ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное
учреждение высшего образования
“ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ ИМПЕРАТОРА АЛЕКСАНДРА I”

Кафедра «Высшая математика»

Е.А. Благовещенская

Конспект лекций

по дисциплине

«АЛГЕБРА И ГЕОМЕТРИЯ» (Б1.Б.13)

для специальности
10.05.03 «Информационная безопасность автоматизированных систем»

по специализации
«*Безопасность автоматизированных систем на железнодорожном транспорте*»

Форма обучения – очная

РАЗДЕЛ 2. ТЕОРИЯ ЧИСЕЛ

Санкт-Петербург

Лекция 2. Теория делимости в кольце целых чисел.
Лекция 3. Теория сравнений по модулю.
Лекция 4. Решение сравнений первой и второй степени.
Лекция 5. Основные числовые функции.
Лекция 6. Малая теорема Ферма, теорема Эйлера.
Лекция 7. Решение систем сравнений. Система RSA.

Лекция 2. Теория делимости в кольце целых чисел.

В теории чисел изучаются свойства целых чисел. Множество целых чисел $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ замкнуто относительно операций сложения, вычитания и умножения и, следовательно, образует кольцо.

Определение 1.1 *Число* a *делится на число* b, если существует $c \in \mathbb{Z}$ такое, что $a = b \cdot c$. Число b при этом называется *делителем числа* a (обозначается – $b \mid a$), а число a *– кратным числа* b (обозначается $a \vdots b$).

Ясно, что любое целое число a делится на $\pm a$, ± 1. Эти числа называются *тривиальными делителями* числа a. Остальные делители, если они есть, называются *нетривиальными делителями* числа a.

Основные свойства делимости:

1. Если два целых числа a и b делятся на целое число c, то их сумма и разность тоже делятся на c:
$a \vdots c,\ b \vdots c \Rightarrow a \pm b \vdots c$.

2. Если целое число a делится на целое число b и k – целое число, то $a \cdot k$ делится на b:
$a \vdots b,\ k \in \mathbb{Z} \Rightarrow a \cdot k \vdots b$.

3. Если целое число a делится на целое число b, а число b делится на целое число c, то число a делится на число c:
$a \vdots b,\ b \vdots c \Rightarrow a \vdots c.$

Теорема 1.1 *(о делении с остатком)***.** Пусть a, $b \in \mathbb{Z}$ и $b \neq 0$. Существуют целые числа q (неполное частное) и r (остаток) такие, что $a = b \cdot q + r$ и $0 \leq r \leq |b| - 1$. Эти требования однозначно определяют q и r.

Определение 1.2 *Наибольшим общим делителем* целых чисел a и b, отличных от нуля, называется наименьшее натуральное число k, являющееся кратным числа как a, тик и числа b.

Наибольший общий делитель чисел a и b обозначается $\text{НОД}(a, b)$ или просто (a, b).

Определение 1.3 *Наименьшим общим кратным* целых чисел a и b, из которых по крайне мере одно отлично от нуля, называется наибольшее натуральное число d, являющееся делителем как для a, так и для b.

Наименьшее общее кратное чисел a и b обозначается $\text{НОК}(a,b)$ или просто $[a,b]$.

Замечание. Для целых положительных чисел a и b справедливо:

$$a \cdot b = (a,b) \cdot [a,b].$$

Теорема 1.2 *(основные свойства* НОД*).* Пусть a, b – целые числа, одно из которых отлично от 0, и пусть d – их наибольший общий делитель. Тогда

1. существуют целые числа u и v такие, что $d = a \cdot u + b \cdot v$;
2. если d_1 – какой-либо общий делитель чисел a и b, то d делится на d_1.

Алгоритм Евклида.

Для нахождения наибольшего общего делителя применяется алгоритм Евклида.

