

Министерство образования и науки Российской Федерации

Ярославский государственный университет
им. П. Г. Демидова

Кафедра алгебры и математической логики

С. И. Яблокова

Задачи по алгебраической алгоритмике

Практикум

Ярославль

ЯрГУ

2016

УДК 512+519.6
ББК В14я73+В18я73
Я82

*Рекомендовано
Редакционно-издательским советом университета
в качестве учебного издания. План 2016 года*

Рецензент

кафедра алгебры и математической логики ЯрГУ

Светлана Ивановна Яблокова

Я82 Задачи по алгебраической алгоритмике : практикум /
С. И. Яблокова ; Яросл. гос. ун-т им. П. Г. Демидова. –
Ярославль : ЯрГУ, 2016. – 76 с.

Содержит задачи по алгебраической алгоритмике и основные формулы, используемые при решении этих задач. Практикум снабжен указаниями и примерами с подробным разбором методов решения.

УДК 512+519.6
ББК В14я73+В18я73

© ЯрГУ, 2016

В практикуме содержатся задачи по алгебраической алгоритмике по темам, изучаемым в четвертом семестре студентами специальности "Компьютерная безопасность" в курсе "Алгебраическая алгоритмика." Для решения предлагаемых задач требуется знать основные алгебраические и числовые алгоритмы и связанные с ними определения и понятия курса, такие как алгоритм Евклида для нахождения наибольшего общего делителя целых чисел; расширенный алгоритм Евклида для чисел; понятие диофантова уравнения и метод его решения; определение и свойства непрерывных дробей; определение и свойства сравнений по натуральному модулю, методы решения сравнений; китайская теорема об остатках для чисел; определение и свойства кольца целых гауссовых чисел; основные утверждения и понятия теории чисел; основные сведения о группах, в частности о мультипликативных группах колец вычетов; основы модульной арифметики. Требуется умение применять эти знания для решения задач. Наибольшие трудности, как правило, представляют задания, связанные со строением колец вычетов и мультипликативных групп колец вычетов, а также с вычислениями в кольце целых гауссовых чисел. Обычно это вычислительные проблемы, хотя особое внимание надо уделить пониманию того, что такое кольцо вычетов по данному модулю, что представляют из себя элементы этого кольца.

Практикум начинается с напоминания основных понятий, формул и алгоритмов, используемых при решении задач. Эти понятия и алгоритмы иллюстрируются примерами. Далее предлагаются задачи по курсу для решения на практических занятиях. Они снабжены указаниями и ответами для контроля правильности решения. В заключение предлагаются задачи для самостоятельного решения, которые могут быть использованы для контрольных и расчетно-графических работ.

ОСНОВНЫЕ ФОРМУЛЫ И АЛГОРИТМЫ

Наибольший общий делитель и алгоритмы его нахождения

Определение 1. Число $d > 0$ называется наибольшим общим делителем (НОД) двух целых чисел a и b , если оно удовлетворяет следующим условиям:

- 1) $d \mid a$ и $d \mid b$;
- 2) если $c \mid a$ и $c \mid b$, то $c \mid d$.

Наибольший общий делитель двух чисел a и b , $a \geq b > 0$, можно найти с помощью *алгоритма Евклида*, который основан на том, что если

$$a = bq + r, \quad 0 \leq r < b,$$

то $\text{НОД}(a, b) = \text{НОД}(r, b)$.

Алгоритм Евклида состоит из следующих шагов вычисления $(r_0 = a, r_1 = b)$:

$$r_{i-1} = r_i q_i + r_{i+1}, \quad 0 < r_{i+1} < r_i, \quad (i = 1, 2, \dots).$$

Если $r_{n+1} = 0$ – первый нулевой остаток, то $\text{НОД}(a, b) = r_n$.

Еще один способ нахождения наибольшего общего делителя двух чисел: найти каноническое разложение этих чисел на простые множители. Пусть

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}, & \alpha_i &\geq 0, & (i = 1, \dots, s), \\ b &= p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}, & \beta_i &\geq 0, & (i = 1, \dots, s), \end{aligned}$$

где p_1, p_2, \dots, p_s – попарно различные простые целые числа. Тогда

$$\text{НОД}(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_s^{\gamma_s},$$

где $\gamma_i = \min\{\alpha_i, \beta_i\}$ ($i = 1, 2, \dots, s$).

Можно также искать наибольший общий делитель двух чисел с помощью бинарного алгоритма, который основан на следующих свойствах наибольшего общего делителя:

- 1) $\text{НОД}(2n, 2m) = 2\text{НОД}(n, m)$;
- 2) $\text{НОД}(2n + 1, 2m) = \text{НОД}(2n + 1, m)$;
- 3) $\text{НОД}(n, m) = \text{НОД}(n - m, m)$ ($n \geq m$);
- 4) $\text{НОД}(n, m) = \text{НОД}(m, n)$;
- 5) $\text{НОД}(n, 0) = n$.

С учетом этих свойств получаем следующий алгоритм:

1. Если $2^k \mid a$ и $2^k \mid b$, а 2^{k+1} не делит одно из этих чисел, то запомнить $d_0 = 2^k$ и положить a равным $\frac{a}{2^k}$, b – равным $\frac{b}{2^k}$ (при этом одно из чисел a и b обязательно является нечетным);

2. Если одно из чисел a и b четно, то поделить его на наибольшую возможную степень двойки так, чтобы оба числа a и b стали нечетными. Если оба числа нечетны, то сразу переходим к следующему шагу;

3. Сравним полученные числа, пусть $a \geq b$. Тогда положим a равным $a - b$. Если $a \neq 0$, то возвращаемся на шаг 2, иначе переходим к шагу 4.

4. Положить $\text{НОД}(a, b) = d_0 \cdot b$.

Этот алгоритм потребует больше шагов, чем алгоритм Евклида, но преимуществом его является то, что он содержит только деления на 2, поэтому он очень удобен для работы с числами, представленными в двоичной системе счисления. В этой системе деление на 2 означает сдвиг вправо на один разряд, а наибольшая степень двойки, на которую можно поделить данное число, определяется количеством последних нулевых разрядов в двоичной записи числа.

Пример 1. Найти $\text{НОД}(1236, 584)$.

Решение. Последовательно применим все три способа нахождения наибольшего общего делителя. Начнем с алгоритма Евклида:

$r_0 = 1236$, $r_1 = 584$. Из цепочки делений

$$1236 = 584 \cdot 2 + 68,$$

$$584 = 68 \cdot 8 + 40,$$

$$68 = 40 \cdot 1 + 28,$$

$$40 = 28 \cdot 1 + 12,$$

$$28 = 12 \cdot 2 + 4,$$

$$12 = 4 \cdot 3$$

следует, что $\text{НОД}(1236, 584) = 4$.

Теперь разложим исходные числа на простые множители:

$$1236 = 2^2 \cdot 3 \cdot 103,$$

$$584 = 2^3 \cdot 73,$$

значит, $\text{НОД}(1236, 584) = 2^2 \cdot 3^0 \cdot 73^0 \cdot 103^0 = 2^2 = 4$.

Наконец, воспользуемся бинарным алгоритмом. Сначала найдем d_0 . Так как $2^2 \mid 1236$ и $2^2 \mid 584$, а 2^3 не делит 1236, то $d_0 = 2^2$. Делим оба числа на 2^2 , получаем 309 и 146. Поскольку 146 четно, то делим его на 2 и получаем

нечетное число 73. Теперь повторяем шаги 3 и 2 бинарного алгоритма:

$$\begin{aligned} \text{НОД}(309, 73) &= \text{НОД}(309 - 73, 73) = \text{НОД}(236, 73) = \text{НОД}(2^2 \cdot 59, 73) = \\ &= \text{НОД}(59, 73) = \text{НОД}(73, 59) = \text{НОД}(73 - 59, 59) = \text{НОД}(14, 59) = \\ &= \text{НОД}(2 \cdot 7, 59) = \text{НОД}(59, 7) = \text{НОД}(59 - 7, 7) = \text{НОД}(52, 7) = \\ &= \text{НОД}(2^2 \cdot 13, 7) = \text{НОД}(13, 7) = \text{НОД}(13 - 7, 7) = \text{НОД}(6, 7) = \\ &= \text{НОД}(7, 2 \cdot 3) = \text{НОД}(7, 3) = \text{НОД}(7 - 3, 3) = \text{НОД}(4, 3) = \\ &= \text{НОД}(2^2 \cdot 1, 3) = \text{НОД}(1, 3) = \text{НОД}(3, 1) = \text{НОД}(3 - 1, 1) = \text{НОД}(2, 1) = \\ &= \text{НОД}(2 - 1, 1) = \text{НОД}(1, 1) = \text{НОД}(1 - 1, 1) = \text{НОД}(0, 1) = 1. \end{aligned}$$

Итак, $\text{НОД}(1236, 584) = d_0 \cdot 1 = 2^2 = 4$.

Пример 2. Найти НОД двух чисел, записанных в двоичной системе счисления :

$$a = 111010110100_2, \quad b = 1011010000_2.$$

Решение. Очевидно, оба числа делятся на 100_2 , поэтому $d_0 = 100_2$. Делим оба числа на d_0 , т. е. сдвигаем оба числа на два разряда вправо (отсекаем два последних нуля), получаем числа 1110101101_2 и 10110100_2 . Второе число является четным, сдвигаем его вправо на два разряда, получаем 101101_2 . Теперь последовательно выполняем шаги 3 и 2 (в дальнейшем опускаем показатель основания системы счисления):

$$\begin{aligned} \text{НОД}(1110101101, 101101) &= \text{НОД}(1110101101 - 101101, 101101) = \\ &= \text{НОД}(1110000000, 101101) = \text{НОД}(111, 101101) = \text{НОД}(101101, 111) = \\ &= \text{НОД}(101101 - 111, 111) = \text{НОД}(100110, 111) = \text{НОД}(10011, 111) = \\ &= \text{НОД}(10011 - 111, 111) = \text{НОД}(1100, 111) = \text{НОД}(11, 111) = \\ &= \text{НОД}(111, 11) = \text{НОД}(111 - 11, 11) = \text{НОД}(100, 11) = \text{НОД}(1, 11) = \\ &= \text{НОД}(11, 1) = \text{НОД}(11 - 1, 1) = \text{НОД}(10, 1) = \text{НОД}(1, 1) = 1. \end{aligned}$$

Значит, $\text{НОД}(111010110100_2, 1011010000_2) = d_0 \cdot 1 = 100_2$.

Центрированное деление числа a на число b характеризуется тем, что остаток от деления по абсолютной величине является наименьшим возможным, т. е.

$$a = bq + r, \quad \text{где } |r| \leq \frac{b}{2}.$$

Алгоритм Евклида, использующий центрированное деление, в общем случае требует меньшего числа шагов для получения результата.

Пример 3. Найти НОД двух чисел : $a = 297$ и $b = 84$, используя центрированное деление.

Решение. Получаем цепочку делений :

$$\begin{aligned}297 &= 84 \cdot 4 - 39, \\84 &= (-39) \cdot (-2) + 6, \\-39 &= 6 \cdot (-7) + 3, \\6 &= 3 \cdot 2,\end{aligned}$$

откуда $\text{НОД}(297, 84) = 3$.

Расширенный алгоритм Евклида используется для того, чтобы, кроме наибольшего общего делителя двух чисел a , b , найти представление его в виде

$$\text{НОД}(a, b) = au + bv, \quad \text{где } u, v \in \mathbb{Z}.$$

Для этого в ходе работы алгоритма Евклида дополнительно строятся две числовые последовательности $\{u_i\}_{i=0,1,\dots,n+1}$ и $\{v_i\}_{i=0,1,\dots,n+1}$, такие что

$$r_i = au_i + bv_i \quad (i = 0, 1, \dots, n+1).$$

Если $r_n = \text{НОД}(a, b)$, то $r_n = au_n + bv_n$, т. е. $u = u_n$, $v = v_n$. Числа u и v называются *коэффициентами Безу*.

Очевидно, $u_0 = 1$, $v_0 = 0$; $u_1 = 0$, $v_1 = 1$. В дальнейшем элементы последовательностей $\{u_i\}_{i=0,1,\dots,n+1}$ и $\{v_i\}_{i=0,1,\dots,n+1}$ строятся по рекуррентным формулам :

$$\begin{aligned}u_{i+1} &= u_{i-1} - q_i u_i, \\v_{i+1} &= v_{i-1} - q_i v_i, \quad (i = 1, 2, \dots, n),\end{aligned}$$

где q_i определено из i -го деления алгоритма Евклида, т. е.

$$r_{i-1} = q_i r_i + r_{i+1}, \quad 0 < r_{i+1} < r_i.$$

Пример 4. Найти НОД чисел $a = 348$ и $b = 256$ и коэффициенты Безу.

Решение. Воспользуемся расширенным алгоритмом Евклида. Имеем $r_0 = 348$, $r_1 = 256$. Проведем алгоритм Евклида, вычисляя на каждом шаге элементы последовательностей $\{u_i\}$ и $\{v_i\}$:

$$\begin{aligned}348 &= 256 \cdot 1 + 92, \quad q_1 = 1, \text{ откуда } u_2 = 1, \quad v_2 = -1, \\256 &= 92 \cdot 2 + 72, \quad q_2 = 2, \text{ откуда } u_3 = -2, \quad v_3 = 3, \\92 &= 72 \cdot 1 + 20, \quad q_3 = 1, \text{ откуда } u_4 = 3, \quad v_4 = -4, \\72 &= 20 \cdot 3 + 12, \quad q_4 = 3, \text{ откуда } u_5 = -11, \quad v_5 = 15, \\20 &= 12 \cdot 1 + 8, \quad q_5 = 1, \text{ откуда } u_6 = 14, \quad v_6 = -19, \\12 &= 8 \cdot 1 + 4, \quad q_6 = 1, \text{ откуда } u_7 = -25, \quad v_7 = 34, \\8 &= 4 \cdot 2, \quad q_7 = 2.\end{aligned}$$

Таким образом, $\text{НОД}(348, 256) = r_7 = 4$. Последовательные остатки от делений можно теперь выразить с помощью построенных последовательностей $\{u_i\}$ и $\{v_i\}$:

$$\begin{aligned} r_0 &= 348 \cdot 1 + 256 \cdot 0, \\ r_1 &= 348 \cdot 0 + 256 \cdot 1, \\ r_2 &= 348 \cdot 1 + 256 \cdot (-1), \\ r_3 &= 348 \cdot (-2) + 256 \cdot 3, \\ r_4 &= 348 \cdot 3 + 256 \cdot (-4), \\ r_5 &= 348 \cdot (-11) + 256 \cdot 15, \\ r_6 &= 348 \cdot 14 + 256 \cdot (-19), \\ r_7 &= 348 \cdot (-25) + 256 \cdot 34. \end{aligned}$$

Значит, коэффициентами Безу являются числа $u = u_7 = -25$, $v = v_7 = 34$.

Все приведенные вычисления удобно записывать в виде следующей таблицы, которая содержит повторения, облегчающие вычислительный процесс по рекуррентным формулам:

i	q_i	u_i	v_i	r_i	u_{i+1}	v_{i+1}	r_{i+1}
0	—	1	0	348	0	1	256
1	1	0	1	256	1	-1	92
2	2	1	-1	92	-2	3	72
3	1	-2	3	72	3	-4	20
4	3	3	-4	20	-11	15	12
5	1	-11	15	12	14	-19	8
6	1	14	-19	8	-25	34	4
7	2	-25	34	4	64	-87	0

Из приведенной таблицы видно, что $u_8 = 64$, $v_8 = -87$, т. е. $0 = 64 \cdot 348 + (-87) \cdot 256$. На самом деле, u_8 и v_8 нам не нужны, их можно не вычислять.

Диофантовы уравнения первой степени

Диофантовым уравнением первой степени от двух неизвестных называется уравнение

$$ax + by = c, \quad (1)$$

где $a, b, c \in \mathbb{Z}$. Решения этого уравнения также ищутся в кольце \mathbb{Z} .

Уравнение (1) разрешимо тогда и только тогда, когда $d = \text{НОД}(a, b)$ делит c . Поделив обе части уравнения на d , приходим к уравнению

$$a_1x + b_1y = c_1, \quad (2)$$

где $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$, $c_1 = \frac{c}{d}$, $\text{НОД}(a_1, b_1) = 1$.

С помощью расширенного алгоритма Евклида можно найти такие целые числа u, v , что

$$a_1 u + b_1 v = 1.$$

Умножая полученное равенство на c_1 , получаем

$$a_1(uc_1) + b_1(vc_1) = c_1,$$

т. е. $x_0 = uc_1$, $y_0 = vc_1$ есть целочисленное решение уравнения (1). Остальные целочисленные решения получаются по формулам :

$$\begin{cases} x = x_0 - b_1 t, \\ y = y_0 + a_1 t, \end{cases} \quad t \in \mathbb{Z}.$$

Пример 5. Решить в целых числах уравнение $27x - 12y = 84$.

Решение. Очевидно, $\text{НОД}(27, 12) = 3$ делит 84, поэтому уравнение разрешимо. Поделив обе части уравнения на 3, получаем

$$9x - 4y = 28.$$

Так как

$$1 = \text{НОД}(9, 4) = 9 \cdot 1 + 4 \cdot (-2),$$

то $u = 1$, $v = -2$. Умножая u и v на 28, получаем частное решение исходного уравнения $x_0 = 28$, $y_0 = (-2) \cdot 28 = -56$. Значит, целочисленными решениями нашего уравнения являются

$$\begin{cases} x = 28 + 4t, \\ y = -56 + 9t, \end{cases} \quad t \in \mathbb{Z}.$$

Непрерывные (цепные) дроби

Рассмотрим рациональное число $\frac{a}{b}$ ($b \neq 0$, $a, b \in \mathbb{Z}$). Если $\frac{a}{b} < 0$, то всегда считаем $a < 0$, $b > 0$. Применим к числам a и b алгоритм Евклида :

$$r_0 = q_1 r_1 + r_2, \quad 0 < r_2 < r_1, \quad (r_0 = a, \quad r_1 = b)$$

$$r_1 = q_2 r_2 + r_3, \quad 0 < r_3 < r_2,$$

.....

$$r_{k-2} = q_{k-1} r_{k-1} + r_k, \quad 0 < r_k < r_{k-1},$$

$$r_{k-1} = q_k r_k, \quad r_{k+1} = 0.$$

Поделив каждое соотношение $r_{i-1} = q_i r_i + r_{i+1}$ на r_i , получаем

$$\begin{aligned}\frac{r_0}{r_1} &= q_1 + \frac{r_2}{r_1}, \\ \frac{r_1}{r_2} &= q_2 + \frac{r_3}{r_2}, \\ &\dots\dots\dots \\ \frac{x-2}{x-1} &= q_{k-1} + \frac{r_k}{r_{k-1}}, \\ \frac{x-1}{r_k} &= q_k,\end{aligned}$$

откуда

$$\frac{a}{b} = \frac{r_0}{r_1} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\ddots + \frac{1}{q_k}}}} \quad . \quad (3)$$

Это и есть представление рационального числа $\frac{a}{b}$ в виде непрерывной (цепной) дроби. Для сокращения записи формулу (3) будем записывать в строчку, перечисляя через запятую все последовательные неполные частные q_i , т. е. в виде

$$\frac{a}{b} = [q_1, q_2, q_3, \dots, q_k].$$

В алгоритме Евклида используется классическое деление, поэтому $q_i > 0$ для $i = 2, 3, \dots, k$. Лишь q_1 может быть отрицательным в случае, когда $a < 0$. Кроме того, $q_k > 1$.

Справедливо утверждение о том, что *любое рациональное число однозначно представляется в виде конечной непрерывной дроби. Обратно: значением конечной непрерывной дроби является рациональное число.*

Пример 6. Разложить в непрерывную дробь число $-\frac{795}{79}$.

Решение. Воспользуемся алгоритмом Евклида :

$$-795 = 79 \cdot (-11) + 74,$$

$$79 = 74 \cdot 1 + 5,$$

$$74 = 5 \cdot 14 + 4.$$

$$5 = 4 \cdot 1 + 1,$$

$$4 = 1 \cdot 4,$$

T. e. $q_1 = -11$, $q_2 = 1$, $q_3 = 14$, $q_4 = 1$, $q_5 = 4$

И

$$-\frac{795}{79} = [-11, 1, 14, 1, 4].$$

Определение 2. Пусть дана непрерывная дробь $\frac{a}{b} = [q_1, q_2, \dots, q_n]$.

Рациональное число $\frac{P_k}{Q_k} = [q_1, q_2, \dots, q_k]$, $(1 \leq k \leq n)$ называют k -й подходящей дробью к числу $\frac{a}{b} = \frac{P_n}{Q_n}$.

Свойства подходящих дробей:

1. $\frac{P_n}{Q_n} = q_1 + \frac{1}{[q_2, q_3, \dots, q_n]}$;
2. $\frac{P_n}{Q_n} = [q_1, q_2, \dots, q_{n-1} + \frac{1}{q_n}]$;
3. $\frac{P_n}{Q_n} = [q_1, q_2, \dots, q_{s-1} + \frac{1}{[q_s, \dots, q_n]}]$ $(2 \leq s \leq n)$;
4. $P_k Q_{k-1} - P_{k-1} Q_k = (-1)^k \quad (k \geq 1)$;
5. $\text{НОД}(P_k, Q_k) = 1$;
6. $\frac{P_k}{Q_k} = \frac{P_{k-1}}{Q_{k-1}} + \frac{(-1)^k}{Q_k Q_{k-1}} \quad (k \geq 2)$;
7. $P_k = q_k P_{k-1} + P_{k-2}$,
 $Q_k = q_k Q_{k-1} + Q_{k-2} \quad (k \geq 2)$;
8. $\frac{P_k}{Q_k} - \frac{P_{k-2}}{Q_{k-2}} = \frac{q_k (-1)^{k-1}}{Q_k Q_{k-2}} \quad (k > 2)$;
9. $\frac{P_n}{Q_n} = \frac{P_1}{Q_1} + \sum_{k=2}^n \frac{(-1)^k}{Q_k Q_{k-1}}$;
10. $Q_k \geq 2^{\frac{k-2}{2}} \quad (k \geq 2)$.

Пример 7. Свернуть конечную непрерывную дробь

$$[-3, 5, 4, 2, 1, 6, 3].$$

Решение. Можно, конечно, записать эту непрерывную дробь в виде (3) и постепенно сворачивать ее, начиная снизу, но у нас есть более удобный способ. Надо воспользоваться свойством 7 подходящих дробей, посчитать числитель и знаменатель нашей рациональной дроби, тогда останется только записать ответ. Наша искомая дробь есть $\frac{P_7}{Q_7}$. По рекуррентным формулам получаем

$$\begin{aligned} P_0 &= 1, \\ P_1 &= -3, \end{aligned}$$

$$\begin{aligned}
P_2 &= 5 \cdot (-3) + 1 = -14, \\
P_3 &= 4 \cdot (-14) + (-3) = -59, \\
P_4 &= 2 \cdot (-59) + (-14) = -132, \\
P_5 &= 1 \cdot (-132) + (-59) = -191, \\
P_6 &= 6 \cdot (-191) + (-132) = -1278, \\
P_7 &= 3 \cdot (-1278) + (-191) = -4025,
\end{aligned}$$

$$\begin{aligned}
Q_0 &= 0, \\
Q_1 &= 1, \\
Q_2 &= 5 \cdot 1 + 0 = 5, \\
Q_3 &= 4 \cdot 5 + 1 = 21, \\
Q_4 &= 2 \cdot 21 + 5 = 47, \\
Q_5 &= 1 \cdot 47 + 21 = 68, \\
Q_6 &= 6 \cdot 68 + 47 = 455, \\
Q_7 &= 3 \cdot 455 + 68 = 1433.
\end{aligned}$$

Итак,

$$[-3, 5, 4, 2, 1, 6, 3] = -\frac{4025}{1433}.$$

Для разложения произвольного вещественного числа a в непрерывную дробь следует применить следующий алгоритм. Выделим целую и дробную части числа a :

$$a = [a] + \{a\} = a_1 + \alpha,$$

тогда $a = a_1 + \frac{1}{\alpha_1}$, где $\alpha_1 = \frac{1}{\alpha} > 1$.

