МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ
М. В. ЛОМОНОСОВА
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ
КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Смирнов Дмитрий Константинович
Троянок Татьяна Тимуровна

Введение в теорию чисел и приложение

ЛЕКЦИОННЫЙ КУРС

Лекторы:

Снурницын Павел Владимирович
Строева Екатерина Николаевна

Содержание

Введение

Перечень используемых сокращений

$\mathbb{N}$	Множество натуральных чисел
$\mathbb{Z}$	Множество целых чисел
$\mathbb{Q}$	Множество рациональных чисел
$\mathbb{R}$	Множество действительных чисел
p	Простое число
$a\|b$	Число a делит число b
$[a,b]$	НОК чисел a и b
(a,b)	НОД чисел a и b
$A = \{x_1a_1 + \dots + x_na_n,\ x_i \in \mathbb{Z}\} = (a_1, \dots, a_n)$	$(a_1, \dots, a_n)$ - Идеал
$\sigma(n)$	Сумма делителей числа n
$\nu(n)$	Число делителей числа n
$ord_p(a)$	Порядок/показатель числа a по основанию p
$\forall$	Для любого
$\exists$	Существует
$[x]$	Целая часть числа x

Часть I

Элементарная теория чисел

1. Тема №1. Простые числа

Определение 1.1. Число a делит натуральное число b, если $\exists$ такое число c, что $a = bc$. Если b делится на a, то будем обозначать $a \mid b$.

Определение 1.2. Число $p \in \mathbb{Z}_{>1}$ назыается простым, если $d \mid p$, где $d \in \{1, p\}$.

Теорема 1.1 (Теорема Евклида)**.** $\exists$ бесконечно много простых чисел.

Доказательство. Пусть заданы числа $p_1 \ldots, p_n$ - конечное множество простых чисел и $N = p_1 \cdot p_m + 1$. Для каждого p_i такого, что $1 \leqslant i \leqslant m$ справедливо: $p_i \nmid N$ (так как $p_i \mid p_1 \cdot \ldots p_m$ и если $p_i \mid N$, то $p_i = 1$ - противоречие). Если p - такое число, что $p \mid N$, и $p \in \{p_1, \ldots p_m\}$, то получили противоречие того, что множество конечно. □

Теорема 1.2. Каждое ненулевое целое число может быть представлено в виде произведения простых чисел.

Доказательство. Пусть существует число, которое не может быть представлено в таком виде. Пусть N - наименьшее положительно целое число с таким свойством. Так как N само не может быть простым, то $N = m \cdot k$, где $1 < m, k < N$. Но так как m и k положительны и меньше N, они должны быть произведениями простых чисел. А тогда произведением простых чисел будет и $N = mk$ (противоречие). □

Лемма 1.1 (Деление с остатком)**.** Всякое целое a представляется единственным способом через положительное целое b в форме:

$$a = b \cdot q + r,\ 0 \leqslant r < b,\ a \in \mathbb{Z},\ b \in \mathbb{Z}_{>0}. \tag{1.1}$$

Доказательство. Рассмотрим множество всех целых чисел вида $a - bx$, где $x \in \mathbb{Z}$. Это множество содержит положительные элементы. Пусть $r = a - q \cdot b$ - наименьший неотрицательный элемент этого множества. Мы утверждаем, что $0 \leqslant r < b$. В противном случае, $r = a - q \cdot b \geqslant b$, а поэтому
$0 \leqslant a - (q+1) \cdot b < r$, что противоречит минимальности r. □

Определение 1.3. Для $a_1, a_2, \dots, a_n \in \mathbb{Z}$ определим $\big(a_1, a_2, \dots a_n\big)$ как множество всех целых чисел вида $a_1 \cdot x_1 + a_2 \cdot x_2 + \dots + a_n \cdot x_n$,
где $x_1, x_2, \dots x_n \in \mathbb{Z}$.

Обозначение:

$$A = \{x_1 \cdot a_1 + \dots x_n \cdot a_n,\ x_i \in \mathbb{Z}\} = \big(a_1, \dots, a_n\big) \tag{1.2}$$

На языке теории колец A является *идеалом* в кольце $\mathbb{Z}$.

Свойства:

— Если $a, b \in A$, то $a + b \in A$;

— Если $a \in A$, $r \in \mathbb{Z}$, то $r \cdot a \in A$.

Лемма 1.2. Если $a, b \in \mathbb{Z}$, то существует такой элемент $d \in \mathbb{Z}$, что $(a, b) = (d)$.