Пусть a и b – положительные целые числа и $a > b$. Тогда

$$a = b \cdot q_1 + r_1, \qquad 0 < r_1 < b,$$
$$b = r_1 \cdot q_2 + r_2, \qquad 0 < r_2 < r_1,$$
$$r_1 = r_2 \cdot q_3 + r_3, \qquad 0 < r_3 < r_2,$$
$$\cdots\cdots\cdots\cdots \quad \cdots\cdots\cdots\cdots$$
$$r_{n-3} = r_{n-2} \cdot q_{n-1} + r_{n-1}, \qquad 0 < r_{n-1} < r_{n-2}$$
$$r_{n-2} = r_{n-1} \cdot q_n.$$

Этот ряд равенств заканчивается тогда, когда получаем некоторое $r_n = 0$. При этом $(a,b) = r_{n-1}$.

Определение 1.4 Два целых числа a и b называют *взаимно простыми,* если их наибольший общий делитель равен единице, т.е. $(a,b) = 1$.

Свойства взаимно простых чисел:

1. Для того чтобы целые числа a и b были взаимно простыми, необходимо и достаточно существование целых чисел u и v таких, что $a \cdot u + b \cdot v = 1$.

2. Если целые числа a_1, a_2 взаимно просты с целым числом b, то их произведение $a_1 \cdot a_2$ тоже взаимно просто с b.

3. Если целые числа $a_1,\ldots,a_n$ все взаимно просты с b, то произведение $a_1 \cdots a_n$ тоже взаимно просто с b.

4. Если целые числа $a_1,\ldots,a_n$ и $b_1,\ldots,b_m$ таковы, что каждое число a_i, $i = 1,\ldots,n$, взаимно просто с каждым числом b_j, $j = 1,\ldots,m$, то их произведения $a_1 \cdots a_n$ и $b_1 \cdots b_m$ взаимно просты.

5. Если числа a и b взаимно просты, то при натуральных k и l числа a^k и b^l взаимно просты.

6. Если произведение $a \cdot b$ двух целых чисел a и b делится на целое число c и число a взаимно просто с c, то b делится на c.

7. Если целое число a делится на целые взаимно простые числа b_1 и b_2, то a делится и на их произведение.

Определение 1.5 Целое положительное число, большее единицы, называется *простым*, если оно не имеет нетривиальных делителей.

Замечание. Число 1 не относится ни к простым, ни к составным числам.

Свойства простых чисел:

1. Любое целое число, большее 1, делится по крайне мере на одно простое число.

2. Каково бы ни было конечное множество простых чисел $\{p_1,\ldots,p_n\}$, всегда найдется простое число, не принадлежащее этому множеству.

3. Если целое число n не делится на простое число p, то n и p взаимно просты.

4. Если p_1 и p_1 – два различных простых числа, то они взаимно просты.

5. Если произведение двух целых чисел делится на простое число, то по крайне мере один из сомножителей делится на это простое число.

6. Если произведение нескольких целых чисел делится на простое число, то на него делится хотя бы один из сомножителей.

Теорема 1.3 *(основная теорема арифметики)*. Любое число, большее 1, может быть представлено в виде простых сомножителей и притом единственным образом (без учета порядка следования сомножителей).

Разложение числа a вида $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, где $p_1, p_2,\ldots, p_n$ – различные простые сомножители, $\alpha_1,\alpha_2,\ldots,\alpha_n$ – их кратности, называется к*аноническим разложением* числа a на сомножители.

Лекция 3. Теория сравнений по модулю.

Определение 5.1 Если два целых числа a и b при делении на целое положительное m имеет один и тот же остаток, то они называются *сравнимыми по модулю* m:

$$a \equiv b \pmod{m}.$$

Это равноостаточные числа: если $a = mq_1 + r, \quad b = mq_2 + r$, то $a \equiv b \pmod{m}$ *. Для того чтобы данные числа были сравнимы по данному модулю, необходимо и достаточно, чтобы их разность делилась на этот модуль.*

Основные свойства сравнений:

1. Любое целое число сравнимо с самим собой по любому модулю:
$a \equiv a \pmod{m}$ (рефлексивность).

2. Части сравнения можно менять местами:
$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ (симметричность).

3. Числа, сравнимые с одним и тем же числом, сравнимы между собой:

$a \equiv b \pmod m,\ b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$ (транзитивность).

