не перестанет быть равенством. Значит, свойство выполняется.

ЛЕММА 6.8. Если $ac \equiv bc \pmod m$, и $(c,m)=1$, то $a \equiv b \pmod m$.

Доказательство. Если $ac \equiv bc \pmod m$, то $c(a - b) = mt$ (1), где $t \in Z$. Из равенства (1) следует, что $m \mid (a - b)$, так как $(c,m) = 1$. Значит, отсюда следует, что $a \equiv b \pmod m$.

ЛЕММА 6.9. Если $ad \equiv bd \pmod{dm}$, то $a \equiv b \pmod{m}$ $(d \neq 0)$.

Доказательство. Если $ad \equiv bd \pmod{dm}$, то $d(a - b) = dmt$ (1), где $t \in Z$. Равенство (1) можно сократить на ненулевой делитель d. Из этого получаем, что $m|(a - b)$. Значит, отсюда следует, что $a \equiv b \pmod{m}$.

ЛЕММА 6.10. Если $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, то $a \equiv b \pmod{[m_1,m_2]}$, где $[m_1,m_2]$ – наименьшее общее кратное двух натуральных чисел m_1 и m_2.

Доказательство. Если $a \equiv b \pmod{m_1}$, то $a - b = m_1$ (1), где $t_1 \in Z$, и $a \equiv b \pmod{m_1}$, и $a - b = m_2$ (1), где $t_2 \in Z$. Из свойств делимости отсюда следует, что $[m_1,m_2]|(a - b)$. Значит, отсюда следует, что $a \equiv b \pmod{[m_1,m_2]}$.

Рассмотрим ещё два свойства, которые нам будут нужны в дальнейшем.

ЛЕММА 6.11. Если $(a, m)=1$ и x пробегает приведенную систему вычетов по модулю m, то значения выражения ax также пробегают приведенную систему вычетов по модулю m.

Доказательство. Заметим, что если $(a_1, a_2, \ldots, a_{\varphi(m)})$ – приведенная система вычетов по модулю m. Тогда после умножения на a, данная система примет вид $(a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_{\varphi(m)})$. Если найдутся какие-то два элемента из этой системы $a \cdot a_i$ и $a \cdot a_j$, которые сравнимы между собой по модулю m, т. е. $a \cdot a_i \equiv a \cdot a_j \pmod{m}$.Отсюда получаем, в силу свойства леммы 6.8, что $a_i \equiv a_j \pmod{m}$, так как $(a,m)=1$. Значит, есть $\varphi(m)$ элементов, которые попарно не сравнимы по модулю m. Отсюда они также образуют приведенную систему вычетов по модулю m.

ЛЕММА 6.12. Если $(a, m)=1$ и x пробегает полную систему вычетов по модулю m, то $ax+b$, где b – любое целое число, также пробегают полную систему вычетов по модулю m.

Доказательство. Заметим, что если $(a_1, a_2, \ldots, a_m)$ – полная система вычетов по модулю m. Тогда после умножения на a и прибавления b, получим, что данная система примет вид $(a \cdot a_1 + b, a \cdot a_2 + b, \ldots, a \cdot a_{\varphi(m)} + b)$. Если найдутся какие-то два элемента из этой системы $a \cdot a_i + b$ и $a \cdot a_j + b$, которые сравнимы по между собой по модулю m, т. е. $a \cdot a_i + b \equiv a \cdot a_j + b \pmod{m}$. Отсюда получаем, сначала в силу свойства леммы 6.4, а затем в силу леммы 6.8, что $a_i \equiv a_j \pmod{m}$, так как $(a, m)=1$. Значит, есть m элементов, которые попарно не сравнимы по модулю m. Отсюда они также образуют полную систему вычетов по модулю m.

§ 7. ФУНКЦИЯ ЭЙЛЕРА

В предыдущем параграфе мы занимались тем, что изучали, что такое отношение сравнимости по модулю натурального числа m на множестве целых чисел, и изучали их свойства. Сегодня мы будем говорить об одной из важнейших функций в теории чисел – функции Эйлера, которая уже была введена в параграфе 6, как число элементов в приведённой системы вычетов по модулю m.

Так как мы можем всегда рассматривать приведенную систему вычетов по модулю m, как множество, элементы которого лежат в полной системе вычетов, состоящей из чисел (0,1,2,..,m-1), то другими словами можно полагать, что **φ(m)** – это количество натуральных чисел, не превосходящих m, взаимно простых с m.

ПРИМЕР. Функция Эйлера $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$, $\varphi(7)=6$, $\varphi(8)=4$, $\varphi(9)=6$, $\varphi(10)=4$.

А сейчас рассмотрим вопрос нахождения формулы, для вычисления функции Эйлера.

Сначала подумаем о том, как вычислить функцию Эйлера для некоторых частных случаев, например, когда речь идет о простых числах. Сначала заметим, что если p – простое число, то

$$\varphi(p) = p-1; \quad \varphi(p^2) = p(p-1); \quad \varphi(p^k) = p^{k-1}(k-1),$$

так как если есть p^k чисел, то среди них есть ровно p^{k-1} чисел, которые делятся на p, т. е. не взаимно просты с p^k.

УПР. Доказать, что $\varphi(p_1p_2) = (p_1 - 1)(p_2 - 1)$; $\varphi(p_1^2p_2^2) = p_1p_2(p_1 - 1)(p_2 - 1)$. Оказывается, справедлива следующая теорема.

ТЕОРЕМА 7.1. Если a и b – натуральные числа, такие что (a, b)=1, то $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$.

Доказательство. Пусть M – множество чисел не больших ab. Каждое число из M может быть единственным образом представлено в виде

$$n = bq + r, \text{ где } q = \{0,1,2,..,a\}, r = \{0,1,2,..,b-1\}.$$

Когда (n, b)=1? Понятно, что это тогда, когда (b, r) = 1.

Сколько таких r существует? Ровно $\varphi(b)$. Рассмотрим какое-то одно такое $r = r_1$. Тогда числа r_1, $b + r_1$, $2b + r_1$,..., $(a-1)b + r_1$ образуют полную систему вычетов по mod a.

Это можно показать, так как если какие-то два элемента сравнимы между собой по модулю a, т. е. если $kb + r_1 \equiv tb + r_1 \pmod a$, получаем, что $(k-t)b \equiv 0 \pmod a$. Однако, число $(k - t)$ не могут делиться на a, так как $|k - t| < |a|$, кроме случая, когда k=t, а (a,b)=1.

Сколько среди них вычетов, которые взаимно просты с a? Понятно, что ровно $\varphi(a)$.

Отсюда получаем, что каждому числу r_1 соответствует ровно $\varphi(a)$ чисел, взаимно простых с a чисел. Среди остатков ровно $\varphi(b)$ взаимно простых с b. Отсюда получаем, что общее число вычетов, взаимно простых с $a \cdot b$ равно $\varphi(a) \cdot \varphi(b)$. Отсюда нужный вывод теоремы.

