БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра высшей математики

СБОРНИК ЗАДАЧ ПО ПРИКЛАДНОЙ АЛГЕБРЕ

Для студентов
факультета прикладной математики и информатики

МИНСК
2011

УДК 512(075.8)
ББК 22.14я73
С23

Авторы:
**Д. Ф. Базылев, М. М. Васьковский,
Г. В. Матвеев, Г. П. Размыслович, В. М. Ширяев**

Рекомендовано
ученым советом факультета
прикладной математики и информатики
18 октября 2011г., протокол № 2

Рецензент
кандидат физико-математических наук,
доцент *В. И. Чесалин*

Сборник задач по прикладной алгебре: для студентов
С23 факультета прикладной математики и информатики /
Д. Ф. Базылев [и др.]. – Минск: БГУ, 2011. – 67 с.

Представлены задачи по теории чисел, групп, колец, полей, теории кодирования и шифрования. Изложен краткий теоретический материал, даны практические рекомендации, указания и примеры решений.

Предназначено для студентов факультета прикладной математики и информатики.

© БГУ, 2011

ПРЕДИСЛОВИЕ

Курс прикладной алгебры, как раздел общего курса по геометрии и алгебре, читается на факультете прикладной математики и информатики на протяжении многих лет. Данный сборник задач является продолжением и дополнением к курсу лекций по данному предмету, поскольку здесь использован опыт проведения практических занятий. Содержание задачника соответствует программе курса.

Сборник состоит из десяти параграфов. Все десять параграфов условно можно разделить на три составные части: теория чисел (1 – 5), алгебраические структуры (6 – 8), основы криптологии (9,10). В начале каждого параграфа приводятся основные определения и факты из теории, формулы и решения типичных примеров.

В конце сборника приведены ответы для практически всех представленных задач.

1. КАНОНИЧЕСКОЕ РАЗЛОЖЕНИЕ, НОД, НОК, АЛГОРИТМ ЕВКЛИДА

Натуральное число *n*, большее единицы, называется *простым* числом, если его натуральными делителями являются лишь единица и само число *n*. Другие натуральные числа, большие единицы, называются *составными*.

Каноническим разложением натурального числа *n*, большего единицы, называется представление числа *n* в виде произведения примарных степеней $p_i^{a_i}$, т.е. $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$, где $p_1, \ldots, p_k$ – различные простые числа, $a_1, \ldots, a_k$ – натуральные числа. Говорят, что простое число p_i входит в каноническое разложение n с показателем a_i, и пишут $\mathrm{ord}_{p_i} n = a_i$. Каноническое разложение натурального числа существует и притом единственно с точностью до порядка следования множителей.

Пусть $a_1, \ldots, a_n$ – целые числа, не равные нулю.

Целое число d называется общим делителем чисел $a_1,\ldots,a_n$, если число d делит эти числа. *Наибольшим общим делителем* (НОД) чисел $a_1, \ldots, a_n$ называется натуральное число *D* такое, что числа $a_1, \ldots, a_n$ делятся на *D*, причем *D* само делится на любой другой общий делитель чисел $a_1, \ldots, a_n$. Наибольший общий делитель чисел $a_1, \ldots, a_n$ обозначается НОД$\{a_1, \ldots, a_n\}$ или $(a_1, \ldots, a_n)$.

Целое ненулевое число *k* называется общим кратным чисел $a_1, \ldots, a_n$, если число *к* делится на эти числа. *Наименьшим общим кратным* (НОК) чисел $a_1, \ldots, a_n$ называется натуральное число *K* такое, что число *K* делится на числа $a_1, \ldots, a_n$, причем любое общее кратное чисел $a_1, \ldots, a_n$ делится на *K*. Наименьшее общее кратное чисел $a_1, \ldots, a_n$ обозначается НОК$\{a_1, \ldots, a_n\}$ или $[a_1, \ldots, a_n]$.

Если известны представления натуральных чисел *a* и *b* в виде произведения примарных степеней, а именно, $a = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$, $b = p_1^{b_1} \cdot \ldots \cdot p_k^{b_k}$, то $(a,b) = p_1^{c_1} \cdot \ldots \cdot p_k^{c_k}$, $[a,b] = p_1^{d_1} \cdot \ldots \cdot p_k^{d_k}$, где $c_i = \min(a_i, b_i)$, $d_i = \max(a_i, b_i)$. В частности, $(a,b)\,[a,b] = ab$.

Для нахождения НОД и НОК верны следующие соотношения: $[a_1, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n]$, $(a_1, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n)$.

Пусть *a, b* – целые не нулевые числа, тогда существует единственная пара целых чисел *q, r* такая, что $a = bq + r$, причем $0 \le r < |b|$ (*теорема о делении с остатком*).

Кроме указанного выше метода нахождения наибольшего общего делителя двух чисел, который использует их канонические разложения, наибольший общий делитель можно найти также с помощью *алгоритма Евклида*. Для этого число a разделим на b с остатком: $a = bq_1 + r_1$, где $0 \le r_1 < |b|$. Если $r_1 = 0$, то $(a,b) = |b|$. Если $r_1 > 0$, то разделим b на r_1 с остатком: $b = r_1 q_2 + r_2$, где $0 \le r_2 < r_1$. Если $r_2 = 0$, то $(a,b) = r_1$. Если $r_2 > 0$, то разделим r_1 на r_2 с остатком: $r_1 = r_2 q_3 + r_3$, где $0 \le r_3 < r_2$. И так далее продолжаем эту процедуру. Конечный не нулевой остаток и будет наибольшим общим делителем чисел a и b.

С помощью алгоритма Евклида наибольший общий делитель чисел $a_1,\ldots,a_l$ можно представить в виде линейной комбинации этих чисел, а именно, существуют целые числа $y_1,\ldots,y_l$ такие, что $(a_1,\ldots,a_l) = y_1a_1+\ldots+y_la_l$. Такое представление называется линейным разложением наибольшего общего делителя чисел $a_1,\ldots,a_l$.

Числа $a_1,\ldots,a_l$ называются *взаимно простыми*, если $(a_1,\ldots,a_l)=1$. Числа $a_1,\ldots,a_l$ называются *попарно взаимно простыми*, если (a_1,a_k) для любых $i \ne k$.

Сформулируем некоторые свойства взаимно простых чисел:

1) если (a,b)=1, тогда (a,b)=(a,c);
2) если ab делится на c, $(b,c)=1$, то a делится на c;
3) если a делит c и b делит c и (a,b)=1, то ab делит c;
4) $(a_1,b)=1,\ldots,(a_n,b)=1$ тогда и только тогда, когда $(a_1\cdot\ldots\cdot a_n,b)=1$;
5) $(a,b)=1$ тогда и только тогда, когда $(a^m,b^n)=1$, где m, n – натуральные числа;
6) (a,b)=1 тогда и только тогда, когда найдутся числа u и v, такие, что имеет место равенство ua+vb=1.

Пример 1. Найдите наибольший общий делитель d и наименьшее общее кратное чисел 8633 и 7387, а также найдите целые числа a,b, такие, что $8633a + 7387b = d$.

Решение. Воспользуемся алгоритмом Евклида. Последовательно произведем следующие деления с остатком: $8633=7387\cdot1+1246$, $7387=1246\cdot5+1157$, $1246=1157\cdot1+89$, $1157=89\cdot13+0$. Следовательно,

$$\text{НОД}(8633,7387) = 89,\ \text{НОК}(8633,7387) = \frac{8633\cdot7387}{\text{НОД}(8633,7387)} = 716539.$$

Найдем линейное разложение наибольшего общего делителя. Так как $89=1\cdot1246-1\cdot1157=1\cdot1246-1\cdot(1\cdot7387-5\cdot1246)=6\cdot1246-1\cdot7387=6\cdot(1\cdot8633-1\cdot7387)-1\cdot7387=6\cdot8633-7\cdot7387$, то $d = 8633\cdot6 + 7387\cdot(-7)$ – искомое линейное разложение наибольшего общего делителя.

Пример 2. Определите, сколькими нулями оканчивается число $500!$.

Решение. Так как число нулей, которыми оканчивается число $500!$ есть максимальная степень 10, на которую делится $500!$, $10 = 2 \cdot 5$, то искомое число нулей равно $\min\{\text{ord}_2(500!), \text{ord}_5(500!)\}$. Ясно, что

$$\min\{\text{ord}_2(500!), \text{ord}_5(500!)\} = \text{ord}_5(500!) = \left[\frac{500}{5}\right] + \left[\frac{500}{25}\right] + \left[\frac{500}{125}\right] = 124$$ (см. задачи № 1.11, 1.12).

1.1. Найдите канонические разложения чисел:
1) 16 900, 2) 60 480, 3) 555 555, 4) $2^{22}+1$, 5) 3^6+5^6.

1.2. Докажите, что если натуральное число n, большее 1, не делится ни на одно простое число, не превосходящее $\sqrt{n}$, то число n является простым.

1.3. Какие из следующих чисел являются простыми: 161, 1001, 1087, 1357, 2011, 11111?

1.4. (*Евклид*) Докажите, что существует бесконечно много простых чисел.

1.5. Докажите, что существует бесконечно много простых чисел вида:
1) $3k+2$ ($k \in \mathrm{N}$), 2) $4k+3$ ($k \in \mathrm{N}$), 3) $6k+5$ ($k \in \mathrm{N}$).

1.6. Пусть n – натуральное число. Докажите, что существует натуральное число m, такое что числа $m, m+1, \ldots, m+n+1$ являются составными.

1.7. Пусть m, n – натуральные числа, большие 1.
1) (*Жермен*) Докажите, что число n^4+4 является составным;
2) докажите, что число $n^4+4^n m^4$ является составным.

1.8. Пусть n – натуральное число, большее 4.
1)Докажите, что число n является простым тогда и только тогда, когда $(n-1)!$ не делится на n;
2) (*Вильсон*) пусть n – натуральное число. Докажите, что число n является простым тогда и только тогда, когда $(n-1)!+1$ делится на n.

1.9. 1) Докажите, что число $\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{n}$ не является натуральным при $n>1$;
2) Докажите, что число $\frac{1}{1}+\frac{1}{3}+\ldots+\frac{1}{2n+1}$ не является натуральным для любого $n \in N$, $n>1$.

1.10. Докажите, что для любого натурального значения n произведение $(n+1)(n+2)\cdot\ldots\cdot(n+n)$ делится на 2^n.

1.11. Пусть $[x]$ обозначает наибольшее целое число, не превосходящее x. Докажите, что $\operatorname{ord}_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$ для любого натурального n и любого простого p.

1.12. 1) Сколькими нулями оканчивается число 2011!
2) Найдите максимальную степень, в которой число 21 входит в разложение числа 2011.

1.13. Вычислите наибольшие общие делители с помощью алгоритма Евклида и найдите их линейные разложения:
1) (187, 221), 2) (6188, 4709), 3) (2419, 1189, 1711), 4) (549, 387), 5) (78, 60, 24).

1.14. Вычислите наименьшие общие кратные:
1) [1189, 2419, 1711], 2) [6408, 9256, 4272], 3) [551, 899], 4) [549, 387], 5) [78, 60, 24].

1.15. Пусть $(a,b)=1$. Докажите, что
1) $(7a+6b, 8a+7b)=1$; 2) $(a+b, a^2+b^2)=1$ либо 2.

1.16. Найдите наибольшее возможное число шагов алгоритма Евклида для двух трёхзначных чисел.

1.17. Докажите, что для любого натурального $n>1$ отрезок $[n,n!]$ содержит простое число.

1.18. Докажите, что для любых натуральных m, n $(m \neq n)$ числа Ферма $f_m = 2^{2^m}+1$, $f_n = 2^{2^n}+1$ взаимно просты.

1.19. Пусть a, b - натуральные взаимно простые числа, произведение которых является точным квадратом. Докажите, что числа a и b являются точными квадратами.

1.20. Докажите, что если квадрат рационального положительного числа a является натуральным числом, то число a натуральное.

1.21. Существует ли многочлен с целыми коэффициентами от целой переменной, значениями которого могут быть только простые числа или им противоположные?

1.22. Найдите все натуральные n, такие, что $(n-1)!$ не делится на n^2.

1.23. Найдите все натуральные n, для которых n^2+1 делится на $n+1$.

1.24. Докажите, что $2^{f_n}-2$ делится на f_n для любого натурального n.

1.25. Докажите, что существует бесконечно много нечётных натуральных k, для которых все числа $f_{n,k} = 2^{2^n}+k$ $(n=1,2,\ldots)$ являются составными.

1.26. Докажите, что C_{600}^{300} делится на 7, а C_{1000}^{500} - нет.

2. СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ. ЛИНЕЙНЫЕ ДИОФАНТОВЫ УРАВНЕНИЯ

Пусть a, b – целые числа, m – натуральное число. Говорят, что a сравнимо с b по модулю m, если $a-b$ делится на m. В этом случае будем писать $a \equiv b(\mathrm{mod}\, m)$.

Приведем основные свойства сравнений:

1) $a \equiv a(\mathrm{mod}\, m)$;

2) если $a \equiv b(\mathrm{mod}\, m)$, то $b \equiv a(\mathrm{mod}\, m)$;

3) если $a \equiv b(\mathrm{mod}\, m)$, $b \equiv c(\mathrm{mod}\, m)$, то $a \equiv c(\mathrm{mod}\, m)$;

4) если $a \equiv b(\mathrm{mod}\, m)$, то $ca \equiv cb(\mathrm{mod}\, m)$;

5) если $ca \equiv cb(\mathrm{mod}\, m)$, $(c,m)=1$, то $a \equiv b(\mathrm{mod}\, m)$;

6) если $a \equiv b(\mathrm{mod}\, m)$, то $ca \equiv cb(\mathrm{mod}\, cm)$;

7) если $a \equiv b(\mathrm{mod}\, m)$, $c \equiv d(\mathrm{mod}\, m)$, то $a \pm c \equiv b \pm d(\mathrm{mod}\, m)$, $ac \equiv bd(\mathrm{mod}\, m)$;

8) если $a \equiv b(\mathrm{mod}\, m)$, то $a^n \equiv b^n(\mathrm{mod}\, m)$ для любого натурального n;

9) если $a \equiv b(\mathrm{mod}\, m)$, $f(x)$ – многочлен с целыми коэффициентами, то $f(a) \equiv f(b)\ (\mathrm{mod}\, m)$;

10) $a \equiv b(\mathrm{mod}\, m_1), \ldots, a \equiv b(\mathrm{mod}\, m_k)$ тогда и только тогда, когда $a \equiv b(\mathrm{mod}\, [m_1,...,m_k])$;

11) если $a \equiv b(\mathrm{mod}\, m)$ и m делится на d, то $a \equiv b(\mathrm{mod}\, d)$;

12) если $a^k \equiv b^k(\mathrm{mod}\, m)$ и n делится на k, то $a^n \equiv b^n(\mathrm{mod}\, m)$.

Пусть a, b – целые числа, $a \neq 0$, m – натуральное число. Сравнение $ax \equiv b(\mathrm{mod}\, m)$ называется *разрешимым*, если существует целое число x_0 такое, что $ax_0 \equiv b(\mathrm{mod}\, m)$. В этом случае число x_0 называется решением сравнения $ax \equiv b(\mathrm{mod}\, m)$.

Сравнение $ax \equiv b(\mathrm{mod}\, m)$ разрешимо тогда и только тогда, когда b делится на (a, m). Причем, если x_0 - это одно из решений сравнения $ax \equiv b(\mathrm{mod}\, m)$, то множество всех решений этого сравнения имеет вид:

$$\left\{x_0 + \frac{m}{(a,m)}t : t \in Z\right\}, \text{ т.е. } ax \equiv b(\mathrm{mod}\, m) \Leftrightarrow x \equiv x_0\left(\mathrm{mod}\frac{m}{(a,m)}\right).$$

Вышеуказанное решение линейного сравнения $ax \equiv b(\mathrm{mod}\, m)$ позволяет найти все решения *линейного диофантова уравнения* $ax + by = c,$ где a, b, c – целые числа, $a, b \neq 0.$ Диофантово уравнение $ax + by = c$ имеет решение в целых числах *x, y* тогда и только тогда, когда *c* делится на (*a,b*). Причем, если (x_0, y_0) – это одно из решений этого уравнения, то множество всех решений задается в виде $x = x_0 + \frac{b}{(a,b)}t, y = y_0 - \frac{a}{(a,b)}t,$ где *t* пробегает множество всех целых чисел. Частное решение (x_0, y_0) можно найти с помощью алгоритма Евклида. Индукцией по числу переменных аналогичным образом можно решить линейное диофантово уравнение от *n* переменных $a_1x_1 + ... + a_nx_n = b.$

Пусть $m_1, ..., m_k$ – попарно взаимно простые натуральные числа и $m = m_1 \cdot ... \cdot m_k,$ а $c_1, ..., c_k$ – целые числа. Тогда множество решений системы сравнений $\begin{cases} x \equiv c_1(\mathrm{mod}\, m_1) \\ ..... \\ x \equiv c_k(\mathrm{mod}\, m_k) \end{cases}$ имеет вид $x \equiv c_1x_1\frac{m}{m_1} + ... + c_kx_k\frac{m}{m_k}(\mathrm{mod}\, m),$ где x_i – произвольное целое число, удовлетворяющее сравнению $x_i\frac{m}{m_i} \equiv 1(\mathrm{mod}\, m_i)$ (*китайская теорема об остатках*).

Пример 1. Решите сравнение $15x \equiv 39(\mathrm{mod}\, 84).$

Решение. С помощью алгоритма Евклида найдем частное решение x_0 исходного сравнения. Имеем 84=15·5+9,15=9·1+6,9=6·1+3,6=3·2+0. Поэтому 3=9–6·1=9–(15–9·1)·1=9·2–15·1=(84–15·5)·2–15·1=84·2+15·(–11), следовательно, 39=3·13=84·26+15·(–143), т.е. 15·(–143)≡39(mod 84), значит, $x_0 = -143.$ Поэтому множество всех решений исходного сравнения имеет вид $x \equiv -143\left(\mathrm{mod}\frac{84}{(15,84)}\right),$ т.е. $x \equiv -3\,(\mathrm{mod}\, 28).$

Пример 2. Решите уравнение $6x + 10y + 15z = 7$ в целых числах.

Решение. Зафиксируем переменную z и рассмотрим исходное уравнение как диофантово уравнение относительно переменных x, y. Уравнение $6x + 10y = 7 - 15z$ разрешимо тогда и только тогда, когда $(6,10) = 2 \mid 7 - 15z$, т.е. при $z = 2s + 1,\ s \in Z.$ Поэтому $6x + 10y = -8 - 30s$. Найдем частное решение x_0, y_0. Используя алгоритм Евклида, находим линейное разложение наибольшего общего делителя чисел 6 и 10: 10=1·6+4, 6=1·4+2, 4=2·2+0, откуда следует, что 2-1·6–1·4=1·6–1·(1·10–

$-1\cdot 6)=2\cdot 6-1\cdot 10$. Поэтому $x_0=2\cdot(-4-15s)=-8-30s$, $y_0=-1\cdot(-4-15s)=4+15s$. Общее решение исходного уравнения: $x=-8-30s+5t$, $y=4+15s-3t$, $z=1+2s$, где $s,t\in Z$.

Ответ: $x=-8-30s+5t$, $y=4+15s-3t$, $z=1+2s$, где $s,t\in Z$.

Пример 3. Решите систему сравнений $\begin{cases}7x\equiv 11(\mathrm{mod}\,18),\\ 8x\equiv 1(\mathrm{mod}\,27),\\ 9x\equiv 13(\mathrm{mod}\,28).\end{cases}$

Решение. Преобразуем исходную систему:

$$\begin{cases}7x\equiv 11(\mathrm{mod}\,18),\\ 8x\equiv 1(\mathrm{mod}\,27),\\ 9x\equiv 13(\mathrm{mod}\,28)\end{cases}\Leftrightarrow\begin{cases}7x\equiv 11(\mathrm{mod}\,2), 7x\equiv 11(\mathrm{mod}\,3^2),\\ 8x\equiv 1(\mathrm{mod}\,3^3),\\ 9x\equiv 13(\mathrm{mod}\,2^2), 9x\equiv 13(\mathrm{mod}\,7),\end{cases}\Leftrightarrow$$

$$\begin{cases}x\equiv 1(\mathrm{mod}\,2), x\equiv 8(\mathrm{mod}\,3^2),\\ x\equiv 17(\mathrm{mod}\,3^3),\\ x\equiv 1(\mathrm{mod}\,2^2), x\equiv 3(\mathrm{mod}\,7),\end{cases}\Leftrightarrow\begin{cases}x\equiv 3(\mathrm{mod}\,7),\\ x\equiv 17(\mathrm{mod}\,3^3),\\ x\equiv 1(\mathrm{mod}\,2^2).\end{cases}$$

К последней системе применим китайскую теорему об остатках. Найдем частные решения сравнений $108x_1\equiv 1(\mathrm{mod}7)$, $28x_2\equiv 1(\mathrm{mod}27)$, $189x_3\equiv 1(\mathrm{mod}4)$. Имеем $x_1=5$, $x_2=1$, $x_3=1$. Поэтому решение исходной системы имеет вид: $x\equiv 3\cdot 5\cdot 27\cdot 4+17\cdot 1\cdot 7\cdot 4+1\cdot 1\cdot 7\cdot 27(\mathrm{mod}\,756)$, т.е. $x\equiv 17(\mathrm{mod}\,756)$.

Пример 4 . Решите систему уравнений $\begin{cases}4x-4y+3z=3,\\ 5x-7y+6z=4,\end{cases}$ в целых числах.

Решение. Решаем систему методом Гаусса:

$$\left[\begin{array}{ccc|c}4&-4&3&3\\5&-7&6&4\end{array}\right]\sim\left[\begin{array}{ccc|c}4&-4&3&3\\-3&1&0&-2\end{array}\right]\sim\left[\begin{array}{ccc|c}-8&0&3&-5\\-3&1&0&-2\end{array}\right]\sim\left[\begin{array}{ccc|c}-8/3&0&1&-5/3\\-3&1&0&-2\end{array}\right].$$

Откуда следует, что $(x,y,z)=(\alpha,3\alpha-2,8\alpha/3-5/3)$, $\alpha\in Z$, $8\alpha/3-5/3\in Z$. Следовательно, $1-\alpha\in 3Z$, т.е. $\alpha=3t+1$, $t\in Z$. Окончательно получаем $(x,y,z)=(1+3t,1+9t,1+8t)$, $t\in Z$.

