МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН

САМАРКАНДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ АЛИШЕРА НАВОИ

КАФЕДРА АЛГЕБРЫ И ГЕОМЕТРИИ

С Р А В Н Е Н И Я В К О Л Ь Ц Е Ц Е Л Ы Х Ч И С Е Л

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

САМАРКАНД - 2014

СРАВНЕНИЯ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ

Ключевые слова и выражения: *сравнимые числа; теорема о смысле сравнения; класс чисел; вычет по данному модулю; полная система вычетов по данному модулю, приведенная система вычетов по данному модулю, теорема Эйлера, теорема Ферма; аддитивная группа классов вычетов по данному модулю; кольцо классов вычетов по данному модулю; классов вычетов взаимно простых с модулем; мультипликативная группа простых с модулем; абсолютно псевдопростое число; сравнение n-й степени с одним неизвестным; решение сравнения; равносильные сравнения; сравнение первой степени; система сравнений первой степени с одним и тем же неизвестным; решения системы сравнений с одним и тем же неизвестным.*

§1. Понятие сравнения и свойства сравнений

Два целых числа a и b, дающие при делении на целое положительное число m один и тот же остаток

$$a = mq_1 + r \qquad \text{и} \qquad b = mq_2 + r,$$

называются *равноостаточными* или *сравнимыми* между собой по модулю m, что записывается как:

$$a \equiv b \ (mod\ m)$$

и читается: "a сравнимо с b по модулю m".

Если $a \equiv b \ (mod\ m)$, то разность $a - b$ делится на m, и наоборот, если разность между двумя числами a и b делится на m, то $a \equiv b \ (mod\ m)$ (*теорема о смысле сравнения*).

Всякое целое число сравнимо со своим остатком по любому модулю m, т.е. если $a = mq + r$, то $a \equiv r \ (mod\ m)$.

В частности, если $r = 0$, то $a \equiv 0 \ (mod\ m)$; это сравнение показывает, что $m \mid a$ и, наоборот, если $m \mid a$, то пишут $a \equiv 0 \ (mod\ m)$.

Основные свойства сравнений (аналогичные свойствам равенств)

1. Если $a \equiv c \ (mod\ m)$ и $b \equiv c \ (mod\ m)$, то $a \equiv b \ (mod\ m)$.
2. Если $a \equiv b \ (mod\ m)$ и $c \equiv d \ (mod\ m)$, то $a \pm c \equiv b \pm d \ (mod\ m)$.
3. Если $a + b \equiv c \ (mod\ m)$, то $a \equiv c - b \ (mod\ m)$.
4. Если $a \equiv b \ (mod\ m)$, то $a \pm mk \equiv b \ (mod\ m)$, или $a \equiv b \pm mk \ (mod\ m)$.
5. Если $a \equiv b \ (mod\ m)$ и $c \equiv d \ (mod\ m)$, то $ac \equiv bd \ (mod\ m)$.

6. Если $a \equiv b \ (mod\ m)$, то $a^n \equiv b^n \ (mod\ m)$ $(n \in \mathbf{N})$.
7. Если $a \equiv b \ (mod\ m)$, то $ak \equiv bk \ (mod\ m)$.
8. Если $ak \equiv bk \ (mod\ m)$ и $(k,m) = 1$, то $a \equiv b \ (mod\ m)$.
9. Если $f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_n$ $(a_i \in \mathbf{Z})$ и если $x \equiv x_1 \ (mod\ m)$, то $f(x) \equiv f(x_1) \ (mod\ m)$.

Особые свойства сравнений

1. Если $a \equiv b \ (mod\ m)$, то $ak \equiv bk \ (mod\ mk)$ $(m \in \mathbf{N})$.
2. Если $a \equiv b \ (mod\ m)$ и $a = a_1 d$, $b = b_1 d$, $m = m_1 d$, то $a_1 \equiv b_1 \ (mod\ m_1)$.
3. Если $a \equiv b \ (mod\ m)$, $a \equiv b \ (mod\ m)$, ..., $a \equiv b \ (mod\ m)$, то $a \equiv b \ (mod\ M)$, где $M = [m_1, m_2, ..., m_k]$.
4. Если сравнение имеет место по модулю m, то оно имеет место и по модулю d равному любому натуральному делителю числа m.
5. Если одна часть сравнения и модуль делятся на какое-либо число, то и другая часть сравнения делится на это число.

П р и м е р 1. Записать в виде сравнений условия:

a) числа 219 и 128 дают одинаковые остатки при делении на 7;

b) число (-352) при делении на 31 дает остаток, равный 20;

c) число 487-7 делится на 12; d) 20 – остаток от деления числа 389 на 41;

e) число N четно; f) число N нечетно; g) число N имеет вид $4k + 1$;

h) число N имеет вид $10k + 3$; i) число N имеет вид $8k – 3$.

Решение. По теореме о смысле сравнения имеем:

a) $219 \equiv 128 \ (mod\ 7)$; b) $–352 \equiv 20 \ (mod\ 31)$; c) $487 \equiv 7 \ (mod\ 12)$; d) $389 \equiv 20 \ (mod\ 41)$;

e) $N \equiv 0 \ (mod\ 2)$; f) $N \equiv 1$ или $-1 \ (mod\ 2)$; g) $N \equiv 1 \ (mod\ 4)$; h) $N \equiv 3 \ (mod\ 10)$;

i) $N \equiv -3 \ (mod\ 8) \equiv 5 \ (mod\ 8)$. ■

П р и м е р 2. Найти значения m, удовлетворяющие условию:

$$20 \equiv 8 \ (mod\ m).$$

Решение. Значения m (по теореме о смысле сравнения) равны делителям числа $20 – 8 = 12$, т.е. 1; 2; 3; 4; 6; 12. ■

П р и м е р 3. Доказать, что $2^{5n} – 1$ делится на 31 $(n \in \mathbf{N})$.