Из теоремы 7.1 и основной теоремы арифметики уже следуют известные результаты, т. е. формулы для вычисления функции Эйлера для произвольного натурального числа n.

ЛЕММА 7.2. Значение функции Эйлера для $n = \prod_{з_и|m} p^{\alpha_i}$ вычисляется по формуле $\boldsymbol{\varphi}(n) = \prod_{p_i|n} \varphi(p_i) = \prod_{p_i|n} p^{a_i-1}(p_i - 1)$, где p_i – различные простые делители n.

Доказательство. Мы уже научились вычислять $\boldsymbol{\varphi}(p^k)=p^{k-1}(p-1)$. Так как произвольное натуральное n можно разложить в произведение степеней простых, то получаем, что

$$\boldsymbol{\varphi}(p^{k1}p^{k2}...p^{ks}) = \boldsymbol{\varphi}(p^{k1})\ \boldsymbol{\varphi}(p^{k2}).. \boldsymbol{\varphi}(p^{ks}) = \prod_{p_i|n} p^{a_i-1}(p_i - 1)$$

Рассмотрим пример использования формулы для нахождения значения функции Эйлера на примере.

УПР. Найти $\varphi(100)$. Заметим, что $300 = 2^2 \cdot 3 \cdot 5^2$. Отсюда

$$\varphi(300) = \varphi(2^2) \cdot \varphi(3) \cdot \varphi(5^2) = 2 \cdot (2-1) \cdot (3-1) \cdot 5 \cdot (5-1) = 80.$$

Заметим, что разложение на простые числа единственно по основной теореме арифметики. Конечно, мы можем разложить число 300 на два взаимно простых множителя не одним способом, однако, для подсчёта значения функции Эйлера так или иначе всё равно придётся использовать формулу для вычисления значения функции Эйлера на степени простого числа т. е. то, что мы уже показали ранее, что $\varphi(p^k) = p^{k-1}(k-1)$.

§ 8. ТЕОРЕМА ФЕРМА И ТЕОРЕМА ЭЙЛЕРА. ИХ ИСПОЛЬЗОВАНИЕ ДЛЯ РЕШЕНИЯ ЛИНЕЙНЫХ СРАВНЕНИЙ ОТ ОДНОЙ НЕИЗВЕСТНОЙ

Данный параграф очень небольшой, но очень важный. Прежде всего, нужно отметить, что нахождение значения функции Эйлера нам нужно, для того, чтобы использовать её в следующей теореме.

ТЕОРЕМА 8.1

а) (Малая теорема Ферма) Когда m = p – простое число, то справедливо $a^{p-1} \equiv 1 (\mathrm{mod} p)$.

б) (Теорема Эйлера) При m>1 и (a,m)=1 справедливо $a^{\varphi(m)} \equiv 1 (\mathrm{mod} m)$.

Доказательство. Заметим, что пункт а) теоремы, т. е. малая теорема Ферма, является частным случаем п. б) этой теоремы, т. е. теоремы Эйлера, так как φ(p) = p – 1, если p – простое число.

б) Пусть $\{x_1, x_2, x_3, .. x_{\varphi(m)}\}$ – приведенная система вычетов по модулю m. Пусть переменная x пробегает эту систему, тогда по лемме 6.11, ax также пробегает приведенную систему вычетов по модулю m, если (a,m) = 1. Перемножим все элементы обеих систем. Получим один и тот же результат:

$$a^{\varphi(m)} x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_{\varphi(m)} \equiv x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_{\varphi(m)} \ (\mathrm{mod}\ m)$$

Отсюда, согласно лемме 6.8, мы можем сократить сравнение на $x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_{\varphi(m)}$, и получаем, что

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

Заметим, что малая теорема Ферма может быть переформулирована ещё и следующим образом.

Пусть p простое число, тогда для любого целого a справедливо сравнение $a^p \equiv a \ (\mathrm{mod} p)$.

Перед тем, как рассмотреть вопрос использования данных теорем для нахождения решения линейных сравнений от одной переменной, попробуем использовать данные теоремы для нахождения остатков при делении на натуральное число m степеней натуральных чисел.

ПРИМЕР. Найти остаток натурального числа 13^{2025} при делении на 19.

Решение. По теореме Ферма $13^{18} \equiv 1 (\mathrm{mod}\ 19)$. Значит, отсюда получаем, что

$$13^{2025} \equiv 13^{18 \cdot 112 + 9} \equiv 13^9 \equiv (169)^4 \cdot 13 \equiv (17)^4 \cdot 13 \equiv (-2)^4 \cdot 13 \equiv 16 \cdot 13 \equiv (-3) \cdot (-6) \equiv 18 \ (\mathrm{mod}\ 19).$$

Отсюда остаток $(13^{2025})_{19} = 18$. Интересно заметить, что так как $18 \equiv -1 \pmod{19}$, то если бы степень была равна, например, 4050, тогда $(13^{4050})_{19} = 1$.

ЛИНЕЙНЫЕ СРАВНЕНИЯ ОТ ОДНОЙ НЕИЗВЕСТНОЙ

ОПР. В кольце классов вычетов также можно решать **линейные уравнения, относительно одной неизвестной, или сравнения первой степени с одной переменной.** Они имеют вид

$$ax \equiv b \pmod{m} \qquad (1).$$

ОПР. **Решением сравнения первой степени по модулю m** называется класс вычетов по модулю m, произвольный вычет из которого при подстановке в сравнение (1) обращает его в верное сравнение.

ПРИМЕР: например, решением сравнения $5x \equiv 2 \pmod{17}$ будет класс вычетов $\overline{14}$ по модулю 17, так как $5 \cdot 14 \equiv 70 \equiv 2 \pmod{17}$. Понятно, что если мы подставим, любой другой вычет из этого класса, например, - 3, то сравнение по-прежнему останется верным.

Рассмотрим вопрос о том, когда сравнение $ax \equiv b \pmod{m}$ имеет решение, и как его найти. Для ответа на вопрос о том, что решение существует, используются свойства сравнений, которые мы рассматривали выше. А для ответа на вопрос о нахождении решения, нам поможет теорема Эйлера.

ТЕОРЕМА 8.2. Пусть (a, m) = d. Сравнение $ax \equiv b \pmod{m}$ неразрешимо, если b не делится на d. При b, кратном d, сравнение имеет ровно d решений.

Доказательство. Пусть (a, m)=1. Тогда согласно одному из свойств сравнений, связанных с пробеганием x полной системы вычетов по модулю m, ax – b также пробегает полную систему вычетов по модулю m, значит, только один класс вычетов будет обладать требуемому свойству. То есть решение существует и только одно.