Замечание. Отметим, что способ, изложенный выше при решении этой задачи слишком трудоемок, если n–rank $A>1$, где n число неизвестных.

2.1. Решите следующие сравнения:

1) $25x \equiv 10 (\mathrm{mod}\, 855)$, 2) $22x \equiv 63 (\mathrm{mod}\, 119)$, 3) $6x \equiv 13 (\mathrm{mod}\, 127)$,

4) $88x \equiv 324 (\mathrm{mod}\, 404)$.

2.2. Решите следующие уравнения в целых числах:

1) $15x + 84y = 39$, 2) $18x + 35y = 1$, 3) $91x + 117y = 156$,

4) $258x + 172y = 112$, 5) $53x + 47y = 1$.

2.3. Решите следующие уравнения в целых числах:

1) $4x - 4y + 3z = 3$, 2) $5x + 8y - 14z - 6u = 5$,

3) $25x - 13y + 7z = 4$, 4) $3x - 6y + 8z - 12u = 1$.

2.4. Пусть $a_1, ..., a_n, b$ - целые числа, не все из которых равны 0.

1) Докажите, что уравнение $a_1x_1 + ...a_nx_n = b$ разрешимо в целых числах тогда и только тогда, когда $(a_1, ..., a_n) \mid b$.

2) Пусть $(x_1^0, ..., x_n^0)$ - частное решение неоднородного уравнения $a_1x_1 + ...a_nx_n = b$, $(x_1^1, ..., x_n^1), ..., (x_1^{n-1}, ..., x_n^{n-1})$ - линейно независимые решения однородного уравнения $a_1x_1 + ...a_nx_n = 0$. Докажите, что общее решение неоднородного уравнения $a_1x_1 + ...a_nx_n = b$ задается формулой $(x_1^0, ..., x_n^0) + (x_1^1, ..., x_n^1)t_1 + ... + (x_1^{n-1}, ..., x_n^{n-1})t_{n-1}$, где $t_1, ..., t_{n-1}$ - произвольные целые числа.

2.5. Используя китайскую теорему об остатках, решите следующие системы сравнений:

1) $\begin{cases} x \equiv 1 (\mathrm{mod}\, 4), \\ x \equiv 3 (\mathrm{mod}\, 5), \\ x \equiv 2 (\mathrm{mod}\, 7); \end{cases}$ 2) $\begin{cases} x \equiv 3 (\mathrm{mod}\, 5), \\ x \equiv 2 (\mathrm{mod}\, 7), \\ x \equiv 1 (\mathrm{mod}\, 11); \end{cases}$ 3) $\begin{cases} x \equiv 3 (\mathrm{mod}\, 7), \\ x \equiv 2 (\mathrm{mod}\, 11), \\ x \equiv 3 (\mathrm{mod}\, 13); \end{cases}$

4) $\begin{cases} 2x \equiv 1 (\mathrm{mod}\, 3), \\ 3x \equiv 2 (\mathrm{mod}\, 5), \\ 4x \equiv 2 (\mathrm{mod}\, 7); \end{cases}$ 5) $\begin{cases} 2x \equiv 3 (\mathrm{mod}\, 13), \\ 3x \equiv 1 (\mathrm{mod}\, 31), \\ 4x \equiv 5 (\mathrm{mod}\, 23); \end{cases}$ 6) $\begin{cases} 4x \equiv 11 (\mathrm{mod}\, 13), \\ 9x \equiv 2 (\mathrm{mod}\, 17), \\ 5x \equiv 3 (\mathrm{mod}\, 9), \\ 8x \equiv 4 (\mathrm{mod}\, 14); \end{cases}$

7) $\begin{cases} x \equiv 11 (\mathrm{mod}\, 100), \\ x \equiv 15 (\mathrm{mod}\, 24), \\ x \equiv 6 (\mathrm{mod}\, 35); \end{cases}$ 8) $\begin{cases} x \equiv 2 (\mathrm{mod}\, 15), \\ x \equiv -3 (\mathrm{mod}\, 20), \\ x \equiv -2 (\mathrm{mod}\, 6); \end{cases}$ 9) $\begin{cases} 5x \equiv 8 (\mathrm{mod}\, 12), \\ 7x \equiv 16 (\mathrm{mod}\, 18), \\ 11x \equiv 8 (\mathrm{mod}\, 42). \end{cases}$

2.6. Решите следующие системы уравнений в целых числах:

1) $\begin{cases} 3x+28y-26z+15u=16, \\ x+14y-14z+9u=10, \end{cases}$ 2) $\begin{cases} 7x+5y-z+5u=16, \\ 3x+y-z+2u=5, \\ 5x+7y+z+4u=17, \end{cases}$

3) $\begin{cases} 2x+y-4z=0, \\ 3x+5y-7z=0, \end{cases}$ 4) $\begin{cases} 2x-y+5z+7u=0, \\ 4x-2y+7z+5u=0. \end{cases}$

2.7. Найдите все натуральные решения уравнения $x^2+y^2=z^2$.

2.8. Докажите, что уравнение $x^4+y^4=z^2$ не имеет решений в натуральных числах.

2.9. Пусть x,y,z - целые числа, удовлетворяющие равенству $x^3+2y^3+4z^3=0$. Докажите, что $x=y=z=0$.

2.10. Докажите, что уравнение $15x^2-7y^2=9$ не имеет решений в целых числах.

2.11. Докажите, что для любого натурального m найдутся целые числа a,b,c, такие, что уравнение $ax+by+c=0$ имеет ровно m решений в натуральных числах x,y.

2.12. Докажите, что для любых натуральных m,n найдутся целые числа a,b,c, такие, что уравнение $ax+by+c=0$ имеет единственное решение $x=m$, $y=n$ в натуральных числах.

2.13. Найдите все простые числа p и натуральные числа x,y,n, удовлетворяющие уравнению $x(x+1)=p^{2n}y(y+1)$.

3. ФУНКЦИЯ ЭЙЛЕРА

Пусть m – натуральное число, большее единицы. Количество натуральных чисел, меньших m и которые взаимно просты с m обозначается через $\varphi(m)$. Функция φ, определяемая на множестве N – натуральных чисел, называется *функцией Эйлера*.

По определению полагается $\varphi(1)=1$.

Отметим, что функция Эйлера мультипликативна, т.е. для любых взаимно простых натуральных чисел m, n выполняется равенство $\varphi(mn)=\varphi(m)\varphi(n)$ и если $p_1^{a_1}\cdot\ldots\cdot p_k^{a_k}$ – каноническое разложение числа m, то

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right) = p_1^{a_1-1}\cdot\ldots\cdot p_k^{a_k-1}\cdot(p_1-1)\cdot\ldots\cdot(p_k-1).$$

Если m – натуральное , а a – целое число и их НОД равен единице, то $a^{\varphi(m)} \equiv 1 (\mathrm{mod} m)$ (*теорема Эйлера*).

Следствием теоремы Эйлера является *теорема Ферма*: если p – простое, а a – целое число, причем $(a, p) = 1$, то $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. Теорему Ферма можно сформулировать иначе: пусть p – простое число, a – целое число, тогда $a^p \equiv a (\mathrm{mod}\, p)$.

Говорят, что целые числа $a_0, a_1, ..., a_{m-1}$ образуют *полную систему вычетов* по модулю m, если они попарно не сравнимы по модулю m. Целые числа $a_1, ..., a_{\varphi(m)}$ образуют *приведенную систему вычетов* по модулю m, если они взаимно просты с числом m и попарно не сравнимы между собой по модулю m. Легко проверить, что числа $a_0, a_1, ..., a_{m-1}$ образуют полную систему вычетов по модулю m тогда и только тогда, когда эти числа дают различные остатки при делении на m.

Пример 1. Используя теорему Ферма, вычислите остаток при делении 17^{108} на 29.

Решение. Имеем $17^{108} = 17^{28\cdot 3+24} \equiv 17^{24} = 289^{12} \equiv (-1)^{12} = 1 (\mathrm{mod}\, 29)$.

Пример 2. Используя теорему Эйлера и китайскую теорему об остатках, найдите остаток при делении $8\cdot 5^{41}$ на 96.

Решение. Пусть $x \equiv 8\cdot 5^{41} (\mathrm{mod}\, 2^5\cdot 3)$, тогда $\begin{cases} x \equiv 8\cdot 5^{41} (\mathrm{mod}\, 2^5), \\ x \equiv 8\cdot 5^{41} (\mathrm{mod}\, 3). \end{cases}$

Используя теорему Эйлера, находим, что $\begin{cases} x \equiv 8\cdot 5^{9} (\mathrm{mod}\, 32), \\ x \equiv 1 (\mathrm{mod}\, 3). \end{cases}$

Далее $\begin{cases} x \equiv 8 (\mathrm{mod}\, 32), \\ x \equiv 1 (\mathrm{mod}\, 3). \end{cases}$

Используя китайскую теорему об остатках, находим $x \equiv 40 (\mathrm{mod}\, 96)$.

3.1. Вычислите: 1) $\varphi(19)$, 2) $\varphi(121)$, 3) $\varphi(360)$, 4) $\varphi(990)$, 5) $\varphi(4320)$.

3.2. Сколько чисел от 1 до 120 не взаимно просты с числом 30?

3.3. Пусть p, q – простые числа, $p - q = 2, \varphi(pq) = 120$. Найдите p, q.

3.4. Пусть a, b – взаимно простые натуральные числа, p – простое число, $p \equiv 3 (\mathrm{mod}\, 4)$. Докажите, что $a^2 + b^2$ не делится на p.

3.5. Найдите все простые числа p такие, что

1) числа p^2-6, p^2+6 также являются простыми;

2) числа p^3-6, p^3+6 также являются простыми.

3.6. Пусть n – нечетное натуральное число. Докажите, что $2^{n!}-1$ делится на n.

3.7. Используя теорему Ферма, вычислите следующие остатки:

1) $28^{97}\cdot 100^{50}(\mathrm{mod}\,41)$, 2) $37^{97}\cdot 23^{15}(\mathrm{mod}\,61)$, 3) $464^{828}(\mathrm{mod}\,89)$,

4) $7^{100}+11^{100}(\mathrm{mod}13)$.

3.8. Используя теорему Ферма и китайскую теорему об остатках, вычслите следующие остатки:

1) $28^{179}(\mathrm{mod}143)$, 2) $35^{100}(\mathrm{mod}174)$, 3) $11^{1974}\cdot 7^{78}\cdot 3^{9}(\mathrm{mod}1495)$,

4) $50^{199}(\mathrm{mod}\,323)$, 5) $59^{2011}(\mathrm{mod}1001)$.

3.9. Используя теорему Эйлера, вычислите следующие остатки:

1) $17^{2000}(\mathrm{mod}\,27)$, 2) $2^{370}\cdot 3^{549}(\mathrm{mod}\,217)$, 3) $15^{400}\cdot 17^{270}(\mathrm{mod}\,256)$,

4) $7^{243}(\mathrm{mod}\,225)$, 5) $2^{2011}+3^{2011}(\mathrm{mod}\,625)$.

3.10. Используя теорему Эйлера и китайскую теорему об остатках, вычислите следующие остатки:

1) $7\cdot 13^{50}\,\mathrm{mod}(784)$, 2) $11^{2011}\cdot 17^{2012}(\mathrm{mod}\,2160)$, 3) $5^{509}(\mathrm{mod}1323)$,

4) $37^{43}(\mathrm{mod}\,616)$.

3.11. Докажите, что для любого простого числа p и любого целого числа a сравнение $x^x\equiv a(\mathrm{mod}\,p)$ разрешимо.

3.12. Найдите все натуральные числа n, для которых n делится на $\varphi(n)$.

3.13. Докажите, что для простых $p>5$ и натуральных m равенство $(p-1)!+1=p^m$ невозможно.

3.14. Пусть натуральные числа a и b таковы, что b^n+n делится на a^n+n для любого натурального n. Докажите, что $a=b$.

3.15. Найдите все простые числа p, такие, что 2^p+1 делится на p.

3.16. Найдите все натуральные x, удовлетворяющие равенству

1) $\varphi(2x)=\varphi(3x)$, 2) $\varphi(5x)=\varphi(7x)$.

3.17. Докажите, что существует бесконечно много простых чисел вида $4k+1$ $(k\in N)$.

4. ПЕРВООБРАЗНЫЕ КОРНИ И ИНДЕКСЫ

Пусть a, m – натуральные взаимно простые числа, причем $m>1$, тогда, согласно теореме Эйлера, $a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m)$. Наименьшее натуральное

число n такое, что $a^n \equiv 1(\mathrm{mod}\, m)$ называется *показателем*, которому принадлежит число a по модулю m.

Приведем основные свойства показателей:

1) числа $1, a^1, ..., a^{n-1}$ попарно не сравнимы по модулю m;
2) $a^{k_1} \equiv a^{k_2}(\mathrm{mod}\, m)$ тогда и только тогда, когда $k_1 \equiv k_2(\mathrm{mod}\, n)$;
3) $\varphi(m)$ делится на n;
4) если bc – показатель, которому принадлежит число x по модулю m, то b – показатель, которому принадлежит число x^c по модулю m;
5) пусть a – показатель, которому принадлежит число x по модулю m, b – показатель, которому принадлежит число y по модулю m, причем числа a и b взаимно простые, тогда ab – показатель, которому принадлежит число xy по модулю m.

Если $\varphi(m)$ – показатель, которому принадлежит число a по модулю m, то число a называется *первообразным корнем* по модулю m. Известно, что первообразный корень по модулю m существует тогда и только тогда, когда $m = 2, 4, p^k, 2p^k$, где p – нечетное простое число.

Для нахождения первообразных корней удобно использовать следующий факт. Пусть $q_1^{r_1} ... q_k^{r_k}$ – каноническое разложение числа $\varphi(m)$, g – натуральное число, взаимно простое с числом m. Число g является первообразным корнем по модулю m тогда и только тогда, когда $g^{\frac{\varphi(m)}{q_i}}$ не сравнимо с единицей по модулю m для любого i.

Пусть $m = p^k$ или $2p^k$, $c = \varphi(m)$, g – первообразный корень по модулю m, тогда числа $1, g, ..., g^{c-1}$ образуют приведенную систему вычетов по модулю m. Пусть число a взаимно просто с числом m. Целое неотрицательное число d называется *индексом* числа a по модулю m при основании g, если $g^d \equiv a(\mathrm{mod}\, m)$. Индекс d обозначают $ind_g a$ или $ind\ a$. Вообще говоря, индекс определен не однозначно, но если известен один из индексов d, то любой другой индекс d' можно найти по формуле $d' \equiv d(\mathrm{mod}\, c)$.

Свойства индексов:

1) $ind_g\ a_1 \cdot ... \cdot a_n \equiv ind_g a_1 + ... + ind_g a_n\ (\mathrm{mod}\, c)$;
2) $ind_g\ a^n \equiv n \cdot ind_g\ a(\mathrm{mod}\, c)$ для любого натурального значения n.

Если $(a, m) = 1, x^n \equiv a(\mathrm{mod}\, m)$ для некоторого целого значения x, то число a называется *вычетом* степени n по модулю m. В противном случае, число a называется *невычетом* степени n по модулю m. В приведенной системе вычетов по модулю m число вычетов степени n по модулю

m равно $\frac{\varphi(m)}{(\varphi(m),n)}$. Число a является вычетом степени n по модулю m тогда и только тогда, когда $a^q \equiv 1(\mathrm{mod}\, m)$, где $q = \frac{\varphi(m)}{(\varphi(m),n)}$.

Пусть $c = \varphi(m)$. Показатель, которому принадлежит число a по модулю m, равен $\frac{c}{(c, ind\ a)}$. В частности, число a является первообразным корнем по модулю m тогда и только тогда, когда $(c, ind\ a) = 1$. В приведенной системе вычетов по модулю m количество чисел, принадлежащих показателю t, равно $\varphi(t)$. В частности, количество первообразных корней в приведенной системе вычетов по модулю m равно $\varphi(\varphi(m))$.

Системой индексов нечетного числа a по модулю 2^k ($k \in N$) называется пара чисел (γ, γ_0) такая, что $(-1)^\gamma 5^{\gamma_0} \equiv a(\mathrm{mod}\, 2^k)$. Зная одну пару индексов (γ, γ_0), можно найти все такие пары индексов (δ, δ_0) по формулам $\delta \equiv \gamma(\mathrm{mod}\, c), \delta_0 \equiv \gamma_0(\mathrm{mod}\, c_0)$, где $\begin{cases} c = 1, c_0 = 1 \text{ при k} = 1, \\ c = 2, c_0 = 2^{k-2} \text{ при k} > 1. \end{cases}$

Пусть $2^{\alpha_0} p_1^{\alpha_1} ... p_k^{\alpha_k}$ – каноническое разложение числа m, m>1, (a,m)=1, g_i – первообразный корень по модулю $p_i^{\alpha_i}$. Упорядоченный набор $(\gamma, \gamma_0, \gamma_1, ..., \gamma_k)$ называется *системой индексов числа a по модулю m*, если $(-1)^\gamma 5^{\gamma_0} \equiv a(\mathrm{mod}\, 2^{\alpha_0})$, $g_i^{\gamma_i} \equiv a(\mathrm{mod}\, p_i^{\alpha_i})$ для любого $i = 1, ..., k$. Любая другая система индексов $(\delta, \delta_0, \delta_1, ..., \delta_k)$ связана с исходной следующим образом: $\delta \equiv \gamma(\mathrm{mod}\, c), \delta_i \equiv \gamma_i(\mathrm{mod}\, c_i)$, где

$$\begin{cases} c = 1, c_0 = 1 \text{ при k} = 1, \\ c = 2, c_0 = 2^{k-2} \text{ при k} > 1, \\ c_i = \varphi(p_i^{\alpha_i}) \text{ при i} = 1, ..., k. \end{cases}$$

Пример 1. Найдите число первообразных корней в приведенной системе вычетов по модулю 31, и найдите эти первообразные корни.

Решение. Число первообразных корней в приведенной системе вычетов по модулю 31 равно $\varphi(\varphi(31)) = \varphi(30) = 8$. Так как $\varphi(31) = 30 = 2 \cdot 3 \cdot 5$ и $3^{15} \equiv 30 \not\equiv 1(\mathrm{mod}\, 31)$, $3^{10} \equiv 25 \not\equiv 1(\mathrm{mod}\, 31)$, $3^6 \equiv 16 \not\equiv 1(\mathrm{mod}\, 31)$, то число 3 является первообразным корнем по модулю 31. Число a является первообразным корнем по модулю 31 тогда и только тогда, когда $(\mathrm{ind}_3\ a, \varphi(31)) = 1$. Отсюда следует, что $\mathrm{ind}_3\ a \in \{1,7,11,13,17,19,23,29\}$.

Следовательно, $a \equiv 3^1, 3^7, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{29} (\mathrm{mod}\, 31)$. Первообразные корни по модулю 31: 3, 17, 13, 24, 22, 12, 11, 21.

Пример 2. Найдите число вычетов степени 6 в приведенной системе вычетов по модулю 31, а также найдите эти вычеты.

Решение. Искомое число вычетов равно $\dfrac{\varphi(31)}{(\varphi(31), 6)} = 5$. Число a является вычетом степени 6 по модулю 31 тогда и только тогда, когда $a^5 \equiv 1 (\mathrm{mod}\, 31)$. Так как число 3 является первообразным корнем по модулю 31, то сравнение $a^5 \equiv 1 (\mathrm{mod}\, 31)$ равносильно сравнению $5 \mathrm{ind}_3 a \equiv 0 (\mathrm{mod}\, 30)$. Отсюда $\mathrm{ind}_3 a \equiv 0 (\mathrm{mod}\, 6)$, то есть $\mathrm{ind}_3 a \in \{6, 12, 18, 24, 30\}$. Следовательно, $a \equiv 3^6, 3^{12}, 3^{18}, 3^{24}, 3^{30} (\mathrm{mod}\, 31)$. Вычеты степени 6 в приведенной системе вычетов по модулю 31: 16, 8, 4, 2, 1.

Пример 3. Найдите, какому показателю принадлежит число 5 по модулю 29.

Решение. Так как $\varphi(29) = 28$, то показатель n, которому принадлежит число 5 по модулю 29, делит число 28. Поскольку $5^1 \equiv 5 \not\equiv 1 (\mathrm{mod}\, 29)$, $5^2 \equiv 25 \not\equiv 1 (\mathrm{mod}\, 29)$, $5^4 \equiv 16 \not\equiv 1 (\mathrm{mod}\, 29)$, $5^7 \equiv 28 \not\equiv 1 (\mathrm{mod}\, 29)$, $5^{14} \equiv 1 (\mathrm{mod}\, 29)$, то $n = 14$.

Пример 4. Постройте систему индексов числа 17 по модулю 8928, выбрав наименьшие положительные первообразные корни.

Решение. Имеем $8928 = 2^5 \cdot 3^2 \cdot 31$. Используя таблицу индексов

$(-1)^{\gamma} 5^{\gamma_0} (\mathrm{mod}\, 32)$	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
γ	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
γ_0	8	3	1	2	6	5	7	4	4	7	5	6	2	1	3	8

по модулю 32, находим, что $17 \equiv (-1)^2 5^4 (\mathrm{mod}\, 32)$. Так как число 2 является первообразным корнем по модулю 9, число 3 является первообразным корнем по модулю 31, $\mathrm{ind}_2 17 (\mathrm{mod}\, 9) = 3$, $\mathrm{ind}_3 17 (\mathrm{mod}\, 31) = 7$, то набор $(2, 4, 3, 7)$ является системой индексов числа 17 по модулю 8928.

4.1. Найдите число первообразных корней по модулю:
1) 59, 2) 143, 3) 2011, 4) 67, 5) 54.

4.2. Найдите все первообразные корни по модулю:
1) 41, 2) 29, 3) 50, 4) 54, 5) 23.

4.3. Найдите число вычетов четвертой степени в приведенной системе вычетов по модулю: 1) 41, 2) 29, 3) 50, 4) 54, 5) 23.

4.4. Найдите вычеты четвертой степени в приведенной системе вычетов по модулю:
1) 41, 2) 29, 3) 50, 4) 54, 5) 23.

4.5. Является ли число g первообразным корнем по модулю m, если
1) $g=2,\ m=29$; 2) $g=3,\ m=61$; 3) $g=7,\ m=2012$;
4) $g=9,\ m=17$, 5) $g=3,\ m=2011$?

4.6. Найдите показатель, которому принадлежит число 2 по модулю 31.