Далее применяем тот же прием к α_1 ;

$$\alpha_1 = [\alpha_1] + \{\alpha_1\} = a_2 + \frac{1}{\alpha_2},$$

где $\alpha_2 = \frac{1}{\{\alpha_1\}} > 1$ и так далее. В результате получаем

$$a = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots}}}$$

где a_1, a_2, a_3, \dots — целые числа.

Теорема. Любое иррациональное вещественное число однозначно представляется в виде бесконечной непрерывной дроби с целыми неполными частными. Обратно: значением всякой бесконечной непрерывной дроби с целыми неполными частными является иррациональное вещественное число.

Определение 3. Бесконечная непрерывная дробь $[a_1, a_2, \dots, a_n, \dots]$ называется *периодической*, если существуют натуральные числа k_0 и t такие, что для любого $k > k_0$ выполняется равенство $a_{k+t} = a_k$, т. е. последовательность $\{a_k\}_{k=1,2,\dots}$ начиная с некоторого момента является периодической:

$$[a_1, \dots, a_{k_0}, a_{k_0+1}, \dots, a_{k_0+t}, a_{k_0+1}, \dots, a_{k_0+t}, \dots] = [a_1, \dots, a_{k_0}, (a_{k_0+1}, \dots, a_{k_0+t})].$$

t называется *длиной периода*, k_0 – *индексом вхождения в период*.

Определение 4. Действительное число называется *квадратичной иррациональностью*, если оно является корнем квадратного уравнения $ax^2 + bx + c = 0$ с целыми коэффициентами.

Любая квадратичная иррациональность может быть представлена в виде $x + y\sqrt{N}$, где $x, y \in \mathbb{Q}$, а $N \in \mathbb{N}$ не является полным квадратом.

Теорема (Лагранж). Квадратичные иррациональности и только они могут быть представлены в виде бесконечной периодической непрерывной дроби.

Пример 8. Разложить в непрерывную дробь иррациональное число $\sqrt{148}$.

Решение. Выделим целую и дробную части нашего числа :

$$\sqrt{148} = [\sqrt{148}] + \{\sqrt{148}\} = 12 + (\sqrt{148} - 12),$$

т. е. $a_1 = 12, \quad \frac{1}{\alpha_1} = \sqrt{148} - 12.$

Рассмотрим

$$\alpha_1 = \frac{1}{\sqrt{148} - 12} = \frac{\sqrt{148} + 12}{148 - 144} = \frac{\sqrt{148} + 12}{4}.$$

В α_1 выделим целую и дробную части:

$$\alpha_1 = \left[\frac{\sqrt{148} + 12}{4} \right] + \left\{ \frac{\sqrt{148} + 12}{4} \right\} = 6 + \left(\frac{\sqrt{148} - 12}{4} \right),$$

т. е. $a_2 = 6, \quad \frac{1}{\alpha_2} = \frac{\sqrt{148} - 12}{4}.$

Продолжаем повторять эти шаги. Так как число $\sqrt{148}$ является квадратичной иррациональностью, то алгоритм будем проводить до тех пор, пока не найдем период.

$$\begin{aligned}\alpha_2 &= \left\lfloor \frac{4}{\sqrt{148} - 12} \right\rfloor + \left\{ \frac{4}{\sqrt{148} - 12} \right\} = \left\lfloor \frac{4(\sqrt{148} + 12)}{4} \right\rfloor + \left\{ \frac{4(\sqrt{148} + 12)}{4} \right\} = \\ &= \lfloor \sqrt{148} + 12 \rfloor + \{ \sqrt{148} + 12 \} = 24 + (\sqrt{148} - 12),\end{aligned}$$

т. е. $a_3 = 24$, $\frac{1}{\alpha_3} = \sqrt{148} - 12$.

Так как $\alpha_3 = \alpha_1$, то далее неполные частные $a_2 = 6$ и $a_3 = 24$ будут повторяться, значит, они составляют период нашей непрерывной дроби, и мы получаем

$$\sqrt{148} = [12, 6, 24, 6, 24, 6, 24, \dots] = [12, (6, 24)].$$

Пример 9. Свернуть бесконечную периодическую непрерывную дробь $[8, 3, (1, 5, 4, 2)]$ и представить иррациональное число в виде $\frac{a + b\sqrt{c}}{d}$, где $a, b, c, d \in \mathbb{Z}$.

Решение. Обозначим через β значение бесконечной периодической непрерывной дроби $[(1, 5, 4, 2)]$, тогда наше иррациональное число есть конечная непрерывная дробь $[8, 3, \beta]$, значение которой можно выразить через β .

Так как

$$\begin{aligned}P_0 &= 1, & Q_0 &= 0, \\ P_1 &= 8, & Q_1 &= 1, \\ P_2 &= 3 \cdot 8 + 1 = 25, & Q_2 &= 3 \cdot 1 + 0 = 3, \\ P_3 &= \beta \cdot 25 + 8, & Q_3 &= \beta \cdot 3 + 1,\end{aligned}$$

$$\text{то } [8, 3, \beta] = \frac{25\beta + 8}{3\beta + 1}.$$

Теперь найдем значение β . Поскольку β есть бесконечная периодическая дробь, то

$$\beta = [1, 5, 4, 2, \beta],$$

откуда, опять применяя рекуррентные формулы свойства 7 подходящих дробей, получаем

$$\begin{aligned}P_0 &= 1, & Q_0 &= 0, \\ P_1 &= 1, & Q_1 &= 1,\end{aligned}$$

$$\begin{aligned}
P_2 &= 5 \cdot 1 + 1 = 6, & Q_2 &= 5 \cdot 1 + 0 = 5, \\
P_3 &= 4 \cdot 6 + 1 = 25, & Q_3 &= 4 \cdot 5 + 1 = 21, \\
P_4 &= 2 \cdot 25 + 6 = 56, & Q_4 &= 2 \cdot 21 + 5 = 47, \\
P_5 &= \beta \cdot 56 + 25, & Q_5 &= \beta \cdot 47 + 21,
\end{aligned}$$

значит, $\beta = \frac{56\beta + 25}{47\beta + 21}$, откуда

$$(47\beta + 21)\beta = 56\beta + 25.$$

Получили квадратное уравнение относительно β :

$$47\beta^2 - 35\beta - 25 = 0,$$

решения которого $\beta_{1,2} = \frac{35 \pm 5\sqrt{237}}{94}$.

Искомое число β положительно, следовательно, выбираем положительный корень $\beta = \frac{35 + 5\sqrt{237}}{94}$.

Тогда

$$\begin{aligned}
[8, 3, \beta] &= \frac{25 \cdot \frac{35 + 5\sqrt{237}}{94} + 8}{3 \cdot \frac{35 + 5\sqrt{237}}{94} + 1} = \frac{25 \cdot 35 + 125\sqrt{237} + 8 \cdot 94}{105 + 15\sqrt{237} + 94} = \\
&= \frac{1627 + 125\sqrt{237}}{199 + 15\sqrt{237}} = \frac{1627 + 125\sqrt{237}}{199 + 15\sqrt{237}} \cdot \frac{199 - 15\sqrt{237}}{199 - 15\sqrt{237}} = \\
&= \frac{-120602 + 470\sqrt{237}}{-13724} = \frac{1283 - 5\sqrt{237}}{146}.
\end{aligned}$$

Лемма. Пусть $\alpha = [c_1, c_2, \dots, c_n, \alpha_n]$ – иррациональное число, где $\alpha_n = [c_{n+1}, c_{n+2}, \dots]$, $n \geq 1$. Тогда при $k \geq 1$

$$\frac{1}{2Q_{k+1}Q_k} < \left| \alpha - \frac{P_k}{Q_k} \right| < \frac{1}{Q_{k+1}Q_k} < \frac{1}{Q_k^2}. \quad (4)$$

Пример 10. Заменить число $a = 5,341276$ подходящей дробью $\frac{P_5}{Q_5}$ и оценить погрешность приближения.

Решение. Сначала представим число a непрерывной дробью. Имеем $5,341276 = \frac{5341276}{1000000}$, значит, используя алгоритм Евклида, получаем

$$\begin{aligned}
5341276 &= 5 \cdot 10^6 + 341276, \\
1000000 &= 2 \cdot 341276 + 317448, \\
341276 &= 1 \cdot 317448 + 23828, \\
317448 &= 13 \cdot 23828 + 7684, \\
23828 &= 3 \cdot 7684 + 776, \\
7684 &= 9 \cdot 776 + 700, \\
776 &= 1 \cdot 700 + 76, \\
700 &= 9 \cdot 76 + 16, \\
76 &= 4 \cdot 16 + 12, \\
16 &= 1 \cdot 12 + 4, \\
12 &= 3 \cdot 4,
\end{aligned}$$

откуда $5, 341276 = [5, 2, 1, 13, 3, 9, 1, 9, 4, 1, 3]$.

Вычислим 5-ю подходящую дробь:

$$\begin{aligned}
P_0 &= 1, & Q_0 &= 0, \\
P_1 &= 5, & Q_1 &= 1, \\
P_2 &= 2 \cdot 5 + 1 = 11, & Q_2 &= 2 \cdot 1 + 0 = 2, \\
P_3 &= 1 \cdot 11 + 5 = 16, & Q_3 &= 1 \cdot 2 + 1 = 3, \\
P_4 &= 13 \cdot 16 + 11 = 219, & Q_4 &= 13 \cdot 3 + 2 = 41, \\
P_5 &= 3 \cdot 219 + 16 = 673, & Q_5 &= 3 \cdot 41 + 3 = 126,
\end{aligned}$$

т. е. $\frac{P_5}{Q_5} = \frac{673}{126} = 5,3(412698)$.

Если оценивать погрешность приближения точно, то получим

$$5, 341276 - 5, 3412698 \approx 0,0000062.$$

Если использовать лемму о погрешности приближения, то следует вычислить еще $Q_6 = 9 \cdot 126 + 41 = 1175$ и тогда, используя формулу (4), получим

$$\left| a - \frac{P_5}{Q_5} \right| < \frac{1}{Q_5 Q_6} = \frac{1}{126 \cdot 1175} = \frac{1}{148050} \approx 0,0000068.$$

Кольцо целых гауссовых чисел

Кольцо $\mathbb{Z}[i]$, состоящее из чисел вида $a + ib$, где $a, b \in \mathbb{Z}$, i – мнимая единица, с естественными операциями сложения и умножения комплексных чисел называется *кольцом целых гауссовых чисел*.

В этом кольце введем норму элемента $z = a + bi$ формулой

$$g(z) = g(a + ib) = a^2 + b^2. \quad (5)$$

Кольцо $\mathbb{Z}[i]$ относительно введенной нормы является *евклидовым* и, следовательно, *факториальным* кольцом. (Любое евклидово кольцо является факториальным.) Кроме того, норма элемента, определенная формулой (5), является мультипликативной, т. е.

$$g(z_1 z_2) = g(z_1) g(z_2).$$

Операцию деления с остатком в $\mathbb{Z}[i]$ определим следующим образом. Пусть $z_1, z_2 \in \mathbb{Z}[i]$, $z_2 \neq 0$. Тогда поделим z_1 на z_2 в поле частных $\mathbb{Q}[i]$ кольца $\mathbb{Z}[i]$

$$\frac{z_1}{z_2} = x + iy, \quad x, y \in \mathbb{Q}.$$

Определим числа r, s : r есть ближайшее целое к x , а s – ближайшее целое к y , т. е.

$$|x - r| \leq \frac{1}{2}, \quad |y - s| \leq \frac{1}{2}.$$

Тогда деление z_1 на z_2 с остатком в $\mathbb{Z}[i]$ определено формулой

$$z_1 = (r + is)z_2 + (u + iv),$$

где $u + iv = z_1 - (r + is)z_2 \in \mathbb{Z}[i]$ таково, что $g(u + iv) < g(z_2)$.

Пример 11. В кольце $\mathbb{Z}[i]$ найти НОД чисел $z_1 = 15 - 23i$ и $z_2 = -11 + 18i$.

Решение. Применим алгоритм Евклида, выполняя последовательные шаги деления по правилу, определенному выше. Поскольку $g(z_1) = 754 > g(z_2) = 445$, то будем делить z_1 на z_2 .

В $\mathbb{Q}[i]$ имеем

$$\frac{z_1}{z_2} = \frac{15 - 23i}{-11 + 18i} = \frac{(15 - 23i)(-11 - 18i)}{(-11 + 18i)(-11 - 18i)} = \frac{-579 - 17i}{445}.$$

Положим $r = -1$, $s = 0$, тогда $z_1 = -z_2 + z_3$, где $z_3 = z_1 + z_2 = (15 - 23i) + (-11 + 18i) = 4 - 5i$ есть остаток от деления, причем $g(z_3) = g(4 - 5i) = 41 < g(z_2)$.

Теперь поделим z_2 на полученный остаток z_3 . В $\mathbb{Q}[i]$ имеем

$$\frac{z_2}{z_3} = \frac{-11 + 18i}{4 - 5i} = \frac{(-11 + 18i)(4 + 5i)}{(4 - 5i)(4 + 5i)} = \frac{-134 + 17i}{41}.$$

Положим $r = -3$, $s = 0$, тогда $z_2 = -3z_3 + z_4$, где $z_4 = z_2 + 3z_3 = (-11 + 18i) + 3(4 - 5i) = 1 + 3i$ и $g(z_4) = g(1 + 3i) = 10 < g(z_3)$.

Делим z_3 на z_4 в $\mathbb{Q}[i]$:

$$\frac{z_3}{z_4} = \frac{4 - 5i}{1 + 3i} = \frac{(4 - 5i)(1 - 3i)}{(1 + 3i)(1 - 3i)} = \frac{-11 - 17i}{10}.$$

Пусть $r = -1$, $s = -2$, тогда $z_3 = (-1 - 2i)z_4 + z_5$, где $z_5 = z_3 - (-1 - 2i)z_4 = (4 - 5i) - (-1 - 2i)(1 + 3i) = -1$ и $g(z_5) = g(-1) = 1 < g(z_4)$.

Так как последний остаток $z_5 = -1$, то он, очевидно, делит z_4 . Таким образом, в $\mathbb{Z}[i]$ числа $15 - 23i$ и $-11 + 18i$ взаимно просты.

Поскольку кольцо $\mathbb{Z}[i]$ факториально, то любой ненулевой элемент этого кольца можно единственным способом представить в виде произведения неприводимых элементов с точностью до порядка сомножителей и умножения их на обратимые элементы кольца.

Теорема.

(1) Множество обратимых элементов в $\mathbb{Z}[i]$ есть

$$\{z \in \mathbb{Z}[i] \mid g(z) = 1\} = \{1, -1, i, -i\};$$

(2) Если p – простое в \mathbb{N} , то p неприводимо в $\mathbb{Z}[i]$ тогда и только тогда, когда оно не является нормой $g(z)$ для $z \in \mathbb{Z}[i]$;

(3) Пусть $z \in \mathbb{Z}[i]$. Элемент z является неприводимым в $\mathbb{Z}[i]$ и не ассоциированным с элементом из \mathbb{Z} тогда и только тогда, когда $g(z)$ – простое число в кольце \mathbb{Z} .

Пример 12. Выяснить, является ли данное число приводимым в кольце $\mathbb{Z}[i]$. Если да, то найти его разложение на неприводимые множители:

а) $15 - 4i$;

б) $9 + 5i$.

Решение. Если $z \in \mathbb{Z}[i]$ приводимо, т. е. $z = z_1 z_2 \dots z_k$, где z_1, z_2, \dots, z_k являются неприводимыми элементами кольца $\mathbb{Z}[i]$, то

$$g(z) = g(z_1)g(z_2) \dots g(z_k),$$

где $g(z_s)$ ($s = 1, \dots, k$) – простые целые числа. Таким образом, норма приводимого элемента кольца $\mathbb{Z}[i]$ раскладывается в произведение простых целых чисел, каждое из которых является нормой неприводимого элемента этого кольца.

Рассмотрим пример а). Поскольку $g(15 - 4i) = 15^2 + 4^2 = 241$ – простое число, то $15 - 4i$ неприводимый элемент кольца $\mathbb{Z}[i]$.

Перейдем к примеру б). Так как $g(9 + 5i) = 9^2 + 5^2 = 106 = 2 \cdot 53$, то $9 + 5i$ должно раскладываться в произведение двух неприводимых элементов кольца $\mathbb{Z}[i]$, нормы которых соответственно 2 и 53. Норму 2 имеют только элементы $\pm 1 \pm i$, норму 53 – элементы $\pm 7 \pm 2i$ и ассоциированные с ними в кольце $\mathbb{Z}[i]$ элементы $\pm 2 \pm 7i$.

Очевидно, $9 + 5i = (1 + i)(7 - 2i)$.

Пример 13. Является ли простое число 617 неприводимым элементом кольца $\mathbb{Z}[i]$?

Решение. Так как 617 можно представить в виде суммы двух квадратов:

$$617 = 19^2 + 16^2,$$

то в $\mathbb{Z}[i]$ оно приводимо, а именно

$$617 = (19 + 16i)(19 - 16i).$$

Сравнения и системы сравнений

Определение. Целые числа a и b называются *сравнимыми по модулю натурального числа m* , если $m \mid a - b$.

(Обозначение: $a \equiv b \pmod{m}$).

Свойства сравнений:

1. Если $a \equiv b \pmod{m}$ и $d \mid m$, то $a \equiv b \pmod{d}$.
2. Если $a \equiv b \pmod{m}$ и $a \equiv b \pmod{n}$, то $a \equiv b \pmod{\text{НОК}(m, n)}$.
3. Если $a \equiv c \pmod{m}$ и $b \equiv d \pmod{m}$, то

$$a + b \equiv c + d \pmod{m};$$

$$a - b \equiv c - d \pmod{m};$$

$$ab \equiv cd \pmod{m}.$$

4. Если $ab \equiv ac \pmod{m}$, то $b \equiv c \pmod{\frac{m}{d}}$, где $d = \text{НОД}(a, m)$.

В частности, если $\text{НОД}(m, a) = 1$, то из $ab \equiv ac \pmod{m}$ следует $b \equiv c \pmod{m}$.

Теорема. Пусть $a, b \in \mathbb{Z}$, $m > 1$ – целое. Сравнение

$$ax \equiv b \pmod{m}$$

разрешимо тогда и только тогда, когда $d = \text{НОД}(a, m) \mid b$. Если оно разрешимо, то имеет единственное решение по модулю $\frac{m}{d}$ и d решений по модулю m .

Пример 14. Найти обратный к элементу 21 по модулю 34.

Решение. Так как числа 21 и 34 взаимно просты, то элемент 21 обратим по модулю 34. Воспользуемся расширенным алгоритмом Евклида:

i	q_i	u_i	v_i	r_i	u_{i+1}	v_{i+1}	r_{i+1}
0	—	1	0	34	0	1	21
1	1	0	1	21	1	−1	13
2	1	1	−1	13	−1	2	8
3	1	−1	2	8	2	−3	5
4	1	2	−3	5	−3	5	3
5	1	−3	5	3	5	−8	2
6	1	5	−8	2	−8	13	1
7	2	−8	13	1	—	—	0

Таким образом, $-8 \cdot 34 + 13 \cdot 21 = 1$.

Рассматривая полученное равенство по модулю 34, получаем

$$13 \cdot 21 \equiv 1 \pmod{34},$$

откуда $21^{-1} \equiv 13 \pmod{34}$.

Пример 15. Найти все решения сравнения $144x \equiv 60 \pmod{156}$.

Решение. Так как $\text{НОД}(144, 156) = 12$ делит 60, то сравнение разрешимо. Поделим обе части сравнения и модуль на 12:

$$12x \equiv 5 \pmod{13}.$$

Полученное сравнение имеет единственное решение по модулю 13. Чтобы его найти, следует умножить обе части сравнения на $12^{-1} \pmod{13}$. Так как $12^{-1} \pmod{13} \equiv 12 \pmod{13}$, то получаем

$$x \equiv 60 \pmod{13} \equiv 8 \pmod{13}.$$

По модулю 156 сравнение имеет 12 решений:

$$8, 21, 34, 47, 60, 73, 86, 99, 112, 125, 138, 151 \pmod{156}.$$

Теорема. Пусть m_1, m_2, \dots, m_k — попарно взаимно простые целые числа, $m_i > 1$ ($i = 1, \dots, k$) и пусть $M = m_1 m_2 \dots m_k$. Тогда единственным неотрицательным решением по модулю M системы сравнений

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots\dots\dots \\ x \equiv a_k \pmod{m_k} \end{cases} \quad (6)$$

является

$$x \equiv \sum_{i=1}^k a_i M_i N_i \pmod{M}, \quad (7)$$

где $M_i = \frac{M}{m_i}$, $i = 1, 2, \dots, k$, N_i – целое, удовлетворяющее условию

$$M_i N_i + m_i n_i = 1 \quad (i = 1, 2, \dots, k).$$

Решать систему сравнений по взаимно простым модулям можно, используя формулу (7) или последовательно решая сравнение и подставляя полученное решение в следующее сравнение системы. В последнем случае решение ищется в виде

$$x = q_0 + q_1 m_1 + q_2 m_1 m_2 + q_3 m_1 m_2 m_3 + \dots + q_{k-1} m_1 m_2 \dots m_{k-1} \pmod{M}. \quad (8)$$

Пример 16. Решить систему сравнений:

$$\begin{cases} 2x \equiv 3 \pmod{7} \\ 5x \equiv 3 \pmod{8} \\ x \equiv 10 \pmod{11} \\ 4x \equiv 3 \pmod{5}. \end{cases}$$

Решение. Сначала приведем систему сравнений к виду (6). Для этого следует первое сравнение умножить на $2^{-1} \pmod{7} \equiv 4$, второе – на $5^{-1} \pmod{8} \equiv 5$, четвертое – на $4^{-1} \pmod{5} \equiv 4$. В результате приходим к системе

$$\begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 7 \pmod{8} \\ x \equiv 10 \pmod{11} \\ x \equiv 2 \pmod{5}. \end{cases}$$

Чтобы использовать формулу (7), следует найти M_i , N_i ($i = 1, 2, 3, 4$). Так как $M = 7 \cdot 8 \cdot 11 \cdot 5 = 3080$, то

$$M_1 = 440, \quad M_2 = 385, \quad M_3 = 280, \quad M_4 = 616.$$

Числа N_i ($i = 1, 2, 3, 4$) ищем с помощью расширенного алгоритма Евклида, который последовательно применяем к каждой паре M_i , m_i . Имеем

$$\begin{aligned} (-1) \cdot 440 + 63 \cdot 7 &= 1, \text{ откуда } N_1 = -1, \\ 1 \cdot 385 + (-48) \cdot 8 &= 1, \text{ откуда } N_2 = 1, \\ (-2) \cdot 280 + 51 \cdot 11 &= 1, \text{ откуда } N_3 = -2, \\ 1 \cdot 616 + (-123) \cdot 5 &= 1, \text{ откуда } N_4 = 1. \end{aligned}$$

Значит,

$$\begin{aligned}x &\equiv 5 \cdot 440 \cdot (-1) + 7 \cdot 385 \cdot 1 + 10 \cdot 280 \cdot (-2) + 2 \cdot 616 \cdot 1 \pmod{3080} \equiv \\&\equiv 2287 \pmod{3080}.\end{aligned}$$

Пример 17. Решить систему сравнений, используя метод последовательного решения сравнений:

$$\begin{cases} 3x \equiv 2 \pmod{5} \\ 2x \equiv 1 \pmod{3} \\ 5x \equiv 3 \pmod{7} \\ 17x \equiv 2 \pmod{11}. \end{cases}$$

Решение. Приведем систему к виду (6). Так как $3^{-1} \equiv 2 \pmod{5}$, $2^{-1} \equiv 2 \pmod{3}$, $5^{-1} \equiv 3 \pmod{7}$, $17 \equiv 6 \pmod{11}$, $6^{-1} \equiv 2 \pmod{11}$, то получаем

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{7} \\ x \equiv 4 \pmod{11}. \end{cases}$$

Из первого сравнения $x = 4 + 5t$, $t \in \mathbb{Z}$. Подставим полученное решение первого сравнения во второе сравнение системы:

$$4 + 5t \equiv 2 \pmod{3}, \quad \text{или} \quad 2t \equiv 1 \pmod{3},$$

откуда $t \equiv 2 \pmod{3}$, т. е. $t = 2 + 3k$, $k \in \mathbb{Z}$. Итак,

$$x = 4 + 5t = 4 + 5(2 + 3k) = 14 + 15k, \quad k \in \mathbb{Z}.$$

Подставляем полученное решение первых двух уравнений в третье уравнение системы:

$$14 + 15k \equiv 2 \pmod{7}, \quad \text{или} \quad k \equiv 2 \pmod{7},$$

откуда $k = 2 + 7s$, $s \in \mathbb{Z}$.

$$\text{Значит, } x = 14 + 15k = 14 + 15(2 + 7s) = 44 + 105s, \quad s \in \mathbb{Z}.$$

Наконец, полученное решение первых трех сравнений подставляем в четвертое сравнение:

$$44 + 105s \equiv 4 \pmod{11}, \quad \text{или} \quad 6s \equiv 4 \pmod{11}.$$

Так как $6^{-1} \equiv 2 \pmod{11}$, то $s \equiv 8 \pmod{11}$, или $s = 8 + 11l$, $l \in \mathbb{Z}$.