Пусть (a,m)=d>1, тогда, чтобы сравнение имело решение, необходимо, чтобы b делилось на d. После сокращения на d всех частей сравнения, получим, что полученное сравнение будет иметь только одно решение $\overline{x_1}$ по модулю $\frac{m}{d}$.

Но тогда исходное сравнение по модулю m будет иметь ровно d решений:

$$\overline{x_1},\ \overline{x_1 + \frac{m}{d}},\ \overline{x_1 + 2 \cdot \frac{m}{d}},\ \ldots,\ \overline{x_1 + (d-1) \cdot \frac{m}{d}}.$$

Ведь все эти классы, совпадающие по модулю $\frac{m}{d}$, входят в различные классы вычетов по модулю m.

Сейчас рассмотрим вопрос о нахождении решения сравнения по модулю m. Нельзя ли найти явное решение сравнения $ax \equiv b \pmod m$, в случае, если $(a,m) = 1$.

По теореме Эйлера $a^{\varphi(m)} = 1 \pmod m$. По свойству сравнений мы можем умножить обе части сравнения на $a^{\varphi(m)-1}$, и после умножения получаем, что $a^{\varphi(m)}x \equiv x \equiv b \cdot a^{\varphi(m)-1} \pmod m$. Значит, решением данного сравнения является $\overline{b \cdot a^{\varphi(m)-1}}$ класс вычетов по модулю m.

Это один из методов решения сравнения, но, заметим, что есть и другие методы нахождения решения данного сравнения. Рассмотрим пример нахождения решения сравнения по модулю m.

Разберём различные варианты сравнений. Сначала рассмотрим случай решения сравнения $ax \equiv b \pmod m$, когда $(a, m) = 1$.

ПРИМЕР: а) Найти все решения сравнения $7x \equiv 11 \pmod{19}$.

Заметим, что $(7,19) = 1$. Значит, решение есть и оно одно. Найдём его. По замечанию выше, так как $\varphi(19) = 18$, то его можно записать в явном виде: это класс вычетов $\overline{11 \cdot 7^{17}}$ по модулю 19. Если же нужно найти наименьший положительный вычет, который лежит в этом классе вычетов, тогда нужно проделать некоторые дополнительные вычисления. Заметим, что $7^3 \equiv 1 \pmod{19}$, поэтому

$11 \cdot 7^{17} \equiv 11 \cdot (7^3)^5 \cdot 3^2 \equiv 99 \equiv 4 \pmod{19}$. Отсюда ответ можно записать и таким образом – это класс вычетов $\overline{4}$ по модулю 19.

Рассмотрим ещё один пример.

б) Найти все решения сравнения $33x \equiv 102 \pmod{123}$.

Заметим, что $(33,123) = 3$. Так как $3 \mid 102$, то сравнение разрешимо и имеет ровно 3 корня по модулю 123. Сначала мы сократим сравнение на 3, и перейдём к сравнению $11x \equiv 34 \pmod{41}$.

Здесь уже $(11,41) = 1$. Значит, решение у этого сравнения есть, и оно одно. Найдём его. По замечанию выше, так как $\varphi(41) = 40$, то его можно записать в явном виде: это класс вычетов $\overline{34 \cdot 11^{39}}$ по модулю 41. Опять же, если нужно найти наименьший положительный вычет, который лежит в этом классе вычетов, тогда нужно проделать некоторые дополнительные вычисления.

Заметим, что $11^2 \equiv -2 \pmod{41}$, поэтому

$$34 \cdot (11^2)^{19} \cdot 11 \equiv 34 \cdot (-2)^{19} \cdot 11 \equiv 5 \cdot (-2)^{19} \equiv 5 \cdot (2^7)^2 \cdot (-2)^5 \equiv 5 \cdot (5)^2 \cdot (-32) \equiv (5)^3 \cdot (-32) \equiv -64 \equiv 18 \pmod{41}$$

Значит, решение сравнения $11x \equiv 34 \pmod{41}$ можно записать и так: $\overline{34 \cdot 11^{39}} = \overline{18} \pmod{41}$.

Однако, нам нужно решения по модулю 123. А здесь мы воспользуемся теоремой 8.2 И все три решения сравнения по модулю 123 запишутся таким образом:

$$\overline{x_o} = \overline{18}; \quad \overline{x_1} = \overline{18+41} = \overline{59} \quad \text{и} \quad \overline{x_2} = \overline{18+41\cdot 2} = \overline{100}.$$

§ 9. ОДНОЗНАЧНОЕ РАЗЛОЖЕНИЕ НА МНОЖИТЕЛИ В ОБЛАСТЯХ ГЛАВНЫХ ИДЕАЛОВ

На втором курсе в курсе «Фундаментальной и компьютерной алгебры» говорились о том, что такое область целостности. Напомним, что это кольцо, в котором из того, что произведение двух элементов равно 0, следует, что один из этих двух множителей равен 0.

Заметим, что основная теорема алгебры, конечно, очень полезна, когда речь идёт об однозначном разложении на простые множители. Но в этом параграфе мы поговорим о более общем понятии разложения элементов кольца на простые элементы кольца. Это нам потребуется в дальнейшем. И в этом параграфе везде далее будем полагать, что А будет обозначать некоторую область целостности.

Определение. Кольцо А называется **евклидовой областью**, если существует какая-либо функция f из множества его ненулевых элементов в множество {0, 1, 2, 3, ...}, обладающая следующим свойством: для любых $a, b \in A$, $b \neq 0$, найдутся такие $c, d \in A$, что $a = cb + d$ и либо $d = 0$, либо $f(d) < f(b)$.

ПРИМЕРЫ: **а)** Кольцо **Z** является евклидовой областью. В **Z** в качестве функции f можно взять обычное абсолютное значение.

б) $k[x]$ оба являются евклидовыми областями. В кольце $k[x]$ нужному условию будет удовлетворять функция, ставящая в соответствие каждому многочлену его степень.

ОПР. Для элементов $a_1, \ldots, a_n \in A$ (произвольное кольцо), положим множество

$$B = (b_1, \ldots, b_n) = \{x_1b_1 + x_2b_2 + \ldots + x_na_n, \text{ где } x_1; x_2; \ldots x_n \text{ произвольные целые числа}\}$$

Заметим, что элементы $b_1, \ldots, bn$ служат образующими множества В.

ОПР. (А-Р с.13) Пусть $I = (b_1, \ldots, b_n)$, где $b_i \in A$, А – кольцо. Заметим, что сумма и разность двух элементов из $(b_1, \ldots, b_n)$ снова лежит

в (b_1, …, b_n). Кроме того, если $a \in I$ и $r \in A$, то $ra \in I$. Тогда I называется **идеалом в кольце A**.

ОПР. Если идеал I совпадает с (b_1, ..., b_n) для некоторых элементов $b_i \in I$, то говорят, что **I конечно порожден.** Если I = (a) для некоторого $a \in I$, то мы говорим, что I - **главный** идеал.