Доказательство. Можно считать, что хотя бы один из элементов a, b ненулевой, так что в (a, b) имеются положительные элементы. Пусть d - наименьший положительный элемент в (a, b). Значит $(d) \subseteq (a, b)$. Покажем, что выполнено и обратное включение.

Пусть $c \in (a, b)$. По лемме 1.1 существуют такие целые числа q, r, что $c = dq+$ и $0 \leqslant c < d$. Так как c и d входят в (a, b), то $r = c - qd$ также входит в (a, b). Поскольку $0 \leqslant r < d$, то $r = 0$. Таким образом, $c = qd \in (d)$. □

Определение 1.4. Пусть $a, b, \in \mathbb{Z}$. Целое число d называется *наибольшим общим делителем* целых чисел a и b, если d делит одновременно a и b и каждый другой общий делитель a и b делит d.

Обозначение:

$$\begin{aligned} &\text{НОД}(a, b) = (a, b) = d, \\ &d \mid a, d \mid b \end{aligned} \tag{1.3}$$

Определение 1.5. Пусть $a, b, \in \mathbb{Z}$. Целое число d называется *наименьшим общим кратным* целых чисел a и b, если a делит одновременно d, b делит d и каждое другое общее кратное a и b делится на d.

Обозначение:

$$
\begin{aligned}
&\text{НОК}(a, b) = [a, b] = d, \\
&a \mid d, b \mid d
\end{aligned}
\tag{1.4}
$$

Определение 1.6. Два целых числа a и b взаимно просты, если их единственными общими делителями являются единицы ± 1.

Лемма 1.3. Пусть $a, b \in \mathbb{Z}$. Если $(a, b) = (d)$, то d - является наибольшим общим делителем чисел a и b.

Доказательство. Так как $a \in (d)$ и $b \in (d)$, мы видим, что d - общий делитель a и b. Предположим, что c - их общий делитель. Тогда c делит каждое число вида $ax + by$. В частности, $c \mid d$. □

Утверждение 1.1. Предположим, что $a \mid bc$, и что $(a, b) = 1$. Тогда $a \mid c$

Доказательство. Так как $(a, b) = 1$, то существуют целые числа r и s, для которых $ra + sb = 1$. Поэтому $rac + sbc = c$. Так как a делит левую часть этого равеннства, то $a \mid c$. □

Следствие 1.1. Если p-простое число и $p \mid bc$, то либо $p \mid b$, либо $p \mid c$.

Доказательство. Единственными делителями числа p являются ± 1, $\pm p$. Таким образом, $(p, b) = 1$ или p, то есть, либо $p \mid b$, либо p и b взаимно просты. Если $p \mid b$, то доказательство закончено. Если $p \nmid b$, то $(p, b) = 1$ и, согласно предположению 1.1, $p \mid c$. □

Определение 1.7. *Показателем* или *порядком* числа n по основанию p называется такое число α, что $p^{\alpha} \mid n$, $p^{\alpha+1} \nmid n$.

Обозначение:

$$\alpha = ord_p(n) \tag{1.5}$$

Утверждение 1.2. Предположим, что p - простое число и $a, b \in \mathbb{Z}$. Тогда $ord_p(ab) = ord_p(a) + ord_p(b)$.

Доказательство. Пусть $\alpha = ord_p(a)$, $\beta = ord_p(b)$. Тогда $a = p^{\alpha}c$ и $b = p^{\beta}d$, где $p \nmid c$ и $p \nmid d$. Далее, $ab = p^{\alpha+\beta} \cdot c \cdot d$ и, согласно следствию 1.1 $p \nmid c \cdot d$. Таким образом, $ord_p(a \cdot b) = \alpha + \beta = ord_p(a) + ord_p(b)$. □

Замечание 1.1. В дальнейшем будем использовать следующие факты:

— $ord_q(-1) = 0$;

— $ord_q(p) = 0$, при $p \neq q$;

— $ord_q(q) = 1$.

Собирая вместе одинаковые простые числа, можно записать $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, где p_i - простые числа и a_i - неотрицательные целые числа. Будем использовать следующую запись:

$$n = (-1)^{\varepsilon(n)} \prod_p p^{\alpha(n)}, \tag{1.6}$$

где $\varepsilon(n) = 0$ или 1 в зависимости от того, будет n положительным или отрицательным, а произведение берётся по всем положительным простым числам. Показатели степени $\alpha(p)$ - неотрицательные целые числа и, конечно, $\alpha(p) = 0$ для всех простых чисел, кроме конечного их числа.

Теорема 1.3. Для любого ненулевого целого числа n имеется разложение на простые множители:

$$n = (-1)^{\varepsilon(n)} \prod_p p^{\alpha(n)},$$

с показателями степени, которые однозначно определяются числом n. На самом деле $\alpha(n) = ord_p(n)$.