В результате получаем

$$x = 44 + 105s = 44 + 105(8 + 11l) = 884 + 1155l, \quad l \in \mathbb{Z}.$$

Таким образом,

$$x \equiv 884 \pmod{1155}$$

есть решение нашей системы сравнений.

Нашу систему можно решить быстрее, если заметить, что по двум модулям 5 и 11 x сравнимо с 4, т. е. $x \equiv 4 \pmod{55}$, и по модулям 3 и 7 x сравнимо с 2, т. е. $x \equiv 2 \pmod{21}$.

Поэтому получаем систему из двух сравнений:

$$\begin{cases} x \equiv 4 \pmod{55} \\ x \equiv 2 \pmod{21}. \end{cases}$$

Из первого сравнения $x = 4 + 55t$, $t \in \mathbb{Z}$. Подставим полученное значение x во второе сравнение $4 + 55t \equiv 2 \pmod{21}$, откуда $13t \equiv -2 \pmod{21}$. Так как $13^{-1} \equiv 13 \pmod{21}$, то $t \equiv -26 \equiv 16 \pmod{21}$, или $t = 16 + 21k$, $k \in \mathbb{Z}$. Следовательно,

$$x = 4 + 55t = 4 + 55(16 + 21k) = 884 + 1155k, \quad k \in \mathbb{Z},$$

или $x \equiv 884 \pmod{1155}$.

Теоремы Ферма и Эйлера. Дихотомический алгоритм

Теорема (малая теорема Ферма). Если n – простое число, а a – произвольное целое, не делящееся на n , то справедливо

$$a^{n-1} \equiv 1 \pmod{n}.$$

Следствие. Если n – простое число, то для любого целого a , не делящегося на n , выполняется

$$a^{n-2} \equiv a^{-1} \pmod{n}.$$

Обобщением малой теоремы Ферма является теорема Эйлера.

Теорема (Эйлер). Пусть $n > 1$ – натуральное число и a – целое такое, что a и n взаимно просты, тогда

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

где $\varphi(n)$ – функция Эйлера.

Следствие. Пусть $n > 1$ – натуральное число. Для любого целого a , взаимно простого с n , справедливо

$$a^{\varphi(n)-1} \equiv a^{-1} \pmod{n}.$$

Определение. Составные числа, которые ведут себя как простые в теореме Ферма для данного основания a , называются *псевдопростыми по основанию a* .

Определение. Число n называется *числом Кармайкла*, если оно псевдопростое по любому основанию a , взаимно простому с n , но само при этом простым не является.

Пример 18. Является ли число 105 псевдопростым по основанию 13?

Решение. Проверим, выполняется ли сравнение Ферма для данной пары чисел:

$$13^{104} \pmod{105} = (13^2)^{52} \pmod{105} \equiv 64^{52} \pmod{105} \equiv (64^2)^{26} \pmod{105} \equiv 1^{26} \pmod{105} = 1.$$

Таким образом, число 105 является псевдопростым по основанию 13.

Лемма. Пусть p_1, p_2, \dots, p_k , $k \geq 3$ – нечетные простые, попарно различные числа и $m = \prod_{i=1}^k p_i$. Если p_i таковы, что $(p_i - 1) \mid (m - 1)$ для каждого $i = 1, 2, \dots, k$, то m является числом Кармайкла.

Определение. Пусть m – целое нечетное число и $m - 1 = 2^s q$, где q – нечетное. Число m называется *сильно псевдопростым по основанию $a \in \mathbb{Z}$* , если выполняются следующие условия:

либо $a^q \equiv 1 \pmod{m}$,

либо найдется такое i , $0 \leq i \leq s - 1$, что $a^{2^i q} \equiv -1 \pmod{m}$.

Дихотомический алгоритм в мультипликативной форме предназначен для уменьшения количества умножений при вычислении натуральной степени элемента некоторого кольца \mathbb{A} . Пусть требуется вычислить a^n . Разложим n по базису двоичной системы счисления:

$$n = \sum_{i=0}^k 2^i k_i, \quad \text{где } k_i = \begin{cases} 0 \\ 1, \end{cases} \quad k = \lfloor \log_2 n \rfloor.$$

Тогда

$$a^n = a^{\sum_{i=0}^k 2^i k_i} = \prod_{i=0, k_i \neq 0}^k a^{2^i}.$$

Поэтому следует найти числа a^{2^i} ($i = 0, 1, \dots, k$) и затем перемножить те из них, для которых $k_i \neq 0$.

Аддитивная форма дихотомического алгоритма решает задачу замены умножения элемента $a \in \mathbb{A}$ на целое число b как можно меньшим количеством сложений в кольце \mathbb{A} .

Разложим b по базису двоичной системы счисления:

$$b = \sum_{i=0}^k 2^i k_i, \quad \text{где } k_i = \begin{cases} 0 \\ 1, \end{cases} \quad k = \lfloor \log_2 b \rfloor.$$

Тогда

$$a \cdot b = a \cdot \sum_{i=0}^k 2^i k_i = \sum_{i=0, k_i \neq 0}^k 2^i a.$$

Значит, следует найти числа $2^i a = 2^{i-1} a + 2^{i-1} a$ ($i = 0, 1, \dots, k$) и затем сложить те из них, которые соответствуют $k_i \neq 0$.

Пример 19. Найти $17^{-1} \pmod{19}$.

Решение. Так как 19 – простое число и 17 не делится на 19, то можно воспользоваться следствием из малой теоремы Ферма, т. е.

$$17^{-1} \equiv 17^{19-2} \equiv 17^{17} \pmod{19}.$$

Чтобы провести вычисления быстрее, воспользуемся мультипликативной формой дихотомического алгоритма. Имеем $17 = 10001_2$, найдем числа 17^{2^i} ($i = 0, 1, 2, 3, 4$) :

$$\begin{aligned} 17^{2^0} &\equiv 17 \pmod{19}, \\ 17^{2^1} &\equiv 17 \cdot 17 \equiv 289 \equiv 4 \pmod{19}, \\ 17^{2^2} &\equiv 4^2 \equiv 4 \cdot 4 \equiv 16 \equiv -3 \pmod{19}, \\ 17^{2^3} &\equiv (-3)^2 \equiv (-3) \cdot (-3) \equiv 9 \pmod{19}, \\ 17^{2^4} &\equiv 9^2 \equiv 9 \cdot 9 \equiv 81 \equiv 5 \pmod{19}. \end{aligned}$$

Следовательно, $17^{17} \equiv 5 \cdot 17 \equiv 85 \equiv 9 \pmod{19}$.

Пример 20. Найти $15^{-1} \pmod{22}$.

Решение. Так как $\text{НОД}(15, 22) = 1$, то 15 обратимо по модулю 22. Воспользуемся следствием из теоремы Эйлера:

$$15^{-1} \equiv 15^{\varphi(22)-1} \pmod{22}.$$

Так как $\varphi(22) = \varphi(2 \cdot 11) = \varphi(2) \varphi(11) = 10$, то

$$15^{-1} \equiv 15^{10-1} \equiv 15^9 \pmod{22}.$$

Опять воспользуемся дихотомическим алгоритмом: $9 = 1001_2$.

Найдем 15^{2^i} ($i = 0, 1, 2, 3$) :

$$15^{2^0} \equiv 15 \pmod{22},$$

$$15^{2^1} \equiv 15 \cdot 15 \equiv 225 \equiv 5 \pmod{22},$$

$$15^{2^2} \equiv 5^2 \equiv 5 \cdot 5 \equiv 25 \equiv 3 \pmod{22},$$

$$15^{2^3} \equiv 3^2 \equiv 3 \cdot 3 \equiv 9 \pmod{22}.$$

Значит, $15^9 \equiv 9 \cdot 15 \equiv 135 \equiv 3 \pmod{22}$.

Пример 21. Найти число сложений, требующихся для вычисления $143 \cdot 51$ с помощью дихотомического алгоритма.

Решение. Число 51 – меньшее из двух данных чисел. Если его разложить по базису двоичной системы счисления и использовать дихотомический алгоритм, то сложений получится меньше, чем если бы мы начали с числа 143. Имеем

$$51 = 2^5 + 2^4 + 2 + 1, \quad 51 = 110011_2.$$

Вычислим последовательность чисел $143 \cdot 2^i$ ($i = 0, 1, \dots, 5$) :

$$143 \cdot 2^1 = 143 + 143 = 286,$$

$$143 \cdot 2^2 = 286 + 286 = 572,$$

$$143 \cdot 2^3 = 572 + 572 = 1144,$$

$$143 \cdot 2^4 = 1144 + 1144 = 2288,$$

$$143 \cdot 2^5 = 2288 + 2288 = 4576,$$

поэтому

$$143 \cdot 51 = 4576 + 2288 + 286 + 143 = 7293.$$

Нам потребовалось всего 8 операций сложения.

Пример 22. Является ли число 1105 псевдопростым по основанию 2?

Решение. Так как $1105 - 1 = 1104$, то следует проверить, выполняется ли сравнение $2^{1104} \equiv 1 \pmod{1105}$?

Первый способ. Чтобы возвести число 2 в степень, воспользуемся дихотомическим алгоритмом. Имеем

$$1104 = 2^{10} + 2^6 + 2^4 = 10001010000_2.$$

Тогда

$$2^2 \equiv 4 \pmod{1105},$$

$$\begin{aligned}
2^{2^2} &\equiv 16 \pmod{1105}, \\
2^{2^3} &\equiv 256 \pmod{1105}, \\
2^{2^4} &\equiv 341 \pmod{1105}, \\
2^{2^5} &\equiv 256 \pmod{1105}.
\end{aligned}$$

Очевидно, далее степени будут повторяться:

$$2^{2^6} \equiv 2^{2^8} \equiv 2^{2^{10}} \equiv 341 \pmod{1105}, \quad 2^{2^7} \equiv 2^{2^9} \equiv 256 \pmod{1105}.$$

$$2^{1104} = 2^{2^{10}} \cdot 2^{2^6} \cdot 2^4 \equiv 341^3 \equiv 1 \pmod{1105}.$$

Значит, 1105 является псевдопростым по основанию 2.

Второй способ. Можно заметить, что $1105 = 5 \cdot 13 \cdot 17$, т. е. раскладывается в произведение различных простых чисел. Воспользуемся китайской теоремой об остатках. Так как

$$\begin{cases} 2^4 \equiv 1 \pmod{5} \\ 2^{12} \equiv 1 \pmod{13} \\ 2^8 \equiv 1 \pmod{17} \end{cases}$$

и $\text{НОК}(2, 8, 12) = 24$, то

$$\begin{cases} 2^{24} \equiv 1 \pmod{5} \\ 2^{24} \equiv 1 \pmod{13} \\ 2^{24} \equiv 1 \pmod{17}. \end{cases}$$

Из последней системы следует: $2^{24} \equiv 1 \pmod{1105}$. Остается заметить, что $24 \mid 1104$, т. е.

$$2^{1104} = (2^{24})^{46} \equiv 1^{46} \equiv 1 \pmod{1105}.$$

И мы приходим к тому же выводу.

Замечание. На самом деле 1105 является числом Кармайкла. Действительно, $p_1 = 5$, $p_2 = 13$, $p_3 = 17$. Все числа $p_1 - 1 = 4$, $p_2 - 1 = 12$, $p_3 - 1 = 16$ делят 1104. Остается применить теорему о числах Кармайкла.

Пример 23. Является ли число 25 сильно псевдопростым по основанию 2?

Решение. Имеем $25 - 1 = 24 = 2^3 \cdot 3$.

Так как $2^3 \equiv 8 \equiv 1 \pmod{25}$, то проверяем сравнения

$$2^{3^i} \equiv -1 \pmod{25} \quad \text{для } i = 1, 2.$$

Получаем

$$(2^3)^2 \equiv 64 \equiv 14 \pmod{25},$$

$$(2^3)^{2^2} \equiv 14^2 \equiv 196 \equiv 21 \pmod{25},$$

значит, 25 не является сильно псевдопростым по основанию 2.

Мультипликативная группа кольца вычетов

Определение. Мультипликативной группой \mathbb{Z}_n^* кольца вычетов \mathbb{Z}_n называется группа обратимых элементов этого кольца с операцией умножения.

Теорема. Пусть $a \in \mathbb{Z}_n$. Элемент a имеет мультипликативный обратный по модулю n тогда и только тогда, когда $\text{НОД}(a, n) = 1$.

Лемма (Гаусс). Если p – простое нечетное число, то для любого целого $\alpha \geq 1$ группа $\mathbb{Z}_{p^\alpha}^*$ является циклической.

Теорема. Группа $\mathbb{Z}_{2^m}^*$ имеет порядок 2^{m-1} и при $m \geq 3$ является прямым произведением циклической группы порядка 2^{m-2} и циклической группы порядка 2.

Теорема (Гаусс). Мультипликативная группа кольца \mathbb{Z}_n является циклической в том и только том случае, когда n – одно из чисел

$$2, 4, p^\alpha, 2p^\alpha,$$

где $\alpha \geq 1$ – целое, а p – нечетное простое число.

Определение. Прямым (или декартовым) произведением групп (G_1, \star) и (G_2, \circ) называется множество пар (g_1, g_2) с покомпонентным выполнением операций, т. е.

$$(g_1, g_2) \cdot (h_1, h_2) = (g_1 \star h_1, g_2 \circ h_2).$$

Обозначаем декартово произведение символом $G_1 \times G_2$.

Декартово произведение групп, очевидно, также является группой.

Данное определение можно обобщить на случай любого конечного числа групп.

Определение. Прямым (или декартовым) произведением

$$G_1 \times G_2 \times \cdots \times G_m$$

групп (G_i, \circ) ($i = 1, 2, \dots, m$) называется множество последовательностей (g_1, g_2, \dots, g_m) , $g_i \in G_i$ ($i = 1, 2, \dots, m$) с покомпонентным выполнением операций, т. е.

$$(g_1, g_2, \dots, g_m) \cdot (h_1, h_2, \dots, h_m) = (g_1 \circ_{G_1} h_1, \dots, g_m \circ_{G_m} h_m).$$

Теорема. Пусть $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, где p_1, p_2, \dots, p_s – попарно взаимно простые целые положительные числа, $\alpha_i > 0$ ($i = 1, \dots, s$) – целые. Тогда мультипликативная группа кольца \mathbb{Z}_m изоморфна прямому произведению мультипликативных групп колец $\mathbb{Z}_{p_i^{\alpha_i}}$, т. е.

$$\mathbb{Z}_m^* \cong \mathbb{Z}_{p_1^{\alpha_1}}^* \times \mathbb{Z}_{p_2^{\alpha_2}}^* \times \dots \times \mathbb{Z}_{p_s^{\alpha_s}}^*.$$

Определение. Если мультипликативная группа \mathbb{Z}_n^* является циклической, то ее образующая называется *примитивным корнем* (или *примитивным элементом*) по модулю n .

Если g – примитивный корень по модулю n , то элемент g^k , где $k > 1$ – целое, также является примитивным корнем по модулю n тогда и только тогда, когда k взаимно просто с $\varphi(n)$. Отсюда следует, что число примитивных корней по модулю n равно $\varphi(\varphi(n))$.

Пример 24. Является ли группа \mathbb{Z}_{98}^* циклической? Определить ее порядок. Если группа циклическая, то найти образующую.

Решение. Так как $98 = 2 \cdot 7^2$, то по теореме Гаусса \mathbb{Z}_{98}^* является циклической группой, порядок ее равен

$$\varphi(98) = \varphi(2 \cdot 7^2) = \varphi(2)\varphi(7^2) = 7(7 - 1) = 42.$$

Значит, надо найти элемент порядка 42. В качестве кандидата на образующую попробуем наименьший положительный представитель класса вычетов [3] :

$$\begin{array}{ll} 3^1 \equiv 3 \pmod{98}, & 3^{10} \equiv 249 \equiv 53 \pmod{98}, \\ 3^2 \equiv 9 \pmod{98}, & 3^{11} \equiv 159 \equiv 61 \pmod{98}, \\ 3^3 \equiv 27 \pmod{98}, & 3^{12} \equiv 183 \equiv 85 \pmod{98}, \\ 3^4 \equiv 81 \pmod{98}, & 3^{13} \equiv 255 \equiv 59 \pmod{98}, \\ 3^5 \equiv 243 \equiv 47 \pmod{98}, & 3^{14} \equiv 177 \equiv 79 \pmod{98}, \\ 3^6 \equiv 141 \equiv 43 \pmod{98}, & 3^{15} \equiv 237 \equiv 41 \pmod{98}, \\ 3^7 \equiv 129 \equiv 31 \pmod{98}, & 3^{16} \equiv 123 \equiv 25 \pmod{98}, \\ 3^8 \equiv 93 \pmod{98}, & 3^{17} \equiv 75 \pmod{98}, \\ 3^9 \equiv 279 \equiv 83 \pmod{98}, & 3^{18} \equiv 225 \equiv 29 \pmod{98}, \end{array}$$

$$\begin{array}{l} 3^{19} \equiv 87 \pmod{98}, \\ 3^{20} \equiv 261 \equiv 65 \pmod{98}, \\ 3^{21} \equiv 195 \equiv 97 \equiv -1 \pmod{98}. \end{array}$$

Далее можно заметить, что следующие последовательные степени числа 3 будут повторять уже полученные числа, начиная с 3, только с отрицательными знаками, т. е. $3^{22} \equiv -3 \pmod{98}$, $3^{23} \equiv -9 \pmod{98}$ и так далее. Значит, $3^{42} \equiv 1 \pmod{98}$, $\text{ord}_{\mathbb{Z}_{98}^*}(3) = 42$, следовательно, класс вычетов [3] является образующей нашей мультипликативной группы.

Пример 25. В циклической группе \mathbb{Z}_{50}^* найти все образующие.

Решение. Порядок группы \mathbb{Z}_{50}^* равен $\varphi(50) = \varphi(2 \cdot 5^2) = \varphi(2)\varphi(5^2) = 5(5-1) = 20$. Значит, образующей является элемент порядка 20. Попробуем элемент 3 – представитель класса вычетов [3] :

$$\begin{array}{ll} 3^1 \equiv 3 \pmod{50}, & 3^{11} \equiv -3 \pmod{50}, \\ 3^2 \equiv 9 \pmod{50}, & 3^{12} \equiv -9 \pmod{50}, \\ 3^3 \equiv 27 \pmod{50}, & 3^{13} \equiv -27 \pmod{50}, \\ 3^4 \equiv 81 \equiv 31 \pmod{50}, & 3^{14} \equiv -31 \pmod{50}, \\ 3^5 \equiv 93 \equiv 43 \pmod{50}, & 3^{15} \equiv -43 \pmod{50}, \\ 3^6 \equiv 129 \equiv 29 \pmod{50}, & 3^{16} \equiv -29 \pmod{50}, \\ 3^7 \equiv 87 \equiv 37 \pmod{50}, & 3^{17} \equiv -37 \pmod{50}, \\ 3^8 \equiv 111 \equiv 11 \pmod{50}, & 3^{18} \equiv -11 \pmod{50}, \\ 3^9 \equiv 33 \pmod{50}, & 3^{19} \equiv -33 \pmod{50}, \\ 3^{10} \equiv 99 \equiv -1 \pmod{50}, & 3^{20} \equiv 1 \pmod{50}. \end{array}$$

Значит, $\text{ord}_{\mathbb{Z}_{50}^*}(3) = 20$. Теперь найдем числа, меньшие числа 20 и взаимно простые с ним. Их должно быть

$$\varphi(20) = \varphi(2^2 \cdot 5) = \varphi(2^2)\varphi(5) = 2 \cdot 4 = 8.$$

Очевидно, это следующие числа: 1, 3, 7, 9, 11, 13, 17, 19. Тогда

$$\begin{array}{l} 3^1 \equiv 3, \quad 3^3 \equiv 27, \quad 3^7 \equiv 37, \quad 3^9 \equiv 33, \quad 3^{11} \equiv 47, \\ 3^{13} \equiv 23, \quad 3^{17} \equiv 13, \quad 3^{19} \equiv 17 \pmod{50}. \end{array}$$

Получаем, что образующими нашей мультипликативной группы являются классы вычетов, представители которых есть числа 3, 27, 37, 33, 47, 23, 13, 17.

Пример 26. Найти порядок группы \mathbb{Z}_{72}^* , описать ее структуру и найти элементы максимального порядка.

Решение. Порядок группы равен

$$\varphi(72) = \varphi(2^3 \cdot 3^2) = \varphi(2^3)\varphi(3^2) = 2^2 \cdot 3(3-1) = 24.$$

Эта группа, очевидно, не является циклической. Поскольку $72 = 2^3 3^2$, где 2 и 3 взаимно просты, то

$$\mathbb{Z}_{72}^* \cong \mathbb{Z}_{2^3}^* \times \mathbb{Z}_{3^2}^*,$$

где $\mathbb{Z}_{2^3}^*$ есть декартово произведение двух циклических групп порядка 2 $\mathbb{Z}_{2^3}^* \cong G_1 \times G_2$, а $\mathbb{Z}_{3^2}^*$ есть циклическая группа порядка 6.

Если $(a, b) \in \mathbb{Z}_n \times \mathbb{Z}_m$, где $\text{НОД}(n, m) = 1$, то этой паре в группе \mathbb{Z}_{nm} соответствует класс вычетов, которому принадлежит элемент x , удовлетворяющий системе сравнений

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m}. \end{cases}$$

При этом, если $\text{ord}_{\mathbb{Z}_n^*}(a) = k$, $\text{ord}_{\mathbb{Z}_m^*}(b) = s$, то $\text{ord}_{\mathbb{Z}_{nm}^*}(ab) = \text{НОК}(k, s)$.

Очевидно, $\mathbb{Z}_{2^3}^* = \{[1], [3], [5], [7]\}$, причем порядки всех отличных от [1] элементов этой группы равны 2. В циклической группе $\mathbb{Z}_{3^2}^*$ есть два элемента [2] и [5], имеющих порядок 6, и два элемента [4] и [7], имеющих порядок 3. Тогда парам

$$\begin{aligned} &([3], [2]), ([3], [5]), ([5], [2]), ([5], [5]), ([7], [2]), ([7], [5]), ([3], [4]), \\ &([3], [7]), ([5], [4]), ([5], [7]), ([7], [4]), ([7], [7]), ([1], [2]), ([1], [5]) \end{aligned}$$

из $\mathbb{Z}_{2^3}^* \times \mathbb{Z}_{3^2}^*$ соответствуют элементы порядка 6 группы \mathbb{Z}_{72}^* .

Первой паре $([3], [2])$ соответствует класс вычетов, которому принадлежит x , удовлетворяющий системе сравнений

$$\begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 2 \pmod{9}. \end{cases}$$

Решением этой системы является $x \equiv 11 \pmod{72}$. Таким образом, класс вычетов [11] есть элемент порядка 6 группы \mathbb{Z}_{72}^* .

Рассматривая остальные пары и решая для каждой соответствующую систему сравнений, получаем классы вычетов:

$$[59], [29], [5], [47], [23], [67], [43], [13], [61], [31], [7], [65], [41].$$

Итак, в группе \mathbb{Z}_{72}^* имеются 14 элементов порядка 6.

Модульная арифметика

Модульная арифметика используется для выполнения точных арифметических действий с большими целыми числами. Наиболее удобен способ, при котором используется несколько небольших модулей.

