

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Кафедра «Высшая математика»

Е.В. Рунёв

**Методические указания
по выполнению практических заданий
по дисциплине
«АЛГЕБРА И ГЕОМЕТРИЯ» (Б1.Б.24)**

для специальности
10.05.03 «Информационная безопасность автоматизированных систем»

по специализации
«Информационная безопасность автоматизированных систем на
транспорте»

Форма обучения – очная

РАЗДЕЛ 5. ТЕОРИЯ ЧИСЕЛ

Санкт-Петербург 2020

ТЕМА 1.

Деление с остатком.
Наибольший общий делитель (НОД).
Наименьшее общее кратное (НОК).
Линейное представление НОД.
Алгоритм Евклида.
Расширенный алгоритм Евклида.
Критерий взаимной простоты.

ПРИМЕРЫ

1. Найти $(6188, 4709)$ и $[6188, 4709]$.

Решение. Воспользуемся алгоритмом Евклида для нахождения $(6188, 4709)$.

$$6188 = 4709 \cdot 1 + 1479,$$

$$4709 = 1479 \cdot 3 + 272,$$

$$1479 = 272 \cdot 5 + 119,$$

$$272 = 119 \cdot 2 + 34,$$

$$119 = 34 \cdot 3 + 17,$$

$$34 = 17 \cdot 2.$$

Таким образом, $(6188, 4709) = 17$. Для нахождения $[6188, 4709]$ воспользуемся равенством: $a \cdot b = (a, b) \cdot [a, b]$. Следовательно,

$$[6188, 4709] = \frac{6188 \cdot 4709}{(6188, 4709)} = \frac{21939292}{17} = 1714076.$$

Ответ: $(6188, 4709) = 17$, $[6188, 4709] = 1714076$.

2. Решить систему уравнений, если $x, y \in \mathbb{Z}$:

$$\begin{cases} x + y = 150, \\ (x, y) = 30. \end{cases}$$

Решение. Заметим, что равенство $(x, y) = 30$ равносильно системе:

$$\begin{cases} x = 30 \cdot u, \\ y = 30 \cdot v, \\ (u, v) = 1. \end{cases}$$

Подставляя выражения для x и y в первое уравнение исходной системы, получаем: $u + v = 5$. Отсюда находим $u = 1, 2, 3, 4$ и $x = 30, 60, 90, 120$. Соответствующие значения для y находятся по формуле $y = 150 - x$.

Ответ: $\begin{cases} x_1 = 30 \\ y_1 = 120 \end{cases}; \begin{cases} x_2 = 60 \\ y_2 = 90 \end{cases}; \begin{cases} x_3 = 90 \\ y_3 = 60 \end{cases}; \begin{cases} x_4 = 120 \\ y_4 = 30 \end{cases}.$

3. Решить уравнение: $7x + 13y = 2$, если $x, y \in \mathbb{Z}$.

Решение. Заметим, что $(7, 13) = 1$. Согласно теореме об основных свойствах НОД, существуют целые числа u и v такие, что $7 \cdot u + 13 \cdot v = 1$. Найдем эти числа:

$$\begin{aligned} 13 &= 7 \cdot 1 + 6, \\ 7 &= 6 \cdot 1 + 1. \end{aligned} \Rightarrow \underline{1} = 7 - 6 \cdot 1 = 7 - (13 - 7 \cdot 1) \cdot 1 = \underline{7 \cdot 2 + 13 \cdot (-1)}.$$

Следовательно, $u = 2, v = -1$. Умножим равенство $7 \cdot u + 13 \cdot v = 1$ на 2. Получим: $7 \cdot (2 \cdot u) + 13 \cdot (2 \cdot v) = 2$. Отсюда следует, что $x_0 = 2 \cdot u = 4$, $y_0 = 2 \cdot v = -2$ являются частными решениями исходного уравнения.