ОПР. Кольцо A называется **областью главных идеалов** или **кольцом главных идеалов** (ОГИ или КГИ), если каждый идеал в нем главный.

ЛЕММА 9.1 Если A – некоторая евклидова область и I – идеал, то существует такой элемент $a \in A$, что $I = aA = \{a \cdot r \mid r \in A\}$.

Доказательство. Рассмотрим множество неотрицательных целых чисел $\{f(b) \mid b \in I, b \neq 0\}$ Ввиду того что каждое множество неотрицательных целых чисел содержит наименьший элемент, существует такой элемент $a \in I$, $a \neq 0$, что $f(a) < f(b)$ для всех $b \in I$, $b \neq 0$. Мы утверждаем, что I = aA. Очевидно, что $aA \in I$. Предположим, что $b \in I$,: тогда, как мы знаем, существуют такие элементы $c,d \in A$, что b = ca + d, где либо d = 0, либо к $f(d) < f(a)$. Так как $d = b - ca \in I$, не может выполняться неравенство $f(d) < f(a)$. Таким образом, d = 0 и $b = ca \in A$. Поэтому $I \in aA$ и предложение доказано.

Таким образом, из Леммы 9.1 (Предложение 1.3.1) мы получили, что евклидово кольцо является кольцом главных идеалов.

Обращение этого утверждения неверно, хотя не так просто привести соответствующие примеры.

Везде дале будем полагать, что любое кольцо A будет кольцом главных идеалов (или сокращенно КГИ). Использование евклидовости области полезно, поскольку на практике можно показать, что многие кольца являются КГИ, установив сначала, что они – евклидовы области.

Введем несколько терминов. Если $a, b \in A$, $b \neq 0$, то мы будем говорить, что **b делит a**, если a = bc для некоторого $c \in A$; обозначение: $b \mid a$. Элемент A называется **единицей**, если он делит 1.

Два элемента $a, b \in A$ **ассоциированы**, если a = bu для некоторой единицы u.

Элемент $p \in A$, не являющийся единицей, называется **неприводимым**, если a|p означает, что элемент a – либо единица, либо ассоциирован с p.

Не единица $p \in A$ называется **простым** элементом, если $p \neq 0$ и из p|ab следует, что p|a или p|b.

Определение. Элемент $d \in A$ называется **наибольшим общим делителем** (НОД) двух элементов $a, b \in A$, если

(a) $d \mid a$ и $d \mid b$

b) $d' \mid a$ и $d' \mid \rightarrow d' \mid d$.

Как нетрудно убедиться, если оба элемента d и d' суть НОД для элементов a и b, то d и d' ассоциированы.

В произвольном кольце НОД двух элементов не обязательно существует. Однако справедливо следующее утверждение.

ЛЕММА 9.2. Пусть A является ОГИ и $a, b \in A$. Тогда элементы a и b имеют наибольший общий делитель d *и* $(a, b) = (d)$.

Доказательство. Образуем идеал (a, b). Ввиду того что A есть ОГИ, существует такой элемент d, что $(a, b) = (d)$. Так как $(a) \subseteq (d)$ и $(b) \subseteq (d)$, то $d|a$ и $d|b$. Если $d'|a$ и $d'|b$, то $(a) \subseteq (d')$ и $(b) \subseteq (d')$. Поэтому $(d) = (a, b) \subseteq (d')$ и $d'|d$. Мы доказали, что d есть НОД элементов a и b и что $(a, b) = (d)$.

Два элемента a и b называются **взаимно простыми,** если их единственными общими делителями являются единицы.

Следствие 1. *Если A является КГИ и $a, b \in A$ взаимно просты, то $(a, b) = A$.*

Следствие 2. *Если A является КГИ и элемент $p \in A$ неприводим, то p – простой элемент.*

Доказательство. Предположим, что $p|ab$ и p не делит a. Так как p не делит a, то их общими делителями будут только единицы. Согласно следствию I, $(a, p) = A$. Таким образом, $(ab, pb) = \{b\}$. Ввиду того что $ab \in (p)$ и $pb \in (p)$, имеем $(b) \subseteq (p)$. Итак, $p|b$.

Следствие 3. Нетрудно убедиться в том, что простой элемент в КГИ неприводим.

Начиная с этого места, кольцо A будет КГИ, и мы используем термины простой и неприводимый как синонимы.

Наша цель – показать, что каждый ненулевой элемент из R представляется в виде произведения неприводимых элементов. Доказательство проводится в два этапа. Сначала мы покажем, что для заданного элемента $a \in R$, $a \neq 0$, существует неприводимый элемент, делящий a. Затем мы убедимся в том, что элемент a представляется в виде произведения неприводимых элементов.

ЛЕММА 9.3 *Пусть $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq$ ... – возрастающая цепь идеалов в A – КГИ. Тогда существует такое целое число k, что $(a_k) = (a_{k+l})$ для $l = 0, 1, 2, \ldots$. Другими словами, цепь обрывается после конечного числа шагов.*

Доказательство. Пусть $I = \bigcup_{i \in J} (a_i)$, где J – некоторое множество. Нетрудно убедиться в том, что I – идеал. Таким образом, $I = (a)$ для некоторого $a \in A$. Но поскольку $a \in \bigcup_{i \in J} (a_i)$, то $a \in (a_k)$ при некотором $k \in N$, откуда следует, что $I = (a) \in (a_k)$. Значит, $I = (a_h) = (a_{k+1}) = \ldots$.

ЛЕММА 9.4. Каждый ненулевой элемент из A, не являющийся единицей, представляется в виде произведения неприводимых элементов.

Доказательство. Пусть $a \in A$, $a \neq 0$, a – не единица. Прежде всего, мы хотим показать, что a делится на некоторый неприводимый элемент. Если сам a неприводим, то мы получили то, что хотели. В противном случае, $a = a_1 \cdot b_1$, где a_1 и b_1 – не единицы.

Если a_1 неприводим, то опять получено то, что было нужно. В противном случае $a_1 = a_2 \cdot b_2$, где a_2 и b_2 – не единицы. Если a_2 неприводим, то мы опять получили то, что хотели. В противном случае продолжаем рассуждение, как прежде. Заметим, что $(a) \subseteq (a_1) \subseteq (a_2) \subseteq (a_3)$ ... . Согласно лемме 8.3 (Лемме 1), эта цепь не может быть бесконечной. Таким образом, при некотором *k* элемент a_k неприводим.

Теперь мы покажем, что элемент a представляется в виде произведения неприводимых элементов.

Если a сам неприводим, то мы получили, что хотели. В противном случае пусть p_1 – такой неприводимый элемент, что $p_1 | a$. Тогда $a = p_1 c_1$. Если c_1 – единица, то нужное разложение получено.