Пусть требуется найти значение некоторой функции

$$r = f(t_1, t_2, \dots, t_n)$$

от целочисленных аргументов $t_1, t_2, \dots, t_n \in \mathbb{Z}$. Предположим, что мы можем заранее оценить результат $r \in \mathbb{Z}$.

Тогда выбираются несколько небольших взаимно простых модулей m_1, m_2, \dots, m_h так, чтобы $m_1 m_2 \dots m_h > |r|$. Для каждого i ($1 \leq i \leq h$) вычисляем

$$r_i = f(t_{1i}, t_{2i}, \dots, t_{ni}), \quad \text{где } t_{ji} \equiv t_j \pmod{m_i}; \quad (j = 1, 2, \dots, n).$$

В результате получаем значения нашей функции в \mathbb{Z}_{m_i} ($i = 1, 2, \dots, h$). Для того чтобы найти r , остается решить систему сравнений

$$\left\{ \begin{array}{l} r \equiv r_1 \pmod{m_1} \\ r \equiv r_2 \pmod{m_2} \\ \dots\dots\dots \\ r \equiv r_h \pmod{m_h}, \end{array} \right.$$

пользуясь китайской теоремой об остатках для чисел.

Вектор

$$\beta = \{m_1, m_2, \dots, m_h\}$$

называется *вектором оснований*.

Стандартным набором остатков числа n относительно вектора оснований β называется вектор

$$n \pmod{\beta} = \{n_1, n_2, \dots, n_h\},$$

где $n_j \equiv n \pmod{m_j}$, $0 \leq n_j < m_j$, ($j = 1, 2, \dots, h$).

Для того чтобы можно было выполнять операцию деления (обращения) элементов по модулю β , следует выбирать в качестве чисел m_j различные простые целые числа. Тогда

$$n^{-1} \pmod{\beta} = \{n_1^{-1} \pmod{m_1}, n_2^{-1} \pmod{m_2}, \dots, n_h^{-1} \pmod{m_h}\}.$$

Основная трудность при работе с многомодульными системами заключается в сравнении величин целых чисел или определении знака числа без

перевода числа к обычному виду. Задача определения знака числа может быть решена с помощью преобразования числа x к представлению со смешанными основаниями, т. е. к виду

$$x = q_1 + q_2 m_1 + q_3 m_1 m_2 + \dots + q_h m_1 m_2 \dots m_{h-1}, \quad (9)$$

где $q_i < m_i$ ($i = 1, 2, \dots, h$).

Число q_h называется *старшим членом* числа x . Из (9) следует, что знак числа x совпадает со знаком его старшего члена. Пусть x представлен стандартным набором остатков $\{a_1, a_2, \dots, a_h\}$ относительно вектора оснований $\beta = \{m_1, m_2, \dots, m_h\}$. Из (9) следует

$$x \equiv q_1 \pmod{m_1},$$

значит, $q_1 = a_1$. Тогда

$$x - q_1 \pmod{\beta} = \{0, a_2 - q_1 \pmod{m_2}, \dots, a_h - q_1 \pmod{m_h}\}.$$

Так как первая цифра в представлении $x - q_1$ равна 0, то первую цифру всех последующих чисел можно не рассматривать. Значит, можно сократить длину вектора $x - q_1 \pmod{\beta}$, убрав его первую компоненту, а также сократить вектор оснований β на первую компоненту, которая не будет участвовать в дальнейших вычислениях, т. е.

$$\beta_2 = \{m_2, m_3, \dots, m_h\},$$

$$x - q_1 \pmod{\beta_2} = \{a_2 - q_1 \pmod{m_2}, \dots, a_h - q_1 \pmod{m_h}\}.$$

Найдем $m_1^{-1} \pmod{\beta_2}$ и вычислим

$$x_2 = (x - q_1) m_1^{-1} = q_2 + q_3 m_2 + q_4 m_2 m_3 + \dots + q_h m_2 \dots m_{h-1},$$

т. е. находим q_2 . Этот процесс повторяем до тех пор, пока не получим q_h . Если число q_h меньше, чем $\frac{m_h}{2}$, x – положительное число, если $q_h \geq \frac{m_h}{2}$, то x – отрицательное число. При $m_h = 2$ это определяется очень просто: если $q_h = 0$, то x – положительное число; если $q_h = 1$, то оно отрицательно. Поэтому удобно в качестве последнего модуля выбирать $m_h = 2$.

Пример 27. Определить знак числа x , представленного относительно вектора оснований $\beta = \{11, 7, 5, 3, 2\}$ стандартным набором остатков $\{4, 3, 2, 1, 1\}$.

Решение. Имеем $q_1 = 4$, откуда

$$x - q_1 = \{0, -1 \pmod{7}, -2 \pmod{5}, -3 \pmod{3}, -3 \pmod{2}\} = \{0, 6, 3, 0, 1\}.$$

Отбрасываем первые компоненты числа $x - q_1$ и вектора оснований:

$$\beta_2 = \{7, 5, 3, 2\}, \quad x - q_1 \pmod{\beta_2} = \{6, 3, 0, 1\}.$$

Вычислим

$$11^{-1} \pmod{\beta_2} = \{11^{-1} \pmod{7}, 11^{-1} \pmod{5}, 11^{-1} \pmod{3}, 11^{-1} \pmod{2}\} = \{2, 1, 2, 1\},$$

тогда

$$x_2 = (x - q_1)m_1^{-1} = \{6 \cdot 2 \pmod{7}, 3 \cdot 1 \pmod{5}, 0 \cdot 2 \pmod{3}, 1 \cdot 1 \pmod{2}\} = \{5, 3, 0, 1\},$$

откуда $q_2 = 5$.

$$x_2 - q_2 = \{0, -2 \pmod{5}, -5 \pmod{3}, -4 \pmod{2}\} = \{0, 3, 1, 0\}.$$

Отбрасываем первые компоненты векторов $x_2 - q_2$ и β_2 :

$$\beta_3 = \{5, 3, 2\}, \quad x_2 - q_2 \pmod{\beta_3} = \{3, 1, 0\}.$$

Вычисляем

$$7^{-1} \pmod{\beta_3} = \{7^{-1} \pmod{5}, 7^{-1} \pmod{3}, 7^{-1} \pmod{2}\} = \{3, 1, 1\}$$

и находим

$$x_3 = (x_2 - q_2)m_2^{-1} = \{3 \cdot 3 \pmod{5}, 1 \cdot 1 \pmod{3}, 0 \cdot 1 \pmod{2}\} = \{4, 1, 0\},$$

откуда $q_3 = 4$.

Далее,

$$x_3 - q_3 = \{0, -3 \pmod{3}, -4 \pmod{2}\} = \{0, 0, 0\}, \quad \beta_4 = \{3, 2\},$$

$$x_3 - q_3 \pmod{\beta_4} = \{0, 0\}.$$

Так как

$$5^{-1} \pmod{\beta_4} = \{5^{-1} \pmod{3}, 5^{-1} \pmod{2}\} = \{2, 1\},$$

то $x_4 = (x_3 - q_3)5^{-1} = \{0 \cdot 2 \pmod{3}, 0 \cdot 1 \pmod{2}\} = \{0, 0\}$, откуда $q_4 = 0$ и $x_4 - q_4 = \{0, 0\}$.

Опять отбрасываем первые компоненты полученных на последнем шаге векторов:

$$\beta_5 = \{2\}, \quad x_4 - q_4 \pmod{\beta_5} = \{0\}.$$

При умножении нуля на $3^{-1} \pmod{\beta_5} = 3^{-1} \pmod{2} = 1$ получим $q_5 = 0$. Следовательно, наше число x положительно.

Задачи

Задание 1

Пусть $\{f_i\}_{i=0,1,2,\dots}$ – последовательность Фибоначчи, т. е. $f_0 = 0$, $f_1 = 1$, $f_{i+2} = f_{i+1} + f_i$ ($i \geq 0$). Доказать следующие соотношения:

1). $f_1 + f_2 + \dots + f_n = f_{n+2} - 1$;

2). $f_1 + f_3 + \dots + f_{2n-1} = f_{2n}$;

Указание. Воспользоваться соотношениями $f_{i+1} = f_{i+2} - f_i$.

3). $f_2 + f_4 + \dots + f_{2n} = f_{2n+1} - 1$;

4). $f_1^2 + f_2^2 + \dots + f_n^2 = f_n f_{n+1}$;

Указание. Воспользоваться соотношениями $f_k^2 = f_k f_{k+1} - f_{k-1} f_k$.

5). $f_{n+m} = f_{n-1} f_m + f_n f_{m+1}$;

Указание. Воспользоваться математической индукцией по m .

6). Если $m|n$, то $f_m|f_n$.

7). $\text{НОД}(f_n, f_m) = f_{\text{НОД}(m,n)}$ (теорема Люка);

8). Если $f_m|f_n$, то $m|n$;

9). $f_{n+1} f_{n-1} - f_n^2 = (-1)^n$;

10). $f_{m+n} = f_n f_{m+1} + f_{n-1} f_m$.

Указание. Использовать матрицу A . Вычислить A^n ,

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Задание 2

Пусть $\varphi = \frac{1 + \sqrt{5}}{2}$ есть число "золотого сечения" и $\tilde{\varphi} = \frac{1 - \sqrt{5}}{2}$.

1). Показать, что $\cos \frac{\pi}{5} = \frac{\varphi}{2}$;

2). Представить $\varphi^n + \tilde{\varphi}^n$ как функцию от чисел Фибоначчи;

3). Представить φ^n как функцию от чисел Фибоначчи.

Задание 3

Найти наибольший общий делитель (НОД) чисел a и b , используя алгоритм Евклида:

1). $a = 481$, $b = 325$;

2). $a = 8771$, $b = 3206$;

3). $a = 473$, $b = 385$;

4). $a = 1235$, $b = 608$;

5). $a = 8075$, $b = 1463$;

6). $a = 1955$, $b = 1885$;

7). $a = 6105$, $b = 5863$;

8). $a = 8075$, $b = 1463$;

- 9). $a = c^m - 1$, $b = c^n - 1$, где $c \in \mathbb{Z}$, $m, n \in \mathbb{N}$;
 10). $a = c^m - d^m$, $b = c^n - d^n$, где $c, d \in \mathbb{Z}$, $m, n \in \mathbb{N}$, $\text{НОД}(c, d) = 1$.

Задание 4

Найти наибольший общий делитель чисел a и b и представить его в виде $\text{НОД}(a, b) = au + bv$, $u, v \in \mathbb{Z}$:

- | | |
|-----------------------------|------------------------------|
| 1). $a = 136$, $b = 51$; | 6). $a = 1020$, $b = 782$; |
| 2). $a = 34$, $b = 21$; | 7). $a = 889$, $b = 427$; |
| 3). $a = 187$, $b = 165$; | 8). $a = 1235$, $b = 608$; |
| 4). $a = 153$, $b = 96$; | 9). $a = 113$, $b = 27$; |
| 5). $a = 473$, $b = 385$; | 10). $a = 241$, $b = 96$. |

Задание 5

Используя бинарный алгоритм, найти наибольший общий делитель двух данных чисел, записанных в двоичной системе счисления:

- 1). 10100101, 1111101;
- 2). 1000100, 1101110;
- 3). 1000100, 110011;
- 4). 111011100111, 1011111011001;
- 5). 11000001000, 11110000100;
- 6). 1000001111, 1101100011;
- 7). 1011100101, 1000110001;
- 8). 1001011101, 1000110001;
- 9). 1000011100, 111010001;
- 10). 11110100011, 11101011101.

Задание 6

Найти все целочисленные решения уравнения:

- | | |
|--------------------------|--------------------------|
| 1). $12x + 21y = 1$; | 6). $192x + 54y = 18$; |
| 2). $13x - 8y = 7$; | 7). $138x + 74y = 4$; |
| 3). $21x - 23y = 3$; | 8). $91x + 29y = 12$; |
| 4). $184x + 272y = 40$; | 9). $101x + 83y = -11$; |
| 5). $133x - 29y = 7$; | 10). $37x - 14y = 57$. |

Задание 7

Разложить рациональное число в непрерывную (цепную) дробь:

1). $\frac{127}{52}$;

5). $-\frac{243}{112}$;

8). $-\frac{387}{49}$;

2). $-\frac{289}{113}$;

6). $-\frac{143}{27}$;

9). $\frac{139}{57}$;

3). $\frac{123}{100}$;

7). $\frac{24}{35}$;

10). $-\frac{203}{47}$.

4). $-\frac{145}{91}$;

Задание 8

Свернуть конечную непрерывную (цепную) дробь:

1). $[2, 4, 1, 3, 2]$;

6). $[-3, 2, 4, 5, 6, 3]$;

2). $[-2, 1, 2, 4, 5]$;

7). $[1, 2, 3, 5, 4]$;

3). $[-1, 3, 1, 2, 2, 3]$;

8). $[2, 3, 1, 4, 2, 2]$;

4). $[-3, 8, 2, 1, 4]$;

9). $[5, 3, 1, 2, 4, 3]$;

5). $[3, 2, 1, 4, 5]$;

10). $[-1, 5, 2, 4, 3, 2]$.

Задание 9

Разложить в непрерывную дробь. Найти период:

1). $\sqrt{2}$;

5). $\sqrt{18}$;

8). $\sqrt{47}$;

2). $\sqrt{7}$;

6). $\sqrt{21}$;

9). $\sqrt{13}$;

3). $\frac{5 + \sqrt{2}}{2}$;

7). $\sqrt{22}$;

10). $\sqrt{29}$.

4). $\sqrt{11}$;

Задание 10

Свернуть бесконечную периодическую цепную дробь. Представить иррациональность в виде $\frac{a + \sqrt{b}}{c}$, где a, b, c – целые числа:

1). $[(1, 2, 3, 2)]$;

3). $[0, 1, 1, 1, 1, (2, 2, 2)]$;

2). $[1, 2, 3, (4)]$;

4). $[3, (1, 6)]$;

- 5). $[5, (3, 2, 3, 10)]$; 8). $[3, 1, (5, 2)]$;
 6). $[(1, 1, 2, 2)]$; 9). $[1, 2, 3, (4, 3)]$;
 7). $[2, (1, 1)]$; 10). $[5, 6, (2, 1)]$.

Задание 11

Найти иррациональность $\alpha = [a_1, a_2, \dots, a_k, \alpha_k]$, если даны ее k -я подходящая дробь $\frac{P_k}{Q_k}$ и полное частное α_k . Представить иррациональность в

виде $\frac{a + \sqrt{b}}{c}$, где a, b, c – целые числа:

- | | |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------|
| 1). $\frac{P_k}{Q_k} = \frac{10}{3}, \alpha_k = \sqrt{2};$ | 6). $\frac{P_k}{Q_k} = \frac{11}{43}, \alpha_k = \sqrt{3} - 1;$ |
| 2). $\frac{P_k}{Q_k} = \frac{37}{13}, \alpha_k = \frac{1 + \sqrt{3}}{2};$ | 7). $\frac{P_k}{Q_k} = \frac{123}{43}, \alpha_k = \sqrt{2} + 1;$ |
| 3). $\frac{P_k}{Q_k} = \frac{43}{15}, \alpha_k = \frac{\sqrt{2} - 1}{3};$ | 8). $\frac{P_k}{Q_k} = \frac{33}{19}, \alpha_k = \frac{1 + \sqrt{2}}{2};$ |
| 4). $\frac{P_k}{Q_k} = \frac{19}{13}, \alpha_k = \frac{\sqrt{5} - 1}{2};$ | 9). $\frac{P_k}{Q_k} = \frac{31}{49}, \alpha_k = \frac{\sqrt{2} - 1}{2};$ |
| 5). $\frac{P_k}{Q_k} = \frac{47}{23}, \alpha_k = 1 + \sqrt{2};$ | 10). $\frac{P_k}{Q_k} = \frac{21}{37}, \alpha_k = \frac{\sqrt{7} - 1}{6}.$ |

Задание 12

Разложить в непрерывную дробь. Найти период:

- 1). $\sqrt{n^2 + 1}, n \in \mathbb{N};$
 2). $\sqrt{(mn)^2 + 2mn}, m, n \in \mathbb{N};$

Задание 13

Оценить точность приближения числа α данной подходящей дробью $\frac{P_k}{Q_k} = [a_1, a_1, \dots, a_k]:$

- 1). $\alpha = \sqrt{45}, \frac{P_k}{Q_k} = [6, 1, 2, 2, 2, 1, 12, 1, 2];$
 2). $\alpha = \sqrt{27}, \frac{P_k}{Q_k} = [5, 5, 10, 5, 10, 5];$
 3). $\alpha = 5 - \sqrt{3}, \frac{P_k}{Q_k} = [3, 3, 1, 2, 1, 2, 1];$
 4). $\alpha = \frac{5 + \sqrt{3}}{2}, \frac{P_k}{Q_k} = [3, 2, 1, 2, 1, 2, 1].$

Задание 14

Оценить близость k -й подходящей дроби к числу α :

1). $\alpha = \frac{7 - \sqrt{2}}{3}, \quad k = 5;$

2). $\alpha = \frac{7 - \sqrt{3}}{4}, \quad k = 6;$

3). $\alpha = \frac{1 + \sqrt{2}}{3}, \quad k = 5;$

4). $\alpha = \sqrt{3} + 1, \quad k = 7.$

Задание 15

Найти неполное частное и остаток от деления z_1 на z_2 в кольце целых гауссовых чисел $\mathbb{Z}[i]$:

1). $z_1 = 13 + 13i, \quad z_2 = 3 + 11i;$

2). $z_1 = 12 - 4i, \quad z_2 = 7 + 5i;$

3). $z_1 = 10 + 3i, \quad z_2 = 6 - 5i;$

4). $z_1 = 8 + 13i, \quad z_2 = 11 + 2i;$

5). $z_1 = 9 + 21i, \quad z_2 = 13 - 8i;$

6). $z_1 = 18 - 4i, \quad z_2 = 2 - 9i;$

7). $z_1 = 16 + 3i, \quad z_2 = 3 - 4i;$

8). $z_1 = 12 + 5i, \quad z_2 = 10 - 7i;$

9). $z_1 = 17 + 15i, \quad z_2 = 13 - 4i;$

10). $z_1 = 24 - i, \quad z_2 = 17 + 2i.$

Задание 16

Найти наибольший общий делитель двух чисел в кольце $\mathbb{Z}[i]$:

1). $13 + 13i, \quad 3 + 24i;$

2). $17 - 19i, \quad 14 + 31i;$

3). $17 + 5i, \quad 31 + 24i;$

4). $12 + 5i, \quad 10 - 3i;$

5). $16 + 4i, \quad 3 - 4i;$

6). $18 - 4i, \quad 2 - 11i;$

7). $31 + 27i, \quad 33 + i;$

8). $52 - 4i, \quad 5 - 15i;$

9). $58 + 6i, \quad 17 - 31i;$

10). $17 + 3i, \quad 11 - 5i.$

Задание 17

Является ли данное число приводимым в кольце $\mathbb{Z}[i]$? Если да, то разложить его в произведение неприводимых элементов этого кольца:

- | | |
|-----------------|-------------------|
| 1). $13 + 7i$; | 5). $14 + 5i$; |
| 2). $15 + 8i$; | 6). $17 + 11i$; |
| 3). $12 + 5i$; | 7). $19 + 13i$; |
| 4). $13 + 6i$; | 8). $-12 + 31i$. |

Задание 18

Является ли данное простое число приводимым элементом кольца $\mathbb{Z}[i]$? Если да, то представить его в виде произведения неприводимых элементов этого кольца:

- | | | |
|----------|----------|----------|
| 1). 113; | 4). 641; | 7). 809; |
| 2). 137; | 5). 701; | 8). 881; |
| 3). 281; | 6). 733; | 9). 929. |

Задание 19

Используя метод пробных делений, найти все простые числа в данном интервале:

- | | | |
|--------------------|--------------------|---------------------|
| 1). $[31, 109]$; | 5). $[201, 353]$; | 8). $[711, 827]$; |
| 2). $[43, 117]$; | 6). $[401, 523]$; | 9). $[723, 901]$; |
| 3). $[101, 159]$; | 7). $[517, 623]$; | 10). $[859, 999]$. |
| 4). $[127, 191]$; | | |

Задание 20

Используя расширенный алгоритм Евклида, решить сравнение:

- | | |
|---------------------------------|-----------------------------------|
| 1). $5x \equiv 3 \pmod{11}$; | 6). $31x \equiv 30 \pmod{101}$; |
| 2). $7x \equiv 2 \pmod{13}$; | 7). $15x \equiv 63 \pmod{97}$; |
| 3). $24x \equiv 15 \pmod{35}$; | 8). $21x \equiv -6 \pmod{43}$; |
| 4). $41x \equiv 27 \pmod{53}$; | 9). $23x \equiv 27 \pmod{37}$; |
| 5). $19x \equiv 2 \pmod{49}$; | 10). $35x \equiv 60 \pmod{121}$. |

Задание 21

Используя расширенный алгоритм Евклида, решить сравнение. Найти все решения по данному модулю:

- | | |
|------------------------------------|------------------------------------|
| 1). $42x \equiv 9 \pmod{81}$; | 6). $132x \equiv 154 \pmod{275}$; |
| 2). $125x \equiv 575 \pmod{45}$; | 7). $99x \equiv 108 \pmod{117}$; |
| 3). $93x \equiv 324 \pmod{33}$; | 8). $56x \equiv 133 \pmod{721}$; |
| 4). $64x \equiv 152 \pmod{44}$; | 9). $55x \equiv 95 \pmod{155}$; |
| 5). $424x \equiv 312 \pmod{120}$; | 10). $36x \equiv 24 \pmod{78}$. |

Задание 22

С помощью расширенного алгоритма Евклида найти a^{-1} в кольце \mathbb{Z}_m :

- | | |
|-------------------------|--------------------------|
| 1). $a = 45, m = 142$; | 6). $a = 37, m = 96$; |
| 2). $a = 17, m = 38$; | 7). $a = 16, m = 135$; |
| 3). $a = 83, m = 254$; | 8). $a = 47, m = 99$; |
| 4). $a = 51, m = 121$; | 9). $a = 85, m = 124$; |
| 5). $a = 28, m = 143$; | 10). $a = 99, m = 305$. |

Задание 23

Решить систему сравнений, используя метод последовательного решения пары сравнений:

- | | |
|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| 1). $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 3 \pmod{7} \\ x \equiv 7 \pmod{11} \end{cases}$ | 6). $\begin{cases} 2x \equiv 2 \pmod{3} \\ 5x \equiv 4 \pmod{11} \\ 9x \equiv 3 \pmod{17} \end{cases}$ |
| 2). $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{7} \\ x \equiv 1 \pmod{11} \end{cases}$ | 7). $\begin{cases} 7x \equiv 1 \pmod{12} \\ 4x \equiv 4 \pmod{7} \\ 8x \equiv -1 \pmod{5} \end{cases}$ |
| 3). $\begin{cases} 2x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{5} \\ 3x \equiv 1 \pmod{4} \\ x \equiv 10 \pmod{13} \end{cases}$ | 8). $\begin{cases} 6x \equiv 1 \pmod{11} \\ 5x \equiv 3 \pmod{12} \\ 3x \equiv 5 \pmod{7} \end{cases}$ |
| 4). $\begin{cases} 3x \equiv 1 \pmod{5} \\ 2x \equiv 6 \pmod{7} \\ x \equiv 10 \pmod{11} \end{cases}$ | 9). $\begin{cases} 5x \equiv 6 \pmod{9} \\ 7x \equiv 3 \pmod{13} \\ 8x \equiv 21 \pmod{23} \end{cases}$ |
| 5). $\begin{cases} 2x \equiv 2 \pmod{5} \\ 3x \equiv 2 \pmod{7} \\ 5x \equiv 11 \pmod{13} \end{cases}$ | 10). $\begin{cases} 3x \equiv 6 \pmod{7} \\ 8x \equiv 13 \pmod{15} \\ 9x \equiv 3 \pmod{26} \end{cases}$ |