Составим систему:

$$\begin{cases} 7x + 13y = 2, \\ 7x_0 + 13y_0 = 2. \end{cases}$$

Вычитая из первого уравнения второе, получаем:

$$(*) \quad 7(x - x_0) = -13(y - y_0).$$

Поскольку правая часть уравнения $(*)$ делится на 13, то левая часть тоже должна делиться на 13, следовательно:

$$x - x_0 = 13 \cdot k, \text{ где } k \in \mathbb{Z}.$$

Поскольку левая часть $(*)$ делится на 7, то правая часть тоже должна делиться на 7, следовательно:

$$y - y_0 = 7 \cdot l, \text{ где } l \in \mathbb{Z}.$$

Подставляем полученные выражения в $(*)$:

$$7 \cdot 13 \cdot k = -13 \cdot 7 \cdot l \Rightarrow l = -k.$$

Следовательно, $x = x_0 + 13 \cdot k = 4 + 13 \cdot k$, $y = y_0 - 7 \cdot k = -2 - 7 \cdot k$, $k \in \mathbb{Z}$.

Ответ: $x = 4 + 13 \cdot k$, $y = -2 - 7 \cdot k$, $k \in \mathbb{Z}$.

Замечание. Уравнения вида $ax + by = c$, где $a, b, x, y \in \mathbb{Z}$ называются *диофантовыми* уравнениями.

ТЕМА 2.

Сравнение по модулю. Свойства сравнений.

Множество классов вычетов по модулю.

Обратимость в $\mathbb{Z}_m$.

Малая теорема Ферма.

Теорема Эйлера.

Сравнения с одним неизвестным.

Системы сравнений с одним неизвестным.

Китайская теорема об остатках.

Основные функции теории чисел: функция Эйлера, функция Мёбиуса, функция количества положительных делителей, функция суммы положительных делителей числа – свойства и вычисление.

ПРИМЕРЫ

1. Найти остаток от деления 171^{2147} на 52.

Решение. Заметим, что $(171, 52) = 1$. Вычислим $\varphi(52) = 24$. Тогда остаток от деления x :

$$x \equiv 171^{2147} \equiv 15^{24 \cdot 89 + 11} \equiv 15^{11} = (15^3)^3 \cdot 15^2 = (3375)^3 \cdot 225 \equiv (47)^3 \cdot 17 \equiv (-5)^3 \cdot 17 \equiv -21 \cdot 17 \equiv 7 \pmod{52}.$$

Ответ: остаток равен 7.

2. Найти остаток от деления 676^{221} на 28.

Решение. Заметим, что $(676, 28) = 4$. Если $x \equiv 676^{221} \pmod{28}$, то $x = 4x_1$, $x_1 \equiv 169 \cdot 676^{220} \equiv 169 \cdot 676^{36 \cdot 6 + 4} \equiv 169 \cdot 676^4 \equiv 676^4 \equiv 4^4 \equiv 4 \pmod{7}$, и тогда $x \equiv 16 \pmod{28}$.

Ответ: остаток равен 16.

3. Доказать, что $1 + 3^x + 9^x$ делится на 13, если $x = 3n + 1$, $n = 0, 1, 2, \dots$

Решение. Покажем, что $1 + 3^x + 9^x \equiv 0 \pmod{13}$, если $x = 3n + 1$, $n = 0, 1, 2, \dots$

$$1 + 3^{3n+1} + 9^{3n+1} \equiv 1 + 3 \cdot 27^n + 9 \cdot (-4)^{3n} \equiv 1 + 3 + 9 \cdot (-64)^n \equiv 4 + 9 \cdot 1^n = 13 \equiv 0 \pmod{13}.$$

4. На какую цифру заканчивается число 333^{777} ?

Решение. Решим сравнение $x \equiv 333^{777} \pmod{10}$.

$$x \equiv 333^{777} \equiv 3^{777} = 3 \cdot 3^{2 \cdot 388} = 3 \cdot 9^{388} \equiv 3 \cdot (-1)^{388} = 3 \pmod{10}.$$

Ответ: последняя цифра 3.