В противном случае пусть p_2 – такой неприводимый элемент, что $p_2 | c_1$. Тогда $a = p_1 p_2 c_2$. Если c_2 – единица, то опять искомое разложение найдено.

В противном случае продолжаем рассуждение, как прежде. Заметим, что $(a) \subseteq (c_1) \subseteq (c_2) \subseteq$ ... . Эта цепь не может продолжаться бесконечно ввиду леммы 8.3 (Лемме 1). Таким образом, при некотором k имеем $a = p_1 p_2 \ldots p_k \cdot c_k$, где c_k – единица. Так как $p_k c_k$ неприводим, доказательство предложения закончено.

ЛЕММА 9.5 Пусть p – некоторый простой элемент и $a \neq 0$**.** Тогда существует такое целое число n, что $p^n | a$, но p^{n+1} не делит a.

Доказательство. Если бы утверждение леммы не выполнялось, то для каждого целого числа $m > 0$ существовал бы такой элемент b_m, что $a = p^m b_m$. Тогда $p b_{m+1} = b_m$ и последовательность $(b_1) \subseteq (b_2) \subseteq (b_3)$ ... была бы бесконечной возрастающей цепью идеалов, которая не обрывалась бы. Это противоречит лемме 9.3.

Целое число n, определенное в лемме 9.5, однозначно определяется элементами *p* и *a.* Мы полагаем $n = \mathrm{ord}_p\, a$.

ЛЕММА 9.6. Если $a, b \in R$ и $a, b \neq 0$, то $\mathrm{ord}_p\, ab = \mathrm{ord}_p\, a + \mathrm{ord}_p b$.

Доказательство. Положим $a = \mathrm{ord}_p\, a$ и $= \mathrm{ord}_p b$. Тогда $a = p^a c$ и $b = p^\beta d$, где p не делит c и c не делит d. Таким образом, $ab = p^{\alpha+\beta} cd$. Так как p – простой элемент, то p не делит cd. Следовательно, $\mathrm{ord}_p ab = \alpha + \beta = \mathrm{ord}_p a + \mathrm{ord}_p b$.

Мы теперь можем сформулировать и доказать основную теорему этого параграфа.

Пусть S – некоторое множество простых элементов в S со следующими двумя свойствами:

а) Каждый простой элемент в S ассоциирован с некоторым простым элементом из S.

б) Никакие два простых элемента из S не ассоциированы.

Для получения такого множества S выберем по одному представителю из каждого класса ассоциированных простых элементов. В таком выборе имеется, конечно, большая доля произвольности. В кольцах Z и k[x] имелся единственный способ произвести этот выбор. В Z в качестве S выбирается множество положительных простых чисел.

В k[x] в качестве S берется множество приведенных неприводимых многочленов. В общем случае естественного способа произвести указанный выбор нет, что приводит иногда к осложнениям.

ТЕОРЕМА 9.7 Пусть A является КГИ и S – некоторое множество простых элементов с заданными выше свойствами. Тогда для $a \in S$, $a \neq 0$, можно записать

$$a = u \prod_{p \in S} p^{e(p)}, \qquad (1)$$

где u – единица и произведение берется по всем элементам из S. Единица u, а также показатели степени e(p) определены элементом a однозначно. На самом деле $e(p) = \mathrm{ord}_p a$.

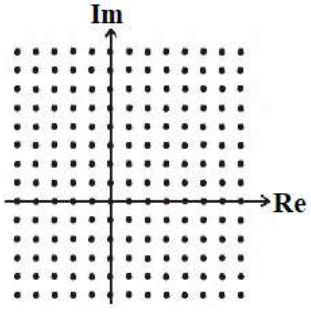
Доказательство. Существование выписанного представления сразу же следует из леммы 9.4.

Для доказательства однозначности считаем q простым элементом из S и применяем функцию ord_p к обеим частям равенства (1). Используя лемму 9.6, получаем

$$\mathrm{ord}_p a = \mathrm{ord}_p u + \sum_{p|a} e(p) \cdot ord_a p .$$

Далее, согласно определению функции ord_p, $\mathrm{ord}_q u = 0$ и $\mathrm{ord}_q p = 0$ при $q \neq p$ и $\mathrm{ord}_q p = 1$ при $q = p$. Таким образом, $\mathrm{ord}_q a = e(q)$. Так как показатели степени e(q) определены однозначно, то однозначно определена и единица u. Это завершает доказательство.

§ 10. КОЛЬЦО ЦЕЛЫХ ГАУССОВЫХ ЧИСЕЛ



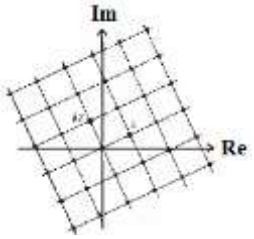
ОПР. Комплексное число $a + bi$ называют **целым гауссовым,** если a u b – целые числа.

Так как сумма, разность и произведение целых гауссовых чисел – целые гауссовы числа, то как несложно прове-

рить все свойства и показать, что множество Z[*i*] = {a+b*i*, a, b из Z} – целых гауссовых чисел является кольцом.

ОПР. Целое гауссово число u **кратно целому гауссову числу v**, если существует такое целое гауссово число w, что u = v·w.

Отметив на плоскости целые гауссовы числа, мы получим решетку (см. рисунок).



Интересно, что числа, кратные данному числу z, тоже образуют решетку (рис.).

Произведение (a + b*i*)(a - b*i*) = $a^2 + b^2$ комплексного числа z = a + b*i* и сопряженного с ним числа $\bar{z}$ = a - b*i* является числом вещественным. Поэтому для любого ненулевого целого гауссова числа z существует кратное ему натуральное число $z\cdot\bar{z} = a^2 + b^2$.

ТЕОРЕМА 10.1 Если числа a и b взаимно просты, то наименьшим натуральным числом n, которое кратно числу a + b*i*, является именно число $a^2 + b^2$.

Доказательство**.** Поскольку $\frac{n}{a+bi} = \frac{n(a-bi)}{(a+bi)(a+bi)} = \frac{na}{a^2+b^2} - \frac{nbi}{a^2+b^2}$.

Поэтому натуральное число n кратно числу a+b*i*, только в тех случаях, когда na и nb делятся на $(a^2 + b^2)$. Поскольку a и b взаимно просты, это будет только тогда, когда n делится на $(a^2 + b^2)$.

ТЕОРЕМА 10.2 Z[*i*] – евклидово кольцо (или евклидова область).

Доказательство. Заметим, что Z[*i*] - кольцо, так как операции + и x на нём замкнуты и есть и 0 и 1.

В качестве функции f: Z[*i*] - N_o возьмем $f(a + bi) = a^2 + b^2$.