Задание 24

Решить систему сравнений, используя формулу

$$x \equiv \sum_{i=1}^k a_i M_i N_i \pmod{M} :$$

- | | |
|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| 1). $\begin{cases} 2x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{5} \\ 3x \equiv 1 \pmod{4} \\ x \equiv 10 \pmod{13} \end{cases}$ | 6). $\begin{cases} 5x \equiv 6 \pmod{9} \\ 7x \equiv 3 \pmod{13} \\ 8x \equiv 21 \pmod{23} \end{cases}$ |
| 2). $\begin{cases} 3x \equiv 1 \pmod{5} \\ 2x \equiv 6 \pmod{7} \\ x \equiv 10 \pmod{11} \end{cases}$ | 7). $\begin{cases} 3x \equiv 6 \pmod{7} \\ 8x \equiv 13 \pmod{15} \\ 9x \equiv 3 \pmod{26} \end{cases}$ |
| 3). $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{7} \\ x \equiv 1 \pmod{11} \end{cases}$ | 8). $\begin{cases} 2x \equiv 2 \pmod{5} \\ 3x \equiv 2 \pmod{7} \\ 5x \equiv 11 \pmod{13} \end{cases}$ |
| 4). $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 3 \pmod{7} \\ x \equiv 7 \pmod{11} \end{cases}$ | 9). $\begin{cases} 2x \equiv 2 \pmod{3} \\ 5x \equiv 4 \pmod{11} \\ 9x \equiv 3 \pmod{17} \end{cases}$ |
| 5). $\begin{cases} 6x \equiv 1 \pmod{11} \\ 5x \equiv 3 \pmod{12} \\ 3x \equiv 5 \pmod{7} \end{cases}$ | 10). $\begin{cases} 7x \equiv 1 \pmod{12} \\ 4x \equiv 4 \pmod{7} \\ 8x \equiv -1 \pmod{5} \end{cases}$ |

Задание 25

Вычислить значение функции Эйлера от числа $n \in \mathbb{N}$:

- | | | |
|------------------|------------------|------------------|
| 1). $n = 2044$; | 5). $n = 625$; | 8). $n = 1125$; |
| 2). $n = 1546$; | 6). $n = 1120$; | 9). $n = 1840$; |
| 3). $n = 6875$; | 7). $n = 999$; | 10). $n = 312$. |
| 4). $n = 240$; | | |

Задание 26

Вычислить значение функции Мебиуса от числа $n \in \mathbb{N}$:

- | | | |
|------------------|------------------|------------------|
| 1). $n = 165$; | 5). $n = 1955$; | 8). $n = 7735$; |
| 2). $n = 7007$; | 6). $n = 663$; | 9). $n = 855$; |
| 3). $n = 1230$; | 7). $n = 1540$; | 10). $n = 880$. |
| 4). $n = 7161$; | | |

Задание 27

Используя теорему Ферма, найти a^{-1} в кольце \mathbb{Z}_p :

- | | |
|-------------------------|-------------------------|
| 1). $a = 15, p = 47$; | 6). $a = 24, p = 37$; |
| 2). $a = 6, p = 19$; | 7). $a = 15, p = 41$; |
| 3). $a = 11, p = 31$; | 8). $a = 19, p = 29$; |
| 4). $a = 5, p = 43$; | 9). $a = 17, p = 23$; |
| 5). $a = 41, p = 113$; | 10). $a = 21, p = 53$. |

Задание 28

Используя теорему Эйлера, найти a^{-1} в кольце \mathbb{Z}_p :

- | | |
|------------------------|-------------------------|
| 1). $a = 2, m = 35$; | 6). $a = 14, m = 33$; |
| 2). $a = 5, m = 36$; | 7). $a = 15, m = 32$; |
| 3). $a = 11, m = 42$; | 8). $a = 17, m = 38$; |
| 4). $a = 13, m = 18$; | 9). $a = 16, m = 45$; |
| 5). $a = 25, m = 44$; | 10). $a = 55, m = 84$. |

Задание 29

Найти минимальное число умножений, требующихся для вычисления a^n , $n \in \mathbb{N}$:

- | | | |
|-----------------|-----------------|-------------------|
| 1). $n = 145$; | 5). $n = 231$; | 8). $n = 322$; |
| 2). $n = 98$; | 6). $n = 148$; | 9). $n = 1026$; |
| 3). $n = 234$; | 7). $n = 196$; | 10). $n = 1102$. |
| 4). $n = 165$; | | |

Задание 30

Найти минимальное число сложений, требующихся для вычисления числа AB , $A, B \in \mathbb{Z}$:

- | | | |
|----------------------|----------------------|------------------------|
| 1). $143 \cdot 95$; | 5). $123 \cdot 49$; | 8). $187 \cdot 97$; |
| 2). $194 \cdot 47$; | 6). $213 \cdot 57$; | 9). $365 \cdot 81$; |
| 3). $83 \cdot 56$; | 7). $311 \cdot 63$; | 10). $423 \cdot 101$. |
| 4). $63 \cdot 97$; | | |

Задание 31

Найти примитивный корень по модулю n :

- | | | |
|----------------|-----------------|-----------------|
| 1). $n = 54$; | 5). $n = 125$; | 8). $n = 94$; |
| 2). $n = 50$; | 6). $n = 49$; | 9). $n = 121$; |
| 3). $n = 46$; | 7). $n = 98$; | 10). $n = 58$. |
| 4). $n = 47$; | | |

Задание 32

Найти все примитивные корни по модулю n :

- | | | |
|-----------------|-----------------|-----------------|
| 1). $n = 46$; | 5). $n = 121$; | 8). $n = 54$; |
| 2). $n = 58$; | 6). $n = 47$; | 9). $n = 98$; |
| 3). $n = 125$; | 7). $n = 94$; | 10). $n = 49$. |
| 4). $n = 50$; | | |

Задание 33

Является ли мультипликативная группа кольца \mathbb{Z}_n циклической? Найти порядок группы. Если группа циклическая, найти образующую:

- | | | |
|-----------------|-----------------|-----------------|
| 1). $n = 125$; | 5). $n = 81$; | 8). $n = 94$; |
| 2). $n = 26$; | 6). $n = 98$; | 9). $n = 46$; |
| 3). $n = 486$; | 7). $n = 242$; | 10). $n = 58$. |
| 4). $n = 121$; | | |

Задание 34

Описать структуру мультипликативной группы кольца \mathbb{Z}_n . Найти порядок группы. Найти элемент максимального порядка:

- | | | |
|-----------------|-----------------|-----------------|
| 1). $n = 15$; | 5). $n = 100$; | 8). $n = 45$; |
| 2). $n = 56$; | 6). $n = 44$; | 9). $n = 48$; |
| 3). $n = 108$; | 7). $n = 68$; | 10). $n = 36$. |
| 4). $n = 52$; | | |

Задание 35

Определить, является ли данное число n по основанию a

а) псевдопростым?

б) сильно псевдопростым?

- | | |
|-------------------------|-------------------------|
| 1). $a = 7, n = 25$; | 6). $a = 5, n = 213$; |
| 2). $a = 5, n = 217$; | 7). $a = 8, n = 63$; |
| 3). $a = 6, n = 217$; | 8). $a = 12, n = 145$; |
| 4). $a = 8, n = 105$; | 9). $a = 14, n = 195$; |
| 5). $a = 13, n = 105$; | 10). $a = 8, n = 255$. |

Задание 36

Число x представлено стандартным набором остатков относительно вектора оснований $\beta = \{3, 5, 7, 11, 2\}$. Не находя числа x , определить его знак:

- | | |
|------------------------|-------------------------|
| 1). $[1, 2, 1, 5, 1];$ | 6). $[1, 1, 0, 3, 1];$ |
| 2). $[2, 2, 5, 3, 1];$ | 7). $[2, 2, 1, 9, 1];$ |
| 3). $[2, 3, 5, 7, 1];$ | 8). $[0, 2, 5, 1, 0];$ |
| 4). $[2, 3, 2, 1, 1];$ | 9). $[1, 3, 4, 5, 1];$ |
| 5). $[1, 4, 1, 3, 1];$ | 10). $[2, 1, 2, 3, 1].$ |

Ответы и указания

2. 1). Указание: $-\cos\left(\frac{\pi}{5}\right) = \cos\left(\pi - \frac{\pi}{5}\right)$ представить через половинный угол; 2). Указание: Использовать соотношения $f_n = \frac{\varphi^n - \tilde{\varphi}^n}{\varphi - \tilde{\varphi}}$, $\varphi\tilde{\varphi} = -1$, $1 - \varphi = \tilde{\varphi}$; 3). Указание: использовать формулы, полученные в задаче 2.

3. 1). 13; 2). 7; 3). 11; 4). 19; 5). 19; 6). 5; 7). 11; 8). 19; 9). $c^d - 1$, где $d = \text{НОД}(m, n)$; 10). $c^t - d^t$, где $t = \text{НОД}(m, n)$. Указание: воспользоваться соотношением: $c^m - d^m = (c^n - d^n)c^{m-n} + (c^{m-n} - d^{m-n})d^n$.

4. 1). $17 = (-1) \cdot 136 + 3 \cdot 51$; 2). $1 = (-8) \cdot 34 + 13 \cdot 21$; 3). $11 = (-7) \cdot 187 + 8 \cdot 165$; 4). $3 = (-5) \cdot 153 + 8 \cdot 96$; 5). $11 = (-13) \cdot 473 + 16 \cdot 385$; 6). $34 = 10 \cdot 1020 - 13 \cdot 782$; 7). $7 = (-12) \cdot 889 + 25 \cdot 427$; 8). $19 = 1 \cdot 1235 - 2 \cdot 608$; 9). $1 = 11 \cdot 113 - 46 \cdot 27$; 10). $1 = (-47) \cdot 241 + 118 \cdot 96$.

5. 1). 101_2 ; 2). 10_2 ; 3). 10001_2 ; 4). 101_2 ; 5). 100_2 ; 6). 10001_2 ; 7). 11_2 ; 8). 1011_2 ; 9). 1111_2 ; 10). 101_2 .

6. 1). \emptyset ; 2). $x = -21 + 8t$, $y = -35 + 13t$; 3). $x = 33 + 23t$, $y = 30 + 21t$; 4). $x = 15 - 34t$, $y = -10 + 23t$; 5). $x = -3 + 29t$, $y = -14 + 133t$; 6). $x = 6 - 9t$, $y = -21 + 32t$; 7). $x = -30 - 37t$, $y = 56 + 69t$; 8). $x = 3 - 29t$, $y = -9 + 91t$; 9). $x = 4 - 83t$, $y = -5 + 101t$; 10). $x = -3 + 14t$, $y = -12 + 37t$.

7. 1). $[2, 2, 3, 1, 5]$; 2). $[-3, 2, 3, 1, 5, 2]$; 3). $[1, 4, 2, 1, 7]$; 4). $[-2, 2, 2, 5, 1, 2]$; 5). $[-3, 1, 4, 1, 8, 2]$; 6). $[-6, 1, 2, 2, 1, 2]$; 7). $[0, 1, 2, 5, 2]$; 8). $[-8, 9, 1, 4]$; 9). $[2, 2, 3, 1, 1, 3]$; 10). $[-5, 1, 2, 7, 2]$.

8. 1). $\frac{95}{43}$; 2). $-\frac{89}{68}$; 3). $-\frac{65}{89}$; 4). $-\frac{337}{117}$; 5). $\frac{245}{73}$; 6). $-\frac{2349}{920}$; 7). $\frac{222}{155}$; 8). $\frac{233}{103}$; 9). $\frac{817}{155}$; 10). $-\frac{298}{365}$.

9. 1). $[1, (2)]$; 2). $[2, (1, 1, 1, 4)]$; 3). $[3, (4, 1)]$; 4). $[3, (3, 6)]$; 5). $[4, (4, 8)]$; 6). $[4, (1, 1, 2, 1, 1, 8)]$; 7). $[4, (1, 2, 4, 2, 1, 8)]$; 8). $[6, (1, 5, 1, 12)]$; 9). $[3, (1, 1, 1, 1, 6)]$; 10). $[5, (2, 1, 1, 2, 10)]$.

10. 1). $\frac{2 + \sqrt{14}}{4}$; 2). $\frac{18 - \sqrt{5}}{11}$; 3). $\frac{10 - \sqrt{2}}{14}$; 4). $\sqrt{15}$; 5). $\sqrt{28}$; 6). $\frac{9 + \sqrt{221}}{14}$; 7). $\frac{3 + \sqrt{5}}{2}$; 8). $3 + \frac{\sqrt{35}}{7}$; 9). $\frac{4 + \sqrt{3}}{4}$; 10). $\frac{306 - \sqrt{3}}{59}$.

11. 1). $\frac{57 - \sqrt{2}}{17}$; 2). $\frac{166 + \sqrt{3}}{59}$; 3). $\frac{396 - \sqrt{2}}{138}$; 4). $\frac{559 + \sqrt{5}}{382}$; 5). $\frac{986 - \sqrt{2}}{482}$; 6). $\frac{1029 - \sqrt{3}}{4026}$; 7). $\frac{3428 - \sqrt{2}}{1198}$; 8). $\frac{15 - 2\sqrt{2}}{7}$; 9). $\frac{2961 - 2\sqrt{2}}{4681}$; 10). $\frac{904 + \sqrt{7}}{1593}$.

12. 1). $[n, (2n)]$; 2). $[mn, (1, 2mn)]$.

13. 1). $< \frac{1}{963 \cdot 2255} \approx 0,0000005$; 2). $< \frac{1}{157801 \cdot 13515} \approx 0,0000000005$; 3). $< \frac{1}{153 \cdot 56} \approx 0,0001167$; 4). $< \frac{1}{41 \cdot 112} \approx 0,0002178$.

14. 1). $< \frac{1}{2396 \cdot 985} \approx 0,0000042$; 2). $< \frac{1}{571 \cdot 3691} \approx 0,0000005$;
 3). $< \frac{1}{169 \cdot 1393} \approx 0,0000042$; 4). $< \frac{1}{41 \cdot 56} \approx 0,0004355$.
15. 1). $z_1 = (1 - i)z_2 + (-1 + 5i)$; 2). $z_1 = (1 - i)z_2 - 2i$;
 3). $z_1 = (1 + i)z_2 + (-1 + 2i)$; 4). $z_1 = (1 + i)z_2 - 1$; 5). $z_1 = iz_2 + (1 + 8i)$;
 6). $z_1 = (1 + 2i)z_2 + (-2 + i)$; 7). $z_1 = (1 + 3i)z_2 + (1 - 2i)$;
 8). $z_1 = (1 + i)z_2 + (-5 + 2i)$; 9). $z_1 = (1 + i)z_2 + 6i$; 10). $z_1 = z_2 + (7 - 3i)$.
16. 1). $2 + 3i$; 2). $3 + 2i$; 3). $5 + 2i$; 4). $-i$; 5). 1 ; 6). $2 - i$; 7). $1 + i$;
 8). $1 + 3i$; 9). $-1 - 7i$; 10). $-1 + i$.
17. 1). $(1 + i)(10 - 3i)$; 2). $(4 + i)^2$; 3). $(2 + 3i)(3 - 2i)$; 4). $(2 - i)(4 + 5i)$;
 5). $(2 - 3i)(1 + 4i)$; 6). $(4 + 5i)(1 + i)(1 - 2i)$; 7). $(7 + 2i)(1 - i)(1 + 2i)$;
 8). $(4 + i)(3 + 2i)(1 + 2i)$.
18. 1). $(8 + 7i)(8 - 7i)$; 2). $(11 + 4i)(11 - 4i)$; 3). $(16 + 5i)(16 - 5i)$;
 4). $(25 + 4i)(25 - 4i)$; 5). $(26 + 5i)(26 - 5i)$; 6). $(27 + 2i)(27 - 2i)$; 7). $(28 + 5i)(28 - 5i)$;
 8). $(25 + 16i)(25 - 16i)$; 9). $(23 + 20i)(23 - 20i)$.
20. 1). $5 \pmod{11}$; 2). $4 \pmod{13}$; 3). $5 \pmod{35}$; 4). $11 \pmod{53}$;
 5). $13 \pmod{49}$; 6). $14 \pmod{101}$; 7). $43 \pmod{97}$; 8). $12 \pmod{43}$;
 9). $6 \pmod{37}$; 10). $19 \pmod{121}$.
21. 1). $6, 33, 60 \pmod{81}$; 2). $1, 10, 19, 28, 37 \pmod{45}$; 3). $1, 12, 23 \pmod{33}$;
 4). $1, 12, 23, 34 \pmod{44}$; 5). $3, 18, 33, 48, 63, 78, 93, 108 \pmod{120}$; 6). $22, 47,$
 $72, 97, 122, 147, 172, 197, 222, 247, 272 \pmod{275}$; 7). $7, 20, 35, 46, 59, 72, 85,$
 $98, 111 \pmod{117}$; 8). $41, 144, 247, 350, 453, 556, 659 \pmod{721}$; 9). $13, 44,$
 $75, 106, 137 \pmod{155}$; 10). $5, 18, 31, 44, 57, 70 \pmod{78}$.
22. 1). 101 ; 2). 9 ; 3). 101 ; 4). 19 ; 5). 46 ; 6). 13 ; 7). 76 ; 8). 59 ;
 9). 89 ; 10). 114 .
23. 1). $73 \pmod{154}$; 2). $89 \pmod{1155}$; 3). $127 \pmod{780}$;
 4). $87 \pmod{385}$; 5). $101 \pmod{455}$; 6). $91 \pmod{561}$; 7). $43 \pmod{420}$;
 8). $123 \pmod{924}$; 9). $201 \pmod{2691}$; 10). $191 \pmod{2730}$.
24. 1). $127 \pmod{780}$; 2). $87 \pmod{385}$; 3). $89 \pmod{1155}$;
 4). $73 \pmod{154}$; 5). $123 \pmod{924}$; 6). $201 \pmod{2691}$; 7). $191 \pmod{2730}$;
 8). $101 \pmod{455}$; 9). $91 \pmod{561}$; 10). $43 \pmod{420}$.
25. 1). 864 ; 2). 772 ; 3). 5000 ; 4). 64 ; 5). 500 ; 6). 384 ; 7). 648 ;
 8). 600 ; 9). 704 ; 10). 96 .
26. 1). -1 ; 2). 0 ; 3). 1 ; 4). 1 ; 5). -1 ; 6). -1 ; 7). 0 ; 8). 1 ; 9). 0 ;
 10). 0 .
27. 1). 22 ; 2). 16 ; 3). 17 ; 4). 26 ; 5). 102 ; 6). 17 ; 7). 11 ; 8). 26 ;
 9). 19 ; 10). 48 .
28. 1). 18 ; 2). 29 ; 3). 23 ; 4). 7 ; 5). 37 ; 6). 26 ; 7). 15 ; 8). 9 ; 9). 31 ;

10). 55.

29. 1). 9; 2). 8; 3). 11; 4). 10; 5). 12; 6). 9; 7). 9; 8). 10; 9). 11; 10). 14.

30. 1). 11; 2). 9; 3). 7; 4). 10; 5). 7; 6). 8; 7). 10; 8). 8; 9). 8; 10). 9.

31. 1). [5]; 2). [3]; 3). [5]; 4). [5]; 5). [2]; 6). [3]; 7). [3]; 8). [5]; 9). [2]; 10). [3].

32. 1). {[5], [33], [43], [17], [11], [21], [19], [15], [7], [37]};

2). {[3], [27], [11], [21], [15], [19], [55], [31], [47], [37], [43], [39]};

3). {[2], [8], [3], [12], [48], [67], [72], [38], [27], [108], [103], [37], [23], [92], [97], [13], [52], [83], [78], [62], [123], [117], [122], [113], [77], [58], [53], [87], [98], [17], [22], [88], [102], [33], [28], [112], [73], [42], [47], [63]};

4). {[3], [27], [37], [33], [47], [23], [13], [17]};

5). {[2], [8], [7], [28], [85], [29], [116], [101], [41], [51], [83], [90], [73], [50], [79], [74], [95], [17], [68], [30], [117], [57], [107], [18], [72], [46], [63], [39], [35], [19], [62], [6], [24], [96], [84], [13], [52], [106], [61]};

6). {[5], [31], [23], [11], [40], [13], [43], [41], [38], [10], [15], [22], [33], [26], [39], [35], [29], [20], [30], [45], [44], [19]};

7). {[5], [31], [23], [11], [87], [13], [43], [41], [85], [57], [15], [69], [33], [73], [39], [35], [29], [67], [77], [45], [91], [19]};

8). {[5], [47], [41], [29], [23], [11]};

9). {[3], [47], [61], [59], [75], [87], [89], [17], [5], [45], [73], [33]};

10). {[3], [47], [12], [10], [26], [38], [40], [17], [5], [45], [24], [33]}.

33. 1). Циклическая группа порядка 100 с образующей [2]; 2). Циклическая группа порядка 12 с образующей [7]; 3). Циклическая группа порядка 162 с образующей [5]; 4). Циклическая группа порядка 110 с образующей [2]; 5). Циклическая группа порядка 54 с образующей [2]; 6). Циклическая группа порядка 42 с образующей [3]; 7). Циклическая группа порядка 110 с образующей [7]; 8). Циклическая группа порядка 46 с образующей [5]; 9). Циклическая группа порядка 22 с образующей [5]; 10). Циклическая группа порядка 28 с образующей [3].

34. 1). $|\mathbb{Z}_3^* \times \mathbb{Z}_5^*| = 8$, $([2], [2]) \rightarrow [2]_{15}$, $ord([2]) = 4$;

2). $|\mathbb{Z}_{23}^* \times \mathbb{Z}_7^*| = 24$, $([3], [3]) \rightarrow [3]_{56}$, $ord([3]) = 6$;

3). $|\mathbb{Z}_{22}^* \times \mathbb{Z}_{33}^*| = 36$, $([3], [2]) \rightarrow [83]_{108}$, $ord([83]) = 18$;

4). $|\mathbb{Z}_{22}^* \times \mathbb{Z}_{13}^*| = 24$, $([3], [2]) \rightarrow [15]_{52}$, $ord([15]) = 12$;

5). $|\mathbb{Z}_{22}^* \times \mathbb{Z}_{52}^*| = 40$, $([3], [2]) \rightarrow [27]_{100}$, $ord([27]) = 20$;

6). $|\mathbb{Z}_{22}^* \times \mathbb{Z}_{11}^*| = 20$, $([3], [2]) \rightarrow [35]_{44}$, $ord([35]) = 10$;

7). $|\mathbb{Z}_{22}^* \times \mathbb{Z}_{17}^*| = 32$, $([3], [3]) \rightarrow [3]_{68}$, $ord([3]) = 16$;

8). $|\mathbb{Z}_5^* \times \mathbb{Z}_{32}^*| = 24$, $([2], [2]) \rightarrow [2]_{45}$, $ord([2]) = 12$;

9). $|\mathbb{Z}_{2^4}^* \times \mathbb{Z}_3^*| = 16$, $([3], [2]) \rightarrow [35]_{48}$, $ord([35]) = 4$;

10). $|\mathbb{Z}_{2^2}^* \times \mathbb{Z}_{3^2}^*| = 12$, $([3], [2]) \rightarrow [11]_{36}$, $ord([11]) = 6$.

35. 1). Псевдопростое, сильно псевдопростое; 2). Псевдопростое, не является сильно псевдопростым; 3). Псевдопростое, сильно псевдопростое; 4). Псевдопростое, не является сильно псевдопростым; 5). Псевдопростое, не является сильно псевдопростым; 6). Не является псевдопростым и сильно псевдопростым; 7). Псевдопростое, не является сильно псевдопростым; 8). Псевдопростое, сильно псевдопростое; 9). Псевдопростое, не является сильно псевдопростым; 10). Не является псевдопростым и сильно псевдопростым.

36. 1). $x < 0$; 2). $x > 0$; 3). $x < 0$; 4). $x > 0$; 5). $x < 0$; 6). $x > 0$; 7). $x < 0$; 8). $x > 0$; 9). $x < 0$; 10). $x < 0$.