ПРИМЕРЫ

1. Решить сравнение $5x \equiv 4 \pmod{13}$.

Решение. Так как $(5, 13) = 1$, то сравнение имеет единственное решение.

Найдем его по формуле $x \equiv a^{\varphi(m)-1} b \pmod{m}$. Вычислим $\varphi(13) = 12$. Тогда $x \equiv 5^{12-1} \cdot 4 = 5^{11} \cdot 4 = 5 \cdot 4 \cdot 25^5 \equiv 7 \cdot (-1)^5 = -7 \equiv 6 \pmod{13}$.

Ответ: $x \equiv 6 \pmod{13}$.

2. Решить сравнение $6x \equiv 7 \pmod{17}$.

Решение. Заметим, что $(6, 17) = 1$, следовательно сравнение имеет единственное решение. Найдем обратный элемент к 6.

$$17u + 6v = 1 \Rightarrow u_0 = -1, v_0 = 3, \text{ следовательно } a^{-1} = 3. \text{ Умножаем сравнение: } 3 \cdot 6x \equiv 3 \cdot 7 \pmod{17}, x \equiv 21 \equiv 4 \pmod{17}.$$

Ответ: $x \equiv 4 \pmod{17}$.

3. Решить сравнение $93x \equiv 42 \pmod{15}$.

Решение. Так как $(93, 15) = 3$ и 42 делится на 3, то сравнение имеет три решения. Делим обе части сравнения и модуль на 3. Получаем сравнение

$31x \equiv 14 \pmod{5}$. Решим это сравнение $x \equiv 31^4 \cdot 14 \equiv 1^3 \cdot (-1) \equiv -1 \equiv 4 \pmod{5}$.

Следовательно решениями будут:

$$x \equiv 4 \pmod{15};$$

$$x \equiv 4 + 5 \pmod{15} \equiv 9 \pmod{15};$$

$$x \equiv 4 + 5 \cdot 2 \pmod{15} \equiv 14 \pmod{15}.$$

Ответ: $x \equiv 4 \pmod{15}$; $x \equiv 9 \pmod{15}$; $x \equiv 14 \pmod{15}$.

4. Решить сравнение $55x \equiv 7 \pmod{87}$.

Решение. Так как $(55, 87) = 1$, то сравнение имеет единственное решение.

Решение найдем по формуле $x \equiv (-1)^{s-1} b P_{s-1} \pmod{m}$.

Разложим $\frac{87}{55}$ в непрерывную дробь:

$$\begin{aligned} \frac{87}{55} &= 1 + \frac{32}{55} = 1 + \frac{1}{\frac{55}{32}} = 1 + \frac{1}{1 + \frac{23}{32}} = 1 + \frac{1}{1 + \frac{1}{\frac{32}{23}}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{9}{23}}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{23}{9}}}} = \\ &= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{5}{9}}}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{\frac{9}{5}}}}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{4}{5}}}}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{4}}}}}} \end{aligned}$$

q_s		1	1	1	2	1	1	4
P_s	1	1	2	3	8	11	19	87

Поэтому

$$x \equiv (-1)^6 \cdot 7 \cdot P_6 \pmod{87} \equiv 133 \pmod{87} \equiv 46 \pmod{87}.$$

Ответ: $x \equiv 46 \pmod{87}$.

ПРИМЕРЫ

1. Решить систему сравнений $\begin{cases} x \equiv 5 \pmod{13} \\ x \equiv 3 \pmod{7} \end{cases}$.

Решение. Так как $(13, 7) = 1$, то система сравнений имеет решение. Из первого сравнения имеем $x = 13 \cdot t + 5$. Поскольку этот x должен удовлетворять и второму сравнению, то $x = 13 \cdot t + 5 \equiv 3 \pmod{7}$. Таким образом, для t получили сравнение $13 \cdot t \equiv -2 \pmod{7}$. Находим решение для t : $t \equiv 13^5 \cdot (-2) \equiv (-1)^5 \cdot (-2) = 2 \pmod{7}$, т.е. $t = 7 \cdot l + 2$. Подставляем значение t в выражение для x : $x = 13 \cdot (7 \cdot l + 2) + 5 = 91 \cdot l + 31$ или $x \equiv 31 \pmod{91}$.