4. Сравнения по одному и тому же модулю можно почленно складывать, вычитать и перемножать:

$a_1 \equiv b_1 \pmod m, a_2 \equiv b_2 \pmod m \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod m, a_1 a_2 \equiv b_1 b_2 \pmod m.$

5. К частям сравнений можно прибавлять (вычитать) одно и то же целое число:

$a \equiv b \pmod m \Rightarrow a \pm k \equiv b \pm k \pmod m.$

6. Части сравнения можно умножать на одно и то же целое число, возводить в одну и ту же натуральную степень:

$a \equiv b \pmod m \Rightarrow na \equiv nb \pmod m, a^n \equiv b^n \pmod m.$

7. К любой части сравнения можно прибавлять (вычитать) число, кратное модулю:

$a \equiv b \pmod m \Rightarrow a \equiv b \pm mk \pmod m.$

8. Части сравнения можно делить на их общий делитель, взаимно простой с модулем:

$ac \equiv bc \pmod m,\ (c,m) = 1 \Rightarrow a \equiv b \pmod m.$

9. Части сравнения и модуль можно делить (умножать) на одно и то же целое число:

$$a \equiv b \pmod m \Rightarrow ak \equiv bk \pmod{mk}, \frac{a}{k} \equiv \frac{b}{k} \left(\mod \frac{m}{k} \right).$$

10. Если числа сравнимы по данному модулю, то они сравнимы по модулю – делителю данного модуля:

$a \equiv b \pmod{mk} \Rightarrow a \equiv b \pmod m.$

11. Если числа сравнимы по нескольким модулям, то они сравнимы по модулю – наименьшему общему кратному данных модулей:

$a \equiv b \pmod{m_1},\ a \equiv b \pmod{m_2} \Rightarrow a \equiv b \pmod{[m_1, m_2]}.$

12. Значения многочленов от сравнимых между собой чисел сравнимы между собой:

$a \equiv b \pmod m, P(x) - \text{многочлен} \Rightarrow P(a) \equiv P(b) \pmod m.$

13. Любое целое число сравнимо с одним из следующих чисел $1, 2, \ldots, m-1$ по модулю m, причем сами эти числа между собой попарно не сравнимы.

Лекция 4. Решение сравнений первой и второй степени.

Сравнение вида $f(x) \equiv 0 \pmod m$, где $f(x)$ – многочлен, называются *сравнениями с неизвестной величиной* x. Под решением сравнения понимаются все вычеты из полной системы вычетов, которые удовлетворяют этому уравнению.

Сравнение первой степени с одним неизвестным имеет вид:

$$ax \equiv b \pmod m. \qquad \textbf{(5)}$$

Теорема 6.1. Пусть $(a,m) = d$. Тогда сравнение (5) не имеет решений, если b не делится на d. Если b делится на d, то сравнение имеет ровно d решений:

$x \equiv x_0,\ x_0 + \frac{m}{d},\ x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d} \left(\mathrm{mod}\ \frac{m}{d} \right)$, где x_0 – значение x, удовлетворяющее сравнению: $\frac{a}{d} x \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d} \right)$.

Замечание. Если $(a,m) = 1$, то сравнение (5) имеет единственное решение, которое может быть найдено:

1. по формуле $x \equiv a^{\varphi(m)-1} b \ (\mathrm{mod}\ m)$;
2. умножением сравнения на обратный элемент a^{-1};
3. с помощью непрерывных дробей по формуле $x \equiv (-1)^{S-1} b P_{S-1} \ (\mathrm{mod}\ m)$, где P_{S-1} – числитель $(S-1)$-й подходящей дроби.

Лекция 5. Основные числовые функции.

Определение 2.1 *Функцией Эйлера* $\varphi(m)$ числа m, называется число положительных чисел, меньших m и взаимно простых с m.

Теорема 2.1 1. Если $(a,b) = 1$, то $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$;

2. Если $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, то $\varphi(m) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1} \right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1} \right)$.

Замечание. Иногда удобно функцию Эйлера считать по формуле:

$$\varphi(m) = m \left(1 - \frac{1}{p_1} \right) \cdots \left(1 - \frac{1}{p_k} \right).$$

Определение 2.2 *Функцией Мебиуса* $\mu(m)$ называется мультипликативная функция, определяемая равенством:

$$\mu\left(p^{\alpha} \right) = \begin{cases} -1, & \text{если } \alpha = 1; \\ 0, & \text{если } \alpha > 1; \\ 1, & \text{если } p = 1. \end{cases}$$

Определение 2.3 Обозначим через $\tau(a)$ *число положительных делителей числа* a.