Задачи для самостоятельного решения

Задание 1

С помощью алгоритма Евклида найти наибольший общий делитель двух чисел. Найти наименьшее общее кратное этих же чисел:

- | | | |
|---------------|----------------|----------------|
| 1. 345, 253; | 11. 1023, 735; | 21. 955, 785; |
| 2. 482, 344; | 12. 1020, 364; | 22. 843, 522; |
| 3. 868, 344; | 13. 1133, 517; | 23. 746, 852; |
| 4. 1028, 528; | 14. 1256, 662; | 24. 957, 377; |
| 5. 456, 282; | 15. 996, 510; | 25. 646, 456; |
| 6. 844, 564; | 16. 854, 245; | 26. 258, 147; |
| 7. 1236, 852; | 17. 1111, 407; | 27. 583, 231; |
| 8. 403, 845; | 18. 884, 561; | 28. 646, 343; |
| 9. 451, 1927; | 19. 1486, 328; | 29. 497, 322; |
| 10. 978, 636; | 20. 581, 497; | 30. 1144, 845. |

Задание 2

Найти наибольший общий делитель чисел алгоритмом Евклида, используя центрированное деление:

- | | | |
|------------------|----------------|----------------|
| 1. 2431, -385; | 11. 236, -193; | 21. 333, -181; |
| 2. 2431, -132; | 12. 592, -483; | 22. 294, -173; |
| 3. 813, -132; | 13. 538, -328; | 23. 937, -258; |
| 4. 819, -495; | 14. 453, -197; | 24. 843, -368; |
| 5. 1540, -819; | 15. 357, -83; | 25. 757, -383; |
| 6. 11011, -168; | 16. 876, -257; | 26. 473, -281; |
| 7. 11011, -2975; | 17. 391, -173; | 27. 267, -83; |
| 8. 168, -363; | 18. 943, -183; | 28. 379, -181; |
| 9. 526, -346; | 19. 357, -191; | 29. 653, -137; |
| 10. 453, -328; | 20. 457, -184; | 30. 385, -168. |

Задание 3

Найти наибольший общий делитель двух чисел, представленных в двоичной системе счисления, используя бинарный алгоритм:

1. 111111111, 101101111;
2. 111111100, 101101100;
3. 10001101101, 1000000101;
4. 10011101000, 1010010110;
5. 1111100100, 111111110;
6. 1101010110, 11110101;
7. 10001010111, 110010111;
8. 1101110100, 1000110001;
9. 10111001110, 101001000;
10. 1001000101, 111110001;
11. 1110111011, 1100010001;
12. 1101001011, 1000001010;
13. 1011101010, 1101010100;
14. 1110111101, 101111001;
15. 1010000110, 111001000;
16. 100000010, 10010011;
17. 1001000111, 11100111;
18. 1010000110, 101010111;
19. 111110001, 101000010;
20. 10001111000, 1101001101;
21. 101011001, 11111101;
22. 111100010, 101011000;
23. 1101100100, 101011000;
24. 10000000100, 100010000;
25. 111001000, 100011010;
26. 1101001100, 1000110100;
27. 10011010100, 1101010100;
28. 1101001101, 110010011;
29. 11110000111, 111000011;
30. 1111010010, 1001111100.

Задание 4

Найти наибольший общий делитель чисел и коэффициенты Безу, воспользовавшись расширенным алгоритмом Евклида:

- | | | |
|---------------|----------------|---------------|
| 1. 867, 231; | 11. 886, 358; | 21. 483, 357; |
| 2. 979, 346; | 12. 453, 391; | 22. 891, 327; |
| 3. 453, 123; | 13. 657, 578; | 23. 644, 538; |
| 4. 377, 285; | 14. 678, 526; | 24. 346, 283; |
| 5. 734, 992; | 15. 316, 218; | 25. 459, 196; |
| 6. 1178, 943; | 16. 328, 254; | 26. 948, 754; |
| 7. 854, 348; | 17. 236, 168; | 27. 886, 546; |
| 8. 943, 562; | 18. 254, 178; | 28. 315, 192; |
| 9. 592, 484; | 19. 303, 124; | 29. 528, 452; |
| 10. 495, 343; | 20. 1094, 278; | 30. 348, 194. |

Задание 5

Разложить рациональное число в непрерывную (цепную) дробь:

- | | | |
|-------------------------|--------------------------|--------------------------|
| 1. $\frac{153}{37}$; | 11. $\frac{189}{67}$; | 21. $\frac{343}{214}$; |
| 2. $-\frac{171}{35}$; | 12. $-\frac{266}{87}$; | 22. $-\frac{453}{217}$; |
| 3. $\frac{128}{91}$; | 13. $\frac{237}{149}$; | 23. $\frac{457}{142}$; |
| 4. $-\frac{452}{131}$; | 14. $-\frac{137}{24}$; | 24. $-\frac{597}{438}$; |
| 5. $\frac{473}{84}$; | 15. $\frac{277}{145}$; | 25. $\frac{593}{194}$; |
| 6. $-\frac{345}{171}$; | 16. $-\frac{354}{191}$; | 26. $-\frac{762}{323}$; |
| 7. $\frac{231}{43}$; | 17. $\frac{153}{87}$; | 27. $\frac{697}{321}$; |

- | | | | | | |
|-----|--------------------|-----|---------------------|-----|---------------------|
| 8. | $-\frac{147}{25};$ | 18. | $-\frac{931}{346};$ | 28. | $-\frac{453}{142};$ |
| 9. | $\frac{143}{93};$ | 19. | $\frac{149}{93};$ | 29. | $\frac{771}{325};$ |
| 10. | $-\frac{248}{47};$ | 20. | $-\frac{267}{141};$ | 30. | $-\frac{358}{97}.$ |

Задание 6

Разложить иррациональное число в непрерывную (цепную) дробь. Найти период:

- | | | | | | |
|-----|--------------|-----|--------------|-----|--------------|
| 1. | $\sqrt{31};$ | 11. | $\sqrt{21};$ | 21. | $\sqrt{43};$ |
| 2. | $\sqrt{44};$ | 12. | $\sqrt{58};$ | 22. | $\sqrt{28};$ |
| 3. | $\sqrt{59};$ | 13. | $\sqrt{22};$ | 23. | $\sqrt{46};$ |
| 4. | $\sqrt{41};$ | 14. | $\sqrt{67};$ | 24. | $\sqrt{71};$ |
| 5. | $\sqrt{62};$ | 15. | $\sqrt{23};$ | 25. | $\sqrt{47};$ |
| 6. | $\sqrt{34};$ | 16. | $\sqrt{69};$ | 26. | $\sqrt{52};$ |
| 7. | $\sqrt{57};$ | 17. | $\sqrt{29};$ | 27. | $\sqrt{55};$ |
| 8. | $\sqrt{14};$ | 18. | $\sqrt{70};$ | 28. | $\sqrt{32};$ |
| 9. | $\sqrt{19};$ | 19. | $\sqrt{33};$ | 29. | $\sqrt{53};$ |
| 10. | $\sqrt{61};$ | 20. | $\sqrt{73};$ | 30. | $\sqrt{54}.$ |

Задание 7

Свернуть непрерывную дробь:

- | | | | |
|-----|------------------------|-----|-----------------------|
| 1. | $[3, 2, 1, 4, 5,];$ | 16. | $[-1, 1, 2, 1, 3];$ |
| 2. | $[4, 1, 2, 3, 8];$ | 17. | $[4, 4, 2, 4, 2];$ |
| 3. | $[5, 6, 1, 2, 2];$ | 18. | $[-5, 2, 1, 1, 3];$ |
| 4. | $[1, 1, 2, 3, 2];$ | 19. | $[3, 3, 3, 2, 2];$ |
| 5. | $[-1, 4, 5, 6, 2];$ | 20. | $[-2, 2, 2, 3, 2];$ |
| 6. | $[-3, 5, 4, 1, 1, 2];$ | 21. | $[4, 1, 1, 4, 1, 2];$ |
| 7. | $[0, 2, 1, 3, 5, 4];$ | 22. | $[5, 2, 2, 3, 4];$ |
| 8. | $[2, 2, 1, 7, 4];$ | 23. | $[-3, 1, 1, 1, 2];$ |
| 9. | $[1, 4, 4, 5, 3];$ | 24. | $[-5, 2, 4, 3, 5];$ |
| 10. | $[-4, 3, 2, 1, 2];$ | 25. | $[3, 4, 1, 1, 2].$ |
| 11. | $[-2, 3, 3, 4, 5];$ | 26. | $[-2, 1, 1, 1, 5];$ |

- | | | | |
|-----|---------------------|-----|---------------------|
| 12. | $[-2, 1, 1, 2, 3];$ | 27. | $[4, 5, 4, 5, 3];$ |
| 13. | $[-3, 4, 5, 1, 2];$ | 28. | $[-2, 2, 2, 1, 2];$ |
| 14. | $[-1, 1, 2, 2, 3];$ | 29. | $[-4, 3, 2, 3, 5];$ |
| 15. | $[6, 1, 1, 2, 3];$ | 30. | $[3, 2, 3, 5, 4].$ |

Задание 8

Свернуть периодическую непрерывную дробь (период указан в круглых скобках):

- | | | | | | |
|-----|-------------------|-----|----------------------|-----|----------------------|
| 1. | $[(1, 2, 2)];$ | 11. | $[(1, 1, 2, 3)];$ | 21. | $[(5, 1, 2, 2)];$ |
| 2. | $[0, 2, 1, (3)];$ | 12. | $[2, 3, 2, (1, 2)];$ | 22. | $[4, 2, (2, 2, 3)];$ |
| 3. | $[(2, 1, 3)];$ | 13. | $[(2, 1, 1, 3)];$ | 23. | $[(2, 3, 1, 2)];$ |
| 4. | $[0, 1, 2, (2)];$ | 14. | $[3, 2, 2, (1, 3)];$ | 24. | $[1, 2, (3, 1, 2)];$ |
| 5. | $[(1, 2, 1, 2)];$ | 15. | $[(1, 2, 1, 3)];$ | 25. | $[(1, 2, 2, 3)];$ |
| 6. | $[1, 3, 2, (4)];$ | 16. | $[0, 2, 2, (3, 4)];$ | 26. | $[3, 2, (1, 3, 1)];$ |
| 7. | $[(3, 1, 2, 2)];$ | 17. | $[(3, 3, 2, 2)];$ | 27. | $[(3, 3, 1, 2)];$ |
| 8. | $[1, 2, (3, 1)];$ | 18. | $[2, 3, 2, (5)];$ | 28. | $[2, 3, 1, (2, 4)];$ |
| 9. | $[(2, 1, 3, 2)];$ | 19. | $[(1, 1, 3, 2)];$ | 29. | $[(3, 1, 3, 2)];$ |
| 10. | $[2, 1, (2, 3)];$ | 20. | $[1, 2, (3, 2, 1)];$ | 30. | $[3, 3, 2, (1, 5)].$ |

Задание 9

Найти иррациональность α и представить ее в виде $\alpha = \frac{a + b\sqrt{c}}{d}$, $a, b, c, d \in \mathbb{Z}$, если:

- $\frac{P_k}{Q_k} = \frac{15}{7}, \quad \alpha_{k+1} = \sqrt{5};$
- $\frac{P_k}{Q_k} = \frac{21}{8}, \quad \alpha_{k+1} = \sqrt{7};$
- $\frac{P_k}{Q_k} = \frac{13}{5}, \quad \alpha_{k+1} = \sqrt{11} - 1;$
- $\frac{P_k}{Q_k} = \frac{24}{13}, \quad \alpha_{k+1} = \sqrt{3} - 1;$
- $\frac{P_k}{Q_k} = \frac{43}{17}, \quad \alpha_{k+1} = \frac{\sqrt{2} + 1}{3};$
- $\frac{P_k}{Q_k} = \frac{37}{19}, \quad \alpha_{k+1} = \sqrt{3};$
- $\frac{P_k}{Q_k} = \frac{29}{15}, \quad \alpha_{k+1} = \sqrt{2} + 1;$

8. $\frac{P_k}{Q_k} = \frac{31}{17}, \quad \alpha_{k+1} = \frac{\sqrt{7}-2}{3};$
9. $\frac{P_k}{Q_k} = \frac{25}{7}, \quad \alpha_{k+1} = \frac{1+\sqrt{3}}{2};$
10. $\frac{P_k}{Q_k} = \frac{47}{18}, \quad \alpha_{k+1} = \sqrt{5}+1;$
11. $\frac{P_k}{Q_k} = \frac{23}{16}, \quad \alpha_{k+1} = \frac{1+\sqrt{2}}{3};$
12. $\frac{P_k}{Q_k} = \frac{13}{5}, \quad \alpha_{k+1} = \frac{3+\sqrt{5}}{2};$
13. $\frac{P_k}{Q_k} = \frac{18}{7}, \quad \alpha_{k+1} = \frac{\sqrt{7}-1}{2};$
14. $\frac{P_k}{Q_k} = \frac{19}{8}, \quad \alpha_{k+1} = \frac{\sqrt{3}-1}{4};$
15. $\frac{P_k}{Q_k} = \frac{83}{75}, \quad \alpha_{k+1} = \sqrt{3}-1;$
16. $\frac{P_k}{Q_k} = \frac{13}{7}, \quad \alpha_{k+1} = \sqrt{13}-3;$
17. $\frac{P_k}{Q_k} = \frac{23}{9}, \quad \alpha_{k+1} = \sqrt{5}-1;$
18. $\frac{P_k}{Q_k} = \frac{43}{19}, \quad \alpha_{k+1} = \sqrt{2}+1;$
19. $\frac{P_k}{Q_k} = \frac{36}{13}, \quad \alpha_{k+1} = \frac{\sqrt{3}-2}{5};$
20. $\frac{P_k}{Q_k} = \frac{24}{13}, \quad \alpha_{k+1} = \frac{1-\sqrt{5}}{2};$
21. $\frac{P_k}{Q_k} = \frac{23}{15}, \quad \alpha_{k+1} = \frac{\sqrt{2}+1}{5};$
22. $\frac{P_k}{Q_k} = \frac{42}{19}, \quad \alpha_{k+1} = \sqrt{3}+1;$
23. $\frac{P_k}{Q_k} = \frac{53}{23}, \quad \alpha_{k+1} = \sqrt{2}-1;$
24. $\frac{P_k}{Q_k} = \frac{51}{16}, \quad \alpha_{k+1} = \frac{1}{\sqrt{3}};$
25. $\frac{P_k}{Q_k} = \frac{47}{24}, \quad \alpha_{k+1} = \frac{1}{\sqrt{2}};$

26. $\frac{P_k}{Q_k} = \frac{19}{11}, \quad \alpha_{k+1} = \sqrt{7} - 1;$
27. $\frac{P_k}{Q_k} = \frac{22}{15}, \quad \alpha_{k+1} = \frac{\sqrt{3}}{6};$
28. $\frac{P_k}{Q_k} = \frac{21}{13}, \quad \alpha_{k+1} = \frac{\sqrt{3} - 1}{2};$
29. $\frac{P_k}{Q_k} = \frac{45}{13}, \quad \alpha_{k+1} = \frac{\sqrt{3} - 1}{5};$
30. $\frac{P_k}{Q_k} = \frac{38}{21}, \quad \alpha_{k+1} = \frac{\sqrt{2} - 1}{2}.$

Задание 10

Следующее число n заменить подходящей дробью $\frac{P_k}{Q_k}$ и оценить погрешность приближения:

- | | |
|------------------------------------------------|--------------------------------------------------|
| 1. $k = 4, \quad n = \frac{695}{106};$ | 16. $k = 3, \quad n = \frac{347}{83};$ |
| 2. $k = 4, \quad n = 3,14159;$ | 17. $k = 6, \quad n = 3,5149;$ |
| 3. $k = 5, \quad n = \frac{1 + \sqrt{5}}{2};$ | 18. $k = 5, \quad n = \frac{11 - \sqrt{2}}{9};$ |
| 4. $k = 5, \quad n = \frac{347}{97};$ | 19. $k = 4, \quad n = \frac{257}{61};$ |
| 5. $k = 4, \quad n = 2,7142;$ | 20. $k = 5, \quad n = 2,4712;$ |
| 6. $k = 4, \quad n = \frac{2 + \sqrt{3}}{5};$ | 21. $k = 4, \quad n = \frac{17 + \sqrt{3}}{5};$ |
| 7. $k = 4, \quad n = \frac{458}{301};$ | 22. $k = 5, \quad n = \frac{389}{113};$ |
| 8. $k = 5, \quad n = 1,5342;$ | 23. $k = 6, \quad n = 4,5373;$ |
| 9. $k = 4, \quad n = \frac{1 - \sqrt{3}}{2};$ | 24. $k = 4, \quad n = \frac{9 + \sqrt{5}}{7};$ |
| 10. $k = 3, \quad n = \frac{293}{119};$ | 25. $k = 3, \quad n = \frac{493}{211};$ |
| 11. $k = 6, \quad n = 4,3537;$ | 26. $k = 4, \quad n = 5,4325;$ |
| 12. $k = 3, \quad n = \frac{2 - \sqrt{3}}{7};$ | 27. $k = 5, \quad n = \frac{16 - \sqrt{3}}{11};$ |
| 13. $k = 3, \quad n = \frac{573}{123};$ | 28. $k = 3, \quad n = \frac{173}{38};$ |
| 14. $k = 7, \quad n = 5,7189;$ | 29. $k = 5, \quad n = 1,9817;$ |

$$15. \quad k = 3, \quad n = \frac{3 + \sqrt{5}}{7}; \quad 30. \quad k = 5, \quad n = \frac{14 - \sqrt{7}}{5}.$$

Задание 11

Найти все целочисленные решения уравнения:

- | | |
|-----------------------------|----------------------------|
| 1. $15x - 13y + 5 = 0;$ | 16. $83x + 24y - 2 = 0;$ |
| 2. $29x + 14y - 2 = 0;$ | 17. $56x - 23y - 3 = 0;$ |
| 3. $41x + 11y - 46 = 0;$ | 18. $39x + 26y - 221 = 0;$ |
| 4. $37x - 25y + 1 = 0;$ | 19. $117x - 29y - 5 = 0;$ |
| 5. $21x + 16y - 31 = 0;$ | 20. $36x + 93y - 18 = 0;$ |
| 6. $19x - 12y - 11 = 0;$ | 21. $21x - 44y - 3 = 0;$ |
| 7. $34x - 42y - 18 = 0;$ | 22. $38x + 52y - 6 = 0;$ |
| 8. $111x + 74y - 37 = 0;$ | 23. $131x - 98y - 7 = 0;$ |
| 9. $31x - 28y - 5 = 0;$ | 24. $119x + 84y - 77 = 0;$ |
| 10. $15x + 23y - 24 = 0;$ | 25. $103x + 66y - 2 = 0;$ |
| 11. $75x - 125y + 100 = 0;$ | 26. $97x - 85y - 3 = 0;$ |
| 12. $19x + 41y + 25 = 0;$ | 27. $45x + 38y - 2 = 0;$ |
| 13. $22x + 35y - 7 = 0;$ | 28. $87x - 36y - 15 = 0;$ |
| 14. $12x + 47y - 13 = 0;$ | 29. $107x + 93y - 5 = 0;$ |
| 15. $91x - 46y - 8 = 0;$ | 30. $101x - 73y - 39 = 0.$ |

Задание 12

Найти наибольший общий делитель двух данных чисел в кольце целых гауссовых чисел $\mathbb{Z}[i]$:

- | | |
|--------------------------|---------------------------|
| 1. $11 + i, -4 - 10i;$ | 16. $34 + 6i, 10 - i;$ |
| 2. $13 - 11i, 7 - 4i;$ | 17. $67 - 3i, 34 + 40i;$ |
| 3. $8 + i, 9 + 28i;$ | 18. $68 - 50i, 67 - 3i;$ |
| 4. $13 - 21i, 23 - 36i;$ | 19. $49 + 24i, 31 + 25i;$ |
| 5. $28 - 9i, 19 + 13i;$ | 20. $19 + 48i, 16 + 11i;$ |
| 6. $-1 + 27i, -23 + i;$ | 21. $34 - 12i, 11 + 17i;$ |
| 7. $55 + 25i, 26 - 18i;$ | 22. $38 - 44i, 29 + 15i;$ |
| 8. $28 - 26i, 48 - 26i;$ | 23. $16 + 2i, 1 + 9i;$ |

- | | |
|---------------------------------|---------------------------------|
| 9. $91 + 19i$, $46 - 28i$; | 24. $23 + 11i$, $-3 + 14i$; |
| 10. $12 + 14i$, $-1 + 11i$; | 25. $20 - 30i$, $19 + 7i$; |
| 11. $19 + 35i$, $27 - 5i$; | 26. $8 + 27i$, $25 + 8i$; |
| 12. $-35 + 43i$, $-20 + 37i$; | 27. $-40 - 13i$, $-31 + 24i$; |
| 13. $61 + 36i$, $16 - 11i$; | 28. $13 + 21i$, $23 + i$; |
| 14. $36 + 23i$, $27 + i$; | 29. $17 + 4i$, $12 - 11i$; |
| 15. $33 + i$, $12 - 2i$; | 30. $-9 + 23i$, $13 + 19i$. |

Задание 13

Элемент кольца $\mathbb{Z}[i]$ разложить на неприводимые множители:

- | | | |
|------------------|--------------------|-------------------|
| 1. $11 + 8i$; | 11. $19 + 17i$; | 21. $93 + 16i$; |
| 2. $19 + 7i$; | 12. $23 + 24i$; | 22. $19 + 15i$; |
| 3. $19 + 9i$; | 13. $9 + 8i$; | 23. $11 + 7i$; |
| 4. $15 + 7i$; | 14. $23 + 15i$; | 24. $2 - 24i$; |
| 5. $9 + 7i$; | 15. $-5 + 25i$; | 25. $11 + 5i$; |
| 6. $49 + 37i$; | 16. $19 + 15i$; | 26. $33 - 17i$; |
| 7. $16 + 7i$; | 17. $1 + 21i$; | 27. $31 + 77i$; |
| 8. $19 + 3i$; | 18. $-35 - 35i$; | 28. $11 + 9i$; |
| 9. $53 + 31i$; | 19. $19 + 11i$; | 29. $21 + 38i$; |
| 10. $18 + 11i$; | 20. $-151 + 28i$; | 30. $-67 - 49i$. |

Задание 14

Является ли данное простое число неприводимым элементом кольца $\mathbb{Z}[i]$? Если оно приводимо, то разложить его в произведение неприводимых элементов кольца $\mathbb{Z}[i]$:

- | | | |
|---------|----------|----------|
| 1. 997; | 7. 233; | 13. 569; |
| 2. 797; | 8. 157; | 14. 433; |
| 3. 601; | 9. 977; | 15. 397; |
| 4. 521; | 10. 877; | 16. 277; |
| 5. 409; | 11. 757; | 17. 193; |
| 6. 353; | 12. 613; | 18. 937; |

- | | | |
|----------|----------|----------|
| 19. 821; | 23. 593; | 27. 953; |
| 20. 769; | 24. 457; | 28. 853; |
| 21. 709; | 25. 373; | 29. 773; |
| 22. 653; | 26. 293; | 30. 673. |

Задание 15

Решить сравнение:

- | | |
|----------------------------------|------------------------------------|
| 1. $5x \equiv 3 \pmod{11}$; | 16. $34x \equiv 27 \pmod{39}$; |
| 2. $7x \equiv 4 \pmod{13}$; | 17. $343x \equiv 12 \pmod{107}$; |
| 3. $142x \equiv 81 \pmod{181}$; | 18. $245x \equiv 84 \pmod{123}$; |
| 4. $33x \equiv 94 \pmod{52}$; | 19. $25x \equiv 3 \pmod{34}$; |
| 5. $15x \equiv 21 \pmod{23}$; | 20. $52x \equiv 17 \pmod{19}$; |
| 6. $17x \equiv 2 \pmod{19}$; | 21. $96x \equiv 85 \pmod{125}$; |
| 7. $27x \equiv 55 \pmod{112}$; | 22. $151x \equiv 244 \pmod{347}$; |
| 8. $174x \equiv 93 \pmod{79}$; | 23. $53x \equiv 142 \pmod{193}$; |
| 9. $22x \equiv 15 \pmod{41}$; | 24. $87x \equiv 135 \pmod{59}$; |
| 10. $16x \equiv 9 \pmod{19}$; | 25. $92x \equiv 11 \pmod{111}$; |
| 11. $183x \equiv 52 \pmod{71}$; | 26. $8x \equiv 19 \pmod{105}$; |
| 12. $241x \equiv 18 \pmod{96}$; | 27. $18x \equiv 39 \pmod{103}$; |
| 13. $24x \equiv 43 \pmod{47}$; | 28. $31x \equiv 25 \pmod{48}$; |
| 14. $132x \equiv 55 \pmod{71}$; | 29. $54x \equiv 23 \pmod{95}$; |
| 15. $93x \equiv 16 \pmod{43}$; | 30. $124x \equiv 75 \pmod{59}$. |