Ответ: $x \equiv 31 \pmod{91}$.

2. Решить систему сравнений
$$\begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 5 \pmod{9} \\ x \equiv 11 \pmod{11} \end{cases}$$

Решение. Сначала решим систему, состоящую из первых двух сравнений. Так как $(7, 9) = 1$, то система совместна. Имеем: $x = 9 \cdot t + 5 \equiv 2 \pmod{7}$, $2 \cdot t \equiv 3 \pmod{7}$, $t \equiv 2 \pmod{7}$, $t = 7 \cdot l + 2$, $x = 9 \cdot (7 \cdot l + 2) + 5 \equiv 23 \pmod{63}$. Таким образом, первоначальная система эквивалентна системе:

$$\begin{cases} x \equiv 23 \pmod{63} \\ x \equiv 11 \pmod{15} \end{cases}$$

В этой системе $(63, 15) = 3$ и $23 - 11 = 12$ делится на 3, следовательно, система совместна.

$$x = 63 \cdot l + 23 \equiv 11 \pmod{15}, \quad 3 \cdot l \equiv 3 \pmod{15}, \quad l \equiv 1 \pmod{5}, \quad y = 5 \cdot m + 1, \\ y = 5 \cdot m + 1, \quad x = 63 \cdot (5 \cdot m + 1) + 23 = 315 \cdot m + 86, \quad x \equiv 86 \pmod{315}.$$

Ответ: $x \equiv 86 \pmod{315}$.

ТЕМА 3.

Непрерывные дроби.

Алгоритм Евклида представления несократимой дроби в виде непрерывной дроби.

Запись иррационального числа в виде непрерывной дроби.

n — я подходящая дробь.

Уравнение Эйлера второй степени.

ПРИМЕРЫ

1. Разложить в цепную дробь обыкновенную дробь $\frac{37}{79}$.

Решение.

$$\frac{37}{79} = \frac{1}{\frac{79}{37}} = \frac{1}{2 + \frac{5}{37}} = \frac{1}{2 + \frac{1}{\frac{37}{5}}} = \frac{1}{2 + \frac{1}{7 + \frac{2}{5}}} = \frac{1}{2 + \frac{1}{7 + \frac{1}{\frac{5}{2}}}} = \frac{1}{2 + \frac{1}{7 + \frac{1}{2 + \frac{1}{2}}}}.$$

Получили конечную цепную дробь.

Ответ:
$$\frac{1}{2 + \frac{1}{7 + \frac{1}{2 + \frac{1}{2}}}}$$

2. Разложить в непрерывную дробь иррациональное число $\sqrt{5}$.

Решение.

$$\alpha = \sqrt{5} = [\sqrt{5}] + \frac{1}{\alpha_1} = 2 + \frac{1}{\alpha_1},$$

$$\alpha_1 = \frac{1}{\sqrt{5} - 2} = \frac{\sqrt{5} + 2}{1} = 4 + \frac{1}{\alpha_2},$$

$$\alpha_2 = \frac{1}{\sqrt{5} + 2 - 4} = \sqrt{5} + 2 = 4 + \frac{1}{\alpha_3},$$

но $\alpha_3 = \alpha_2 = \alpha_1$ и т.д. Тогда

$$\alpha = \sqrt{5} = 2 + \frac{1}{4 + \frac{1}{4 + \dots}}$$

Ответ:
$$2 + \frac{1}{4 + \frac{1}{4 + \dots}}$$

3. Найти наилучшее приближение с точностью до 0,001 числа $\alpha = \sqrt{2}$.