4.7. Пусть $p,\ q$ – простые числа, $2^p \equiv 1(\mathrm{mod}\, q)$. Докажите, что $q \equiv 1(\mathrm{mod}\, p)$.

4.8. Докажите, что не существует натурального числа n, большего 1, такого, что $2^n - 1$ делится на n.

4.9. Найдите все простые числа $p \geq 3$ и целые числа x, y, удовлетворяющие уравнению $x^{p-1} + x^{p-2} + \ldots + x + 2 = y^2$.

4.10. Докажите, что любой натуральный делитель d числа Ферма $f_n = 2^{2^n} + 1$ имеет вид $d = 2^{n+1}x + 1,\ x \in N \cup \{0\}$. Используя этот факт, покажите, что наименьший простой делитель числа f_5 равен 641.

4.11. Найдите все нечетные натуральные n, такие, что $3^n + 1$ делится на n.

4.12. Пусть натуральное число a принадлежит показателю δ по модулю m. Для любого натурального числа γ найдите показатель, которому принадлежит число a^γ по модулю m.

4.13. Пусть натуральное число a принадлежит показателю δ по модулю m. Для любого натурального числа γ найдите натуральное число, которое принадлежит показателю (δ, γ) по модулю m.

4.14. В приведенной системе вычетов найдите все числа, принадлежащие показателю 6 по модулю 43.

4.15. Постройте систему индексов числа a по модулю $m = 2^{a_0} \cdot p_1^{a_1} \cdot \ldots \cdot p_1^{a_k}$, выбрав наименьшие положительные корни по примарным модулям, если:
1) $a=19,\ m=2624$; 2) $a=17,\ m=288$; 3) $a=29,\ m=1001$;
4) $a=23,\ m=2010$; 5) $a=15,\ m=5984$.

5. ПОКАЗАТЕЛЬНЫЕ И ПОЛИНОМИАЛЬНЫЕ СРАВНЕНИЯ

Рассмотрим показательное сравнение

$$a^x \equiv b(\mathrm{mod}\, m), \qquad (5.1)$$

где $(a,m)=1$. Условие $(b,m)=1$ является необходимым для разрешимости сравнения (5.1). Пусть $2^{\alpha_0} p_1^{\alpha_1}...p_k^{\alpha_k}$ - каноническое разложение модуля m, где α_0 может быть нулем. Сравнение (5.1) равносильно системе сравнений:

$$a^x \equiv b(\mathrm{mod}\, 2^{\alpha_0}),\ a^x \equiv b(\mathrm{mod}\, p_i^{\alpha_i}),\ i=\overline{1,k} \qquad (5.2).$$

Пусть $(\gamma,\gamma_0,\gamma_1,...,\gamma_k)$, $(\delta,\delta_0,\delta_1,...,\delta_k)$ - системы индексов соответственно чисел a и b по модулю m, т.е. $(-1)^{\gamma}5^{\gamma_0} \equiv a(\mathrm{mod}\, 2^{\alpha_0})$, $g_i^{\gamma_i} \equiv a(\mathrm{mod}\, p_i^{\alpha_i})$, $(-1)^{\delta}5^{\delta_0} \equiv b(\mathrm{mod}\, 2^{\alpha_0})$, $g_i^{\delta_i} \equiv b(\mathrm{mod}\, p_i^{\alpha_i})$, где g_i - первообразный корень по модулю $p_i^{\alpha_i}$ $(i=\overline{1,k})$. Тогда система (5.2) эквивалентна системе сравнений первого порядка:

$$x\gamma \equiv \delta(\mathrm{mod}\, c),\ x\gamma_0 \equiv \delta_0(\mathrm{mod}\, c_0),\ x\gamma_i \equiv \delta_i(\mathrm{mod}\, c_i),\ i=\overline{1,k}, \qquad (5.3)$$

где $c=\begin{cases}2,\alpha_0 \ge 2,\\ 1,\alpha_0 < 2,\end{cases}$ $c_0=\begin{cases}2^{\alpha_0-2},\alpha_0 \ge 2,\\ 1,\alpha_0 < 2,\end{cases}$ $c_i=\varphi(p_i^{\alpha_i})=p_i^{\alpha_i-1}(p_i-1)$, $i=\overline{1,k}$. Решение системы (5.3), если оно существует, может быть найдено с помощью китайской теоремы об остатках.

Пример 1. Решите показательное сравнение $7^x \equiv 55(\mathrm{mod}\, 576)$.

Решение. Найдем системы индексов чисел $a=7$ и $b=55$ по модулю $m=2^6\cdot 3^2$. Используя таблицу индексов

$(-1)^{\gamma}5^{\gamma_0}(\mathrm{mod}\,64)$	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
γ	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
γ_0	16	3	1	10	6	5	15	4	12	7	13	14	2	9	11	8

$(-1)^{\gamma}5^{\gamma_0}(\mathrm{mod}\,64)$	33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63
γ	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2	1
γ_0	8	11	9	2	14	13	7	12	4	15	5	6	10	1	3	16

по модулю 64, находим, что $7 \equiv (-1)^1 5^{10}(\mathrm{mod}\, 64)$, $55 \equiv (-1)^1 5^6(\mathrm{mod}\, 64)$. Так как $2^1 \not\equiv 1(\mathrm{mod}\, 9)$ $2^2 \not\equiv 1(\mathrm{mod}\, 9)$, $2^3 \not\equiv 1(\mathrm{mod}\, 9)$, то число 2 является первообразным корнем по модулю 9. Учитывая, что $7 \equiv 2^4(\mathrm{mod}\, 9)$, $55 \equiv 2^6(\mathrm{mod}\, 9)$, делаем вывод о том, что $(1,10,4)$, $(1,6,6)$ - системы индек-

сов соответственно чисел a и b по модулю m. Следовательно, сравнение $7^x \equiv 55(\mathrm{mod}\,576)$ равносильно системе сравнений

$$\begin{cases} 1\cdot x \equiv 1(\mathrm{mod}\,2), \\ 10\cdot x \equiv 6(\mathrm{mod}\,2^4), \\ 4\cdot x \equiv 6(\mathrm{mod}\,6). \end{cases}$$

Разрешая эту систему, находим, что $x \equiv 15(\mathrm{mod}\,24)$.

Другой подход к решению показательного сравнения (5.1) заключается в использовании свойств показателей и применении китайской теоремы об остатках. Проиллюстрируем этот приём на следующем примере.

Пример 2. Решите показательное сравнение $5^x \equiv 229(\mathrm{mod}1001)$.

Решение. Так как $1001 = 7\cdot 11\cdot 13$, то сравнение $5^x \equiv 229(\mathrm{mod}1001)$ равносильно системе сравнений:

$$\begin{cases} 5^x \equiv 229(\mathrm{mod}\,7), \\ 5^x \equiv 229(\mathrm{mod}\,11), \\ 5^x \equiv 229(\mathrm{mod}\,13). \end{cases}$$

Показатель δ_m, которому принадлежит число 5 по модулю m делит $\varphi(m)$. Отсюда находим, что $\delta_7 = 6$, $\delta_{11} = 5$, $\delta_{13} = 4$. Так как $5^1 \equiv 5 \equiv 229(\mathrm{mod}\,7)$, $5^4 \equiv 9 \equiv 229(\mathrm{mod}11)$, $5^3 \equiv 8 \equiv 229(\mathrm{mod}13)$ имеем:

$$\begin{cases} 5^x \equiv 229(\mathrm{mod}\,7), \\ 5^x \equiv 229(\mathrm{mod}\,11), \\ 5^x \equiv 229(\mathrm{mod}\,13), \end{cases} \Leftrightarrow \begin{cases} x \equiv 1(\mathrm{mod}\,6), \\ x \equiv 4(\mathrm{mod}\,5), \\ x \equiv 3(\mathrm{mod}\,4), \end{cases} \Leftrightarrow \begin{cases} x \equiv 1(\mathrm{mod}\,3), \\ x \equiv 4(\mathrm{mod}\,5), \\ x \equiv 3(\mathrm{mod}\,4). \end{cases}$$

Применяя к последней системе китайскую теорему об остатках, получаем $x \equiv 19(\mathrm{mod}\,60)$.

Укажем способ решения степенного сравнения

$$ax^n \equiv b(\mathrm{mod}\,m), \qquad (5.4)$$

где $(b,m) = 1$. Пусть $2^{\alpha_0} p_1^{\alpha_1} ... p_k^{\alpha_k}$ - каноническое разложение модуля m, где $\alpha_0 \geq 0$, тогда сравнение (5.4) эквивалентно системе сравнений:

$$ax^n \equiv b(\mathrm{mod}\,2^{\alpha_0}),\ ax^n \equiv b(\mathrm{mod}\,p_i^{\alpha_i}),\ i = \overline{1,k}.$$

Пусть $(\gamma, \gamma_0, \gamma_1, ..., \gamma_k)$, $(\delta, \delta_0, \delta_1, ..., \delta_k)$ - системы индексов соответственно чисел a и b по модулю m, т.е. $(-1)^{\gamma} 5^{\gamma_0} \equiv a(\mathrm{mod}\,2^{\alpha_0})$, $g_i^{\gamma_i} \equiv a(\mathrm{mod}\,p_i^{\alpha_i})$, $(-1)^{\delta} 5^{\delta_0} \equiv b(\mathrm{mod}\,2^{\alpha_0})$, $g_i^{\delta_i} \equiv b(\mathrm{mod}\,p_i^{\alpha_i})$, где g_i - первообразный корень

по модулю $p_i^{\alpha_i}$. Тогда система индексов $(\lambda, \lambda_0, \lambda_1, ..., \lambda_k)$ числа x по модулю m может быть найдена из следующих сравнений:

$\gamma + n\lambda \equiv \delta(\mathrm{mod}\, c),\ \gamma_0 + n\lambda_0 \equiv \delta_0(\mathrm{mod}\, c_0),\ \gamma_i + n\lambda_i \equiv \delta_i(\mathrm{mod}\, c_i),\ i = \overline{1,k}$.

Решение сравнения (5.4) можно найти из системы: $x \equiv (-1)^{\lambda} 5^{\lambda_0} (\mathrm{mod}\, 2^{\alpha_0})$, $x \equiv g_i^{\lambda_i} (\mathrm{mod}\, p_i^{\alpha_i})$, $i = \overline{1,k}$.

Пример 3. Решите степенное сравнение $7x^{17} \equiv 157(\mathrm{mod}1144)$.

Решение. Найдем системы индексов чисел $a = 7$, $b = 157$ по модулю $m = 1144 = 2^3 \cdot 11 \cdot 13$. Имеем $7 \equiv (-1)^1 5^2 (\mathrm{mod}\, 8)$, $157 \equiv 5 = (-1)^2 5^1 (\mathrm{mod}\, 8)$; $\mathrm{ind}_2 7(\mathrm{mod}11) = 7$, $\mathrm{ind}_2 157(\mathrm{mod}11) = \mathrm{ind}_2 3(\mathrm{mod}11) = 8$; $\mathrm{ind}_2 7(\mathrm{mod}13) = 11$, $\mathrm{ind}_2 157(\mathrm{mod}13) = \mathrm{ind}_2 1(\mathrm{mod}13) = 12$. Следовательно, $(1,2,7,11)$ и $(2,1,8,12)$ – системы индексов чисел 7 и 157 по модулю 1144. Для нахождения системы индексов неизвестного числа x получаем систему сравнений:

$$\begin{cases} 1 + 17\lambda \equiv 2(\mathrm{mod}\, 2), \\ 2 + 17\lambda_0 \equiv 1(\mathrm{mod}\, 2), \\ 7 + 17\lambda_1 \equiv 8(\mathrm{mod}10), \\ 11 + 17\lambda_2 \equiv 12(\mathrm{mod}12). \end{cases}$$

Решая систему, находим, что $(1,1,3,5)$ - система индексов числа x. Получаем систему сравнений для нахождения x:

$$\begin{cases} x \equiv -5(\mathrm{mod}\, 8), \\ x \equiv 8(\mathrm{mod}11), \\ x \equiv 32(\mathrm{mod}13). \end{cases}$$

Используя китайскую теорему об остатках, получаем, что $x \equiv 19(\mathrm{mod}1144)$.

Перейдем к рассмотрению полиномиальных сравнений

$$f(x) \equiv 0(\mathrm{mod}\, m) \qquad (5.5),$$

где $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$, $a_i \in Z$ для любого $i = \overline{0,n}$. Сравнение (5.5) равносильно системе сравнений $f(x) \equiv 0(\mathrm{mod}\, p_i^{\alpha_i})$, $i = \overline{1,l}$, где $p_1^{\alpha_1} ... p_l^{\alpha_l}$ - каноническое разложение модуля m. Таким образом, для решения сравнения (5.5) следует решить каждое из сравнений $f(x) \equiv 0(\mathrm{mod}\, p_i^{\alpha_i})$, а затем применить китайскую теорему об остатках.

Приведем способ нахождения решения полиномиального сравнения $f(x) \equiv 0(\mathrm{mod}\, p^{\alpha})$ по примарному модулю:

1) применяя теорему Ферму, сравнение $f(x)\equiv 0(\mathrm{mod}\, p)$ сводим к полиномиальному сравнению $g(x)\equiv 0(\mathrm{mod}\, p)$, где g - многочлен с целыми коэффициентами степени не выше, чем $p-1$. Находим решения сравнения $g(x)\equiv 0(\mathrm{mod}\, p)$: $x\equiv x_1(\mathrm{mod}\, p),...,\ x\equiv x_r(\mathrm{mod}\, p)$;

2) для каждого фиксированного $i=\overline{1,r}$ полагаем $x=x_i+t_i p$, где $t_i\in Z$. Левую часть сравнения $f(x_i+t_i p)\equiv 0(\mathrm{mod}\, p^2)$ раскладываем по формуле Тейлора (принимая во внимание, что число $f^{(j)}(x_i)/j!$ является целым, и отбрасывая члены, кратные p^2): $f(x_i)+t_i p f'(x_i)\equiv 0(\mathrm{mod}\, p^2)$. Сокращая обе части сравнения и модуль на p, получаем $\frac{f(x_i)}{p}+t_i f'(x_i)\equiv 0(\mathrm{mod}\, p)$. Находим решения этого сравнения $t_i\equiv t_{i,1}(\mathrm{mod}\, p),\ldots,\ t_i\equiv t_{i,s}(\mathrm{mod}\, p)$. Таким образом, $x\equiv x_i+t_{i,j}p=x_{i,j}(\mathrm{mod}p^2)$, $i=\overline{1,r}$, $j=\overline{1,s}$;

3) далее для каждых фиксированных $i=\overline{1,r}$, $j=\overline{1,s}$ полагаем $x=x_i+t_{i,j}p+z_{i,j}p^2=x_{i,j}+z_{i,j}p^2$, где $z_{i,j}\in Z$. Аналогично левую часть сравнения $f(x_{i,j}+z_{i,j}p^2)\equiv 0(\mathrm{mod}\, p^3)$ раскладываем по формуле Тейлора и отбрасываем члены, кратные p^3: $f(x_{i,j})+p^2 z_{i,j}f'(x_{i,j})\equiv 0(\mathrm{mod}\, p^3)$. Сокращая сравнение на p^2, получим $\frac{f(x_{i,j})}{p}+z_{i,j}f'(x_{i,j})\equiv 0(\mathrm{mod}\, p)$. Решая сравнение, находим, что $z_{i,j}\equiv z_{i,j,k}(\mathrm{mod}\, p)$, $k=\overline{1,q}$. Подставляя в x, получим $x\equiv x_{i,j}+z_{i,j,k}p=x_{i,j,k}(\mathrm{mod}\, p^3)$;

4) проделывая последовательно для модулей $p^4,...,p^\alpha$ описанную процедуру, найдем решения $x\equiv x_\lambda(\mathrm{mod}\, p^\alpha)$ сравнения $f(x)\equiv 0(\mathrm{mod}\, p^\alpha)$.

Отметим, что в случае $f'(x_i)\not\equiv 0(\mathrm{mod}\, p)$ решение $x\equiv x_i(\mathrm{mod}\, p)$ сравнения $g(x)\equiv 0(\mathrm{mod}\, p)$ даст одно решение $x\equiv\beta_i(\mathrm{mod}\, p^\alpha)$ сравнения $f(x)\equiv 0(\mathrm{mod}\, p^\alpha)$.

Пример 4. Решите полиномиальное сравнение $16x^8-8x^7+9x^4-1\equiv 0(\mathrm{mod}196)$.

Решение. Исходное сравнение эквивалентно системе сравнений:

$$\begin{cases}16x^8-8x^7+9x^4-1\equiv 0(\mathrm{mod}\, 2^2),\\ 16x^8-8x^7+9x^4-1\equiv 0(\mathrm{mod}\, 7^2).\end{cases}$$

Из первого сравнения системы получаем: $x \equiv \pm 1(\mathrm{mod}\,4)$. Обозначим $f(x) = 16x^8 - 8x^7 + 9x^4 - 1$. Найдем решение сравнения $f(x) \equiv 0(\mathrm{mod}\,7)$. Имеем: $f(x) \equiv 2x^2 - x + 2x^4 - 1 \equiv 2x^2 - x + 16x^4 - 1 = (2x-1)(x + 8x^3 + 4x^2 + 2x + 1) \equiv$ $\equiv (2x-1)(x^3 - 3x^2 + 3x + 1) = (2x-1)(x-1)^3 + 2) \equiv 0(\mathrm{mod}7)$. Отсюда получаем, что $x \equiv 4(\mathrm{mod}\,7)$. Пусть $x = 4 + 7t$, $t \in Z$.

Далее $f(x) = f(4 + 7t) \equiv f(4) + 7t \cdot f'(4) \equiv 28 + 14t \equiv 0(\mathrm{mod}\,7^2)$. Следовательно, $t \equiv 5(\mathrm{mod}\,7)$. Таким образом, $x \equiv 39(\mathrm{mod}\,49)$ - решение второго сравнения системы.

Применяя китайскую теорему об остатках к системам

$$\begin{cases} x \equiv 1(\mathrm{mod}\,4), \\ x \equiv 39(\mathrm{mod}\,49), \end{cases} \quad \begin{cases} x \equiv -1(\mathrm{mod}\,4), \\ x \equiv 39(\mathrm{mod}\,49), \end{cases}$$

заключаем, что $x \equiv 137(\mathrm{mod}196)$, $x \equiv 39(\mathrm{mod}196)$.

Рассмотрим двучленное сравнение второй степени

$$x^2 \equiv a(\mathrm{mod}\,m), \tag{5.6}$$

где $(a,m) = 1$. Если сравнение (5.6) имеет решение, то число a называется *квадратичным вычетом* по модулю m, в противном случае a называется *квадратичным невычетом* по модулю m.

Пусть $m = p$, где p - нечетное простое число. Приведенная система вычетов по модулю p состоит из $\frac{p-1}{2}$ квадратичных вычетов и $\frac{p-1}{2}$ квадратичных невычетов. *Символ Лежандра* $\left(\frac{a}{p}\right)$ определяется равенством $\left(\frac{a}{p}\right) = 1$, если a является квадратичным вычетом по модулю p, и равенством $\left(\frac{a}{p}\right) = -1$, если a является квадратичным невычетом по модулю p. Для любых $a, b \in Z$, $(a,p) = (b,p) = 1$ и любого нечётного простого числа q, $(p,q) = 1$, имеют место следующие свойства:

1) $a \equiv b(\mathrm{mod}\,p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

2) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod}\,p)$ (критерий Эйлера);

3) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$;

4) $\left(\frac{a}{p}\right)=(-1)^{\sum\limits_{i=1}^{\frac{p-1}{2}}\left[\frac{2ai}{p}\right]}$;

5) $\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$ (квадратичный закон взаимности).

Пусть теперь P - нечётное натуральное число, большее единицы, и $p_1...p_n$ - разложение числа P на простые множители. Для всякого целого числа a, взаимно простого с P, *символ Якоби* $\left(\frac{a}{P}\right)$ определяется через символы Лежандра по формуле: $\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\cdot\left(\frac{a}{p_2}\right)\cdot...\cdot\left(\frac{a}{p_n}\right)$. Для любых целых a,b, взаимно простых с P, и любого нечётного натурального Q, большего 1 и взаимно простого с P, имеют место следующие свойства символа Якоби:

6) $a\equiv b(\mathrm{mod}\,P)\Rightarrow\left(\frac{a}{P}\right)=\left(\frac{b}{P}\right)$;

7) $\left(\frac{ab}{P}\right)=\left(\frac{a}{P}\right)\cdot\left(\frac{b}{P}\right)$;

8) $\left(\frac{1}{P}\right)=1$;

9) $\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}$;

10) $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$;

11) $\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right)$.

Отметим, что равенство символа Якоби $\left(\frac{a}{P}\right)$ единице является необходимым условием для того, чтобы число a было квадратичным вычетом по модулю P, но не достаточным.

Пример 5. Исследовать на разрешимость сравнение $x^2\equiv219(\mathrm{mod}383)$.

Решение. Вычислим символ Лежандра $\left(\frac{219}{383}\right)$, рассматривая его как символ Якоби и используя свойства символа Якоби:

$$\left(\frac{219}{383}\right)^{11)}=-\left(\frac{383}{219}\right)^{6)}=-\left(\frac{164}{219}\right)^{7)}=-\left(\frac{2}{219}\right)\left(\frac{2}{219}\right)\left(\frac{41}{219}\right)=-\left(\frac{41}{219}\right)^{11)}=-\left(\frac{219}{41}\right)^{6)}=-\left(\frac{14}{41}\right)^{7)}=$$

$$=-\left(\frac{2}{41}\right)\left(\frac{7}{41}\right)^{10)}=-\left(\frac{7}{41}\right)^{11)}=-\left(\frac{41}{7}\right)^{6)}=-\left(\frac{-1}{7}\right)^{9)}=1.$$

Откуда следует, что сравнение разрешимо.

5.1. Используя свойства показателей, решите следующие показательные сравнения по простому модулю:

1) $5^x \equiv 4(\mathrm{mod}\,41)$, 2) $2^x \equiv 5(\mathrm{mod}\,67)$, 3) $13^x \equiv 9(\mathrm{mod}\,29)$,

4) $12^x \equiv 17(\mathrm{mod}\,31)$, 5) $16^x \equiv 11(\mathrm{mod}\,53)$.