Задание 16

Решить сравнение. Выписать все решения по данному модулю:

- | | |
|-----------------------------------|------------------------------------|
| 1. $12x \equiv 44 \pmod{56}$; | 16. $172x \equiv 60 \pmod{196}$; |
| 2. $52x \equiv 65 \pmod{117}$; | 17. $184x \equiv 40 \pmod{192}$; |
| 3. $144x \equiv 72 \pmod{42}$; | 18. $236x \equiv 24 \pmod{400}$; |
| 4. $225x \equiv 100 \pmod{235}$; | 19. $138x \equiv 115 \pmod{161}$; |
| 5. $96x \equiv 160 \pmod{256}$; | 20. $155x \equiv 75 \pmod{205}$; |
| 6. $145x \equiv 58 \pmod{203}$; | 21. $57x \equiv 95 \pmod{76}$; |
| 7. $213x \equiv 27 \pmod{315}$; | 22. $215x \equiv 86 \pmod{301}$; |
| 8. $94x \equiv 42 \pmod{122}$; | 23. $244x \equiv 112 \pmod{356}$; |

- | | |
|------------------------------------|------------------------------------|
| 9. $196x \equiv 52 \pmod{772}$; | 24. $136x \equiv 85 \pmod{187}$; |
| 10. $205x \equiv 82 \pmod{287}$; | 25. $174x \equiv 87 \pmod{261}$; |
| 11. $81x \equiv 36 \pmod{99}$; | 26. $81x \equiv 45 \pmod{117}$; |
| 12. $125x \equiv 100 \pmod{175}$; | 27. $114x \equiv 95 \pmod{209}$; |
| 13. $169x \equiv 91 \pmod{273}$; | 28. $148x \equiv 100 \pmod{164}$; |
| 14. $60x \equiv 15 \pmod{85}$; | 29. $325x \equiv 221 \pmod{169}$; |
| 15. $129x \equiv 42 \pmod{243}$; | 30. $110x \equiv 77 \pmod{143}$. |

Задание 17

Воспользовавшись расширенным алгоритмом Евклида, найти обратный для элемента a кольца \mathbb{Z}_n :

- | | |
|------------------------|------------------------|
| 1. $n = 24, a = 13$; | 16. $n = 25, a = 17$; |
| 2. $n = 29, a = 5$; | 17. $n = 21, a = 8$; |
| 3. $n = 48, a = 11$; | 18. $n = 15, a = 11$; |
| 4. $n = 40, a = 13$; | 19. $n = 27, a = 16$; |
| 5. $n = 42, a = 25$; | 20. $n = 33, a = 19$; |
| 6. $n = 18, a = 13$; | 21. $n = 35, a = 27$; |
| 7. $n = 20, a = 9$; | 22. $n = 39, a = 25$; |
| 8. $n = 22, a = 5$; | 23. $n = 45, a = 26$; |
| 9. $n = 16, a = 11$; | 24. $n = 49, a = 24$; |
| 10. $n = 44, a = 23$; | 25. $n = 51, a = 22$; |
| 11. $n = 38, a = 21$; | 26. $n = 55, a = 29$; |
| 12. $n = 34, a = 25$; | 27. $n = 57, a = 37$; |
| 13. $n = 32, a = 19$; | 28. $n = 63, a = 34$; |
| 14. $n = 30, a = 23$; | 29. $n = 65, a = 24$; |
| 15. $n = 26, a = 15$; | 30. $n = 69, a = 26$. |

Задание 18

Найти обратный для элемента a кольца \mathbb{Z}_n , используя теорему Ферма:

- | | |
|-----------------------|-----------------------|
| 1. $n = 47, a = 11$; | 3. $n = 53, a = 15$; |
| 2. $n = 13, a = 5$; | 4. $n = 29, a = 3$; |

- | | |
|------------------------|------------------------|
| 5. $n = 59, a = 17;$ | 18. $n = 31, a = 6;$ |
| 6. $n = 13, a = 6;$ | 19. $n = 103, a = 15;$ |
| 7. $n = 61, a = 21;$ | 20. $n = 29, a = 4;$ |
| 8. $n = 23, a = 4;$ | 21. $n = 101, a = 57;$ |
| 9. $n = 67, a = 25;$ | 22. $n = 23, a = 3;$ |
| 10. $n = 17, a = 5;$ | 23. $n = 83, a = 31;$ |
| 11. $n = 89, a = 16;$ | 24. $n = 19, a = 2;$ |
| 12. $n = 43, a = 7;$ | 25. $n = 79, a = 41;$ |
| 13. $n = 97, a = 35;$ | 26. $n = 17, a = 8;$ |
| 14. $n = 41, a = 2;$ | 27. $n = 73, a = 38;$ |
| 15. $n = 107, a = 28;$ | 28. $n = 13, a = 7;$ |
| 16. $n = 37, a = 3;$ | 29. $n = 71, a = 36;$ |
| 17. $n = 109, a = 82;$ | 30. $n = 11, a = 5.$ |

Задание 19

Найти обратный для элемента a кольца \mathbb{Z}_n , используя теорему Эйлера:

- | | |
|-----------------------|------------------------|
| 1. $n = 42, a = 5;$ | 16. $n = 102, a = 49;$ |
| 2. $n = 16, a = 7;$ | 17. $n = 26, a = 3;$ |
| 3. $n = 40, a = 3;$ | 18. $n = 168, a = 59;$ |
| 4. $n = 72, a = 11;$ | 19. $n = 24, a = 7;$ |
| 5. $n = 38, a = 23;$ | 20. $n = 66, a = 35;$ |
| 6. $n = 52, a = 19;$ | 21. $n = 22, a = 5;$ |
| 7. $n = 36, a = 11;$ | 22. $n = 58, a = 23;$ |
| 8. $n = 110, a = 13;$ | 23. $n = 20, a = 3;$ |
| 9. $n = 34, a = 7;$ | 24. $n = 74, a = 19;$ |
| 10. $n = 94, a = 23;$ | 25. $n = 16, a = 9;$ |
| 11. $n = 32, a = 5;$ | 26. $n = 44, a = 21;$ |
| 12. $n = 88, a = 37;$ | 27. $n = 18, a = 11;$ |
| 13. $n = 30, a = 11;$ | 28. $n = 46, a = 27;$ |
| 14. $n = 76, a = 53;$ | 29. $n = 14, a = 5;$ |
| 15. $n = 28, a = 9;$ | 30. $n = 112, a = 47.$ |

Задание 20

Найти минимальное число умножений для вычисления a^m :

- | | | |
|-----------------|-----------------|-----------------|
| 1. $m = 193$; | 11. $m = 201$; | 21. $m = 171$; |
| 2. $m = 185$; | 12. $m = 125$; | 22. $m = 195$; |
| 3. $m = 203$; | 13. $m = 138$; | 23. $m = 166$; |
| 4. $m = 122$; | 14. $m = 147$; | 24. $m = 158$; |
| 5. $m = 134$; | 15. $m = 152$; | 25. $m = 189$; |
| 6. $m = 97$; | 16. $m = 168$; | 26. $m = 150$; |
| 7. $m = 174$; | 17. $m = 155$; | 27. $m = 198$; |
| 8. $m = 136$; | 18. $m = 99$; | 28. $m = 219$; |
| 9. $m = 142$; | 19. $m = 139$; | 29. $m = 117$; |
| 10. $m = 103$; | 20. $m = 148$; | 30. $m = 210$. |

Задание 21

Найти минимальное число сложений для вычисления $a \cdot b$:

- | | | |
|----------------------|-----------------------|-----------------------|
| 1. $147 \cdot 45$; | 11. $393 \cdot 147$; | 21. $167 \cdot 67$; |
| 2. $164 \cdot 97$; | 12. $516 \cdot 94$; | 22. $213 \cdot 114$; |
| 3. $213 \cdot 38$; | 13. $108 \cdot 83$; | 23. $187 \cdot 149$; |
| 4. $403 \cdot 19$; | 14. $99 \cdot 74$; | 24. $235 \cdot 115$; |
| 5. $315 \cdot 93$; | 15. $132 \cdot 81$; | 25. $307 \cdot 123$; |
| 6. $807 \cdot 47$; | 16. $193 \cdot 117$; | 26. $491 \cdot 119$; |
| 7. $365 \cdot 113$; | 17. $135 \cdot 87$; | 27. $297 \cdot 98$; |
| 8. $168 \cdot 39$; | 18. $211 \cdot 43$; | 28. $283 \cdot 73$; |
| 9. $171 \cdot 96$; | 19. $134 \cdot 79$; | 29. $174 \cdot 85$; |
| 10. $137 \cdot 37$; | 20. $112 \cdot 56$; | 30. $369 \cdot 91$. |

Задание 22

Решить систему сравнений, последовательно решая пары уравнений, т. е. представить решение системы

$$x \equiv a_i \pmod{m_i} \quad (i = 1, \dots, k)$$

в виде $x = q_1 + q_2(m_1) + q_3(m_1m_2) + \dots + q_k(m_1m_2 \dots m_{k-1})$:

$$1. \quad \begin{cases} 2x \equiv 3 \pmod{5} \\ 11x \equiv 6 \pmod{7} \\ 5x \equiv 7 \pmod{11}; \end{cases}$$

$$2. \quad \begin{cases} 3x \equiv 7 \pmod{13} \\ 5x \equiv 4 \pmod{17} \\ 2x \equiv 3 \pmod{19}; \end{cases}$$

$$3. \quad \begin{cases} 4x \equiv 4 \pmod{5} \\ 3x \equiv 0 \pmod{7} \\ 5x \equiv 13 \pmod{23}; \end{cases}$$

$$4. \quad \begin{cases} 5x \equiv 1 \pmod{2} \\ 9x \equiv 7 \pmod{11} \\ 2x \equiv 3 \pmod{23}; \end{cases}$$

$$5. \quad \begin{cases} 11x \equiv 0 \pmod{3} \\ 2x \equiv 4 \pmod{13} \\ 3x \equiv 7 \pmod{19}; \end{cases}$$

$$6. \quad \begin{cases} 3x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{41} \\ 2x \equiv 0 \pmod{3}; \end{cases}$$

$$7. \quad \begin{cases} x \equiv 2 \pmod{3} \\ 7x \equiv 8 \pmod{11} \\ 3x \equiv 0 \pmod{5}; \end{cases}$$

$$8. \quad \begin{cases} x \equiv 0 \pmod{2} \\ 2x \equiv 4 \pmod{13} \\ 5x \equiv 0 \pmod{11}; \end{cases}$$

$$9. \quad \begin{cases} 3x \equiv 4 \pmod{5} \\ 5x \equiv 0 \pmod{14} \\ 2x \equiv 10 \pmod{23}; \end{cases}$$

$$10. \quad \begin{cases} 2x \equiv 0 \pmod{5} \\ 3x \equiv 16 \pmod{17} \\ 5x \equiv 0 \pmod{3}; \end{cases}$$

$$11. \quad \begin{cases} 3x \equiv 0 \pmod{2} \\ 4x \equiv -1 \pmod{13} \\ 2x \equiv 4 \pmod{5}; \end{cases}$$

$$12. \quad \begin{cases} x \equiv 3 \pmod{11} \\ 2x \equiv 4 \pmod{5} \\ 3x \equiv 5 \pmod{7}; \end{cases}$$

$$13. \quad \begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 1 \pmod{8} \\ 5x \equiv 6 \pmod{21}; \end{cases}$$

$$14. \quad \begin{cases} 2x \equiv 3 \pmod{7} \\ 3x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod{6}; \end{cases}$$

$$15. \quad \begin{cases} 3x \equiv 1 \pmod{4} \\ 2x \equiv 1 \pmod{5} \\ 10x \equiv 6 \pmod{17}; \end{cases}$$

$$16. \quad \begin{cases} x \equiv 7 \pmod{10} \\ 2x \equiv 2 \pmod{3} \\ 5x \equiv 6 \pmod{7}; \end{cases}$$

$$17. \quad \begin{cases} 2x \equiv 9 \pmod{5} \\ x \equiv 2 \pmod{8} \\ 3x \equiv 24 \pmod{77}; \end{cases}$$

$$18. \quad \begin{cases} 2x \equiv 10 \pmod{12} \\ 3x \equiv 23 \pmod{35} \\ 6x \equiv 9 \pmod{11}; \end{cases}$$

$$19. \quad \begin{cases} 2x \equiv -2 \pmod{7} \\ 3x \equiv 6 \pmod{25} \\ 5x \equiv 11 \pmod{13}; \end{cases}$$

$$20. \quad \begin{cases} 2x \equiv 2 \pmod{19} \\ 3x \equiv 12 \pmod{23} \\ x \equiv 0 \pmod{6}; \end{cases}$$

$$21. \begin{cases} x \equiv 18 \pmod{31} \\ 2x \equiv 2 \pmod{5} \\ 5x \equiv 3 \pmod{6}; \end{cases}$$

$$22. \begin{cases} 2x \equiv 14 \pmod{29} \\ 3x \equiv 30 \pmod{55} \\ 2x \equiv 1 \pmod{3}; \end{cases}$$

$$23. \begin{cases} x \equiv 26 \pmod{37} \\ 2x \equiv 10 \pmod{11} \\ 3x \equiv 11 \pmod{10}; \end{cases}$$

$$24. \begin{cases} 3x \equiv 8 \pmod{13} \\ 5x \equiv 6 \pmod{22} \\ 7x \equiv 9 \pmod{31}; \end{cases}$$

$$25. \begin{cases} 2x \equiv 1 \pmod{5} \\ 4x \equiv 3 \pmod{11} \\ 3x \equiv 12 \pmod{23}; \end{cases}$$

$$26. \begin{cases} 2x \equiv 9 \pmod{13} \\ 5x \equiv 0 \pmod{7} \\ 8x \equiv 9 \pmod{15}; \end{cases}$$

$$27. \begin{cases} x \equiv 3 \pmod{20} \\ 2x \equiv 1 \pmod{9} \\ 3x \equiv -7 \pmod{77}; \end{cases}$$

$$28. \begin{cases} 5x \equiv 11 \pmod{12} \\ 2x \equiv 1 \pmod{25} \\ 3x \equiv 6 \pmod{7}; \end{cases}$$

$$29. \begin{cases} 3x \equiv -11 \pmod{50} \\ 2x \equiv 10 \pmod{77} \\ 4x \equiv 11 \pmod{17}; \end{cases}$$

$$30. \begin{cases} 3x \equiv 21 \pmod{41} \\ 5x \equiv 30 \pmod{63} \\ 2x \equiv 2 \pmod{17}. \end{cases}$$

Задание 23

Решить систему сравнений, пользуясь формулой китайской теоремы об остатках для чисел, т. е. представить решение системы $x \equiv a_i \pmod{m_i}$ ($i = 1, \dots, k$) в виде

$$x = \sum_{i=1}^k a_i M_i N_i \pmod{m_1 m_2 \dots m_k} :$$

$$1. \begin{cases} x \equiv 18 \pmod{31} \\ 2x \equiv 2 \pmod{5} \\ 5x \equiv 3 \pmod{6}; \end{cases}$$

$$4. \begin{cases} 3x \equiv 8 \pmod{13} \\ 5x \equiv 6 \pmod{22} \\ 7x \equiv 9 \pmod{31}; \end{cases}$$

$$2. \begin{cases} 2x \equiv 14 \pmod{29} \\ 3x \equiv 30 \pmod{55} \\ 2x \equiv 1 \pmod{3}; \end{cases}$$

$$5. \begin{cases} 2x \equiv 1 \pmod{5} \\ 4x \equiv 3 \pmod{11} \\ 3x \equiv 12 \pmod{23}; \end{cases}$$

$$3. \begin{cases} x \equiv 26 \pmod{37} \\ 2x \equiv 10 \pmod{11} \\ 3x \equiv 11 \pmod{10}; \end{cases}$$

$$6. \begin{cases} 2x \equiv 9 \pmod{13} \\ 5x \equiv 0 \pmod{7} \\ 8x \equiv 9 \pmod{15}; \end{cases}$$

$$7. \quad \begin{cases} x \equiv 3 \pmod{20} \\ 2x \equiv 1 \pmod{9} \\ 3x \equiv -7 \pmod{77}; \end{cases}$$

$$15. \quad \begin{cases} 11x \equiv 0 \pmod{3} \\ 2x \equiv 4 \pmod{13} \\ 3x \equiv 7 \pmod{19}; \end{cases}$$

$$8. \quad \begin{cases} 5x \equiv 11 \pmod{12} \\ 2x \equiv 1 \pmod{25} \\ 3x \equiv 6 \pmod{7}; \end{cases}$$

$$16. \quad \begin{cases} 3x \equiv 1 \pmod{5} \\ x \equiv 1 \pmod{41} \\ 2x \equiv 0 \pmod{3}; \end{cases}$$

$$9. \quad \begin{cases} 3x \equiv -11 \pmod{50} \\ 2x \equiv 10 \pmod{77} \\ 4x \equiv 11 \pmod{17}; \end{cases}$$

$$17. \quad \begin{cases} x \equiv 2 \pmod{3} \\ 7x \equiv 8 \pmod{11} \\ 3x \equiv 0 \pmod{5}; \end{cases}$$

$$10. \quad \begin{cases} 3x \equiv 21 \pmod{41} \\ 5x \equiv 30 \pmod{63} \\ 2x \equiv 2 \pmod{17}; \end{cases}$$

$$18. \quad \begin{cases} x \equiv 0 \pmod{2} \\ 2x \equiv 4 \pmod{13} \\ 5x \equiv 0 \pmod{11}; \end{cases}$$

$$11. \quad \begin{cases} 2x \equiv 3 \pmod{5} \\ 11x \equiv 6 \pmod{7} \\ 5x \equiv 7 \pmod{11}; \end{cases}$$

$$19. \quad \begin{cases} 3x \equiv 4 \pmod{5} \\ 5x \equiv 0 \pmod{14} \\ 2x \equiv 10 \pmod{23}; \end{cases}$$

$$12. \quad \begin{cases} 3x \equiv 7 \pmod{13} \\ 5x \equiv 4 \pmod{17} \\ 2x \equiv 3 \pmod{19}; \end{cases}$$

$$20. \quad \begin{cases} 2x \equiv 0 \pmod{5} \\ 3x \equiv 16 \pmod{17} \\ 5x \equiv 0 \pmod{3}; \end{cases}$$

$$13. \quad \begin{cases} 4x \equiv 4 \pmod{5} \\ 3x \equiv 0 \pmod{7} \\ 5x \equiv 13 \pmod{23}; \end{cases}$$

$$21. \quad \begin{cases} 3x \equiv 0 \pmod{2} \\ 4x \equiv -1 \pmod{13} \\ 2x \equiv 4 \pmod{5}; \end{cases}$$

$$14. \quad \begin{cases} 5x \equiv 1 \pmod{2} \\ 9x \equiv 7 \pmod{11} \\ 2x \equiv 3 \pmod{23}; \end{cases}$$

$$22. \quad \begin{cases} x \equiv 3 \pmod{11} \\ 2x \equiv 4 \pmod{5} \\ 3x \equiv 5 \pmod{7}; \end{cases}$$

$$\begin{array}{ll}
23. \quad \begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 1 \pmod{8} \\ 5x \equiv 6 \pmod{21}; \end{cases} & 27. \quad \begin{cases} 2x \equiv 9 \pmod{5} \\ x \equiv 2 \pmod{8} \\ 3x \equiv 24 \pmod{77}; \end{cases} \\
24. \quad \begin{cases} 2x \equiv 3 \pmod{7} \\ 3x \equiv 5 \pmod{11} \\ x \equiv 3 \pmod{6}; \end{cases} & 28. \quad \begin{cases} 2x \equiv 10 \pmod{12} \\ 3x \equiv 23 \pmod{35} \\ 6x \equiv 9 \pmod{11}; \end{cases} \\
25. \quad \begin{cases} 3x \equiv 1 \pmod{4} \\ 2x \equiv 1 \pmod{5} \\ 10x \equiv 6 \pmod{17}; \end{cases} & 29. \quad \begin{cases} 2x \equiv -2 \pmod{7} \\ 3x \equiv 6 \pmod{25} \\ 5x \equiv 11 \pmod{13}; \end{cases} \\
26. \quad \begin{cases} x \equiv 7 \pmod{10} \\ 2x \equiv 2 \pmod{3} \\ 5x \equiv 6 \pmod{7}; \end{cases} & 30. \quad \begin{cases} 2x \equiv 2 \pmod{19} \\ 3x \equiv 12 \pmod{23} \\ x \equiv 0 \pmod{6}. \end{cases}
\end{array}$$

Задание 24

Вычислить значение функции Эйлера от числа $n \in \mathbb{N}$:

- | | | |
|------------------|------------------|------------------|
| 1. $n = 3135$; | 11. $n = 861$; | 21. $n = 3795$; |
| 2. $n = 9061$; | 12. $n = 2862$; | 22. $n = 399$; |
| 3. $n = 4807$; | 13. $n = 6732$; | 23. $n = 702$; |
| 4. $n = 2275$: | 14. $n = 3404$; | 24. $n = 928$; |
| 5. $n = 4235$; | 15. $n = 5270$; | 25. $n = 1870$; |
| 6. $n = 3800$; | 16. $n = 2431$; | 26. $n = 4433$; |
| 7. $n = 1098$; | 17. $n = 1771$; | 27. $n = 7315$; |
| 8. $n = 10241$; | 18. $n = 3335$; | 28. $n = 1309$; |
| 9. $n = 2050$; | 19. $n = 725$; | 29. $n = 3390$; |
| 10. $n = 1554$; | 20. $n = 1105$; | 30. $n = 455$. |

Задание 25

Вычислить значение функции Мёбиуса от числа $n \in \mathbb{N}$:

- | | | |
|-----------------|-------------------|------------------|
| 1. $n = 1105$; | 11. $n = 1554$; | 21. $n = 455$; |
| 2. $n = 725$; | 12. $n = 2050$; | 22. $n = 3390$; |
| 3. $n = 3335$; | 13. $n = 10241$; | 23. $n = 1309$; |
| 4. $n = 1771$: | 14. $n = 1098$; | 24. $n = 7315$; |
| 5. $n = 2431$; | 15. $n = 3800$; | 25. $n = 4433$; |
| 6. $n = 5270$; | 16. $n = 4235$; | 26. $n = 1870$; |
| 7. $n = 3404$; | 17. $n = 2275$; | 27. $n = 928$; |
| 8. $n = 6732$; | 18. $n = 4807$; | 28. $n = 702$; |
| 9. $n = 2862$; | 19. $n = 9061$; | 29. $n = 399$; |
| 10. $n = 861$; | 20. $n = 3135$; | 30. $n = 3795$. |

Задание 26

Найти порядок мультипликативной группы кольца \mathbb{Z}_n . Описать структуру этой группы:

- | | | |
|-----------------|-----------------|-----------------|
| 1. $n = 49$; | 11. $n = 98$; | 21. $n = 578$; |
| 2. $n = 125$; | 12. $n = 169$; | 22. $n = 111$; |
| 3. $n = 256$; | 13. $n = 625$; | 23. $n = 274$; |
| 4. $n = 81$: | 14. $n = 214$; | 24. $n = 419$; |
| 5. $n = 361$; | 15. $n = 338$; | 25. $n = 262$; |
| 6. $n = 343$; | 16. $n = 244$; | 26. $n = 257$; |
| 7. $n = 521$; | 17. $n = 355$; | 27. $n = 302$; |
| 8. $n = 242$; | 18. $n = 289$; | 28. $n = 158$; |
| 9. $n = 250$; | 19. $n = 229$; | 29. $n = 529$; |
| 10. $n = 162$; | 20. $n = 526$; | 30. $n = 300$. |

Задание 27

Найти все примитивные корни по модулю n :

- | | | |
|---------------|---------------|----------------|
| 1. $n = 53$; | 5. $n = 25$; | 9. $n = 37$; |
| 2. $n = 49$; | 6. $n = 41$; | 10. $n = 27$; |
| 3. $n = 46$; | 7. $n = 38$; | 11. $n = 94$; |
| 4. $n = 43$; | 8. $n = 47$; | 12. $n = 89$; |