Решение. Разложим $\sqrt{2}$ в непрерывную дробь:

$$\alpha = \sqrt{2} = [\sqrt{2}] + \frac{1}{\alpha_1} = 1 + \frac{1}{\alpha_1},$$

$$\alpha_1 = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2} + 1}{1} = 2 + \frac{1}{\alpha_2},$$

$$\alpha_2 = \frac{1}{\sqrt{2} - 1} = \alpha_1.$$

Таким образом,

$$\alpha = \sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \dots}}$$

q_s		1	2	2	2	2	2
P_s	1	1	3	7	17	41	99
Q_s	0	1	2	5	12	29	70

Условию $Q_n > \sqrt{\frac{1}{0,001}} = 31, \dots$ удовлетворяет $\frac{P_6}{Q_6} = \frac{99}{70}$ и $\sqrt{2} \approx \frac{99}{70} (+0,001)$. Но

$\sqrt{2} - \frac{P_5}{Q_5} < \frac{1}{29 \cdot 70} < 0,001$. Поэтому наилучшее приближение $\sqrt{2}$ с точностью

до 0,001 является $\frac{P_5}{Q_5} = \frac{41}{29}$. Проверим $\frac{P_4}{Q_4}$. Имеем $\frac{P_4}{Q_4} - \sqrt{2} > 0,001$.

Ответ: Наилучшее приближение $\frac{41}{29}$.

ПРИМЕР

Найти наименьшие целые положительные значения x и y , удовлетворяющие уравнению $x^2 - 22y^2 = 1$.

Решение. Разложим $\sqrt{22}$ в непрерывную дробь.

$$\sqrt{22} = 4 + \frac{1}{\alpha_1},$$

$$\alpha_1 = \frac{1}{\sqrt{22} - 4} = \frac{\sqrt{22} + 4}{6} = 1 + \frac{1}{\alpha_2},$$

$$\alpha_2 = \frac{1}{\alpha_1 - 1} = \frac{6}{\sqrt{22} - 2} = \frac{\sqrt{22} + 2}{3} = 2 + \frac{1}{\alpha_3},$$

$$\alpha_3 = \frac{1}{\alpha_2 - 2} = \frac{3}{\sqrt{22} - 4} = \frac{\sqrt{22} + 4}{2} = 4 + \frac{1}{\alpha_4},$$

$$\alpha_4 = \frac{1}{\alpha_3 - 4} = \frac{2}{\sqrt{22} - 4} = \frac{\sqrt{22} + 4}{3} = 2 + \frac{1}{\alpha_5},$$

$$\alpha_5 = \frac{1}{\alpha_4 - 2} = \frac{3}{\sqrt{22} - 2} = \frac{\sqrt{22} + 2}{6} = 1 + \frac{1}{\alpha_6},$$

$$\alpha_6 = \frac{1}{\alpha_5 - 1} = \frac{6}{\sqrt{22} - 4} = \sqrt{22} + 4 = 8 + \frac{1}{\alpha_7},$$

$$\alpha_7 = \frac{1}{\alpha_6 - 8} = \frac{1}{\sqrt{22} - 4} = \frac{\sqrt{22} + 4}{6} = \alpha_1.$$

То есть,

$$\sqrt{22} = 4 + \frac{1}{1 + \frac{1}{2 + \frac{1}{4 + \frac{1}{2 + \frac{1}{1 + \frac{1}{8 + \frac{1}{1 + \dots}}}}}}}$$

Период насчитывает 6 членов. Обозначим через k – длину периода: $k = 6$. Тогда $x_0 = P_6$, $y_0 = Q_6$ будут наименьшими значениями x и y , так как в формуле (4) требуется, чтобы $k \cdot n$ было четным. Здесь $k = 6$, значит, в качестве n можно взять 1. Найдём P_6 , Q_6 . Составим таблицу подходящих дробей.

q_s		4	1	2	4	2	1
P_s	1	4	5	14	61	135	197
Q_s	0	1	1	3	13	29	42

Таким образом, $P_6 = 197$, $Q_6 = 42$.

Ответ: $x_0 = 197$, $y_0 = 42$.