5.2. Используя свойства показателей и китайскую теорему об остатках, решите следующие показательные сравнения по составному модулю:

1) $3^x \equiv 92(\mathrm{mod}\,143)$, 2) $6^x \equiv 171(\mathrm{mod}\,225)$, 3) $19^x \equiv 64(\mathrm{mod}\,1001)$,

4) $5^x \equiv 247(\mathrm{mod}\,987)$, 5) $13^x \equiv 97(\mathrm{mod}\,1575)$.

5.3. Решите полиномиальные сравнения, предварительно понизив их степени с помощью теоремы Ферма:

1) $6x^{10}-12x+1 \equiv 0(\mathrm{mod}\,5)$, 2) $x^8-5x^2+4 \equiv 0(\mathrm{mod}\,7)$,

3) $3x^{55}+x^{39}+16x^{20}+18 \equiv 0(\mathrm{mod}\,19)$,

4) $5x^{26}+6x^{16}+2x^{12}+x^2+3 \equiv 0(\mathrm{mod}\,11)$,

5) $10x^7-8x^6-2x^2-1 \equiv 0(\mathrm{mod}\,7)$.

5.4. Докажите, что сравнение $x^8 \equiv 23(\mathrm{mod}\,41)$ не имеет решений.

5.5. Решите следующие сравнения:

1) $x^{12} \equiv 37(\mathrm{mod}\,41)$, 2) $x^9 \equiv 23(\mathrm{mod}\,50)$, 3) $5x^{17} \equiv 13(\mathrm{mod}\,32)$,

4) $29x^{23} \equiv 11(\mathrm{mod}\,64)$, 5) $19x^{11} \equiv 7(\mathrm{mod}\,928)$.

5.6. Решите следующие полиномиальные сравнения:

1) $x^4+7x+4 \equiv 0(\mathrm{mod}\,27)$, 2) $9x^2+29x+62 \equiv 0(\mathrm{mod}\,64)$,

3) $31x^4+57x^3+96x+191 \equiv 0(\mathrm{mod}\,225)$,

4) $x^4+8x^3+25x-64 \equiv 0(\mathrm{mod}\,343)$,

5) $x^3+16x+27 \equiv 0(\mathrm{mod}\,900)$.

5.7. Решите следующие уравнения в натуральных числах

1) $2^x-3^y=5$, 2) $3^x+4^y=5^z$, 3) $3^x+7^y=4^z$.

5.8. Для каждого натурального $m>1$ найдите число вычетов в полной системе вычетов по модулю m, удовлетворяющих сравнению $x^2 \equiv 4(\mathrm{mod}\, m)$.

5.9. Докажите, что нахождение решений сравнения $ax^2+bx+c\equiv \equiv 0(\mathrm{mod} m)$, $(2a,m)=1$, сводится к нахождению решений сравнения вида $x^2 \equiv q(\mathrm{mod}\, m)$.

5.10. В приведенной системе вычетов по модулю 23 найдите все квадратичные вычеты.

5.11. Используя свойства символов Лежандра и Якоби, исследовать на разрешимость сравнения:

1) $x^2 \equiv 2(\mathrm{mod}\, 31)$, 2) $x^2 \equiv 3(\mathrm{mod}\, 31)$, 3) $x^2 \equiv 3(\mathrm{mod}\, 73)$,

4) $x^2 \equiv 556(\mathrm{mod}\, 853)$, 5) $x^2 \equiv 557(\mathrm{mod}\, 854)$.

5.12. Укажите способ решения показательного сравнения $a^x \equiv b(\mathrm{mod}\, m)$, где $(a,m)>1$.

5.13. Укажите способ решения степенного сравнения $ax^n \equiv b(\mathrm{mod}\, m)$, где $(b,m)>1$.

5.14. Пусть p - простое число вида $4k+3$. Для любого целого a найдите решение сравнения $x^2 \equiv a(\mathrm{mod}\, p)$ в явном виде.

6. ГРУППЫ

Непустое множество G с заданной на нем бинарной операцией $\circ$ образует *группу* $(G,\circ)$, если выполнены условия:

1) операция $\circ$ ассоциативна, т.е. $(a\circ b)\circ c = a\circ(b\circ c)$ для любых $a,b,c\in G$;

2) существует нейтральный элемент $e\in G$, т.е. $a\circ e = e\circ a = a$ для любого $a\in G$;

3) для любого элемента $a\in G$ существует обратный элемент $a^{-1}\in G$, т.е. $a\circ a^{-1} = a^{-1}\circ a = e$.

Если операция $\circ$ коммутативна, т.е. $a\circ b = b\circ a$ для любых $a,b\in G$, то группа $(G,\circ)$ называется *коммутативной* или *абелевой*. Если множество G конечное, то группа $(G,\circ)$ называется *конечной*, а число элементов множества G называется *порядком группы* $(G,\circ)$ и обозначается $|G|$. Для любого целого числа n степень a^n элемента a определяется следую-

щим образом: $a^n = \underbrace{a \circ a \circ ... \circ a}_{n \text{ раз}}$, $a^{-n} = \underbrace{a^{-1} \circ a^{-1} \circ ... \circ a^{-1}}_{n \text{ раз}}$ для натуральных n, $a^0 = e$. Натуральное число n называется *порядком* элемента $a \in G$ и обозначается $|a|$, если $a^n = e$ и $a^k \neq e$ для любого натурального k, меньшего n. Если группа $(G,\circ)$ конечна, то для вычисления порядка степеней элементов справедлива формула: $|a^k| = \frac{|a|}{(k,|a|)}$, $k \in Z$.

Если в группе $(G,\circ)$ существует элемент a, такой, что для любого элемента $b \in G$ существует целое число n, такое, что $a^n = b$, то группа $(G,\circ)$ называется *циклической*, а элемент a называется *образующим элементом* группы $(G,\circ)$ и обозначается $G = < a >$.

Пусть H - непустое подмножество множества G.

Если множество H образует группу относительно операции $\circ$, то группу $(H,\circ)$ называют *подгруппой* группы $(G,\circ)$ и пишут $H \leq G$ или $H < G$ в случае $H \neq G$; если же $H \leq G$ и $g^{-1} \circ h \circ g \in H$ для любых $g \in G$, $h \in H$, то говорят, что $(H,\circ)$ - *нормальная подгруппа* (нормальный делитель) группы $(G,\circ)$ и обозначают $H \lhd G$.

Пусть $H \leq G$. Тогда для каждого элемента $a \in G$ множества $L_a = \{a \circ h \mid h \in H\}$, $R_a = \{h \circ a \mid h \in H\}$ называются соответственно *левым смежным классом* и *правым смежным классом.* Мощность множества левых смежных классов по подгруппе H равна мощности ее правых смежных классов и называется индексом группы G по подгруппе H и обозначается $|G:H|$. В случае конечности группы $(G,\circ)$ имеет место равенство $|G| = |G:H| \cdot |H|$ (теорема Лагранжа). Если $H \lhd G$ левый смежный класс L_a совпадает с правым смежным классом R_a и называется *смежным классом по нормальной подгруппе*.

Если $H \leq G$, то для любых элементов $a,b \in G$ смежные классы L_a, L_b либо не пересекаются, либо совпадают и мощность каждого смежного класса равна мощности множества H. Через G/H обозначается множество всех различных смежных классов. Если $H \lhd G$, то G/H образует группу относительно операции $\bullet$ умножения смежных классов и $L_a \bullet L_b = L_{a \circ b}$.

Группа $(G/H,\bullet)$ называется *фактор-группой* группы $(G,\circ)$ по подгруппе $(H,\circ)$; нейтральным элементом фактор-группы $(G/H,\bullet)$ является множество H, а обратным элементом к L_a является смежный класс $L_{a^{-1}}$.

Пусть $(G_1,\circ)$ и $(G_2,*)$ - группы. Отображение $\varphi: G_1 \to G_2$ называется *гомоморфизмом* групп, если $\varphi(a \circ b) = \varphi(a) * \varphi(b)$ для любых $a,b \in G_1$; *ядром* гомоморфизма $\varphi: G_1 \to G_2$ называется множество $\mathrm{Ker}(\varphi) = \{a \in G_1 \mid \varphi(a) = e_2\}$, где e_2 - нейтральный элемент группы $(G_2,*)$; *образом* гомоморфизма $\varphi: G_1 \to G_2$ называется множество $\mathrm{Im}(\varphi) = \{b \in G_2 \mid \exists a \in G_1, \varphi(a) = b\}$; ядро гомоморфизма $\mathrm{Ker}(\varphi)$ образует нормальную подгруппу группы $(G_1,\circ)$, образ гомоморфизма $\mathrm{Im}(\varphi)$ образует подгруппу группы $(G_2,*)$; биективный гомоморфизм называется *изоморфизмом*; группы $(G_1,\circ)$ и $(G_2,*)$ называются *изоморфными*, если существует изоморфизм $\varphi: G_1 \to G_2$, и обозначают $G_1 \cong G_2$; для любого гомоморфизма $\varphi: G_1 \to G_2$ группы $(G_1/\mathrm{Ker}(\varphi),\bullet)$ и $(\mathrm{Im}(\varphi),*)$ являются изоморфными (теорема об изоморфизме); любая конечная циклическая группа порядка n изоморфна группе вычетов $(Z_n,+)$ по модулю n, любая бесконечная циклическая группа изоморфна аддитивной группе целых чисел $(Z,+)$.

Пример 1. Определите, образует ли группу множество $G = \{f \in \mathrm{Sym}(R) \mid \forall x \in R: f(x+\sin x) = f(x) + \sin f(x)\}$ с операцией суперпозиции.

Решение. Проверим, что операция суперпозиции является бинарной операцией на множестве G, т.е. $f_1 \circ f_2 \in G$ для любых $f_1,\ f_2 \in G$. Так как $f_1, f_2 \in \mathrm{Sym}(R)$, то $f_1 \circ f_2 \in \mathrm{Sym}(R)$. Кроме того, для любого $x \in R$:

$$(f_1 \circ f_2)(x+\sin x) = f_1(f_2(x+\sin x)) = f_1(f_2(x) + \sin f_2(x)) =$$
$$= f_1(f_2(x)) + f_1(f_2(\sin x)) = (f_1 \circ f_2)(x) + (f_1 \circ f_2)(\sin x).$$

Очевидно, операция суперпозиции является ассоциативной. Нейтральным элементом является тождественное отображение: $\mathrm{id}(x) = x$, $x \in R$. Покажем, что обратным элементом к $f \in G$ является обратное отображение f^{-1}. Так как $f \in \mathrm{Sym}(R)$, то $f^{-1} \in \mathrm{Sym}(R)$. Возьмём произвольное $x \in R$ и обозначим $y = f^{-1}(x)$, тогда $x = f(y)$, $\sin x = \sin f(y)$. Так как $f \in G$, то $f(y)+\sin f(y) = f(y+\sin y)$. Следовательно, $x+\sin x = f(f^{-1}(x)+\sin f^{-1}(x))$. Отсюда получаем $f^{-1}(x+\sin x) = f^{-1}(x) + \sin f^{-1}(x)$. Множество G с операцией суперпозиции образует группу.

Пример 2. Найдите все подгруппы группы $(Z_n,+)$.

Решение. Докажем, что любая подгруппа группы $(Z_n,+)$ имеет вид $(mZ_n,+)$, где $mZ_n = \{\overline{0},\overline{m},...,\overline{n-m}\}$, m - некоторый натуральный делитель

числа n. Пусть $(H,+)$ - произвольная подгруппа группы $(Z_n,+)$, $\overline{m}$ - наименьший натуральный вычет множества H. Допустим, существует такой элемент $\overline{b}\in H$, что b не делится на m, то есть $b=qm+r$, где $q,r\in N$, $r<m$. Но тогда $\overline{r}=\overline{b}+q(\overline{-m})\in H$, что противоречит минимальности m. Следовательно, для любого $\overline{b}\in H$ найдётся натуральное l, такое, что $b=ma$. Допустим, что n не делится на m, тогда $n=tm+s$, где $t,s\in N$, $s<m$. Отсюда $\overline{s}=t(\overline{-m})\in H$, что противоречит минимальности m. Следовательно, H есть подмножество множества $\{\overline{0},\overline{m},\overline{2m}...,\overline{n-m}\}$. Очевидно, $H=\{\overline{0},\overline{m},\overline{2m}...,\overline{n-m}\}$.

Пример 3. Определите, являются ли группы $([0,1),\{\cdot\})$ и $(\{z\in C\,||\,z|=1\},\cdot)$ изоморфными.

Решение. Обозначим $G_1=[0,1)$, $G_2=\{z\in C\,||\,z|=1\}$. Отображение $\varphi: G_1\to G_2$, действующее по правилу $\varphi(x)=\mathrm{e}^{i2\pi x}$, $x\in G_1$, является гомоморфизмом, так как $\varphi(\{x+y\})=e^{i2\pi\{x+y\}}=\cos(2\pi\{x+y\})+i\sin(2\pi\{x+y\})=$
$=\cos(2\pi(x+y))+i\sin(2\pi(x+y))=e^{i2\pi(x+y)}=e^{i2\pi x}e^{i2\pi y}=\varphi(x)\cdot\varphi(y)$.
Так как гомоморфизм φ биективный, то группы $(G_1,\{\cdot\})$, $(G_2,\cdot)$ являются изоморфными.

Пример 4. Пусть G - циклическая группа 8-го порядка, H - её подгруппа порядка 4. Найдите индекс подгруппы H в группе G и вычислите фактор-группу G/H.

Решение. Пусть a - образующий элемент группы G, тогда $G=\{e,a,a^2,a^3,a^4,a^5,a^6,a^7\}$. Так как $G\cong Z_8$, то $H\cong mZ_8$, где m - некоторый делитель числа 8. Поскольку $|H|=|mZ_8|=8/m=4$, то $m=2$. Следовательно, $H=\{e,a^2,a^4,a^6\}$. Индекс $|G:H|$ равен 2. Фактор-группа G/H состоит из двух смежных классов H и $G\setminus H$.

6.1. Определите, какие из указанных множеств относительно заданных операций, образуют группу:

1) $(A,\cdot)$, где A - одно из множеств N,Z,Q,R,C;

2) $(A,+)$, где A - одно из множеств N,Z,Q,R,C;

3) $(A,-)$, где A - одно из множеств N,Z,Q,R,C;

4) $(A\setminus\{0\},\cdot)$, где A - одно из множеств Z,Q,R,C;

5) $(A_+,\cdot)$, где A - одно из множеств Z,Q,R (A_+ - множество всех положительных чисел из множества A);

6) $(nZ,+)$, где $n \in N$, nZ - множество целых чисел, кратных n;

7) $(\{-1,1\},\cdot)$;

8) множество $R \setminus \{-1\}$ относительно операции $*\colon (x,y) \mapsto x + y + xy$;

9) множество всех комплексных корней K_n из 1 фиксированной степени $n \in N$ относительно умножения;

10) множество всех комплексных корней K_∞ из 1 произвольных степеней относительно умножения;

11) множество всех комплексных чисел с фиксированным модулем $r \in R_+$ относительно умножения;

12) множество всех комплексных чисел с ненулевыми рациональными модулями относительно умножения;

13) положительные действительные числа относительно операции $*\colon (a,b) \mapsto a^b$;

14) целочисленные матрицы порядка $n \in N$ с определителем, равным 1, относительно умножения;

15) невырожденные квадратные матрицы порядка $n \in N$ с элементами из множества A относительно умножения, где A - одно из множеств Q, R, C;

16) $(nZ_m,+)$, где nZ_m - множество классов вычетов по модулю $m \in N$, кратных $n \in N$, причем n делитель m;

17) $(nZ_m,\cdot)$, где $m,n \in N$, причем n делитель m;

18) $(G(Z_m),\cdot)$, где множество $G(Z_m)$ состоит из классов вычетов по модулю $m \in N$, взаимно простых с m;

19) $(2^X,\Delta)$, где 2^X - множество всех подмножеств заданного множества X, Δ - операция симметрической разности множеств;

20) $\left(\left\{\begin{bmatrix} x & y \\ \lambda y & x \end{bmatrix} \neq O_{2,2} \,\middle|\, x,y \in R\right\},\cdot\right)$, где λ - фиксированное действительное число.

6.2. Определите, являются ли изоморфными указанные группы:

1) $(R \setminus \{0\},\cdot)$ и $(R_+,\cdot)$;

2) $(R,+)$ и $(R_+,\cdot)$;

3) $(Q,+)$ и $(Q_+,\cdot)$;

4) $(Z,+)$ и $(nZ,+)$, где $n \in N$;

5) группа мономиальных матриц M_n порядка $n \in N$ относительно умножения и группа подстановок $(S_n,\circ)$;

6) $(C \setminus \{0\}, \cdot)$ и $\left(\left\{ \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} \neq O_{2,2} \middle| \alpha, \beta \in R \right\}, \cdot \right)$.

6.3. Найдите все, с точностью до изоморфизма, группы порядков 2 и 3.

6.4. Приведите пример двух неизоморфных групп одинакового конечного порядка.

6.5. Описать левые смежные классы группы G по подгруппе H в следующих случаях:

1) $G = (Z, +)$, $H = (5Z, +)$;

2) $G = (S_3, \circ)$, $H = \left(\{(1), (1,2)\}, \circ \right)$;

3) $G = (GL(n,R), \cdot)$, $H = (SL(n,R), \cdot)$, где $GL(n,R)$, $SL(n,R)$ - множество всех невырожденных матриц порядка $n \in N$ с действительными коэффициентами и множество матриц порядка n с действительными коэффициентами и определителем, равным 1.

6.6. Найдите все подгруппы группы G и укажите среди них нормальные, если:

1) $G = (S_3, \circ)$;

2) G - циклическая группа 12-го порядка;

3) $G = (Z, +)$.

6.7. Докажите, что в конечной группе нечётного порядка имеется однозначно определенная операция извлечения квадратного корня.

6.8. Докажите, что всякая группа простого порядка является циклической.

6.9. Докажите, что подгруппа индекса 2 в любой группе является нормальной.

6.10. Докажите, что в любой конечной группе чётного порядка есть элемент порядка 2.

6.11. Сколько элементов порядка 6 имеет группа G, если:

1) $G = (Z_{36}, +)$;

2) $G = (G(Z_{36}), \cdot)$;

3) $G = (S_5, \cdot)$.

6.12. Найти порядок указанного элемента a в группе G, если:

1) $a = (1,2,3) \circ (4,5)$, $G = (S_5, \circ)$;

2) $a = (1,2,3,5) \circ (4,6)$, $G = (S_6, \circ)$;

3) $a=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix}$, $G=(GL(4,R),\cdot)$;

4) $a=\begin{bmatrix}-1&\alpha\\0&1\end{bmatrix}$, $G=(GL(2,C),\cdot)$, где $\alpha\in C$.

6.13. Вычислите f^n в группе $(S_{10},\circ)$, если:

1) $f=(1,3,4)\circ(2,5,7)\circ(6,10,8)\circ(9)$, $n=10^5$;

2) $f=(1,3,4,6,7)\circ(2,5,9,8,10)$, $n=150$;

3) $f=(1,3,4,6,7)\circ(2,5,9,8,10)$, $n=201$.

6.14. Найдите X в группе $(S_7,\circ)$, если $AXB^2=C^{-1}$, где
$A=(1,7,4)\circ(2,3)\circ(5,6)$, $B=(1,3,2)\circ(4,7,6,5)$,
$C=(1,5,4,6,7,2)\circ(3)$.

6.15. Найдите X в группе $(S_4,\circ)$, если $A^{-1}XB=C^2$, где
$A=(1,4)\circ(2,3)$, $B=(1,2)\circ(3,4)$, $C=(1,4,2)\circ(3)$.

6.16. Докажите, что в группе Q/Z все элементы имеют конечный порядок.

6.17. Докажите, что множество всех целочисленных ортогональных матриц порядка $n\in N$ образует группу относительно умножения и найдите порядок этой группы.

6.18. Докажите, что если в группе все элементы имеют порядок 2, то группа является абелевой.

6.19. Найдите все гомоморфизмы из группы $(Z_4,+)$ в группу $(Z_6,+)$, а также ядра и образы этих гомоморфизмов.

6.20. Найдите число гомоморфизмов, действующих из группы G_1 в группу G_2, если:

1) $G_1=(Z_6,+)$, $G_2=(Z_{15},+)$;

2) $G_1=(Z_{15},+)$, $G_2=(Z_{12},+)$;

3) $G_1=(Z_{12},+)$, $G_2=(Z_{24},+)$.

6.21. Найдите все образующие элементы группы G, если:

1) $G=Z$;

2) $G=Z_n$, где $n\in N$, $n>1$.

7. КОЛЬЦА

Непустое множество K называется ассоциативным *кольцом*, если на нем определены две алгебраические операции (назовем их сложение и умножение), удовлетворяющие следующим условиям:

1) $(K, +)$ – абелева группа;

2) умножение ассоциативно;

3) сложение и умножение связаны законами дистрибутивности, т.е. $a(b+c) = ab + ac,\ (b+c)a = ba + ca$ для любых $a, b, c \in K$.

Обозначим через 0 нейтральный элемент кольца K относительно сложения.

Далее под словом кольцо будем подразумевать ассоциативное кольцо.

Кольцо называется *коммутативным*, если умножение в нем коммутативно. Кольцо называется *кольцом с единицей*, если в нем существует нейтральный элемент 1 относительно умножения. Кольцо называется кольцом без делителей нуля, если $ab \neq 0$ для любых ненулевых элементов a, b кольца. Коммутативное кольцо с единицей без делителей нуля называется *областью целостности*.

В кольце K с единицей множество $G(K)$ всех обратимых элементов является группой относительно умножения. Группа $G(K)$ называется *группой обратимых элементов кольца K*.

Пусть K, K' - кольца. Отображение $\varphi : K \to K'$ называется *гомоморфизмом* кольца K в кольцо K', если $\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2),\ \varphi(g_1 + g_2) = \varphi(g_1) + \varphi(g_2)$ для любых $g_1, g_2 \in K$. Биективный гомоморфизм колец называется изоморфизмом колец. Обозначение: $K \cong K'$.

Если I - непустое подмножество множества K; если $(I, +, \cdot)$ является кольцом, то кольцо I называется *подкольцом* кольца K и обозначается $I \leq K$. Подкольцо I кольца K называется *идеалом* кольца K, и обозначается $I \lhd K$, если $IK \subset I,\ KI \subset I$. Пусть K - коммутативное кольцо с единицей, $M = \{a_1, ..., a_n\}$ - непустое подмножество кольца K, тогда множество $I = \{a_1 x_1 + ... + a_n x_n \mid x_1, ..., x_n \in K\}$ является идеалом кольца K, называется *идеалом, порождённым множеством M* и обозначается $I = (M)$. Идеал, порождённый одним элементом кольца K называется *главным идеалом*.