Доказательство. Пусть $q \mid n$, и q - простое. Применим функцию ord_q к обеим частям равенства n и воспользуемся её свойством из предположения 1.2.

$$\begin{aligned}
&ord_q(n) = ord_q((-1)^{\varepsilon(n)} \prod_p p^{\alpha(n)}) = \\
&= \varepsilon(n) ord_q(-1) + \sum_{p|n} \alpha(n) ord_q(p) = \\
&= \alpha(n) ord_q(q) = \alpha(n).
\end{aligned}$$

То есть получили, что $\alpha(n) = ord_q(n)$. □

Определение 1.8. $\nu(n)$ - число делителей числа n:

$$\nu(n) = \sum_{d|n} 1 \tag{1.7}$$

$\sigma(n)$ - сумма делителей числа n:

$$\sigma(n) = \sum_{d|n} d \tag{1.8}$$

Замечание 1.2. $(\beta_1, \ldots, \beta_l)$ - кортеж, имеет следующее представление: $p_1^{\beta_1} \ldots p_l^{\beta_l}$.

Утверждение 1.3. Пусть n - целое положительное число с разложением

$\prod_{i=1}^{l} p_i^{\alpha_i}$ на простые множители. Тогда:

$$1)\ \nu(n) = \prod_{i=1}^{l} (\alpha_i + 1),$$
$$2)\ \sigma(n) = \prod_{i=1}^{l} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Доказательство. **Доказательство пункта 1):**

$m \mid n$ тогда и только тогда, когда кортеж $(\beta_1, \ldots, \beta_l)$ такой, что $0 \leqslant \beta_i \leqslant \alpha_i$ для $i \in \{\underline{1, l}\}$, а таких наборов в точности $(\alpha_1 + 1) \ldots (\alpha_l + 1)$.

Доказательство пункта 2):

Заметим, что $\sigma(n) = \sum p_1^{\beta_1} \ldots p_l^{\beta_l}$, где сумма берётся по упомянутым выше l-наборам. Таким образом,

$$\sigma(n) = \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1}\right)\left(\sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2}\right) \ldots \left(\sum_{\beta_l=0}^{\alpha_l} p_l^{\beta_l}\right),$$

откуда и следует доказываемый результат, если воспользоваться формулой суммирования для геометрической прогрессии. □

Определение 1.9. Функция Мёбиуса определяется для всех положительных чисел и задаётся следующим равенством:

$$\mu(a) = \begin{cases} 1, \text{ если } n = 1, \\ 0, \text{ если } d^2 \mid n, \text{ где } d > 1, \\ (-1)^l, \text{ если } n = p_1 \dots p_l \end{cases} \tag{1.9}$$

Утверждение 1.4. При $n > 1$ справедливо: $\sum\limits_{d|n} \mu(d) = 0$.

Доказательство. Если $n = p_1^{\alpha_1} \dots p_l^{\alpha_l}$, то

$$\sum_{d|n} \mu(d) = \sum_{(\varepsilon_1,\dots,\varepsilon_l)},$$

где ε_i есть 0 или 1. Таким образом,

$$\sum_{d|n} \mu(d) = 1 - l + \binom{l}{2} - \binom{l}{3} + \dots + (-1)^l = (1-1)^l = 0$$

□

2. Тема №2. Сравнения

3. Тема №3. Первообразные корни

4. Тема №4. Квадратичные вычеты

Часть II

Конечные поля

5. Конечные поля. Соответствие Галуа

6. Корни из единицы. Круговой многочлен

7. Норма и след. Характеры. Сумма Гаусса

8. Тригонометрические суммы. Уравнения над конечными полями

9. Дзета функции Артина, соотношение Хассе-Дэвенпорта

Часть III

p-адические числа

10. p-адические числа: элементарное определение и свойства

11. Аксиоматическое определение поля p-адических чисел, метризованные поля

12. Лемма Гензеля, сравнения и кольцо целых p-адических чисел

Часть IV

Числовые поля

13. Кольцо целых гауссовых чисел, числовые поля

14. Делимость в кольцах целых алгебраических чисел

15. Квадратичное поле и круговое поле

Часть V

Теорема Дирихле

16. Ряды Дирихле

17. Распределение простых чисел арифметической прогрессии

18. Домашние задания и упражнения

18.1. Упражнения

Упражнение 18.1. Доказать свойства делимости:

— $a \mid a,\ a \neq 0$;

— $a \mid b,\ b \mid a \Rightarrow a = \pm b$;

— $a \mid b,\ b \mid c \Rightarrow a \mid c$;

— $a \mid b,\ a \mid c \Rightarrow a \mid b\ \pm c$.