Теорема 2.2 1. Если $(a,b) = 1$, то $\tau(a \cdot b) = \tau(a) \cdot \tau(b)$;

2. Если $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, то $\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$.

Определение 2.4 Обозначим через $\sigma(a)$ *сумму положительных делителей числа* a.

Теорема 2.3 1. Если $(a,b) = 1$, то $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$;

2. Если $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, то $\sigma(a) = \frac{p_1^{\alpha_1 + 1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2 + 1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k + 1} - 1}{p_k - 1}$.

Лекция 6. Малая теорема Ферма, теорема Эйлера.

Определение 5.2 Объединение всех чисел, сравнимых между собой по модулю m, называется *классом вычетов по модулю* m. Числа из этого класса называются *вычетами.*

Замечания: 1. Числа, входящие в один класс вычетов образуют арифметическую прогрессию с разностью m.

2. В качестве типичного представителя класса вычетов выбирается наименьший положительный элемент.
3. Существует ровно m классов вычетов по модулю m.
4. Множество классов вычетов по модулю m образует кольцо, т.е. оно замкнуто относительно операций сложения, вычитания и умножения.
5. Кольцо вычетов по модулю m обозначается через $\mathbb{Z}_m$.

Теорема 5.1 *(об обратимости в* $\mathbb{Z}_m$*).* Элемент $a \in \mathbb{Z}_m$ имеет обратный тогда и только тогда, когда $(a,m)=1.$

Следствие. Если m – простое число, то $\mathbb{Z}_m$ является полем.

Определение 5.3 Набор чисел, взятых по одному из каждого класса вычетов по модулю m, называется *полной системой вычетов по модулю* m.

Определение 5.4 *Приведенной системой вычетов* называется набор чисел, взятых по одному из каждого класса, представители которого взаимно просты с модулем.

Замечание. Число элементов в полной системе вычетов равно модулю m, а в приведенной равно $\varphi(m)$.

Теорема 5.2 *(теорема Ферма)***.** Если p – простое число и a не делится на p, то $a^{p-1} \equiv 1 (\mathrm{mod}\ p).$

Теорема 5.3 *(теорема Эйлера)***.** При $m>1$ и $(a,m)=1$ справедливо:

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

Лекция 7. Решение систем сравнений. Система RSA.

Система сравнений первой степени с одним неизвестным в общем виде выглядит следующим образом:

$$\begin{cases} a_1 x \equiv b_1 \ (\mathrm{mod}\ n_1), \\ \quad \ldots\ldots\ldots\ldots \\ a_k x \equiv b_k \ (\mathrm{mod}\ n_k). \end{cases} \qquad \textbf{(6)}$$

Если каждое сравнение системы (6) разрешимо, то она может быть приведена к простейшему виду:

$$\begin{cases} x \equiv c_1 \ (\mathrm{mod}\ m_1), \\ \quad \ldots\ldots\ldots\ldots \\ x \equiv c_t \ (\mathrm{mod}\ m_t). \end{cases} \qquad \textbf{(7)}$$

Теорема 7.1 Если модули m_1 и m_2 взаимно просты, то система сравнений $\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \end{cases}$, имеет решение при любых правых частях.

Теорема 7.2 Пусть $(m_1, m_2) = d$, $[m_1, m_2] = k$. Тогда, если $c_2 - c_1$ не делится на d, то система сравнений $\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \end{cases}$ не имеет решений, а если делится на d, то она имеет одно решение, определяющее класс чисел по модулю k.

Непрерывные дроби.

Определение 3.1 *Бесконечной цепной,* или *непрерывной, дробью* называется выражение:

$$q_1 + \cfrac{b_1}{q_2 + \cfrac{b_2}{q_3 + \cfrac{b_3}{q_4 + \ldots}}}, \qquad \textbf{(1)}$$

где $b_1, b_2, \ldots, q_1, q_2, \ldots \in \square$.