Непустое подмножество I кольца K является в K идеалом тогда и только тогда, когда выполняются следующие условия: $a - b \in I$ для любых $a, b \in I$; $ac, ca \in I$ для любых $a \in I, c \in K$.

Идеал I кольца K является подгруппой аддитивной группы кольца K.

На множестве смежных классов фактор-группы K/I определим операцию умножения смежных классов следующим образом: $(a+I)\cdot(b+I)=a\cdot b+I$. Множество всех смежных классов кольца K по идеалу I относительно сложения и умножения классов является кольцом. Это кольцо называется *фактор-кольцом кольца K по идеалу I* и обозначается, как и фактор-группа, K/I.

Пусть K, K'– кольца, $\varphi: K \to K'$ – гомоморфизм колец, 0'– нуль кольца K'. Ядром гомоморфизма φ называется множество $\mathrm{Ker}\varphi = \{a \in K : \varphi(a)=0'\}$. Ядро произвольного гомоморфизма $\varphi: K \to K'$ является идеалом кольца K.

Отметим, что если $\varphi: K \to K'$ – гомоморфизм колец, тогда $\varphi(K) \cong K/\mathrm{Ker}\varphi$.

Пусть m – фиксированное натуральное число. Множество $mZ = \{mc : c \in Z\}$ является идеалом в кольце целых чисел Z. Фактор-кольцо кольца Z по идеалу mZ называется *кольцом вычетов по модулю m* и обозначается Z_m.

Пусть K - область целостности. Функция $\nu: K \setminus \{0\} \to N \cup \{0\}$ называется *нормой* в K, если:

1) $\nu(ab) \geq \nu(a)$ для любых $a, b \in K \setminus \{0\}$;

2) для любых $a \in K$, $b \in K \setminus \{0\}$ существуют $q, r \in K$, такие, что $a = qb + r$ и либо $\nu(r) < \nu(b)$, либо $r = 0$.

Область целостности K, на которой можно задать норму ν, называется *евклидовым кольцом*. Пусть K - евклидово кольцо. Элемент $b \in K$ называется *делителем* элемента a, если существует $q \in K$, такое, что $a = bq$. Пусть a, b - ненулевые элементы евклидова кольца K, элемент $d \in K \setminus \{0\}$ называется *наибольшим общим делителем* элементов a и b, если d является делителем элементов a, b и для любого общего делителя d_1 элементов a, b выполняется условие $\nu(d) \geq \nu(d_1)$ (обозначение наибольшего общего делителя: $d = (a,b)$). Наибольший общий делитель $d = (a,b)$ определён однозначно с точностью до умножения на обратимый элемент кольца K. В евклидовом кольце K для нахождения наибольшего общего делителя чисел $a, b \in K \setminus \{0\}$, $\nu(a) \geq \nu(b)$, используют алгоритм Евклида.

Пример 1. Образует ли кольцо множество рациональных чисел, в несократимой записи которых знаменатели не делятся на фиксированное простое число p?

Решение. Обозначим через A_p множество

$$\left\{\frac{a}{b}\middle| a\in Z, b\in N, (a,b)=1, p\nmid b\right\}.$$

Пусть $\frac{a_1}{b_1},\frac{a_2}{b_2}\in A_p$, тогда $\frac{a_1}{b_1}+\frac{a_2}{b_2}=\frac{a_1b_2+a_2b_1}{b_1b_2}=\frac{a_3}{b_3}$, где $a_3\in Z$, $b_3\in N$, $(a_3,b_3)=1$. Очевидно, $b_3\mid b_1b_2$. Так как p не делит число b_1b_2, то p не делит b_3. Следовательно, $\frac{a_3}{b_3}\in A_p$. Далее $\frac{a_1}{b_1}\cdot\frac{a_2}{b_2}=\frac{a_1a_2}{b_1b_2}=\frac{a_4}{b_4}$, где $a_4\in Z$, $b_4\in N$, $(a_4,b_4)=1$. Так как $b_4\mid b_1b_2$, то p не делит b_4. Отсюда $\frac{a_4}{b_4}\in A_p$. Множество A_p образует абелеву группу относительно сложения: 0 - нейтральный элемент, обратным элементом к $x\in A_p$ является противоположное число $(-x)\in A_p$, сложение ассоциативно и коммутативно. Умножение коммутативно. Кроме того, $a(b+c)=ab+ac$, $(b+c)a=ba+ca$ для любых $a,b,c\in A_p$. Поэтому $(A_p,+,\cdot)$ - кольцо.

Пример 2. В кольце многочленов с действительными коэффициентами $R[x]$ найдите идеал, порождённый множеством $M=\{x^6-1,x^4-1\}$.

Решение. Докажем, что $(M)=\{(x^2-1)f(x)\mid f(x)\in R[x]\}$. С одной стороны, так как $(x^6-1,x^4-1)=x^2-1$, то любой элемент идеала (M) делится на многочлен x^2-1. С другой стороны, так как $(x^4+x^2+1,x^2+1)=1$, то для любого многочлена $f(x)\in R[x]$ существуют многочлены $u(x)$, $v(x)$, такие, что $(x^4+x^2+1)u(x)+(x^2+1)v(x)=f(x)$. Следовательно, $(M)=(x^2-1)R[x]$.

Пример 3. Найдите число гомоморфизмов из кольца Z_{40} в кольцо Z_{60}.

Решение. Пусть $\varphi: Z_{40}\to Z_{60}$ – гомоморфизм, тогда $\varphi(0)=0$. Возьмём произвольное $x\in Z_{40}$, тогда $\varphi(x)=\varphi(\underbrace{1+\ldots+1}_{x\text{ раз}})=\varphi(1)+\ldots+\varphi(1)=x\varphi(1)$.

Очевидно, что любое отображение вида: $\varphi(x)=a\cdot x$ является гомоморфизмом из Z_{40} в Z_{60} тогда и только тогда, когда $a^2\equiv a(\mathrm{mod}60)$ и $40a\equiv 0(\mathrm{mod}60)$. Таким образом, искомое число гомоморфизмов равняется числу вычетов a в полной системе вычетов, удовлетворяющих сравнению $a^2\equiv a(\mathrm{mod}\,60)$. Так как $(a,a-1)=1$, то каждое решение рассматриваемого сравнения удовлетворяет системе:

$$\begin{cases} a \equiv 0 (\mathrm{mod}\, p), \\ a \equiv 1 (\mathrm{mod}\, q), \end{cases}$$

Где pq=60,(p,q)=1. Верно и обратное, каждое решение системы является решением сравнения. При фиксированных p,q система имеет единственное решение в полной системе вычетов по модулю 60. Так как 60= $=2^2 \cdot 3^1 \cdot 5^1$, то количество пар чисел p,q, удовлетворяющих условиям $pq = 60$, $(p,q) = 1$, равняется 8 и таких чисел a, что $a^2 \equiv a (\mathrm{mod} 60)$ и $40a \equiv$ $\equiv 0 (\mathrm{mod} 60)$ будет 4. Следовательно, число гомоморфизмов из кольца Z_{40} в кольцо Z_{60} равняется 4.

7.1. Определите, какие из указанных множеств образуют кольцо относительно заданных операций:

1) $(A,+,\cdot)$, где A - одно из множеств N, Z, Q, R, C;

2) $(2^X, \Delta, \bigcap)$, где X - заданное множество;

3) $(nZ,+,\cdot)$, где $n \in N$;

4) множество чисел вида $x + y\sqrt{2}$, $x, y \in Q$, относительно сложения и умножения;

5) множество $Z[i]$ гауссовых чисел $x + yi$, $x, y \in Z$, относительно сложения и умножения;

6) множество вещественных ортогональных матриц порядка $n \in N$ относительно сложения и умножения матриц;

7) множество матриц вида $\begin{pmatrix} x & y \\ ay & x \end{pmatrix}$, $x, y \in Z$, где a - фиксированное целое число, относительно сложения и умножения матриц;

8) множество вещественных матриц порядка $n \geq 2$, у которых последние две строки нулевые;

9) $(C[a,b],+,\cdot)$;

10) $(R[x],+,\circ)$;

11) множество функций вещественной переменной, обращающихся в 0 на фиксированном подмножестве $D \subset R$, относительно сложения и умножения.

7.2. Найдите все подкольца кольца K, если:

1) $K = Z_7$;

2) $K = Z_{10}$;

3) $K = Z_{12}$;

4) $K = Z_{2010}$.

7.3. Найдите идеал кольца K, порождённый множеством M, если:

1) $K = R$, $M = \{\sqrt[3]{2}\}$;

2) $K = Q$, $M = \{1/3, 1/4\}$;

3) $K = Z$, $M = \{6, 18, 21\}$;

4) $K = R[x]$, $M = \{x^m - 1, x^n - 1\}$, где $m, n \in N$.

7.4. Найдите все обратимые элементы в кольцах:

1) вещественных верхних треугольных матриц порядка $n \in N$;

2) Z_{100};

3) $Z[i]$.

7.5. Найдите число гомоморфизмов из кольца Z_n в кольцо Z_m, если:

1) $n = 12$, $m = 24$;

2) $n = 18$, $m = 18$;

3) $n = 2011^{2010}$, $m = 2010^{2011}$.

7.6. Докажите, что любой идеал кольца Z является главным.

7.7. Приведите пример кольца без единицы.

7.8. Докажите, что кольцо K является евклидовым, если:

1) $K = Z$;

2) $K = R[x]$;

3) $K = Z[i]$.

7.9. Вычислить фактор-кольца K / I, если:

1) $K = Z_2[x]$, $I = (x^2 + 1)$;

2) $K = Z_3[x]$, $I = (x^2 + x + 2)$;

3) $K = Z$, $I = (\{10, 15\})$;

4) $K = Z$, $I = (\{2^m - 1, 2^n - 1, 2^k - 1\})$, где m, n, k - различные натуральные числа.

7.10. Докажите, что если I есть идеал кольца K, то $I[x]$ есть идеал кольца $K[x]$.

7.11. Является ли $C[0,1]$ областью целостности?

7.12. Найдите все гомоморфизмы из кольца Z в кольцо Q.

7.13. Пусть $K = \left\{ \begin{pmatrix} a & b \\ a & b \end{pmatrix} \middle| a, b \in R \right\}$. Докажите, что отображение $f : K \to R$, действующее по правилу $f : A = \begin{pmatrix} a & b \\ a & b \end{pmatrix} \mapsto \mathrm{tr}(A) = a + b$, является

гомоморфизмом колец K, R. Найдите его ядро, образ и фактор-кольцо $K / \mathrm{Ker}(f)$.

7.14. Образуют ли идеал необратимые элементы кольца K, если:

1) $K = Z$;
2) $K = C[x]$;
3) $K = Z_n$, где $n \in N$.

7.15. Докажите, что кольца K_1 и K_2 изоморфны, если:

1) $K_1 = R[x]/(x^2 + 1)$, $K_2 = C$;
2) $K_1 = Q[x]/(x - a)$, $K_2 = Q$, где $a \in Q$;
3) $K_1 = Z[x]/(I)$, $K_2 = Z_2$, где I - множество всех многочленов с чётными свободными членами в кольце $Z[x]$.

8. ПОЛЯ

Коммутативное кольцо P с единицей, состоящее не менее чем из двух элементов, в котором каждый ненулевой элемент обратим, называется *полем*.

Ясно, что если коммутативное кольцо K с единицей ($1 \neq 0$) не содержит нетривиальных идеалов, то K является полем.

Если P – поле, то множество P образует аддитивную абелеву группу, множество $P^* = P \setminus \{0\}$ образует мультипликативную абелеву группу. В поле нет делителей нуля.

Подмножество F поля P называется *подполем* поля P, если F само является полем относительно индуцированных операций из поля P. В этом случае поле P называется *расширением поля* F.

Пусть 1 – единица поля P. Наименьшее натуральное число p, для которого $p \cdot 1 = 0$, т.е. $1 + \ldots + 1 = 0$ (p раз), называется *характеристикой* поля P (обозначение: char P). Если такого числа p не существует, то говорят, что поле P имеет нулевую характеристику. Если натуральное число p является характеристикой поля P, то p является простым числом.

Пусть F – расширение поля P. Система элементов $(x_1, \ldots, x_n)$ из F называется *линейно зависимой* над полем P, если существуют элементы $\alpha_1, \ldots, \alpha_n \in P$, не все из которых нулевые, такие, что $\alpha_1 x_1 + \ldots + \alpha_n x_n = 0$. Если равенство $\alpha_1 x_1 + \ldots + \alpha_n x_n = 0$ выполняется лишь при $\alpha_1 = \ldots = \alpha_n = 0$, то система $(x_1, \ldots, x_n)$ называется *линейно независимой* над полем P. Поле F называется *конечным расширением* поля P, если F – расширение поля P и существует линейно независимая над полем P система $(x_1, \ldots, x_n)$ из

F, такая, что любой элемент $x \in F$ можно единственным образом представить в виде $x = \alpha_1 x_1 + ... + \alpha_n x_n$, где $\alpha_1, ..., \alpha_n \in P$. В таком случае система $(x_1, ..., x_n)$ называется *базисом поля* F над полем P. Число элементов базиса F над P, называется *степенью расширения* и обозначается $[F : P]$. Если F – конечное расширение поля P, T – конечное расширение поля F, то T – конечное расширение поля P, причем $[T:P]=[T:F]\cdot[F:P]$.

Многочлен $f(x)$ положительной степени с коэффициентами из поля P называется *приводимым* над полем P, если существуют многочлены $g(x),\ h(x) \in P[x]$, такие, что $f(x) = g(x)h(x)$ и $\deg g(x) < \deg f(x)$. В противном случае многочлен $f(x)$ положительной степени называется *неприводимым* над полем P.

Пусть F – расширение поля P. Элемент $a \in F$ называется *алгебраическим* над полем P, если существует многочлен $f(x) \in P[x]$, такой, что $f(a) = 0$. Расширение F поля P называется *алгебраическим расширением* поля P, если любой элемент поля F является алгебраическим над P. *Минимальным многочленом* алгебраического элемента $a \in F$ над полем P называется многочлен $f(x) \in P[x]$ наименьшей степени, для которого $f(a) = 0$. Минимальный многочлен определён однозначно с точностью до умножения его на ненулевой элемент поля P и является неприводимым над полем P. Если $f(x)$ - минимальный многочлен элемента $a \in F$ над полем P и $g(x) \in P[x]$ - многочлен, одним из корней которого является элемент a, то многочлен $g(x)$ делится на многочлен $f(x)$. *Степенью* алгебраического элемента $a \in F$ над полем P называется число, равное степени минимального многочлена элемента a. Элемент $\alpha \in C$, который является алгебраическим над полем Q, называется *алгебраическим числом*.

Пусть F - расширение поля P. Обозначим через $P[\alpha]$ наименьшее поле, содержащее поле P и элемент $\alpha \in F$. Переход от поля P к полю $P[\alpha]$ называется *присоединением* к P элемента α, поле $P[\alpha]$ называется *простым расширением* поля P. Если элемент α является алгебраическим степени n над полем P, то $P[\alpha]=\{b_0+b_1\alpha+\ldots+b_{n-1}\alpha^{n-1} | b_0,\ldots,b_{n-1} \in P\}$ и $[P(\alpha) : P] = n$. Расширение F поля P называется *полем разложения* многочлена $f(x) \in P[x]$, если $f(x) = a_0(x - x_1)...(x - x_n)$ в $F[x]$, причем F – наименьшее поле, содержащее P и $x_1, ..., x_n$. Очевидно, поле разложения многочлена $f(x) \in P[x]$ может быть получено последовательным присоединением корней $x_i \in F$, $i = \overline{1,n}$, многочлена $f(x)$.

Если F – конечное поле с единицей e, то F содержит p^n элементов, где p - характеристика поля F, n - степень расширения поля F над полем $P = \{e, 2e, ..., pe\}$.

Кольцо вычетов $Z_m = Z/(m)$ является полем тогда и только тогда, когда m является простым числом.

Пусть P - поле, фактор-кольцо $P[x]/(f(x))$ является полем тогда и только тогда, когда многочлен $f(x)$ неприводим над полем P.

Отметим, что неприводимыми над полем C являются лишь многочлены первой степени, неприводимыми над полем R являются многочлены первой степени и многочлены второй степени, не имеющие действительных корней. Достаточное условие неприводимости многочлена над полем Q даёт следующий признак Эйзенштейна: пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ - многочлен с целыми коэффициентами положительной степени n и существует простое число p, такое, что числа $a_{n-1}, a_{n-2}, ..., a_1$ делятся на p, число a_n не делится на p, число a_0 делится на p, но не делится на p^2, тогда многочлен $f(x)$ неприводим над полем Q.

Пример 1. Пусть P - произвольное поле. Определите, образует ли поле множество $P(x)$, состоящее из рациональных функций $\frac{f(x)}{g(x)}$, где $f(x), g(x)$ - взаимно простые многочлены над полем P, $g(x) \not\equiv 0$.

Решение. Множество $P(x)$ образует абелеву группу относительно операции сложения функций. Умножение функций ассоциативно и коммутативно, выполняется закон дистрибутивности относительно сложения и умножения. Следовательно, множество $P(x)$ образует коммутативное кольцо. Функция $f(x) \equiv 1$ является единицей кольца. Для любой функции $f(x) \not\equiv 0$ элемент $\frac{1}{f(x)}$ принадлежит множеству $P(x)$ и является обратным элементом для $f(x)$. Учитывая, что $|P(x)| \geq 2$, заключаем, что множество $P(x)$ образует поле.

Пример 2. Найдите поле разложения F многочлена $f(x) = x^2 + x + 2$ над полем $P = Z_3$ и укажите степень расширения $[F : P]$.

Решение. Многочлен $f(x)$ неприводим над Z_3. Докажем, что $F = Z_3[x]/(x^2 + x + 2)$. Найдём решения уравнения $\theta^2(x) + \theta(x) + 2 = 0$ в

факторкольце $Z_2[x]/(x^2+x+1)$. Корнями уравнения являются элементы: $x+f(x)Z_3[x]$ и $2+2x+f(x)Z_3[x]$. Присоединяя корни, находим, что $F=\{\bar{0},\bar{1},\bar{2},\bar{x},\overline{x+1},\overline{x+2},\overline{2x},\overline{2x+1},\overline{2x+2}\}$. Т.е. $F=Z_3[x]/(f(x))$ и $[F:P]=3$.

Пример 3. Докажите, что число $\alpha=\sqrt[3]{2}+i$ является алгебраическим.

Решение. Имеем: $\alpha-i=\sqrt[3]{2}$, $\alpha^3-3\alpha^2 i-3\alpha+i=2$, $\alpha^3-3\alpha-2=(3\alpha^2-1)i$, $\alpha^6+9\alpha^2+4-6\alpha^4-4\alpha^3+12\alpha=-9\alpha^4+6\alpha^2-1$, $\alpha^6+3\alpha^4-4\alpha^3+3\alpha^2+12\alpha+5=0$. Следовательно, число α алгебраическое.

8.1. Какие из числовых множеств N,Z,Q,R,C образуют поле относительно операций сложения и умножения?

8.2. Докажите, что конечная область целостности является полем.

8.3. Докажите, что любое конечное поле имеет положительную характеристику.

8.4. Существует ли бесконечное поле положительной характеристики?

8.5. Докажите, что в поле Z_p выполняются равенства:

1) $\sum\limits_{k=1}^{p-1}k^{-1}=0$ $(p>2)$;

2) $\sum\limits_{k=1}^{(p-1)/2}k^{-2}=0$ $(p>3)$.

8.6. Найдите минимальный многочлен для элемента a над полем P, если:

1) $a=\sqrt{2}$, $P=Q$;

2) $a=\sqrt[3]{5}$, $P=Q$;

3) $a=2-3i$, $P=R$;

4) $a=2-3i$, $P=C$;

5) $a=\sqrt{2}+\sqrt{3}$, $P=Q$.

8.7. Докажите, что элемент a является алгебраическим над полем Q, если:

1) $a=\sqrt[3]{1-\sqrt{2}}$;

2) $a=1-i\sqrt{3}$;

3) $a=\sqrt[5]{-2+i\sqrt{2}}$.

8.8. Найдите степень элемента $\sqrt{2}+i$ над полем P, если:

1) $P=Q$;

2) $P=R$;

3) $P = C$.

8.9. Докажите, что если многочлен $f(x) \in Z_p[x]$ неприводим над полем Z_p, то для любых $a, b \in Z_p$, $a \neq 0$, многочлен $f(ax+b)$ неприводим над полем Z_p.

8.10. Пусть n - натуральное число, α - действительное положительное число. Докажите, что если числа α^n и $(\alpha+1)^n$ рациональные, то число α также рациональное.

8.11. Пусть n - натуральное число, α - комплексное число, такие, что числа α^n и $(\alpha+1)^n$ рациональные. Можно ли утверждать, что число α также рациональное?

8.12. Найдите все неприводимые над полем Z_2 многочлены второй степени из $Z_2[x]$.

8.13. При каких значениях $k = 1,2,3,4,5,6$ факторкольцо $Z_7[x]/(x^2+k)$ является полем?

8.14. Применяя алгоритм Евклида, найти наибольший общий делитель многочленов $f(x), g(x)$ с коэффициентами из поля P, если:

1) $f(x) = x^7 + 1$, $g(x) = x^5 + x^3 + 1$, $P = Z_2$;

2) $f(x) = x^5 + x + 1$, $g(x) = x^6 + x^5 + x^4 + 1$, $P = Z_2$;

3) $f(x) = x^8 + 2x^5 + x^3 + x^2 + 1$, $g(x) = 2x^6 + x^5 + 2x^3 + 2x^2 + 2$, $P = Z_3$.

8.15. Докажите неприводимость многочленов $f(x) = x^2 + 1$, $g(x) = x^2 + x + 4$ над полем Z_{11} и построить изоморфизм факторколец $Z_{11}[x]/(f(x))$ и $Z_{11}[x]/(g(x))$.

8.16. Вычислите образ $(2x+1)^{-1}$ в факторкольце $P[x]/(x^3 - 2)$, если:

1) $P = Q$;

2) $P = Z_7$.

8.17. Решите сравнения:

1) $(x^2+1)f(x) \equiv 1 (\mathrm{mod}\, x^3 + 1)$ в $Z_3[x]$;

2) $(x^4 + x^3 + x^2 + 1)f(x) \equiv x^2 + 1 (\mathrm{mod}\, x^3 + 1)$ в $Z_2[x]$.