Берём два произвольных числа $z_1 = a + bi$; $z_2 = c + di$, и допустим, что $z_2 \neq 0$. Тогда $z_1/z_2 = r + si$, где r, s – это рациональные числа. Выберем целые числа m и n из Z:

$$|r - m| \leq 0{,}5; \text{ и } | s - n| \leq 0{,}5.$$

Положим $\delta = m + ni$, $\delta \in Z[i]$. И $f(z_1/z_2) = (r - m)^2 + (s - n)^2 \leq 0{,}25 + 0{,}25 = 0{,}5$. Пусть $\rho = z_1 - \delta\cdot z_2$ тогда ρ лежит в Z[*i*] и либо ρ=0, либо $f(\rho) = f(z_2\cdot(z_1/z_2 - \delta)) = f(z_2)\cdot f(z_1/z_2 - \delta) \leq 0{,}5\cdot f(z_2)$.

Таким образом, f – действительно удовлетворяет свойствам. Значит, Z[*i*] – евклидово кольцо (или евклидова область).

ТЕОРЕМА 10.3. В Z[*i*] нет делителей единицы, кроме чисел 1, *i*, - 1 и - *i*. (Другими словами, целое гауссово число a + b*i* является делителем единицы в том и только том случае, когда $a^2 + b^2 = 1$).

Доказательство**.** Заметим, что модулю единичного элемента в Z[*i*] равен 1. Если **1** = uv, где u, v∈ Z[*i*], то 1 = |u| = |v|. Поскольку модуль ненулевого целого гауссова числа не меньше 1, имеем |u| = |v| = 1, откуда и следует утверждение теоремы.

ТЕОРЕМА 10.4 f(π) = p – простой элемент в Z для некоторого π из Z[*i*]. Доказать, что π – простой элемент в Z[*i*].

Доказательство. Пусть Z[*i*] – это евклидово кольцо, и функция, которая обращает его в евклидово кольцо – это квадрат модуля числа z = a+b*i*. Но модуль числа обладает свойством мультипликативности, т. е. |z·v| = |z|·|v|. Значит, если f(π) = p и π|α·β. Тогда f(π) = p|f(α)·f(β) = p|A·B, где A = f(α) и B = f(β) (A и B – это натуральные числа). По свойствам простых чисел в Z, если p|AB, то p|A или p|B. Значит, либо A либо B равны 1. Значит, либо α, либо β – единица. Значит, либо α, либо β ассоциированы с π. Отсюда π – неприводимый элемент, т. е. простой, так как в КГИ эти термины равносильны.

Таким образом, мы показали, что Z[*i*] – евклидово кольцо, а значит, согласно лемме 8.1 - Z[*i*] является кольцом главных идеалов. Если в этом кольце выбрать надлежащее множество простых элементов S, о котором говорится в §8, то любой элемент в этом можно разложить на простые элементы однозначно, с точностью до перестановки множителей.

§ 11. ПРЕДСТАВЛЕНИЕ ЧИСЕЛ В ВИДЕ СУММЫ КВАДРАТОВ

В данном параграфе мы рассмотрим вопрос, который нас интересует с самого начала: вопрос представления натурального числа в виде суммы двух квадратов. Мы уже познакомились со всей интересующей нас вспомогательной информацией, поэтому всё дальнейшее мы сможем последовательно рассматривать и доказывать.

0	1	4	9	16	25	36	49	64	81	100
1	2	5	10	17	26	37	50	65	82	101
4	5	8	13	20	29	40	53	68	85	104
9	10	13	18	25	34	45	58	73	90	109
16	17	20	25	32	41	52	65	80	97	116
25	26	29	34	41	50	61	74	89	106	125
36	37	40	45	52	61	72	85	100	117	136
49	50	53	58	65	74	85	98	113	130	149
64	65	68	73	80	89	100	113	128	145	164
81	82	85	90	97	106	117	130	145	162	181
100	101	104	109	116	125	136	149	164	181	200

Сначала рассмотрим таблицу, в верхней строке и левом столбце которой – квадраты целых чисел, а в других клетках – суммы соответствующих квадратов.

Наименьшее натуральное число, большее 1, не представимое в виде суммы двух квадратов целых чисел, это число 3. Кратные 3 числа 6, 12, 15, 21 тоже не представимы, а вот числа $9 = 3^2 + 0^2$ и $18= 3^2 + 3^2$ – представимы. Возникает гипотеза: числа, которые кратны 3, но не кратны 9, не представимы в виде суммы двух квадратов. Эта гипотеза верна. Докажем это утверждение.

ТЕОРЕМА 11.1 Если сумма квадратов $x^2 + y^2$ целых чисел x, y кратна 3, то числа x, y тоже кратны 3.

Доказательство. Мы уже рассматривали свойства остатков квадратов при делении на 3 и на 4. В лемме 3.7 было показано, что остатки могут быть только 0 или 1. Значит, сумма остатков двух квадратов при делении на 3, если ни одно из них не делится на 3, может быть только 2. Если же одно делится, а другое нет, тогда 1. Но сумма квадратов может делиться на 3, только если каждое из этих чисел делится на 3. Значит, все доказано.

Следующее после 3 и 6 не представимое в виде суммы двух квадратов число – это 7. Кратные 7 числа 14, 21, 28, 35, 42, 56, 63 не представимы в виде суммы квадратов. Опять возникает гипотеза: если сумма квадратов $x^2 + y^2$ кратна 7, то и сами целые числа x, y кратны 7. Докажем это утверждение.

ТЕОРЕМА 11.2 Если сумма квадратов $x^2 + y^2$ целых чисел x, y кратна 7, то числа x, y тоже кратны 7.

Доказательство. Выпишем остатки от деления квадратов целых чисел на 7. Остатки равны 0, 1, 2, 4. Опять же сумма двух квадратов будет делиться на 7, только если они оба делятся на 7, иначе такого не может быть. Введём новое понятие.

ОПР. Ненулевые остатки от деления квадратов целых чисел на простое число $p > 2$ называют **квадратичными вычетами по модулю p.**

ПРИМЕР. Найти все квадратичные вычеты по модулю 19. Понятно, что достаточно рассмотреть квадраты первых 9 чисел, так как квадрат a и – a одинаков. Поэтому квадратичными вычетами будут числа 1, 4, 9, 16, 6, 11, 8, 5, а все остальные ненулевые будут квадратичными невычетами.

В виде суммы двух квадратов не представимы не только простые числа, которые при делении на 4 дают остаток 3, но и вообще все числа 3, 7, 11, 15, 19, 23, 27,...:

Докажем достаточно важное утверждение.

ТЕОРЕМА 11.3. Всякое представимое в виде суммы квадратов двух целых чисел нечетное число при делении на 4 дает остаток 1, а не 3.