Будем рассматривать дроби (1) при $b_i = 1 \, (i = 1, 2, \ldots)$ и введем обозначение для таких дробей:

$$q_1 \dot{+} \frac{1}{q_2} \dot{+} \frac{1}{q_3} \dot{+} \ldots \dot{+} \frac{1}{q_n} \dot{+} \ldots = (q_1, q_2, \ldots, q_n, \ldots). \qquad \textbf{(2)}$$

Различают конечные и бесконечные непрерывные дроби. Любое вещественное число α представимо в виде непрерывной дроби. Если α – иррациональное число, то непрерывная дробь бесконечна, если же рациональное число, то дробь – конечна. Для разложения рациональной несократимой дроби $\alpha = a/b$ в непрерывную дробь используют алгоритм Евклида.

Алгоритм Евклида для разложения рационального числа.

Конечная дробь

$$\frac{P_n}{Q_n} = q_1 \dot{+} \frac{1}{q_2} \dot{+} \ldots \dot{+} \frac{1}{q_n}$$

называется *n-й подходящей дробью* для бесконечной непрерывной дроби (2). Числитель и знаменатель подходящих дробей можно вычислять по формулам:

$$P_s = q_s \cdot P_{s-1} + P_{s-2}, \quad P_0 = 1, \quad P_1 = q_1,$$

$$Q_s = q_s \cdot Q_{s-1} + Q_{s-2}, \quad Q_0 = 0, \quad Q_1 = 1.$$

Иногда удобно составлять таблицу:

q_s		q_1	q_2	…	q_{s-1}	q_s	…	q_{n-1}	q_n
P_s	1	q_1	P_2	…	P_{s-1}	P_s	…	P_{n-1}	a
Q_s	0	1	Q_2	…	Q_{s-1}	Q_s	…	Q_{n-1}	b

Свойства непрерывных дробей:

1. $P_k \cdot Q_{k-1} - Q_k \cdot P_{k-1} = (-1)^{k-1}, \quad k = 1, 2, \ldots$

2. $(P_k, Q_k) = 1.$

3. С возрастанием порядка подходящие дроби четного порядка возрастают, а нечетного – убывают, причем каждая подходящая дробь четного порядка меньше любой подходящей дроби нечетного порядка.

4. Каждая бесконечная дробь (2) сворачивается в иррациональное число α такое, что

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \ldots < \alpha < \ldots < \frac{P_5}{Q_5} < \frac{P_3}{Q_3} < \frac{P_1}{Q_1},$$

$$\alpha = \lim_{k \to \infty} \frac{P_k}{Q_k}.$$

5. Подходящая дробь $\frac{P_k}{Q_k}$ является наилучшим рациональным приближением действительного числа α. Дробь $\frac{P_k}{Q_k}$ является приближением α с точностью до $\frac{1}{Q_k Q_{k+1}}$.

Замечание. Для того чтобы с помощью подходящих дробей найти приближение с заданной точностью ε, достаточно, чтобы $Q_k > \sqrt{\frac{1}{\varepsilon}}$.

Из неопределенных уравнений второй степени особенно важную роль играют уравнения Ферма вида:

$$x^2 - ay^2 = 1. \qquad \textbf{(3)}$$

Такие уравнения при каждом целом положительном a, отличном от квадрата, имеют бесконечно много решений в целых числах. Решения получаются с помощью непрерывных дробей. Раскладывают $\sqrt{a}$ в непрерывную дробь. Если k – длина периода разложения $\sqrt{a}$ в непрерывную дробь, то все решения уравнения (3) в целых положительных числах будут:

$$x = P_{(k+1)n-1}, \quad y = Q_{(k+1)n-1}, \tag{4}$$

где n – любое натуральное число такое, что $k \cdot n$ – четно, P_i, Q_i – числитель и знаменатель i-й подходящей дроби соответственно.

Библиографический список

1. *В.И. Смирнов.* Курс высшей математики, т.1. – ОГИЗ ГОСТЕХИЗДАТ, 1948.

2. *Прасолов В.В.* Многочлены. – М.: МЦНМО, 2003.

3. *Фаддеев Д.К., Соминский И.С.* Сборник задач по высшей алгебре. – Москва: Наука, 1977.