8.18. Найдите поле разложения F многочлена $f(x)$ над полем P и укажите степень расширения $[F:P]$, если:

1) $f(x) = (x^2 - 3)(x^3 + 1)$, $P = Q$;

2) $f(x) = (x^2 - 3)(x^2 - 2x - 2)$, $P = Q$;

3) $f(x) = x^3 + x + 2$, $P = Q$;

4) $f(x)=x^2+x+1,\ P=Z_2$;

5) $f(x)=x^6-1,\ P=Q$;

6) $f(x)=x^6-1,\ P=Z_7$.

8.19. Докажите, что факторкольцо $Q[x]/(f(x))$ является полем, если:

1) $f(x)=x^7-14$;

2) $f(x)=x^{2010}+x^{2009}+...+x+1$.

8.20. Напишите таблицы умножения для колец $Z_2[x]/(x^2+x+1)$, $Z_2[x]/(x^3+x+1)$, $Z_2[x]/(x^3+x^2+1)$.

8.21. Пусть p - простое число, $f(x)$ - многочлен с коэффициентами из Z_p. Докажите, что $(f(x))^p=f(x^p)$ для любого $x\in Z_p$.

8.22. Разложите многочлен $f(x)$ в произведение неприводимых над полем P многочленов, если:

1) $P=Z_2,\ f(x)=x^9+x+1$;

2) $P=Z_3,\ f(x)=x^7+x^6+x^5-x^3+x^2-x-1$.

8.23. Докажите, что если L - расширение поля K и степень расширения $[L:K]$ - простое число, то единственными полями F, удовлетворяющими условию $K\subseteq F\subseteq L$ являются $F=K$ и $F=L$.

9. ШИФРОВАНИЕ

Отображение $x\to ax+b$, где $a,b,x\in Z_m,\ (a,m)=1$ называется модулярным шифром.

Модулярные шифры составляют основу модулярных криптосистем.

Различают следующие модулярные криптосистемы: криптосистема Рабина,RSA-криптосистема, криптосистема с открытым ключом, криптосистема без передачи ключей, протокол прямого обмена ключами (метод Диффи-Хеллмана), электронная цифровая подпись и пороговая система.

Криптосистема Рабина. Выбираются нечетные простые числа p и q вида $4k+3$, ($p<q$). Они считаются секретными, а модуль $N=pq$ - несекретным. Функция шифрования задается формулой $E(x)=x^2(\mathrm{mod}\,N)$, где $0<x<N$. Дешифрование сводится к решению сравнения $x^2\equiv a(\mathrm{mod}\,N)$, которое распадается на четыре системы

$x \equiv \pm a^{(p+1)/4} (\mathrm{mod}\, p)$, $x \equiv \pm a^{(q+1)/4} (\mathrm{mod}\, q)$. Поскольку система Рабина применяется для шифрования осмысленного текста, то при дешифровании из четырёх возможных решений выбирается вариант, соответствующий осмысленному тексту.

RSA-криптоситема. Пусть $N = pq$, где p и q - большие простые числа. Модуль N не является секретным, а числа p и q держатся в секрете. Число e (открытый ключ) берется взаимно простым с $\varphi(N) = (p-1)(q-1)$. Число d (секретный ключ) находится из условия $1 \le d \le N-1$, $ed \equiv 1 (\mathrm{mod}\, \varphi(N))$. При RSA-шифровании текст или его часть отождествляется с натуральным числом x, $0 < x < N$, $(x, N) = 1$, а алгоритмы шифрования и дешифрования выглядят следующим образом: $E(x) = x^e (\mathrm{mod}\, N)$, $D(x^e) = x^{ed} (\mathrm{mod}\, N)$. RSA-криптосистему можно использовать и для цифровой подписи сообщения x. Для этого обладатель секретного ключа вычисляет $D(x) = x^d (\mathrm{mod}\, N)$. Пара чисел $(x, D(x))$ считается подписанным сообщением. Его подлинность можно проверить с помощью несекретного ключа e: $x \equiv x^{ed} (\mathrm{mod}\, N)$.

Криптосистема с открытым ключом. Пусть абоненты А и В решили организовать для себя возможность секретной переписки. Для этого каждый из них независимо друг от друга выбирает два различных больших простых числа, а именно,

А: p_A, q_A;

В: p_B, q_B.

Пусть $m_A = p_A q_A, m_B = p_B q_B$.

Абонент А выбирает случайное число e_A такое, что $0 < e_A < \varphi(m_A)$, НОД$(e_A, \varphi(m_A)) = 1$. Абонент В выбирает случайное число e_B такое, что $0 < e_B < \varphi(m_B)$, НОД$(e_B, \varphi(m_B)) = 1$.

Абонент А вычисляет d_A такое, что $0 < d_A < \varphi(m_A)$, $d_A e_A \equiv 1 (\mathrm{mod}\, \varphi(m_A))$. Абонент В вычисляет d_B такое, что $0 < d_B < \varphi(m_B)$, $d_B e_B \equiv 1 (\mathrm{mod}\, \varphi(m_B))$.

Затем А и В делают общедоступными следующие книги паролей:

А: e_A, m_A;

В: e_B, m_B.

Теперь можно отправлять конфиденциальные сообщения абонентам А или В.

Например, если пользователь книги паролей хочет отправить сообщение *x* для А, то он поступает следующим образом:

использует *открытый ключ* e_A из книги паролей,

вычисляет $x_1 \equiv x^{e_A} (\mathrm{mod}\, m_A)$,

отправляет сообщение x_1 абоненту А.

Абонент А для дешифровки сообщения x_1 использует *секретный ключ* d_A и вычисляет $x_1^{d_A}$. Используя теорему Эйлера, несложно проверить, что это и будет переданное сообщение *x*.

Криптосистема без передачи ключей. Пусть абоненты А и В условились организовать между собой секретную переписку. Для этого они выбирают достаточно большое простое число p.

Абоненты А и В выбирают себе секретные ключи e_A и e_B соответственно такие, что $0 < e_A < p-1$, НОД$(e_A, p-1) = 1$, $0 < e_B < p-1$, НОД$(e_B, p-1) = 1$.

Затем абоненты А и В находят вторые секретные ключи d_A и d_B соответственно такие, что $0 < d_A < p-1$, $e_A d_A \equiv 1 (\mathrm{mod}\, p-1)$, $0 < d_B < p-1$, $e_B d_B \equiv 1 (\mathrm{mod}\, p-1)$.

Пересылаемые сообщения разбиваются на части, меньшие $p-1$.

Предположим, абонент А решил отправить сообщение *x* абоненту В.

Для этого абонент А вычисляет $x_1 \equiv x^{e_A} (\mathrm{mod}\, p)$ и отправляет абоненту В сообщение x_1.

Абонент В вычисляет $x_2 \equiv x_1^{e_B} (\mathrm{mod}\, p)$ и отправляет абоненту А сообщение x_2.

Абонент А вычисляет $x_3 \equiv x_2^{d_A} (\mathrm{mod}\, p)$ и отправляет абоненту В сообщение x_3.

Абонент В вычисляет $x_4 \equiv x_3^{d_B} (\mathrm{mod}\, p)$, а это и есть переданное сообщение *x*.

Доказательство этого факта основано на теореме Ферма. Корректность работы такой криптосистемы аналогична работе криптосистемы с открытым ключом.

Протокол прямого обмена ключами (метод Диффи-Хеллмена). Натуральное число *n* и простое число *p* считаем общеизвестными.

Абонент А выбирает секретное число x_A, вычисляет $y_A \equiv n^{x_A} (\mathrm{mod}\, p)$, затем отправляет сообщение y_A абоненту В.

Абонент В выбирает секретное число x_B, вычисляет $y_B \equiv n^{x_B} (\mathrm{mod}\, p)$, затем отправляет сообщение y_B абоненту А.

Абонент А вычисляет $k_A \equiv y_B^{x_A} (\mathrm{mod}\, p)$.

Абонент В вычисляет $k_B \equiv y_A^{x_B} (\mathrm{mod}\, p)$.

Несложно проверить, что $k_A = k_B$.

Электронная цифровая подпись. Криптосистема с открытым ключом позволяет любому пользователю книги паролей отправлять сообщения для любого абонента из книги паролей. В криптосистеме с электронной подписью сообщение необходимо "подписывать", т.е. явно указывать на отправителя из книги паролей.

Пусть абоненты $A_1,...,A_n$ независимо друг от друга выбирают и вычисляют ряд чисел точно так же, как и в криптосистеме с открытым ключом, а именно:

1. абонент A_k выбирает два различных больших простых числа p_k, q_k,
2. вычисляет $m_k = p_k q_k$,
3. выбирает открытый ключ e_k такой, что $0 < e_k < \varphi(m_k)$, НОД$(e_k, \varphi(m_k)) = 1$,
4. вычисляет секретный ключ d_k такой, что $0 < d_k < \varphi(m_k)$, $d_k e_k \equiv 1(\mathrm{mod}\,\varphi(m_k))$.

Записи в книге паролей будут иметь следующий вид:

$A_1 : e_1, m_1$;

…

$A_n : e_n, m_n$.

Пусть абонент A_1 решил отправить секретное сообщение абоненту A_2. Если $x \geq \min(m_1, m_2)$, то x разбивается на части, каждая из которых меньше, чем $\min(m_1, m_2)$. Необходимо проделать следующую последовательность действий.

Рассмотрим случай $m_1 \leq m_2$.

1. Абонент A_1 вычисляет $x_1 \equiv x^{d_1}(\mathrm{mod}\,m_1)$ и $x_2 \equiv x_1^{e_2}(\mathrm{mod}\,m_2)$, а затем отправляет сообщение x_2 абоненту A_2.

2. Абонент A_2 вычисляет $x_3 \equiv x_2^{d_2}(\mathrm{mod}\,m_2)$ и $x_4 \equiv x_3^{e_1}(\mathrm{mod}\,m_1)$.

Рассмотрим случай $m_1 > m_2$.

1. Абонент A_1 вычисляет $x_1 \equiv x^{e_2}(\mathrm{mod}\,m_2)$ и $x_2 \equiv x_1^{d_1}(\mathrm{mod}\,m_1)$, а затем отправляет сообщение x_2 абоненту A_2.

2. Абонент A_2 вычисляет $x_3 \equiv x_2^{e_1}(\mathrm{mod}\,m_1)$ и $x_4 \equiv x_3^{d_2}(\mathrm{mod}\,m_2)$.

С помощью теоремы Эйлера несложно показать, что x_4=x.

Отметим также, что фактически предполагается, что НОД{x,m_1}=1, НОД{x,m_2}=1. Но вероятность того, что это не так, ничтожна мала.

Также отметим, что если подписать сообщение открытым образом (например, именем отправителя), то такая подпись будет ничем не защищена от подделки.

Пороговая схема. Будем говорить, что t участников $A_1,...,A_t$ (законных пользователей) $к$-хранят секрет c ($2 \le k \le t$), если

1) каждый A_i знает некоторую информацию (частичный секрет) a_i, неизвестную любому другому участнику;

2) секрет c может быть легко вычислен на основе любых $к$ частичных секретов $a_{i_1},...,a_{i_k}$;

3) знание любых $к - 1$ частичных секретов не дает такой возможности.

Множество $\{a_1,...,a_t\}$, удовлетворяющее этим условиям, называется $(к,t)$-пороговой схемой.

Приведем *способ построения пороговой схемы* на основе теории сравнений.

Пусть зафиксированы числа $к$, t ($2 \le k \le t$).

Пусть $m_1,...,m_t$ – различные натуральные попарно взаимно простые числа ($m_1 < ... < m_t$).

Обозначим через M_1 наименьшее произведение k различных модулей, а через M_2 – наибольшее произведение $к - 1$ различных модулей, т.е. $M_1 = m_1 \cdot ... \cdot m_k$, $M_2 = m_{t-k+2} \cdot ... \cdot m_t$.

Модули $m_1,...,m_t$ следует выбирать так, чтобы $\frac{M_1}{M_2} >> 1$.

Случайным образом выберем число c такое, что $M_2 < c < M_1$.

В качестве секретов участников A_i возьмем наименьшие неотрицательные вычеты секрета c по модулям $m_1,...,m_t$, т.е. $a_i \equiv c(\mathrm{mod}\, m_i)$.

Каждому участнику A_i сообщаем a_i, m_i.

Построенное выше множество $\{a_1,...,a_t\}$ является $(к,t)$-пороговой схемой.

Пример 1. Предположим, что абоненты A и B решили установить скрытую связь без передачи ключей. Для этого абоненты выбрали простое число $p = 23$, абонент A выбирает секретный ключ $e_A = 5$, абонент B выбирает секретный ключ $e_B = 7$. Осуществить передачу сообщения $m = 17$ от абонента A абоненту B.

Решение. Абонент A, решая сравнение $5x \equiv 1(\mathrm{mod}\, \varphi(23))$, находит свой второй секретный ключ $d_A = 9$; абонент B, решая сравнение $7x \equiv 1(\mathrm{mod}\, \varphi(23))$, находит свой второй секретный ключ d_B=19. Затем абонент A шифрует сообщение $m = 17$ своим первым секретным ключом и передаёт шифрованное сообщение абоненту B: $m_1 \equiv 17^5 \equiv 21(\mathrm{mod}\, 23)$.

Абонент B, получив сообщение $m_1 = 23$, шифрует его своим первым секретным ключом и передаёт абоненту A: $m_2 \equiv 21^7 \equiv 10(\mathrm{mod}\,23)$. Абонент A шифрует сообщение m_2 своим вторым секретным ключом и передает абоненту B: $m_3 \equiv 10^9 \equiv 20(\mathrm{mod}\,23)$. Получив это сообщение, абонент B расшифровывает его при помощи своего второго ключа: $m_4 \equiv 20^{19} \equiv 17(\mathrm{mod}\,23)$.

Пример 2. Предположим, что абоненты A и B решили установить скрытую связь с открытым ключом. Пусть $p_A = 7,\ q_A = 23$ - простые числа абонента A, $p_B = 11,\ q_B = 17$ - простые числа абонента B, телефонные книги абонентов A и B имеют вид: $e_A = 7,\ m_A = 161;\ e_B = 9,\ m_B = 187$. Осуществить передачу секретного сообщения $m = 3$ от абонента A к абоненту B и секретного сообщения $x = 5$ от абонента B к абоненту A.

Решение. Решая сравнение $7x \equiv 1(\mathrm{mod}\,\varphi(161))$, абонент A находит секретный ключ $d_A = 19$. Решая сравнение $9x \equiv 1(\mathrm{mod}\,\varphi(187))$, абонент B находит секретный ключ $d_B = 89$. Абонент A шифрует сообщение $m = 3$ открытым ключом абонента B и отправляет шифрованное сообщение абоненту B: $m_1 \equiv 3^9 \equiv 48(\mathrm{mod}187)$. Получив сообщение m_1, абонент B расшифровывает его своим секретным ключом: $m_2 \equiv 48^{89} \equiv 3(\mathrm{mod}187)$. Абонент B шифрует сообщение $x = 5$ открытым ключом абонента A и отправляет зашифрованное сообщение абоненту A: $x_1 \equiv 5^7 \equiv 40(\mathrm{mod}161)$. Далее абонент A расшифровывает полученное сообщение x_1 своим секретным ключом: $x_2 \equiv 40^{19} \equiv 5(\mathrm{mod}161)$.

Пример 3. Предположим, что абоненты A и B решили установить скрытую связь с открытым ключом с электронной подписью. Пусть $p_A = 7,\ q_A = 13$ - простые числа абонента A, $p_B = 11,\ q_B = 23$ - простые числа абонента B, телефонные книги абонентов A и B имеют вид: $e_A = 5,\ m_A = 91;\ e_B = 31,\ m_B = 253$. Осуществить передачу сообщения $m = 41$ с электронной подписью от абонента B к абоненту A.

Решение. Решая сравнения $5x \equiv 1(\mathrm{mod}\,\varphi(91))$ и $31x \equiv 1(\mathrm{mod}\,\varphi(253))$, абоненты A и B находят свои секретные ключи $d_A = 29$, $d_B = 71$. Так как $m_A < m_B$, то абонент B сначала шифрует сообщение $m = 41$ открытым ключом абонента A: $m_1 \equiv 41^5 \equiv 6(\mathrm{mod}\,91)$, а затем шифрует сообщение m_1 своим секретным ключом: $m_2 \equiv 6^{71} \equiv 94(\mathrm{mod}\,253)$ и отправляет сообщение m_2 абоненту A. Абонент A получив сообщение m_2 сначала рас-

шифровывает его открытым ключом абонента B: $m_3 \equiv 94^{31} \equiv 6(\mathrm{mod}\,253)$, а затем расшифровывает сообщение m_3 своим секретным ключом: $m_3 \equiv 6^{29} \equiv 41(\mathrm{mod}\,91)$.

Пример 4. Используя наименьший положительный первообразный корень по модулю $p = 23$ и случайные числа $x_A = 7$, $x_B = 13$, создайте сеансовый ключ для двух пользователей A и B.

Решение. Наименьшим первообразным корнем по модулю $p = 23$ является число $n = 5$. Пользователь A выбирает случайное число $x_A = 7$, вычисляет $y_A \equiv 5^7 \equiv 17(\mathrm{mod}\,23)$ и отправляет сообщение $y_A = 17$ абоненту B. Абонент B выбирает случайное число $x_B = 13$, вычисляет $y_B \equiv 5^{13} \equiv 21(\mathrm{mod}\,23)$ и отправляет сообщение $y_B = 21$ абоненту A. Далее абонент A вычисляет $k_A \equiv y_B^{x_A} = 21^7 \equiv 10(\mathrm{mod}\,23)$, абонент A вычисляет $k_B \equiv y_A^{x_B} = 17^{13} \equiv 10(\mathrm{mod}\,23)$. Число $k_A = k_B = 10$ является общим ключом абонентов A и B.

Пример 5. Проверьте, что модули $m_1 = 97$, $m_2 = 98$, $m_3 = 99$, $m_4 = 101$, $m_5 = 103$ и частичные секреты $a_1 = 73$, $a_2 = 15$, $a_3 = 61$, $a_4 = 61$, $a_5 = 49$ образуют (3,5)-пороговую схему, а также найдите секрет c.

Решение. Так как M_1=97·98·99>M_2=101·103, то модули m_i, $i = \overline{1,5}$, пригодны для реализации пороговой схемы. Система сравнений $c \equiv 15(\mathrm{mod}\,98)$, $c \equiv 61(\mathrm{mod}\,99)$, $c \equiv 61(\mathrm{mod}\,101)$ имеет единственное решение $c \equiv 500011(\mathrm{mod}\,979902)$. Кроме того, $c \equiv a_i(\mathrm{mod}\,m_i)$ для любого $i = \overline{1,5}$. Знание каких-либо двух частичных секретов a_i, a_j не позволяет восстановить секрет $c = 500011$. Следовательно, множество $\{a_1, a_2, a_3, a_4, a_5\}$ образует (3,5)-пороговую схему и $c = 500011$.

9.1. Примените модулярное шифрование $x \to ax + b(\mathrm{mod}\,26)$ к словам ALGEBRA и NUMBER, отождествляя латинский алфавит с Z_{26}, если:
1) $a = 3, b = 2$;
2) $a = 5, b = 7$.

9.2. Найдите обратные преобразования к шифрам из предыдущей задачи и применить их для дешифрования.

9.3. Объясните необходимость условия $(a, m) = 1$ при модулярном шифровании $x \to ax + b(\mathrm{mod}\,m)$.

9.4. Покажите, что композиция двух модулярных шифров $x \to a_1 x + b_1 (\mathrm{mod}\, m)$, $x \to a_2 x + b_2 (\mathrm{mod}\, m)$, где $(a_1, m) = (a_2, m) = 1$, будет снова модулярным шифром.

9.5. Как обратить композицию двух модулярных шифров $f_1 \circ f_2$?

9.6. Пусть M_1: $x \to a_1 x + b_1 (\mathrm{mod}\, m)$, M_2: $x \to a_2 x + b_2 (\mathrm{mod}\, m)$ - модулярные шифры. Найдите все значения параметров a_1, a_2, b_1, b_2, для которых $M_1 \circ M_2 = M_2 \circ M_1$.

9.7. Отождествляя латинский алфавит с Z_{26} и применяя RSA-шифрование с параметрами $N = 3 \cdot 11$, $e = 3$, зашифровать слова ALGEBRA и NUMBER и дешифровать сообщение «17,26,12,12, 9».

9.8. Приняв $N = 17 \cdot 19$, $e = 5$, зашифруйте сообщение $m = 3$. Путем дешифрования убедитесь в корректности работы RSA-криптосистемы с выбранными параметрами. Используйте RSA-криптосистему для подписи сообщения и проверьте его подлинность.

9.9. Вычислите секретный ключ для открытого ключа $e = 97$ в следующих двух случаях: $N_1 = 299$, $N_2 = 527$.

9.10. Пусть E и D - взаимно обратные RSA-преобразования. Покажите, что $D(E(x)) = x$ для любого $x \in Z_N$, а не только для $x \in G(Z_N)$.

9.11. Докажите, что RSA-преобразования при фиксированном N образуют группу относительно операции их композиции.

9.12. Обосновать нестойкость RSA-криптосистемы, если по ошибке вместо $N = pq$ взяли $N = p$.

9.13. Покажите, что кроме двух очевидных решений $x \equiv \pm 1 (\mathrm{mod}\, pq)$ сравнение $x^2 \equiv 1 (\mathrm{mod}\, pq)$ имеет еще два решения $x \equiv \pm c (\mathrm{mod}\, pq)$, $1 < c < pq - 1$.

9.14. Покажите, что, зная $\varphi(N)$, легко факторизовать RSA-модуль $N = pq$.

9.15. Подпишите сообщение $m = 2$ и проверьте подлинность, если $N = 17 \cdot 19$, $e = 5$.

9.16. Покажите, что сообщение $x = 67$ является неподвижным ($E(x) = x$) в RSA-криптосистеме с параметрами $N = 187$, $e = 141$. Найдите все неподвижные сообщения.

9.17. Покажите, что в RSA-криптосистеме с параметрами p, q, e, d имеется $r + s + rs$ неподвижных сообщений x, $0 < x < N = pq$, где $r = (p - 1, e - 1)$, $s = (q - 1, e - 1)$.

9.18. Пусть $N = 23 \cdot 31$. Зашифруйте сообщение $m = 5$ по системе Рабина. Путем дешифрования убедитесь в корректности работы криптосистемы Рабина с выбранными параметрами.