Доказательство. Из двух квадратов, сумма которых нечётна, обязательно один чётен, а другой нечётен. Квадрат чётного числа нацело делится на 4, а квадрат нечётного числа при делении на 4 дает остаток 1 (Это было доказано, когда рассматривались свойства делимости с остатком.

Отметим еще одно важное свойство представимости чисел в виде суммы двух квадратов: если два числа представимы в виде сумм двух квадратов, то и их произведение также можно представить в виде суммы двух квадратов. Это следует из того, что если $n = (a^2 + b^2)$; $m = x^2 + y^2$. Тогда

$$(a^2 + b^2)(x^2 + y^2) = a^2x^2 + b^2x^2 + a^2y^2 + b^2y^2,$$

прибавим и отнимем $2abxy$ и изменим порядок слагаемых:

$$(a^2 + b^2)(x^2 + y^2) = a^2x^2 + b^2x^2 + a^2y^2 + b^2y^2 =$$

$$= a^2x^2 + 2axby + b^2y^2 + b^2x^2 - 2bxay + a^2y^2 = (ax + by)^2 + (bx - ay)^2. \quad (1)$$

В частности, можно заметить, что если число $n = x^2 + y^2$, то

$$(x + y)^2 + (x - y)^2 = x^2 + 2xy + y^2 + x^2 - 2xy + y^2 = 2(x^2 + y^2) = 2n,$$

т. е. и число $2n$ также представимо в виде суммы квадратов. Аналогично можно доказать, что и число $5n$ также представимо в виде суммы квадратов.

Поскольку мы научились представлять произведение сумм двух квадратов в виде суммы двух квадратов, очень важно выяснить, какие простые числа представимы в виде суммы двух квадратов целых чисел, а какие не представимы. Числа вида $4n + 3$, $n \in N$, как утверждает Теорема 11.3, не представимы.

Поэтому остаётся рассмотреть простые числа, которые при делении на 4 дают остаток 1.

Сначала докажем одну несложную теорему – теорему Вильсона.

ТЕОРЕМА 11.4 Для любого простого числа p сумма $(p - 1)! + 1$ кратна p. (Другими словами, произведение $1 \cdot 2 \cdot \ldots (p - 1)$ дает остаток $(p - 1)$ при делении на p.)

Доказательство. Рассмотрим многочлен $x^p - 1$ в Z_p он имеет p-1 корень, $\bar{1}, \bar{2}, \ldots, \overline{p-1}$, т. е. любой ненулевой класс вычетов, поэтому

$$(x^{p-1} - \bar{1}) = (x-\bar{1})(x-\bar{2})\ldots(x-\overline{p-1}) \equiv 0 \pmod p$$

По обобщенной теореме Виета произведение корней многочлена равно свободному члену, если степень многочлена четна, поэтому

$$1 \equiv 1 \times 2 \times \ldots \times (p-1) \pmod p$$

Если же p=2, тогда $x^{p-1} - 1 \equiv x^1 - 1 \equiv x+1 \pmod 2$. Значит, и здесь утверждение теоремы верно.

ЛЕММА 11.5. Для любого простого числа $p = 4n + 1$, где n из N, существует такое целое число m, что $m^2 + 1$ кратно p.

Доказательство. В качестве числа m можно взять число m = (2n)! Чтобы это увидеть, рассмотрим число

$$(p-1)! = (4n)! = 1\cdot 2\cdot\ldots\cdot(2n - 1)..\cdot (2n)\cdot(2n +1)\cdot(2n + 2)\cdot\ldots\cdot(4n) =$$
$$= 1\cdot 2\cdot\ldots\cdot(2n - 1)\cdot(2n)\cdot(p - 2n)\cdot(p - (2p - 1))\cdot\ldots\cdot(p - 2)\cdot(p - 1).$$

Это произведение по модулю p сравнимо с

$$1\cdot 2\cdot\ldots\cdot(2n - 1)\cdot(2n)\cdot(p - 2n)\cdot(p - (2p - 1))\cdot\ldots\cdot(p - 2)\cdot(p - 1) \equiv$$
$$\equiv 1\cdot 2\cdot\ldots\cdot (2n -1)\cdot(2n)\cdot(-1)^{2n}(2n)\cdot(2n - 1)\cdot\ldots\cdot 2\cdot 1 \equiv ((2n)!)^2 = m^2 \pmod p$$

Значит, $m^2 +1$ при делении на p дает такой же остаток, как и число (p - 1)! + 1. Последнее число кратно p по теореме 11.5 (Теореме Вильсона), которая впервые была сформулирована англичанином Эдуардом Варингом (1734–1798), а доказана французом Жозефом Луи Лагранжем (1736–1813).

Заметим, что все нечётные простые натуральные делители числа m^2+1 имеют вид 4n+1, так как по модулю 4 любое число вида m^2+1 не может быть сравнимо с 3 по модулю 4.

ЛЕММА 11.6 Любой простой делитель p числа $m^2 + 1$, где m – целое, представим в виде суммы квадратов двух натуральных чисел.

Доказательство. Число $m^2+1 = (m + i)(m – i)$. Кольцо $Z[i]$ – кольцо целых гауссовых чисел, и мы уже показали выше, что это кольцо евклидово, значит, это кольцо главных идеалов, т. е. это кольцо, в котором разложение на простые происходит единственным образом. Значит, разложение на простые множители в $Z[i]$ единственно в том же смысле, в каком оно единственно для обычных целых чисел.

Итак, делитель p числа $m + i$ и $m - i$ не может быть простым гауссовым числом, так как числа

$(m + i)$ и $(m - i)$ не делятся на p, но p является делителем числа $m^2 + 1$.

Значит, число p - составное в $Z[i]$, и его можно представить в виде произведения двух не единичных элементов:

$$p = (a + bi)(c + di),$$

где целые гауссовы числа $(a + bi)$ и $(c + di)$ – не делители единицы. Поскольку модуль произведения равен произведению модулей, имеем $p = \sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2}$, т. е. $p^2=(a^2 + b^2)\cdot(c^2 + d^2)$, откуда $p = (a^2 + b^2) = (c^2 + d^2)$.

Ну и теперь докажем основную теорему о представлении натурального числа в виде суммы квадратов. Мы уже знаем, что простое число вида 4n+3 не представимо в виде суммы двух квадратов, но мы не знаем, все ли простые числа вида 4n+1 представимы в виде суммы двух квадратов.

ТЕОРЕМА 11.7. Любое простое число p. которое при делении на 4 дает остаток 1, представимо в виде суммы квадратов двух натуральных чисел.

Доказательство. Доказательство мы получим, используя лемму 11.5 и лемму 11.6.

Заметим, что согласно лемме 11.5 для любого простого числа вида 4n+1 найдётся натуральное m, такое, что p делит m^2+1. Согласно лемме 11.6 любой простой делитель числа m^2+1 представим в виде суммы двух квадратов. Отсюда следует, что любое простое число вида 4n+1 представимо ввиду суммы двух квадратов.