- | | | |
|----------------|----------------|----------------|
| 13. $n = 86$; | 19. $n = 71$; | 25. $n = 34$; |
| 14. $n = 83$; | 20. $n = 67$; | 26. $n = 81$; |
| 15. $n = 82$; | 21. $n = 26$; | 27. $n = 58$; |
| 16. $n = 79$; | 22. $n = 29$; | 28. $n = 61$; |
| 17. $n = 74$; | 23. $n = 23$; | 29. $n = 62$; |
| 18. $n = 73$; | 24. $n = 22$; | 30. $n = 31$. |

Задание 28

Описать структуру мультипликативной группы кольца \mathbb{Z}_n . Найти порядки этой группы. Найти элемент максимального порядка в группе:

- | | | |
|----------------|----------------|----------------|
| 1. $n = 80$; | 11. $n = 65$; | 21. $n = 45$; |
| 2. $n = 77$; | 12. $n = 63$; | 22. $n = 40$; |
| 3. $n = 76$; | 13. $n = 60$; | 23. $n = 39$; |
| 4. $n = 78$; | 14. $n = 57$; | 24. $n = 36$; |
| 5. $n = 75$; | 15. $n = 56$; | 25. $n = 33$; |
| 6. $n = 72$; | 16. $n = 55$; | 26. $n = 35$; |
| 7. $n = 70$; | 17. $n = 52$; | 27. $n = 30$; |
| 8. $n = 69$; | 18. $n = 51$; | 28. $n = 28$; |
| 9. $n = 68$; | 19. $n = 48$; | 29. $n = 24$; |
| 10. $n = 66$; | 20. $n = 44$; | 30. $n = 42$. |

Задание 29

Является ли число n псевдопростым по основанию a ? Ответ обосновать:

- | | |
|--------------------------|-------------------------|
| 1. $n = 819, a = 8$; | 11. $n = 121, a = 3$; |
| 2. $n = 1729, a = 12$; | 12. $n = 143, a = 12$; |
| 3. $n = 730, a = 9$; | 13. $n = 105, a = 2$; |
| 4. $n = 1099, a = 13$; | 14. $n = 217, a = 2$; |
| 5. $n = 215, a = 6$; | 15. $n = 121, a = 5$; |
| 6. $n = 12805, a = 14$; | 16. $n = 323, a = 18$; |
| 7. $n = 614, a = 17$; | 17. $n = 105, a = 13$; |
| 8. $n = 325, a = 18$; | 18. $n = 217, a = 3$; |
| 9. $n = 105, a = 8$; | 19. $n = 781, a = 5$; |
| 10. $n = 217, a = 6$; | 20. $n = 25, a = 3$; |

- | | |
|------------------------|------------------------|
| 21. $n = 63, a = 8;$ | 26. $n = 2047, a = 2;$ |
| 22. $n = 217, a = 5;$ | 27. $n = 511, a = 2;$ |
| 23. $n = 1105, a = 2;$ | 28. $n = 1729, a = 5;$ |
| 24. $n = 1023, a = 4;$ | 29. $n = 172, a = 7;$ |
| 25. $n = 1729, a = 2;$ | 30. $n = 215, a = 6.$ |

Задание 30

Является ли число n сильно псевдопростым по основанию a ? Ответ обосновать:

- | | |
|--------------------------|-------------------------|
| 1. $n = 703, a = 4;$ | 16. $n = 1105, a = 7;$ |
| 2. $n = 221, a = 174;$ | 17. $n = 629, a = 154;$ |
| 3. $n = 819, a = 2;$ | 18. $n = 629, a = 149;$ |
| 4. $n = 1261, a = 1225;$ | 19. $n = 703, a = 7;$ |
| 5. $n = 217, a = 149;$ | 20. $n = 325, a = 7;$ |
| 6. $n = 1073, a = 882;$ | 21. $n = 817, a = 7;$ |
| 7. $n = 1025, a = 32;$ | 22. $n = 221, a = 21;$ |
| 8. $n = 559, a = 380;$ | 23. $n = 253, a = 3;$ |
| 9. $n = 247, a = 159;$ | 24. $n = 629, a = 38;$ |
| 10. $n = 817, a = 767;$ | 25. $n = 527, a = 154;$ |
| 11. $n = 451, a = 180;$ | 26. $n = 121, a = 3;$ |
| 12. $n = 301, a = 80;$ | 27. $n = 187, a = 3;$ |
| 13. $n = 325, a = 18;$ | 28. $n = 2047, a = 3;$ |
| 14. $n = 187, a = 186;$ | 29. $n = 703, a = 16;$ |
| 15. $n = 781, a = 5;$ | 30. $n = 253, a = 2.$ |

Задание 31

Является ли число n числом Кармайкла? Ответ обосновать:

- | | | |
|----------------|-----------------|------------------|
| 1. $n = 1105;$ | 6. $n = 1235;$ | 11. $n = 2821;$ |
| 2. $n = 1023;$ | 7. $n = 10585;$ | 12. $n = 1955;$ |
| 3. $n = 1729;$ | 8. $n = 3857;$ | 13. $n = 6601;$ |
| 4. $n = 1173;$ | 9. $n = 29341;$ | 14. $n = 5083;$ |
| 5. $n = 2465;$ | 10. $n = 4301;$ | 15. $n = 62745;$ |

- | | | |
|-------------------|-------------------|-------------------|
| 16. $n = 7429$; | 21. $n = 15841$; | 26. $n = 7657$; |
| 17. $n = 46657$; | 22. $n = 1771$; | 27. $n = 63973$; |
| 18. $n = 2639$; | 23. $n = 41041$; | 28. $n = 4147$; |
| 19. $n = 8911$; | 24. $n = 11063$; | 29. $n = 75361$; |
| 20. $n = 4807$; | 25. $n = 52633$; | 30. $n = 4991$. |

Задание 32

Найти наибольший общий делитель чисел $a^m - 1$ и $a^n - 1$:

1. $m = 111, \quad n = 74, \quad a = 5$;
2. $m = 143, \quad n = 44, \quad a = 8$;
3. $m = 96, \quad n = 34, \quad a = 7$;
4. $m = 148, \quad n = 96, \quad a = 11$;
5. $m = 507, \quad n = 78, \quad a = 17$;
6. $m = 606, \quad n = 486, \quad a = 3$;
7. $m = 935, \quad n = 323, \quad a = 4$;
8. $m = 444, \quad n = 492, \quad a = 6$;
9. $m = 559, \quad n = 286, \quad a = 9$;
10. $m = 527, \quad n = 343, \quad a = 10$;
11. $m = 110, \quad n = 95, \quad a = 13$;
12. $m = 152, \quad n = 133, \quad a = 2$;
13. $m = 161, \quad n = 98, \quad a = 3$;
14. $m = 138, \quad n = 123, \quad a = 9$;
15. $m = 510, \quad n = 264, \quad a = 7$;
16. $m = 612, \quad n = 187, \quad a = 8$;
17. $m = 938, \quad n = 245, \quad a = 5$;
18. $m = 464, \quad n = 145, \quad a = 14$;
19. $m = 561, \quad n = 253, \quad a = 13$;
20. $m = 578, \quad n = 698, \quad a = 10$;
21. $m = 1173, \quad n = 129, \quad a = 11$;
22. $m = 669, \quad n = 171, \quad a = 5$;
23. $m = 333, \quad n = 267, \quad a = 6$;
24. $m = 625, \quad n = 365, \quad a = 8$;
25. $m = 804, \quad n = 622, \quad a = 13$;
26. $m = 726, \quad n = 513, \quad a = 7$;
27. $m = 634, \quad n = 248, \quad a = 9$;
28. $m = 779, \quad n = 738, \quad a = 3$;
29. $m = 345, \quad n = 252, \quad a = 12$;
30. $m = 737, \quad n = 209, \quad a = 6$.

Задание 33

Найти натуральное число $a + b$, если a и b заданы стандартными наборами остатков относительно вектора оснований β :

1. $\beta = \{2, 3, 5, 7\}$, $a = \{1, 2, 2, 3\}$, $b = \{0, 0, 2, 6\}$;
2. $\beta = \{3, 5, 7, 11\}$, $a = \{1, 2, 2, 4\}$, $b = \{0, 1, 6, 1\}$;
3. $\beta = \{2, 3, 7, 13\}$, $a = \{1, 1, 3, 5\}$, $b = \{0, 2, 0, 7\}$;
4. $\beta = \{3, 5, 7, 13\}$, $a = \{1, 4, 0, 10\}$, $b = \{1, 3, 5, 12\}$;
5. $\beta = \{2, 5, 11, 13\}$, $a = \{1, 4, 7, 3\}$, $b = \{1, 2, 10, 9\}$;
6. $\beta = \{3, 5, 11, 13\}$, $a = \{2, 2, 5, 7\}$, $b = \{1, 2, 9, 6\}$;
7. $\beta = \{2, 3, 5, 11\}$, $a = \{1, 0, 0, 6\}$, $b = \{1, 1, 3, 7\}$;
8. $\beta = \{2, 5, 7, 13\}$, $a = \{1, 2, 0, 9\}$, $b = \{1, 4, 6, 9\}$;
9. $\beta = \{2, 5, 7, 11\}$, $a = \{1, 4, 2, 6\}$, $b = \{1, 1, 2, 1\}$;
10. $\beta = \{3, 7, 11, 13\}$, $a = \{1, 4, 4, 1\}$, $b = \{0, 5, 7, 10\}$;
11. $\beta = \{2, 3, 5, 13\}$, $a = \{1, 2, 2, 12\}$, $b = \{1, 1, 2, 1\}$;
12. $\beta = \{2, 3, 11, 13\}$, $a = \{1, 1, 6, 2\}$, $b = \{1, 0, 3, 5\}$;
13. $\beta = \{5, 7, 11, 13\}$, $a = \{1, 0, 9, 9\}$, $b = \{2, 5, 3, 8\}$;
14. $\beta = \{2, 7, 11, 13\}$, $a = \{1, 6, 8, 11\}$, $b = \{1, 0, 3, 11\}$;
15. $\beta = \{2, 3, 7, 11\}$, $a = \{1, 0, 1, 7\}$, $b = \{1, 0, 2, 7\}$;
16. $\beta = \{2, 3, 5, 7\}$, $a = \{0, 0, 1, 1\}$, $b = \{1, 1, 0, 5\}$;
17. $\beta = \{3, 5, 7, 11\}$, $a = \{1, 1, 3, 2\}$, $b = \{1, 1, 4, 3\}$;
18. $\beta = \{2, 3, 7, 13\}$, $a = \{0, 1, 6, 1\}$, $b = \{0, 1, 6, 10\}$;
19. $\beta = \{3, 5, 7, 13\}$, $a = \{0, 0, 3, 12\}$, $b = \{2, 2, 1, 2\}$;
20. $\beta = \{2, 5, 11, 13\}$, $a = \{1, 3, 2, 4\}$, $b = \{0, 3, 6, 8\}$;
21. $\beta = \{3, 5, 11, 13\}$, $a = \{1, 3, 6, 7\}$, $b = \{0, 2, 7, 5\}$;
22. $\beta = \{2, 3, 5, 11\}$, $a = \{1, 0, 2, 10\}$, $b = \{1, 1, 4, 4\}$;
23. $\beta = \{2, 5, 7, 13\}$, $a = \{1, 3, 6, 7\}$, $b = \{0, 4, 4, 10\}$;
24. $\beta = \{2, 5, 7, 11\}$, $a = \{1, 1, 2, 5\}$, $b = \{1, 4, 2, 2\}$;
25. $\beta = \{3, 7, 11, 13\}$, $a = \{1, 6, 3, 9\}$, $b = \{2, 1, 10, 2\}$;
26. $\beta = \{2, 3, 5, 13\}$, $a = \{1, 0, 2, 12\}$, $b = \{1, 1, 3, 4\}$;
27. $\beta = \{2, 3, 11, 13\}$, $a = \{1, 1, 9, 12\}$, $b = \{1, 2, 2, 11\}$;
28. $\beta = \{5, 7, 11, 13\}$, $a = \{4, 6, 9, 5\}$, $b = \{0, 1, 4, 5\}$;
29. $\beta = \{2, 7, 11, 13\}$, $a = \{1, 4, 6, 3\}$, $b = \{1, 5, 7, 0\}$;
30. $\beta = \{2, 3, 7, 11\}$, $a = \{0, 2, 0, 1\}$, $b = \{1, 1, 0, 1\}$.

Задание 34

Найти натуральное число $a \cdot b$, если a и b заданы стандартными наборами остатков относительно вектора оснований β :

1. $\beta = \{2, 3, 7, 11\}$, $a = \{1, 2, 3, 6\}$, $b = \{1, 2, 2, 1\}$;
2. $\beta = \{2, 7, 11, 13\}$, $a = \{1, 5, 10, 1\}$, $b = \{0, 0, 3, 1\}$;
3. $\beta = \{5, 7, 11, 13\}$, $a = \{3, 6, 6, 5\}$, $b = \{0, 0, 2, 9\}$;
4. $\beta = \{2, 3, 11, 13\}$, $a = \{1, 1, 3, 12\}$, $b = \{1, 2, 7, 3\}$;
5. $\beta = \{2, 3, 5, 13\}$, $a = \{0, 0, 3, 5\}$, $b = \{0, 2, 4, 1\}$;
6. $\beta = \{3, 7, 11, 13\}$, $a = \{2, 4, 9, 1\}$, $b = \{2, 5, 3, 8\}$;
7. $\beta = \{2, 5, 7, 11\}$, $a = \{0, 2, 3, 8\}$, $b = \{1, 3, 6, 2\}$;
8. $\beta = \{2, 5, 7, 13\}$, $a = \{0, 4, 3, 11\}$, $b = \{0, 2, 5, 12\}$;
9. $\beta = \{2, 3, 5, 11\}$, $a = \{1, 0, 0, 4\}$, $b = \{0, 0, 3, 7\}$;
10. $\beta = \{3, 5, 11, 13\}$, $a = \{0, 4, 6, 0\}$, $b = \{0, 1, 7, 12\}$;
11. $\beta = \{2, 5, 11, 13\}$, $a = \{1, 2, 5, 1\}$, $b = \{1, 2, 6, 4\}$;
12. $\beta = \{3, 5, 7, 13\}$, $a = \{0, 1, 4, 3\}$, $b = \{1, 3, 6, 0\}$;
13. $\beta = \{2, 3, 7, 13\}$, $a = \{0, 1, 2, 3\}$, $b = \{1, 1, 3, 5\}$;
14. $\beta = \{3, 5, 7, 11\}$, $a = \{2, 3, 6, 6\}$, $b = \{2, 1, 4, 0\}$;
15. $\beta = \{2, 3, 5, 7\}$, $a = \{1, 1, 0, 4\}$, $b = \{1, 0, 4, 2\}$;
16. $\beta = \{2, 3, 7, 11\}$, $a = \{1, 0, 0, 10\}$, $b = \{1, 1, 5, 8\}$;
17. $\beta = \{2, 7, 11, 13\}$, $a = \{0, 1, 1, 0\}$, $b = \{1, 1, 4, 2\}$;
18. $\beta = \{5, 7, 11, 13\}$, $a = \{2, 6, 9, 6\}$, $b = \{4, 3, 2, 11\}$;
19. $\beta = \{2, 3, 11, 13\}$, $a = \{0, 0, 2, 11\}$, $b = \{1, 1, 9, 5\}$;
20. $\beta = \{2, 3, 5, 13\}$, $a = \{1, 2, 2, 4\}$, $b = \{0, 1, 2, 9\}$;
21. $\beta = \{3, 7, 11, 13\}$, $a = \{1, 0, 5, 10\}$, $b = \{1, 2, 4, 11\}$;
22. $\beta = \{2, 5, 7, 11\}$, $a = \{0, 1, 1, 3\}$, $b = \{1, 1, 0, 10\}$;
23. $\beta = \{2, 5, 7, 13\}$, $a = \{1, 4, 5, 6\}$, $b = \{1, 1, 6, 2\}$;
24. $\beta = \{2, 3, 5, 11\}$, $a = \{0, 2, 4, 3\}$, $b = \{1, 1, 4, 8\}$;
25. $\beta = \{3, 5, 11, 13\}$, $a = \{1, 2, 4, 11\}$, $b = \{0, 3, 4, 9\}$;
26. $\beta = \{2, 5, 11, 13\}$, $a = \{0, 2, 10, 6\}$, $b = \{0, 3, 6, 2\}$;
27. $\beta = \{3, 5, 7, 13\}$, $a = \{1, 1, 6, 11\}$, $b = \{2, 4, 0, 1\}$;
28. $\beta = \{2, 3, 7, 13\}$, $a = \{1, 1, 5, 6\}$, $b = \{0, 1, 0, 2\}$;
29. $\beta = \{3, 5, 7, 11\}$, $a = \{1, 4, 2, 2\}$, $b = \{0, 2, 5, 1\}$;
30. $\beta = \{2, 3, 5, 7\}$, $a = \{0, 1, 1, 2\}$, $b = \{1, 2, 1, 4\}$.

Задание 35

Не находя числа x , определить его знак, если относительно вектора оснований β ему соответствует данный стандартный набор остатков:

1. $\beta = \{5, 7.11.13.2\}, \quad x = (3, 0, 4, 6, 1);$
2. $\beta = \{7, 11, 13, 17, 2\}, \quad x = (4, 8, 10, 14, 1);$
3. $\beta = \{5, 11, 17, 19, 2\}, \quad x = (2, 3, 9, 11, 0);$
4. $\beta = \{5, 7.11.13.2\}, \quad x = (0, 1, 4, 2, 1);$
5. $\beta = \{7, 11, 13, 17, 2\}, \quad x = (2, 6, 8, 12, 1);$
6. $\beta = \{5, 11, 17, 19, 2\}, \quad x = (0, 3, 8, 6, 1);$
7. $\beta = \{5, 7.11.13.2\}, \quad x = (4, 3, 0, 2, 1);$
8. $\beta = \{7, 11, 13, 17, 2\}, \quad x = (6, 9, 7, 3, 0);$
9. $\beta = \{5, 11, 17, 19, 2\}, \quad x = (0, 1, 7, 9, 0);$
10. $\beta = \{5, 7.11.13.2\}, \quad x = (1, 4, 9, 2, 0);$
11. $\beta = \{7, 11, 13, 17, 2\}, \quad x = (0, 8, 12, 3, 0);$
12. $\beta = \{5, 11, 17, 19, 2\}, \quad x = (1, 10, 4, 2, 1);$
13. $\beta = \{5, 11, 13, 19, 2\}, \quad x = (3, 10, 1, 7, 0);$
14. $\beta = \{5, 7.11.13.2\}, \quad x = (2, 6, 3, 5, 0);$
15. $\beta = \{7, 11, 13, 17, 2\}, \quad x = (3, 8, 1, 9, 1);$
16. $\beta = \{5, 11, 17, 19, 2\}, \quad x = (2, 8, 14, 16, 1);$
17. $\beta = \{5, 7.11.13.2\}, \quad x = (0, 1, 4, 2, 1);$
18. $\beta = \{7, 11, 13, 17, 2\}, \quad x = (5, 8, 6, 2, 1);$
19. $\beta = \{5, 11, 17, 19, 2\}, \quad x = (1, 8, 3, 5, 0);$
20. $\beta = \{5, 7.11.13.2\}, \quad x = (0, 4, 1, 3, 0);$
21. $\beta = \{7, 11, 13, 17, 2\}, \quad x = (0, 1, 5, 13, 1);$
22. $\beta = \{5, 11, 17, 19, 2\}, \quad x = (0, 9, 3, 1, 0);$
23. $\beta = \{5, 7.11.13.2\}, \quad x = (1, 0, 10, 8, 1);$
24. $\beta = \{7, 11, 13, 17, 2\}, \quad x = (0, 4, 6, 10, 1);$
25. $\beta = \{5, 11, 17, 19, 2\}, \quad x = (3, 5, 4, 0, 0);$
26. $\beta = \{5, 11, 13, 19, 2\}, \quad x = (3, 1, 10, 4, 1);$
27. $\beta = \{5, 13, 17, 19, 2\}, \quad x = (1, 8, 4, 2, 1);$
28. $\beta = \{7, 11, 17, 19, 2\}, \quad x = (2, 6, 12, 14, 1);$
29. $\beta = \{5, 11, 13, 19, 2\}, \quad x = (1, 8, 2, 3, 1);$
30. $\beta = \{7, 11, 17, 19, 2\}, \quad x = (1, 3, 9, 11, 0).$

Задание 36

Для данного линейного генератора сравнений $x_{n+1} = ax_n + b \pmod{m}$ найти индекс вхождения в период, период и его длину при различных значениях первого элемента x_0 последовательности $\{x_n\}_{n \geq 0}$:

1. $a = 3, b = 1, m = 33, x_0 \in \{0, 6\};$
2. $a = 3, b = 1, m = 36, x_0 \in \{0, 2\};$
3. $a = 5, b = 1, m = 35, x_0 \in \{2, 5\};$
4. $a = 2, b = 1, m = 13, x_0 \in \{1, 12\};$
5. $a = 4, b = 1, m = 15, x_0 \in \{1, 3\};$
6. $a = 6, b = 1, m = 56, x_0 \in \{0, 3\};$
7. $a = 2, b = 1, m = 60, x_0 \in \{0, 2\};$
8. $a = 6, b = 1, m = 72, x_0 \in \{0, 6\};$
9. $a = 3, b = 1, m = 33, x_0 \in \{3, 8\};$
10. $a = 3, b = 1, m = 36, x_0 \in \{3, 5\};$
11. $a = 5, b = 1, m = 35, x_0 \in \{0, 8\};$
12. $a = 4, b = 1, m = 52, x_0 \in \{0, 2\};$
13. $a = 6, b = 1, m = 56, x_0 \in \{2, 4\};$
14. $a = 4, b = 1, m = 24, x_0 \in \{0, 6\};$
15. $a = 3, b = 1, m = 56, x_0 \in \{0, 2\};$
16. $a = 2, b = 1, m = 132, x_0 \in \{1, 2\};$
17. $a = 2, b = 1, m = 60, x_0 \in \{4, 5\};$
18. $a = 3, b = 1, m = 33, x_0 \in \{2, 21\};$
19. $a = 3, b = 1, m = 36, x_0 \in \{8, 10\};$
20. $a = 5, b = 1, m = 35, x_0 \in \{10, 11\};$
21. $a = 4, b = 1, m = 15, x_0 \in \{5, 13\};$
22. $a = 6, b = 1, m = 56, x_0 \in \{5, 6\};$
23. $a = 3, b = 2, m = 91, x_0 \in \{1, 4\};$
24. $a = 4, b = 1, m = 24, x_0 \in \{3, 9\};$
25. $a = 3, b = 1, m = 56, x_0 \in \{3, 5\};$
26. $a = 6, b = 1, m = 46, x_0 \in \{0, 2\};$
27. $a = 3, b = 1, m = 33, x_0 \in \{9, 30\};$
28. $a = 3, b = 1, m = 36, x_0 \in \{11, 15\};$

29. $a = 5, \quad b = 1, \quad m = 36, \quad x_0 \in \{1, 2\};$
30. $a = 4, \quad b = 1, \quad m = 52, \quad x_0 \in \{3, 4\}.$

Список литературы

1. Яблокова, С. И. Основы алгебраической алгоритмики. Ч. 1 / С. И. Яблокова. – Ярославль : ЯрГУ, 2008. – 127 с.
2. Яблокова, С. И. Основы алгебраической алгоритмики. Ч. 2 / С. И. Яблокова. – Ярославль : ЯрГУ, 2009. – 120 с.
3. Ноден, П. Алгебраическая алгоритмика / П. Ноден, К. Китте. – М. : Мир, 1999. – 720 с.
4. Акритас, А. Основы компьютерной алгебры с приложениями / А. Акритас. – М. : Мир, 1994. – 544 с.

Учебное издание

Яблокова Светлана Ивановна

Задачи по алгебраической алгоритмике

Практикум

Редактор, корректор Л. Н. Селиванова
Верстка С. И. Яблокова

Подписано в печать 28.01.16. Формат 60×84 1/8
Усл. печ. л. 8,83. Уч.- изд. л. 2,5.
Тираж 3 экз. Заказ 003/016.

Оригинал-макет подготовлен
в редакционно-издательском отделе ЯрГУ.

Ярославский государственный университет
им. П. Г. Демидова
150000, Ярославль, ул. Советская, 14.