9.19. Предположим, что абоненты A и B решили установить секретную переписку с использованием системы Рабина. Для этого они выбрали простые числа p, q вида $4k + 3$, модуль $N = pq$ и договорились, что будут обмениваться лишь такими сообщениями $m \in (0, N)$, для которых $(m, N) = 1$ и m является квадратичным вычетом по модулям p и q. Докажите, что в этом случае дешифрование осуществляется однозначно.

9.20. Пусть $N = pq$, где p, q - различные простые числа вида $4k + 3$. Докажите эквивалентность условий:

1) существует эффективный алгоритм решения сравнения $x^2 \equiv a (\mathrm{mod}\, N)$;

2) существует эффективный алгоритм факторизации модуля N.

9.21. Пусть $N = pq$, $(a, N) = 1$, где p, q - различные простые числа. Докажите, что если сравнение $x^2 \equiv a (\mathrm{mod}\, N)$ имеет одно решение, то оно имеет четыре решения на промежутке $(0, N)$.

9.22. Используя наименьший положительный первообразный корень по модулю $p = 41$, случайные числа $x_A = 11$, $x_B = 13$, создайте сеансовый ключ для двух пользователей A и B.

9.23. Предложите аналог протокола Диффи-Хеллмена, используя вместо целых чисел квадратные невырожденные матрицы и операцию их умножения.

9.24. Покажите, что модули $m_1 = 13, m_2 = 17, m_3 = 19, m_4 = 21, m_5 = 22$ пригодны для построения $(3,5)$-пороговой схемы разделения секрета. Найдите секрет c, если $a_1 = 12$, $a_2 = 14$, $a_3 = 12$, $a_4 = 13$, $a_5 = 10$.

9.25. Пусть $p_1, p_2, ..., p_t$ - различные простые числа. Докажите, что существуют натуральные числа $s_1, s_2, ..., s_t$, такие, что числа $p_1^{s_1}, p_2^{s_2}, ..., p_t^{s_t}$ пригодны для реализации (k, t)-пороговой схемы, $2 \le k \le t$.

9.26. Пусть модули $m_1, m_2, ..., m_{2k}$ реализуют $(k, 2k)$-пороговую схему. Докажите, что они также реализуют все $(t, 2k)$-пороговые схемы, $t > k$.

9.27. Предложите способ генерации модулей для любой (k, t)-пороговой схемы.

10. КОДИРОВАНИЕ

Рассмотрим двоичное кодирование и декодирование, обеспечивающее передачу данных по каналам с “шумом”. Мы будем говорить о вероятности p того, что переданный символ (0 или 1) будет принят правильно и вероятности $q = 1 - p$ того, что переданный символ (0 или 1) будет принят неправильно. При этом предполагается, что ошибки происходят независимо друг от друга. Такая передача данных называется *двоичным симметричным каналом*. Пусть по двоичному симметричному каналу передается n-битовая последовательность. Вероятность того, что она будет принята ровно с k ошибками, равна $P_k = C_n^k p^{n-k} q^k$.

Двоичным (m, n)-кодом называется пара, состоящая из схемы кодирования $E: Z_2^m \to Z_2^n$ и схемы декодирования $D: Z_2^n \to Z_2^m$ $(m \le n)$, где $Z_2^n -$ множество всех двоичных последовательностей длины n, причем функции D и E выбираются так, что функция $H = D \circ T \circ E$ является тождественной с вероятностью, близкой к 1. Функции D и E считаются безошибочными, т.е. $D \circ E$ является тождественной. Функция T называется функцией ошибок. Различают *два вида кодов*:

1) коды с исправлением ошибок (цель: восстановить с вероятностью, близкой к 1, переданное сообщение);

2) коды с обнаружением ошибок (цель: выявить с вероятностью, близкой к 1,наличие ошибок).

Примеры двоичных кодов:

1) **$(m, 3m)$-*код с тройным повторением*.** Сообщение разбивается на блоки длиной m и каждый блок передается трижды. Это определяет функцию E. Функция D определяется следующим образом: принятая строка разбивается на блоки длиной $3m$. В каждом таком блоке $c_1 \ldots c_{3m}$ по тройке символов c_i, c_{i+m}, c_{i+2m} в схеме декодирования восстанавливается символ, чаще всего встречающийся в этой тройке и ставится на i-е место в декодированном блоке.

2) **$(m, m + 1)$-*код с обнаружением ошибок на основе проверки четности*.** В этом случае функции D и E имеют следующий вид:

$$E(a_1 \ldots a_m) = a_1 \ldots a_{m+1}, \text{ где } a_{m+1} = \begin{cases} 0, \text{ если } a_1 + \ldots + a_m \equiv 0 (\mathrm{mod}\, 2), \\ 1, \text{ если } a_1 + \ldots + a_m \equiv 1 (\mathrm{mod}\, 2), \end{cases}$$

$$D(a_1 \ldots a_m a_{m+1}) = \begin{cases} a_1 \ldots a_m, \text{ если } a_1 + \ldots + a_m \equiv 0 (\mathrm{mod}\, 2), \\ \text{"ошибка", если } a_1 + \ldots + a_m \equiv 1 (\mathrm{mod}\, 2). \end{cases}$$

Блочный (*m*, *n*)-код определяется двумя функциями $E: Z_2^m \to Z_2^n$ и $D: Z_2^n \to Z_2^m$ $(m \le n)$, при этом функция $D \circ E$ является тождественной, чтобы сообщение было принято правильно при отсутствии помех.

Расстоянием Хэмминга между двумя двоичными словами $a = a_1 ... a_n$ и $b = b_1 ... b_n$ называется число позиций, в которых $a_i \neq b_i$. Обозначение: $d(a,b)$. *Весом слова* $a = a_1 ... a_n$ называется число единиц среди его координат. Обозначение: $w(a)$. Несложно проверить, что $w(a) = a_1 + ... + a_n$.

Свойства расстояния Хэмминга:

1) $d(a,b)=w(a+b)$;

2) $d(a+c,b+c)=d(a,b)$;

3) вероятность того, что слово $a = a_1 ... a_n$ будет принято как $b = b_1 ... b_n$ равна $p^{n-d(a,b)} q^{d(a,b)}$.

Для того чтобы код давал возможность обнаруживать все ошибки в не более *к* позициях, необходимо и достаточно, чтобы наименьшее расстояние между кодовыми словами было не меньше $k + 1$. Для того чтобы код давал возможность исправлять все ошибки в не более *к* позициях, необходимо и достаточно, чтобы наименьшее расстояние между кодовыми словами было не меньше $2k + 1$.

Если код исправляет не более *к* ошибок, то вероятность правильного приема слова длины *n* будет не меньше, чем $p^n + C_n^1 p^{n-1} q + ... + C_n^k p^{n-k} q^k$. Соответственно вероятность неправильного приема слова длины *n* будет не больше, чем $C_n^{k+1} p^{n-k-1} q^{k+1} + ... + C_n^{n-1} p q^{n-1} + q^n$.

Пусть данное слово $a = a_1 ... a_m$ длины кодируется в кодовое слово $b = b_1 ... b_n$ длины *n*. Двоичный симметричный канал связи при передаче слово *b* переводит в слово $r = r_1 ... r_n$, т.е. добавляет к нему строку ошибок $e = e_1 ... e_n$, а именно, $r_i = b_i + e_i$ (покомпонентное сложение по модулю 2). Система, обнаруживающая ошибки, проверяет, является ли принятое слово кодовым, и сигнализирует об ошибке, если это не так. Система, исправляющая ошибки, переводит слово $r = r_1 ... r_n$ в ближайшее кодовое слово $b = b_1 ... b_n$.

Пусть $E = (e_{ij})$ – некоторая $m \times n$ матрица, состоящая из нулей и единиц. Пусть $b_j = \sum_{i=1}^{n} a_i e_{ij}$ (суммирование по модулю 2), т.е. $b = aE$, где $b = b_1 ... b_n$, $a = a_1 ... a_m$. Эта схема кодирования определяет (m,n) – код, называемый *матричным кодом,* а матрица E называется *кодирующей матрицей*. При матричном кодировании код не должен приписывать одно и то же кодовое слово разным словам. Простой способ добиться этого состо-

ит в том, чтобы первые m столбцов матрицы E образовывали единичную подматрицу. Если a пробегает множество всех слов длины m, то множество полученных кодовых слов aE образует группу. Два матричных кода называются *эквивалентными*, если множества кодовых слов совпадают. Пусть E - кодирующая матрица, матрица H называется *проверочной матрицей*, если выполняются следующие условия: 1) если размер E равен $m\times n$, то размер H равен $n\times(n-m)$; 2) $EH=0$; 3) столбцы матрицы H линейно независимы.

Блочный код называется *групповым*, если его кодовые слова образуют группу. Если код является групповым, то наименьшее расстояние между двумя кодовыми словами равно наименьшему весу ненулевого кодового слова. Схема декодирования исходит из таблицы C всех слов, которые могут быть приняты. Кодовые слова образуют подгруппу B в группе C. Если слово $a=a_1\ldots a_m$ пробегает все двоичные слова, то мы получаем 2^m кодовых слов aE, а именно, $b_0=0\ldots0, b_1, \ldots, b_{2^m-1}$, т.е. $B=\{b_0, b_1, \ldots, b_{2^m-1}\}$. Пусть $c_1\in C, c_1\notin B$. Рассмотрим множество $B_1=\{b_0+c_1, b_1+c_1, \ldots, b_{2^m-1}+c_1\}$. Элемент c_1 называется *лидером* этого класса. Без ограничения общности можно считать, что c_1 действительно является словом наименьшего веса. Далее находим слово c_2 наименьшего веса такое, что $c_2\in C$, $c_2\notin B$, $c_2\notin B_1$.

Рассмотрим множество $B_2=\{b_0+c_2, b_1+c_2, \ldots, b_{2^m-1}+c_2\}$. И так далее продолжаем этот процесс. В результате группу C можно представить в виде объединения классов:

$$C:\begin{matrix} b_0 & b_1 & \ldots & b_{2^m-1} \\ b_0+c_1 & b_1+c_1 & \ldots & b_{2^m-1}+c_1 \\ \ldots & \ldots & \ldots & \ldots \\ b_0+c_{2^{n-m}-1} & b_1+c_{2^{n-m}-1} & \ldots & b_{2^m-1}+c_{2^{n-m}-1} \end{matrix}$$

Декодирование слова $c=c_i+b_i$ состоит в выборе кодового слова b_j в качестве переданного. Если лидерами являются слова наименьшего веса, то кодовое слово, стоящее в данном столбце, является ближайшим кодовым словом ко всем словам этого столбца.

Код Хэмминга – это частный случай (m, n)-кода. В этом случае $m=2^k-k-1$, $n=2^k-1$ ($k\in N$, $k>1$).

Код Хэмминга строится следующим образом:

1) строим матрицу M размерами $(2^k-1)\times k$, в i-ой строке которой стоят цифры двоичного представления числа i.

2) записываем систему уравнений $bM = O$, где $b=(b_0b_1...b_{2^k-1}), O$ – нулевая матрица размерами $(2^k-1)\times 1$.

3) чтобы закодировать сообщение a, берем в качестве $b_j(j\neq 2^q)$ соответствующие биты сообщения a и находим с помощью системы $bM = O$ элементы $b_j(j=2^q)$.

4) декодирование кода Хэмминга происходит следующим образом: пусть b – переданное кодовое слово, e – строка ошибок, тогда $b + e$ – принятое слово. Так как $bM = O$, то $(b+e)M = eM$. Если результат нулевой (т.е. $(b+e)M =O$), как происходит при правильной передаче, то считается, что ошибок не было. Если строка ошибок имеет единицу в i-ой позиции, то eM – это i-ая строка матрицы M, т.е. двоичное представление числа i, следовательно, ошибка произошла в i-ой позиции, поэтому символ в в i-ой позиции числа $b + e$ следует изменить.

Код называется *совершенным*, если он способен исправлять все ошибки не более, чем в k разрядах и не способен исправлять никаких ошибок более чем в k разрядах для некоторого натурального k. Код Хемминга является совершенным кодом.

Пример 1. Пусть по двоичному симметричному каналу передаётся слово длины 6 с помощью (2,3)-кода с обнаружением ошибок на основе проверки четности. Найти вероятность P того, что при приёме сообщения ошибка не будет обнаружена при условии, что ошибка произошла, если вероятность ошибочного приема одного символа равна $q = 0.1$.

Решение. При передаче сообщение длины 6 разбивается на три сообщения длины 2: $a_1a_2\mapsto b_1b_2b_3$, $a_3a_4\mapsto b_4b_5b_6$, $a_5a_6\mapsto b_7b_8b_9$, где $b_1=a_1$, $b_2=a_2$, $b_4=a_3$, $b_5=a_4$, $b_7=a_5$, $b_8=a_6$, $b_3=a_1+a_2(\mathrm{mod}\ 2)$, $b_6=a_3+a_4(\mathrm{mod}\ 2)$, $b_9=a_5+a_6(\mathrm{mod}\ 2)$. Обозначим через A событие, состоящее в том, что при передаче сообщения произошла ошибка, через B обозначим событие, состоящее в том, что при приёме не обнаружена ошибка. Тогда $P = P(B \mid A) = \dfrac{P(AB)}{P(A)}$. Очевидно, $P(A) = 1 - p^9$, где $p = 1 - q$. Допущенная ошибка не будет обнаружена лишь в том случае, когда при передаче каждой из групп символов $b_{3k+1}b_{3k+2}b_{3k+3}$, $k = 0,1,2$, число допущенных ошибок равно 0 или 2, при этом хотя бы в одном из блоков $b_{3k+1}b_{3k+2}b_{3k+3}$ произошло 2 ошибки. Вероятность ошибки в двух символах при передаче группы символов $b_{3k+1}b_{3k+2}b_{3k+3}$ равна $3pq^2$. Поэтому $P(AB)=(3pq^2+p^3)^3-p^9$. Таким образом,

$$P = \frac{(3pq^2 + p^3)^3 - p^9}{1 - p^9} = \frac{(3\cdot 0.9\cdot 0.1^2 + 0.9^3)^3 - 0.9^9}{1 - 0.9^9} \approx 0.073.$$

Пример 2. Пусть по двоичному симметричному каналу передаются слова и вероятность ошибочного приема одного символа равна $q = 0.1$. Найти вероятность P необнаруженной ошибки в одном символе при использовании *(m, 3m)*-кода с тройным повторением.

Решение. Обозначим через A событие, состоящее в том, что при передаче символа c произошла ошибка, через B обозначим событие, состоящее в том, что при приёме не обнаружена ошибка. Очевидно, $P(A) = 1 - p^3$, где $p = 1 - q$. Произошедшая ошибка не будет обнаружена, если символ c принят дважды неправильно или трижды неправильно. Поэтому $P(AB) = 3pq^2 + q^3$. Следовательно,

$$P = \frac{P(AB)}{P(A)} = \frac{3pq^2 + q^3}{1 - p^3} = \frac{3 \cdot 0.9 \cdot 0.1^2 + 0.1^3}{1 - 0.9^3} \approx 0.1.$$

Пример 3. Какие ошибки обнаруживает и какие ошибки исправляет следующий блочный (2,5)-код: a_1=00$\mapsto$00000=b_1, a_2=01$\mapsto$01011=b_2, a_3=10$\mapsto$10101=b_3, a_4=11$\mapsto$11110=b_4?

Решение. Найдем расстояния Хемминга между кодовыми словами: $d(b_1,b_2)$=3, $d(b_1,b_3)$=3, $d(b_1,b_4)$=4, $d(b_2,b_3)$=4, $d(b_2,b_4)$=3, $d(b_3,b_4)$=3. Так как расстояние Хемминга между различными кодовыми словами не меньше 3, то рассматриваемый код обнаруживает ошибки, допущенные в двух разрядах, и исправляет ошибки, допущенные в одном разряде. Итак, код обнаруживает ошибки в двух разрядах и исправляет ошибки в одном разряде.

Пример 4. Проверить, что двоичный код с матрицей

$$E = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

является групповым. Построить схему декодирования, используя в качестве лидеров смежных классов слова наименьшего веса.

Решение. Схема кодирования выглядит следующим образом:

a_0=000$\mapsto$000000=b_0, a_1=001$\mapsto$001111=b_1,

a_2=010$\mapsto$010011=b_2, a_3=011$\mapsto$011100=b_3,

a_4=100$\mapsto$100110=b_4, a_5=101$\mapsto$101001=b_5,

a_6=110$\mapsto$110101=b_6, a_7=111$\mapsto$111010=b_7.

Проверим, что множество B кодовых слов образует абелеву группу относительно побитового сложения. Так как $B = \{aE \mid a \in Z_2^3\}$, то для любых $b_i, b_j \in B$ имеем $b_i + b_j = a_iE + a_jE = (a_i + a_j)E \in B$. Очевидно, опера-

ция побитового сложения коммутативна. Нейтральным элементов множества B является слово b_0. Докажем, что для любого слова $b_i \in B$ существует слово $b_j \in B$, такое, что $b_i + b_j = b_0$. Так как множество Z_2^3 образует абелеву группу относительно побитового сложения, то для любого слова $a_i \in Z_2^3$ существует $a_j \in Z_2^3$, такое, что $a_i + a_j = a_0$. Следовательно, $b_i + b_j = a_i E + a_j E = (a_i + a_j)E = a_0 E = b_0$. Таким образом, матрица E определяет групповой код.

Построим схему декодирования, выбрав в качестве лидеров смежных классов слова из Z_2^6 наименьшего веса:

000000	**001111**	**010011**	**011100**	**100110**	**101001**	**110101**	**111010**
000001	001110	010010	011101	100111	101000	110100	111011
000010	001101	010001	011110	100100	101011	110111	111000
000100	001011	010111	011000	100010	101101	110001	111110
001000	000111	011011	010100	101110	100001	111101	110010
010000	011111	000011	001100	010110	111001	100101	011010
100000	101111	110011	111100	000110	001001	010101	011010
000101	001010	010110	011001	100011	101100	110000	111111

Так как $|Z_2^6| = 64$, $|B| = 8$, то $|Z_2^6 / B| = 8$. Следовательно, мы должны выбрать 8 лидеров смежных классов. Выберем все слова веса 0 и 1: $c_0, ..., c_6$. Выберем любое слово c_7 веса 2, которое не содержится во множестве слов $c_i + b_j$, $i = \overline{0,6}$, $j = \overline{0,7}$. Множество всех слов из Z_2^6 разбивается на смежные классы $c_i + B$, $i = \overline{0,7}$. В первом столбце таблицы указаны лидеры смежных классов c_i, $i = \overline{0,7}$, в первой строке таблицы – кодовые слова b_j, $j = \overline{0,7}$. Чтобы декодировать принятое слово $b_j + e$ следует отыскать его в таблице и выбрать в качестве переданного кодовое слово в том же столбце и первой строке. Например, если принято слово 110011, считается, что было передано слово 010011; если принято 110101, считается, что оно и было передано и т.п. Построенный код исправляет все одинарные ошибки, а также двойную ошибку 000101.

Пример 5. Для передачи двоичных слов длины 4 был использован (4,7)-код Хемминга. Известно, что при передаче слова была допущена ошибка в одном разряде. Определите, какое слово передавалось, если получено сообщение b=0011111.

Решение. Построим матрицу M из 7 строк и 3 столбцов. В i-м столбце стоят символы двоичного разложения числа i:

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

Так как bM=011 и 011 – двоичное представление числа 3, то ошибка произошла в третьем разряде. Следовательно, передавалось кодовое слово b_1=0001111. Символы с номерами 1, 2, 4 являются контрольными. Поэтому исходное слово a_1 - это слово 0111.

10.1. Составьте таблицу вероятностей приёма по двоичному симметричному каналу двухбитовых слов, если вероятность ошибочного приёма одного символа равняется q.

10.2. По двоичному симметричному каналу передаются строки длины 14, вероятность ошибочного приёма одного символа равняется q.

1) Какова вероятность того, что ровно пять символов будут приняты неправильно?

2) Какова вероятность того, что не более пяти символов будут приняты неправильно?

3) Сколько имеется строк, отличающихся от данной не более чем в пяти позициях?

10.3. Рассмотрим (4,5)-код с проверкой на четность. Какова вероятность того, что не будет обнаружена ошибка при передаче слова длины 9, если вероятность ошибочного приёма одного символа равняется q?

10.4. Рассмотрим (4,5)-код с проверкой на четность и (4,12)-код с тройным повторением. Вычислить вероятность P того, что ошибочно переданное слово длины 4 не будет обнаружено, если вероятность правильного приема одного символа равна p=0.9.

10.5. Докажите, что минимальное расстояние от данного кодового слова до остальных не зависит от выбора данного слова в групповом коде.

10.6. Докажите, что следующие преобразования кодирующей матрицы приводят к эквивалентному коду:

1) перестановка строк;

2) перестановка столбцов;

3) прибавление к одной строке другой.

10.7. Пусть E_m - единичная матрица порядка m, B - некоторая $m \times l$ – матрица. Кодирующая матрица вида $[E_m B]$ называется стандартной. Построить стандартную матрицу, порождающую код, эквивалентный коду с матрицей

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

10.8. Для предыдущего кода построить схему декодирования, используя в качестве лидеров смежных классов слова наименьшего веса. Найдите вероятность правильного декодирования, если вероятность ошибки при приёме одного символа равна q.

10.9. Рассмотрим двоичный групповой код с матрицей

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

1) Найдите стандартную матрицу, дающую эквивалентный код.

2) Постройте схему декодирования.

10.10. Для (4,7)-кода Хемминга постройте

1) кодирующую матрицу;

2) найти все кодовые слова с контрольными символами 110.

3) переданные слова, если были приняты 0111110, 0001111.

10.11. Постройте кодирующую матрицу E и проверочную матрицу H для:

1) (6,7)-кода с проверкой на четность;

2) (3,9)-кода с тройным повторением.

10.12. Покажите, что кодовые слова группового кода либо все имеют четный вес, либо половина четный, а половина – нечетный.

10.13. Покажите, что $(n,3n)$ – код, $n>1$, с тройным повторением не может быть совершенным.

10.14. Рассмотрим (3,6)-код с обнаружением ошибок, имеющий матрицу

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

Найдите вероятность того, что ошибка в передаче слова длины 6 не будет обнаружена, если вероятность ошибки при приёме одного символа равна q.