Упражнение 18.2. Алгоритм Евклида. Пусть $a, b \in \mathbb{Z} \setminus 0$, $a > b$, определим последовательность $b > r_1 > r_2 > \ldots > r_n$ следующим образом: $a = bq_0 + r_1$, $b = r_1q_1 + r_2$, $r_1 = r_2q_2 + r_3 \ldots$, $r_n = r_{n-1}q_{n-1} + r_n$. Доказать, что существует $n : r_{n-1} = r_nq_n$ и $r_n = (a, b)$.

Упражнение 18.3. Доказать, что $ord_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$

18.2. Домашние задания

Упражнение 18.4. Доказать, что $\sqrt{2}$ - иррациональное число, то есть не $\nexists$ рационального $r = \frac{a}{b}$ $(a, b\ \in \mathbb{Z})$ такого, что $r^2 = 2$.

Доказательство. Пусть $\sqrt{2}$ - рациональное число. Значит его можно представить в виде несократимой дроби: $\sqrt{2} = \frac{a}{b}$.

$$\sqrt{2} = \frac{a}{b} : \text{ возведём в квадрадт обе части равенства}$$
$$2 = \frac{a^2}{b^2} :$$
$$2 \cdot b^2 = a^2$$

Так как левая часть равенства кратна 2, то a - чётное число. Пусть $a = 2 \cdot k$. Тогда получим:

$$2 \cdot b^2 = (2 \cdot k)^2;$$
$$2 \cdot b^2 = 4 \cdot k^2;$$
$$b^2 = 2 \cdot k^2$$

Так как правая часть равенства кратна 2, то b - чётное число. То есть числа a, b - чётные (по вычислениям). Значит дробь $\frac{a}{b}$ не была несократимой. А значит противоречие (что $\sqrt{2}$ - рациональное число). □

Упражнение 18.5. Пусть $\alpha \in \mathbb{R}$, $b \in \mathbb{Z}_+$. Доказать, что $\left[\frac{[\alpha]}{b}\right] = \frac{\alpha}{b}$

Упражнение 18.6. Пусть $(a, b) = 1$. Доказать, что $(a + b, a - b) = 1$ или $= 2$.

Упражнение 18.7. Пусть $a, b, c, d \in \mathbb{Z}$. Доказать, что уравнение $ax + by = c$ разрешимо в целых числах $\Leftrightarrow d = (a, b) \mid c$. Доказать, что если

x_0, y_0 - решение этого уравнения, то все решения имеют вид:

$$x = x_0 + t \cdot \frac{b}{d}, y = y_0 - t \cdot \frac{b}{d} \text{ где } t \in \mathbb{Z}$$

Упражнение 18.8. Доказать свойства:

— $ord_p([a, b]) = \max(ord_p(a), ord_p(b))$;

— $ord_p(a + b) \geqslant \min(ord_p(a), ord_p(b))$, причём

$ord_p(a + b) = \min(ord_p(a), ord_p(b))$, если $ord_p(a) \neq ord_p(b)$;

— $(a, b)[a, b] = ab$;

— $(a + b, [a, b]) = (a, b)$.

Упражнение 18.9. Пусть $a, b, c, d \in \mathbb{Z}$, $(a, b) = 1$, $(c, d) = 1$. Доказать, что если $\frac{a}{b} + \frac{c}{d} \in \mathbb{Z}$, то $b = \pm d$.

Упражнение 18.10. Пусть $n \in \mathbb{Z}, n > 2$. Доказать, что числа:

$$\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n};$$
$$\frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1}$$

не являются целыми.

Упражнение 18.11. Пусть $f(n)$ - мультипликативная функция. Доказать, что функция

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

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

также мультипликативны.

Упражнение 18.12. Доказать, что для $\forall n \in \mathbb{Z}$:

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \nu(d) = 1$$

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d) = n$$

Упражнение 18.13. Доказать, что для $\forall m, n \in \mathbb{Z}$:

— $\varphi(n)\varphi(m) = \varphi((n,m))\varphi([n,m])$;

— $\varphi(mn)\varphi((m,n)) = (m,n)\varphi(m)\varphi(n)$.

Упражнение 18.14. Пусть $P, Q \in \mathbb{Z}_+$ - нечётные, $(P,Q) = 1$. Доказать, что

$$\sum_{0<x<\frac{Q}{2}} \left[\frac{P}{Q}x\right] + \sum_{0<y<\frac{P}{2}} \left[\frac{Q}{P}y\right] = \frac{P-1}{2}\frac{Q-1}{2}$$