А сейчас рассмотрим вопрос, какие простые числа в Z остаются простыми в Z[*i*]. Этот вопрос для нас также важен, как и в случае целых чисел: какие же простые натуральные числа останутся простыми во множестве целых гауссовых чисел, а какие станут составными? И как устроены разложения «новых составных» чисел?

Во-первых, докажем следующую теорему.

ТЕОРЕМА 11.8 а) Всякое простое натуральное число вида $p = 4n + 3$ является простым в Z[*i*].

б) число 2 ассоциировано с квадратом простого гауссова числа 1+ *i*;

в) всякое простое натуральное число вида $p = 4n + 1$ разлагается в произведение двух сопряженных простых в кольце Z[*i*] чисел: $p = (a + bi)(a - bi)$.

Доказательство. а) Если число $p = 4n + 3$ представлено в виде произведения двух не единичных целых гауссовых чисел $p = (a + bi)(c + di)$, то $= (a + bi)\cdot(c + di)$, значит, $p = a^2 + b^2 = c^2 + d^2$. Но это противоречит тому, что такие простые в Z не могут быть представимы в виде суммы квадратов. Поэтому возможен только вариант, что когда один из множителей $(a^2 + b^2)$ и $(c^2 + d^2)$ равен 1, т. е. числа ассоциированы. Значит, p – неприводим или прост в Z[*i*].

б) Просто проверим, что число $(1+i)^2$ делит 2. Это действительно так, ибо $(-i)(1 + i)^2 = 2$.

в) любое простое из Z вида 4n+1 является делителем числа m^2+1, а любой такой простой (из Z) делитель p числа $m + i$ и $m - i$ не может быть простым гауссовым числом, так как числа $(m + i)$ и $(m - i)$ не делятся на p, но p является делителем числа $m^2 + 1$, т. е. p – не простое число.

Из этой теоремы можно получить ещё один результат, а именно справедлива следующая теорема.

ТЕОРЕМА 11.9 Если простое число p не представимо в виде суммы двух квадратов, и если сумма квадратов $x^2 + y^2$ кратна p, то каждое из целых чисел x, y кратно p.

Доказательство. По теоремам 11.7 и 11.8 следует, что не представимыми в виде суммы квадратов могут быть только простые числа вида 4n+3. Тогда по

теореме 11.8 отсюда следует, что такое простое в Z остаётся простым и в кольце целых гауссовых чисел.

Значит, в рассматриваемой ситуации p – простое гауссово число. Поскольку произведение

$(x + iy)(x - iy) = x^2 + y^2$ кратно p, то хотя бы один из сомножителей кратен p. А отсюда и получаем, что, например, $p|(x + iy)$, тогда найдётся такое целое гауссово число $a + bi$, такое, что $p(a + bi) = x + yi$. А отсюда, в силу равенства двух комплексных чисел, и следует, что $p|x$ и $p|y$. А это и требовалось доказать.

Докажем ещё одно вспомогательное свойство, которое также важно.

ЛЕММА 11.10. Простое натуральное число p нельзя представить в виде произведения более чем двух целых гауссовых чисел, не являющихся делителями единицы. (Другими словами, если p ассоциировано с произведением двух не являющихся делителями единицы целых гауссовых чисел, то эта числа – простые.)

Доказательство. Если $p = (a + bi)(c + di)(e + fi)$, то $|p| = |a + bi|\cdot|c + di|\cdot|e + fi|$,

откуда $p^2 = (a^2 + b^2)(c^2 + d^2)(e^2 + f^2)$. Квадрат простого числа никак не может быть произведением трех отличных от 1 натуральных чисел. Отсюда лемма доказана.

Осталось сделать выводы о том, какие-же числа представимы в виде суммы двух квадратов целых чисел.

По теоремам 11.4 и 11.7, простое число $p > 2$ не представимо в виде суммы двух квадратов, если оно имеет вид $p = 4k + 3$, и представимо – если $p = 4k + 1$, где k – целое.

Согласно формуле (1) данного параграфа, и теореме 11.9 получаем вывод, который сформулируем в виде теоремы 11.11.

ТЕОРЕМА 11.11. Натуральное число m представимо в виде суммы квадратов двух целых чисел тогда и только тогда, когда в его разложение на простые множители любой простой множитель вида $4k + 3$ входит в чётной степени.

Этот критерий впервые был сформулирован голландцем Альбером Жирaром (1595–1632) в следующем виде: натуральное число представимо в виде суммы двух квадратов тогда и только тогда, когда оно является или квадратом, или числом 2, или простым числом, которое на 1 больше, чем некоторое кратное 4, или произведением нескольких вышеперечисленных чисел. Скорее всего, Жирар опирался лишь на изучение таблиц и не претендовал на то, что может доказать необходимость и достаточность своих условий.

ЛИТЕРАТУРА

1.Айерленд К., Роузен Классическое введение в современную теорию чисел. – Москва : Мир, 1987. – 416 с.

2.Бухштаб А.А. Теория чисел. – Москва : Просвещение, 1966. – 384 с.

3.Виноградов И.М. Основы теории чисел. – Москва : Наука, 1972г. – 128 с.

4.Куликов Л.Я. Алгебра и теория чисел : учебное пособие для педагогических вузов. – Москва : Высшая школа, 1979. – 560 с.

5.Коблиц Н. Курс теории чисел и криптографии. – Москва : Научное издательство ТВП, 2001. – 288 с.

6.Маховенко Е.Б. Теоретико-числовые методы в криптографии. – Москва : Гелиос АРВ, 2006. – 320 с.

ОПИСАНИЕ ФУНКЦИОНАЛЬНОСТИ ИЗДАНИЯ:

Интерфейс электронного издания (в формате pdf) можно условно разделить на 2 части.

Левая навигационная часть (закладки) включает в себя содержание книги с возможностью перехода к тексту соответствующей главы по левому щелчку компьютерной мыши.

Центральная часть отображает содержание текущего раздела. В тексте могут использоваться ссылки, позволяющие более подробно раскрыть содержание некоторых понятий.

МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ:

Celeron 1600 Mhz; 128 Мб RAM; Windows XP/7/8 и выше; 8x DVD-ROM; разрешение экрана 1024×768 или выше; программа для просмотра pdf.

СВЕДЕНИЯ О ЛИЦАХ, ОСУЩЕСТВЛЯВШИХ ТЕХНИЧЕСКУЮ ОБРАБОТКУ И ПОДГОТОВКУ МАТЕРИАЛОВ:

Оформление электронного издания : Издательский центр «Удмуртский университет».

Компьютерная верстка: М. В. Сабрекова.

Авторская редакция.

Подписано к использованию 30.12.2025
Объем электронного издания 1,7 Мб
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел. : +7(3412)263-751 E-mail: editorial@udsu.ru