ОТВЕТЫ

1.1. 1) $2^2 \cdot 5^2 \cdot 13^2$; 2) $2^6 \cdot 3^3 \cdot 5 \cdot 7$; 3) $3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 37$; 4) $5 \cdot 397 \cdot 2113$;
5) $2 \cdot 13 \cdot 17 \cdot 37$.
1.3. 1087, 2011.
1.121) 501; 2) 333.
1.13. 1) $17 = 6 \cdot 187 - 5 \cdot 221$; 2) $17 = 121 \cdot 6188 - 159 \cdot 4709$;
3) $1 = 626 \cdot 2419 - 1252 \cdot 1189 - 15 \cdot 1711$; 4) $9 = 12 \cdot 549 - 17 \cdot 387$;
5) $6=1 \cdot 78 - 6 \cdot 60 + 12 \cdot 24$.
1.14. 1) 70151; 2) 166608; 3) 17081; 4) 23607; 5) 1560.
1.16. 13.
1.21. не существует.
1.22. $p, 2p, 8, 9$ (p - простое число).
1.23. 1.
2.1. 1) $x \equiv 103 (\mathrm{mod} 171)$; 2) $x \equiv 84 (\mathrm{mod} 119)$; 3) $x \equiv -19 (\mathrm{mod} 127)$;
4) $x \equiv 45 (\mathrm{mod} 101)$.
2.2. 1) $x = -143 + 28t, y = 26 - 5t$; 2) $x = 2 + 35t$, $y=-1-18t$;
3) $x = 48 + 9t$, $y = -36 - 7t$; 4) решений нет;
5) $x = 8 + 47t$, $y = -9 - 53t$ ($t \in Z$).
2.3. 1) $x = t - 3s$, $y = t$, $z = 1 + 4s$; 2) $x=25+30s+70r+8t$, $y=-15-18s-42r-5t$,
$z = r$, $u = s$; 3) $x = 7r - 4 + 13t$, $y = 14r - 8 + 25t$, $z=r$;
4) $x = 3 + 18r + 36s + 8t$, $y = r$, $z = -1 - 6r - 12s - 3t$, $u = s$ ($t, s, r \in Z$).
2.5. 1) $x \equiv 93 (\mathrm{mod} 140)$; 2) $x \equiv 23 (\mathrm{mod} 385)$; 3) $x \equiv 471 (\mathrm{mod} 1001)$;
4) $x \equiv 74 (\mathrm{mod} 105)$; 5) $x \equiv 7275 (\mathrm{mod} 9269)$; 6) $x \equiv 123 (\mathrm{mod} 13923)$;
7) $x \equiv 111 (\mathrm{mod} 4200)$; 8) решений нет; 9) $x \equiv 100 (\mathrm{mod} 252)$.
2.6. 1) $x = -4 - 14r + 5t$, $y = 1 + 8r - 2t$, $z=7r-t$, $u = t$;
2) $x = t$, $y = 2 - 3r - t$, $z = -1 + 5r + 2t$, $u = 1 + 4r$; 3) $x = 13t$, $y = 2t$, $z = 7t$;
4) $x = r$, $y = 2r - 8t$, $z = -3t$, $u = t$ ($t, r \in Z$).
2.7. $x=2mn$, $y=(m^2-n^2)$, $z=(m^2+n^2)$ или $x=(m^2-n^2)$, $y=mn$, $z=(m^2+n^2)$, где $m,n \in N$, $m>n$, $m,n=1$, 2 не делит $m+n$.
2.13. решений нет.
3.1. 1) 18; 2) 110; 3) 96; 4) 240; 5) 1152.
3.2. 88.
3.3. $p = 13$, $q = 11$.
3.5. 1) 5; 2) 7.
3.7. 1) 12; 2) 27; 3) 44; 4) 12.
3.8. 1) 46; 2) 7; 3) 1067; 4) 50; 5) 136.

3.9. 1) 19; 2) 215; 3) 225; 4) 118; 5) 445.
3.10. 1) 399; 2) 1811; 3) 479;, 4) 317.
3.12. $n=2^a \cdot 3^b$,если $a\in N$, $b\in N\cup\{0\}$, или $n=1$.
3.16. 1) $2k$, $k\in N$, 3 не делит k; 2) решений нет.
3.15. 3.
4.1. 1) 28; 2) 0; 3) 528; 4) 20; 5) 6.
4.2. 1) $6,7,11,12,13,15,17,19,22,24,26,28,29,30,34,35$;
2) $2,3,8,10,11,14,15,18,19,21,26,27$; 3) $3,13,17,23,27,33,37,47$;
4) $5,11,23,29,41,47$; 5) $5,7,10,11,14,15,17,19,20,21$.
4.3. 1) 10; 2) 7; 3) 5; 4) 9; 5) 11.
4.4. 1) $1,4,10,16,18,23,25,31,37,40$; 2) $1,7,16,20,23,24,25$;
3) $1,11,21,31,41$; 4) $a=1,7,13,19,25,31,37,43,49$;
5) $1,2,3,4,6,8,9,12,13,16,18$.
4.5. 1) да; 2) нет; 3) нет; 4) нет; 5) да.
4.6. 5.
4.9. $x=1,\ y=2,\ p=3$; $x=1,\ y=-2,\ p=3$; $x=-2,\ y=2,\ p=3$;
$x=-2,\ y=-2,\ p=3$.
4.11. 1.
4.12. $\delta/(\gamma,\delta)$.
4.13. $a^{\delta/(\delta,\gamma)}$.
4.14. 7, 37.
4.15. 1) $(1,7,9)$; 2) $(2,4,3)$; 3) $(6,7,4)$; 4) $(1,1,1,3,28)$; 5) $(1,4,2,6)$.
5.1. 1) $x\equiv 6(\mathrm{mod}\,20)$; 2) $x\equiv 15(\mathrm{mod}\,66)$; 3) $x\equiv 13(\mathrm{mod}\,14)$;
4) $x\equiv 13(\mathrm{mod}\,30)$; 5) решений нет.
5.2. 1) $x\equiv 9(\mathrm{mod}\,15)$; 2) $x\equiv 4(\mathrm{mod}\,5)$; x=2k, k∈N; 3) $x\equiv 42(\mathrm{mod}\,60)$;
4) $x\equiv 10(\mathrm{mod}\,138)$; 5) $x\equiv 23(\mathrm{mod}\,60)$.
5.3. 1) $x\equiv 1(\mathrm{mod}\,5)$; 2) $x\equiv \pm 1(\mathrm{mod}\,7)$; 3) $x\equiv 1(\mathrm{mod}\,19)$; 4) решений нет;
5) $x\equiv -1(\mathrm{mod}\,7)$.
5.5. 1) $x\equiv 2,18,23,39(\mathrm{mod}\,41)$; 2) $x\equiv 13(\mathrm{mod}\,50)$; 3) $x\equiv 9(\mathrm{mod}\,32)$;
4) $x\equiv 55(\mathrm{mod}\,64)$; 5) $x\equiv 101(\mathrm{mod}\,928)$.
5.6. 1) $x\equiv 22(\mathrm{mod}\,27)$; 2) $x\equiv 22,5(\mathrm{mod}\,64)$; 3) $x\equiv 22,76,122,176(\mathrm{mod}\,225)$,
4) $x\equiv 66(\mathrm{mod}\,343)$; 5) $x\equiv 9(\mathrm{mod}\,900)$.
5.7. 1) $x=3$, $y=1$; $x=5$,$y=3$; 2) $x=2$, $y=2$, $z=2$; 3) $x=2$, $y=1$, $z=2$.
5.8. 2^{k-1} при $\mathrm{ord}_2 m=1$; 2^k при $\mathrm{ord}_2 m=0,2,3$; 2^{k+1} при $\mathrm{ord}_2 m=4$;
2^{k+2} при $\mathrm{ord}_2 m\geq 5$, где k - число простых делителей числа m.
5.10. $1,2,3,4,6,8,9,12,13,16,18$.

5.11. 1), 3) разрешимы; 2),4),5) нет решений.

6.1. 1) ни одно из множеств не образует группу; 2) группы: $(Z,+)$, $(Q,+)$, $(R,+)$, $(C,+)$; 3) не группа; 4) группы: $(Q\setminus\{0\},\cdot)$, $(R\setminus\{0\},\cdot)$, $(C\setminus\{0\},\cdot)$; 5) группы: $(Q_+,\cdot)$, $(R_+,\cdot)$; 6) группа для любого $n\in N$; 7) группа; 8) группа; 9) группа; 10) группа; 11) группа при $r=1$; 12) группа; 13) не группа; 14) группа для любого $n\in N$; 15) группы; 16) группа для любых $m,n\in N$; 17) группа при $m=n$; 18) группа для любого $m\in N$; 19) группа; 20) группа при $\lambda<0$.

6.2. 1) не являются; 2) являются; 3) не являются; 4) являются; 5) являются; 6) являются.

6.3. Z_2, Z_3.

6.4. Z_4, $Z_2\times Z_2$.

6.5. 1) $\{r+5Z\mid r=\overline{0,4}\}$; 2) $\{(1),(1,2)\}$, $\{(1,3),(1,2,3)\}$, $\{(2,3),(1,3,2)\}$; 3) $\{\{A_rS\mid S\in SL(n,R)\}\mid r\in R, r\neq 0\}$, где $\det A_r=r$, $r\in R\setminus\{0\}$.

6.6. 1) $H_1=\{(1)\}$, $H_2=\{(1),(1,2)\}$, $H_3=\{(1),(1,3)\}$, $H_4=\{(1),(2,3)\}$, $H_5=\{(1),(1,2,3),(1,3,2)\}$, $H_6=G$, H_1, H_5, H_6 –нормальные делители;
2) $H_1=\{e\}$, $H_2=\{e,a^6\}$, $H_3=\{e,a^4,a^8\}$, $H_4=\{e,a^3,a^6,a^9\}$, $H_5=\{e,a^2,a^4,a^6,a^8,a^{10}\}$, $H_6=G$, где $<a>=G$; 3) mZ, где $m\in N$. Все подгруппы нормальные.

6.11. 1) 2; 2) 6; 3) 20.

6.12. 1) 6; 2) 4; 3) 4; 4) 2.

6.13. 1) f; 2) e; 3) f.

6.14. $(1,2,3)\circ(4,7)\circ(5)\circ(6)$.

6.15. $(1)\circ(2,3,4)$.

6.19. $\varphi_1(x)\equiv 0$, $\varphi_2(x)=3x$, $x\in Z_4$; $\mathrm{Ker}(\varphi_1)=Z_4$, $\mathrm{Im}(\varphi_1)=6Z_6$, $\mathrm{Ker}(\varphi_2)=2Z_4$, $\mathrm{Im}(\varphi_2)=3Z_6$.

6.20. 1) 3; 2) 3; 3) 12.

6.21. 1) ±1; 2) $G(Z_n)$.

7.1. 1) кольца: Z,Q,R,C; 2) кольцо; 3) кольцо для любого $n\in N$; 4) кольцо; 5) кольцо; 6) не кольцо; 7) кольцо; 8) кольцо; 9) кольцо; 10) не кольцо; 11) кольцо.

7.2. 1) Z_7, $7Z_7$; 2) $Z_{10},2Z_{10},5Z_{10},10Z_{10}$;
3) $Z_{12},2Z_{12},3Z_{12},4Z_{12},6Z_{12},12Z_{12}$;
4) Z_{2010}, $2Z_{2010}$, 3 Z_{2010}, 5 Z_{2010}, 6 Z_{2010}, 10 Z_{2010}, 15 Z_{2010}, 30 Z_{2010}, 67 Z_{2010}, 134 Z_{2010}, 201 Z_{2010}, 335 Z_{2010}, 402 Z_{2010}, 670 Z_{2010}, 1005 Z_{2010}, 2010 Z_{2010}.

7.3. 1) R; 2) Q; 3) $3Z$; 4) $(x^{(m,n)}-1)R[x]$.

7.4. 1) вещественные верхние треугольные матрицы с ненулевыми элементы на диагонали; 2) $G(Z_{100})$; 3) $\{1,-1,i,-i\}$.

7.5. 1) 8; 2) 6; 3) 2012^4.

7.7. $2Z$.

7.9. 1) $\{(x^2+1)Z_2[x],\ 1+(x^2+1)\,Z_2[x],\ x+(x^2+1)\,Z_2[x],\ x+1+(x^2+1)\,Z_2[x]\}$;
2) $\{I,1+I,2+I,x+I,x+1+I,x+2+I,2x+I,2x+1+I,2x+2+I\}$, где
$I=(x^2+x+2)Z_3[x]$; 3) $\{5Z,1+5Z,2+5Z,3+5Z,4+5Z\}$;
4) $\{(2^{(m,n,k)}-1)Z,1+(2^{(m,n,k)}-1)Z,...,2^{(m,n,k)}-2+(2^{(m,n,k)}-1)Z\}$.

7.11. нет.

7.12. два гомоморфизма: $\varphi_1(x)=0$, $\varphi_2(x)=x$.

7.13. $\mathrm{Ker}(f)=\left\{\begin{pmatrix} a & -a \\ a & -a \end{pmatrix}\middle| a\in R\right\}$, $\mathrm{Im}(f)=R$, $K/\mathrm{Ker}(f)$ состоит из смежных классов $M_\alpha=\left\{\begin{pmatrix} c & \alpha-c \\ c & \alpha-c \end{pmatrix}\middle| c\in R\right\}$, $\alpha\in R$.

7.14. 1) не образуют; 2) не образуют; 3) образуют в случае $n=p^\alpha$, где p - простое, $\alpha\in N$.

8.1. Q,R,C.

8.4. существует.

8.6. 1) x^2-2; 2) x^3-5; 3) $x^2-4x+13$; 4) $x-2+3i$; 5) x^4-10x^2+1.

8.8. 1) 4; 2) 2; 3) 1.

8.11. нельзя.

8.12. x^2+x+1.

8.13. $k=1,2,4$

8.14. 1) 1; 2) 1; 3) x^2+2.

8.15. $\varphi(ax+b+(x^2+1)Z_{11}[x])=a(x+6)+b+((x+6)^2+1)Z_{11}[x]$.

8.16. 1) $\frac{4}{17}x^2-\frac{2}{17}x+\frac{1}{17}$; 2) $6x^2+4x+5$.

8.17. 1) нет решений; 2) $f(x)\equiv x(\mathrm{mod}\,x^2+x+1)$.

8.18. 1) $F=\{a+b\sqrt{3}+(c+d\sqrt{3})i\mid a,b,c,d\in Q\}$, $[F:P]=4$;
2) $F=\{a+b\sqrt{3}\mid a,b\in Q\}$, $[F:P]=2$; 3) $F=\{a+b\sqrt{7}\mid a,b\in Q\}$,
$[F:P]=2$; 4) $F=Z_2[x]/(x^2+x+1)$, $[F:P]=2$;
5) $F=\{a+bi\sqrt{3}\mid a,b\in Q\}$, $[F:P]=2$; 6) $F=Z_7$, $[F:P]=1$.

8.20. 1) $f_1f_i=f_1$, $i=\overline{1,4}$, $f_2f_i=f_i$, $i=\overline{2,4}$, $f_3f_3=f_4$, $f_3f_4=f_2$,

$f_4 f_4 = f_3$, где $f_1 = \overline{0}$, $f_2 = \overline{1}$, $f_3 = \overline{x}$, $f_4 = \overline{x+1}$; 2) $f_1 f_i = f_1$, $i = \overline{1,8}$, $f_2 f_i = f_i$, $i = \overline{2,8}$, $f_3 f_3 = f_5$, $f_3 f_4 = f_7$, $f_3 f_5 = f_4$, $f_3 f_6 = f_2$, $f_3 f_7 = f_8$, $f_3 f_8 = f_6$, $f_4 f_4 = f_6$, $f_4 f_5 = f_8$, $f_4 f_6 = f_5$, $f_4 f_7 = f_2$, $f_4 f_8 = f_3$, $f_5 f_5 = f_7$, $f_5 f_6 = f_3$, $f_5 f_7 = f_6$, $f_5 f_8 = f_2$, $f_6 f_6 = f_8$, $f_6 f_7 = f_4$, $f_6 f_8 = f_7$, $f_7 f_7 = f_3$,

8.22. 1) $x^9 + x + 1$; 2) $(x^2+1)(x^2-x-1)(x^3-x^2+1)$.

$f_7 f_8 = f_5$, $f_8 f_8 = f_4$, где $f_1 = \overline{0}$, $f_2 = \overline{1}$, $f_3 = \overline{x}$, $f_4 = \overline{x+1}$, $f_5 = \overline{x^2}$, $f_6 = \overline{x^2+1}$, $f_7 = \overline{x^2+x}$, $f_8 = \overline{x^2+x+1}$; 3) $f_1 f_i = f_1$, $i = \overline{1,8}$, $f_2 f_i = f_i$, $i = \overline{2,8}$, $f_3 f_3 = f_5$, $f_3 f_4 = f_7$, $f_3 f_5 = f_6$, $f_3 f_6 = f_8$, $f_3 f_7 = f_2$, $f_3 f_8 = f_4$, $f_4 f_4 = f_6$, $f_4 f_5 = f_2$, $f_4 f_6 = f_3$, $f_4 f_7 = f_8$, $f_4 f_8 = f_5$, $f_5 f_5 = f_8$, $f_5 f_6 = f_4$, $f_5 f_7 = f_3$, $f_5 f_8 = f_7$, $f_6 f_6 = f_7$, $f_6 f_7 = f_5$, $f_6 f_8 = f_2$, $f_7 f_7 = f_4$, $f_7 f_8 = f_6$, $f_8 f_8 = f_3$, где $f_1 = \overline{0}$, $f_2 = \overline{1}$, $f_3 = \overline{x}$, $f_4 = \overline{x+1}$, $f_5 = \overline{x^2}$, $f_6 = \overline{x^2+1}$, $f_7 = \overline{x^2+x}$, $f_8 = \overline{x^2+x+1}$.

9.1. 1) CJUOFBC, PKMFOB; 2) HKLBMOH, UDPMBO.

9.2. 1) $x \to 9x + 8 (\mathrm{mod}\, 26)$; 2)

9.5. $f_2^{-1} \circ f_1^{-1}$.

9.6. $a_1 b_2 + b_1 \equiv a_2 b_1 + b_2 (\mathrm{mod}\, m)$.

9.7. ALGEBRA $\to$ ALSFBDA; NUMBER $\to$ TOMBFD; 17,26,12,12,9$\to$ $\to$ IFMMP.

9.9. 49; 193.

9.16. $17t$, $17t \pm 1$, $17t \pm 4$, $t \in Z$.

9.22. 30.

9.24. $c = 1000$.

10.2. 1) $C_{14}^5 q^5 (1-q)^9$; 2) $\sum_{i=0}^{5} C_{14}^i q^i (1-q)^{14-i}$; 3) $\sum_{i=1}^{5} C_{14}^i$.

10.3. $(p^5 + 10p^3q^2 + 5pq^4)^2 (p^2 + q^2)$, где $p = 1 - q$.

10.4. 1) $P \approx 0.179$; 2) $P \approx 156$.

10.7 $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$.

10.8. $p^6 + 6p^5 q + p^4 q^2$.

10.9. $\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$.

10.10. 1) $\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$; 2) $0110, 1000$; 3) $1100, 0111$.

10.11. 1) $E = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$, $H = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$;

2) $E = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$, $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$.

10.14. $4p^3q^3 + 3p^2q^4$, где $p = 1 - q$.

ЛИТЕРАТУРА

1. *Айерленд, К.* Классическое введение в современную теорию чисел / К. Айерленд, М. Роузен. — М., 1987.
2. *Арнольд, И. В,* Теория чисел / И. В. Арнольд. — М., 1939.
3. *Беняш-Кривец В.В.* Лекции по алгебре. Группы, кольца, поля / В.В. Беняш-Кривец, О.В. Мельников. — Минск, 2009.
4. *Биркгоф, Г.* Современная прикладная алгебра / Г. Биркгоф, Т. Барти. — М., 1976.
5. *Боревич, З. И.* Теория чисел / З. И. Боревич, И. Р. Шафаревич. — М., 1964.
6. *Виноградов, И. М.* Теория чисел / И. М. Виноградов. — М., 1981.
7. *Гашков, С. Б.* Арифметика. Алгоритмы. Сложность вычислений / С. Б. Гашков, В. Н. Чубариков. — М., 2000.
8. *Конюх, В. С.* Задачи по курсу «Прикладная алгебра» для студентов специальности 2204 / В. С. Конюх, Г. В. Матвеев, В. М. Ширяев. — Минск, 1993.
9. *Лидл, Л.* Конечные поля / Л. Лидл, Г. Нидеррайтер. — М., 1988.
10. Харин Ю.С. Математические и компьютерные основы криптологии / Ю. С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Агиевич. — Минск, 2003.
11. *Нечаев, В. И.* Элементы криптографии (Основы защиты информации) / В. И. Нечаев. — М., 1999.
12. *Размыслович, Г, П.* Геометрия и алгебра / Г. П. Размыслович, М. М. Феденя, В. М. Ширяев. — Минск, 1987.
13. *Размыслович, Г, П.* Сборник задач по геометрии и алгебре / Г. П. Размыслович, М. М. Феденя, В. М. Ширяев. — Минск, 1999.
14. *Сачков, В. Н.* Введение в комбинаторные методы дискретной математики / В. Н. Сачков. — М., 1982.
15. *Серпинский В.* 250 задач по элементарной теории чисел. / В.Серпинский. – М., 1968.
16. *Ширяев В.*М. Прикладная алгебра. Теория чисел. Сборник задач / В.М.Ширяев. — Минск, 2009.
17. *Шнеперман, Л. Б.* Сборник задач по теории чисел / Л. Б. Шнеперман. — Минск, 1982.

ОГЛАВЛЕНИЕ

Учебное издание

Базылев Дмитрий Федорович
Васьковский Максим Михайлович
Матвеев Геннадий Васильевич и др.

Сборник задач по прикладной алгебре

Для студентов
факультета прикладной математики и информатики

В авторской редакции

Ответственный за выпуск *Г. П. Размыслович*

Подписано к печати 09.11.2011. Формат 60×84/16. Бумага офсетная.
Гарнитура Таймс. Усл. печ. л. 3,95 уч.-изд. л. 3,42
Тираж 50 экз. Зак.

Белорусский государственный университет.
ЛИ №02330/0494425 от 08.04.2009.
Пр. Независимости, 4. 220030, Минск.

Отпечатано с оригинала-макета заказчика
на копировально-множительной технике
факультета прикладной математики информатики
Белорусского государственного университета.
Пр.Независимости, 4. 22030, Минск.