Решение. Так как $2^5 – 1 = 31$ делится на 31, то $2^5 \equiv 1 \ (mod\ 31)$. Возводя (по шестому основному свойству) обе части этого сравнения в степень n, получим $2^{5n} \equiv 1 \ (mod\ 31)$, а это означает, что $31 \mid (2^{5n} – 1)$. ■

П р и м е р 4. Найти две последние цифры числа 2^{100}.

Решение. Две последние цифры составляют число, которое является остатком от деления числа 2^{100} на 100. Надо найти x, который удовлетворял бы сравнению:

$$2^{100} \equiv x \ (mod\ 100).$$

Будем постепенно выделять слагаемые, кратные 100:

$$2^{100} = (2^{10})^{10} = (1024)^{10}; (1024)^{10} \equiv (24)^{10} \ (mod\ 100).$$

$(24)^{10} = (576)^5 \equiv 76^5 \equiv (76)^4 \cdot 76 = (5776)^2 \cdot 76 \equiv (76)^2 \cdot 76 = 5776 \cdot 76 \equiv 76^2 \equiv 5776 \equiv 76 \ (mod\ 100)$.

Таким образом, число 2^{100} имеет в качестве двух последних цифр 7 и 6. ■

П р и м е р 5. Доказать, что $C_{p-1}^k \equiv (-1)^k \ (mod\ p)$, где p – простое число.

Решение. Известна следующая формула:
$C_{p-1}^{k} + C_{p-1}^{k-1} = C_{p}^{k}$ для любых p и k, число C_{p}^{k} - целое, делящееся на p, т.к. $k < p$, а p – простое, поэтому оно не может сократиться ни с одним множителем знаменателя. Итак, $C_{p}^{k} \equiv 0 \ (mod\ p)$. Тогда $C_{p-1}^{k} \equiv (-1)\ C_{p-1}^{k-1} \ (mod\ p)$.

Применяя это рекуррентное соотношение далее, будем постепенно уменьшать верхний показатель до 1:

$$C_{p-1}^{k} \equiv (-1)\ C_{p-1}^{k-1} \equiv (-1)^2\ C_{p-1}^{k-2} \equiv (-1)^3\ C_{p-1}^{k-3} \equiv \ldots \equiv (-1)^{k-1}(p-1) \equiv (-1)^k \ (mod\ p).$$ ■

П р и м е р 6. Доказать, что

$$(a + b)^p \equiv a^p + b^p \ (mod\ p),$$

где a и b – любые целые числа, p – простое число.

Решение. По формуле разложения бинома имеет:

$$(a + b)^p = a^p + C_p^1 a^{p-1}b + C_p^2 a^{p-2}b^2 + \ldots + C_p^{p-1} ab^{p-1} + b^p.$$

Слагаемые, начиная со второго до предпоследнего включительно делятся на p, так как

$$C_p^k = \frac{p(p-1)\ldots(p-(k-1)}{1 \cdot 2 \cdot \ldots \cdot k}, \text{ где } k < p.$$

Следовательно, $C_p^i \equiv 0 (mod\ p)$, где $i = 1, 2, \ldots, (p\text{-}1)$.

Отсюда получим, что $(a + b)^p \equiv a^p + b^p \ (mod\ p)$. ■

У П Р А Ж Н Е Н И Я

1. По какому модулю все целые числа сравнимы между собой.

2. Какие из следующих сравнений являются верными:

a) $1 \equiv -5$ (*mod* 6); b) $546 \equiv 0$ (*mod* 13); c) $1956 \equiv 5$ (*mod* 12);

d) $2^3 \equiv 1$ (*mod* 4); e) $3m \equiv -1$ (*mod* m)?

3*. Доказать, что каждое целое число сравнимо со своим остатком по данному модулю.

4. Найти все значения x удовлетворяющие сравнениям:

a) $x \equiv 0$ (*mod* 3); b) $x \equiv 1$ (*mod* 2).

5. Найти значения m, удовлетворяющие условию:

$$3p + 1 \equiv p + 1 \ (mod\ m).$$

6. Указать возможные значения модуля в сравнении $x \equiv 5$ (*mod* m), если известно, что этому сравнению удовлетворяет $x = 13$.

7*. Показать, что если n – нечетное число, то $n^2\text{-}1 \equiv 0$ (*mod* 8).

8*. Показать, что если $100a + 10b + c \equiv 0$ (*mod* 21), то $a - 2b + 4c \equiv 0$ (*mod* 21).

9. Доказать, что если $3^n \equiv -1$ (*mod* 10), то $3^{n+4} \equiv -1$ (*mod* 10), $n \in \mathbf{N}$.

10*. Показать, что $2^{11 \cdot 31} \equiv 2$ (*mod* $11 \cdot 31$).

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

12. С каким наименьшим по абсолютной величине числом сравнимо число $N = 11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19$ по модулю 7?

13. Проверить, что $3^{14} \equiv -1$ (*mod* 29).

14. Найти остаток от деления $1532^5 - 1$ на 9.

15*. Доказать, что если $a \equiv b \ (mod\ p^n)$, то $a^p \equiv b^p \ (mod\ p^{n+1})$.

16. Доказать, что если $ax \equiv bx \ (mod\ m)$, то $a \equiv b\left(mod \frac{m}{(x,,m)}\right)$.

17*. Если $\overline{a_4a_3a_2a_1a_0} \equiv 0\ (mod\ 33)$, то доказать, что $a_4 + \overline{a_3a_2} + \overline{a_1a_0} \equiv 0\ (mod\ 33)$. При $a_{i+1} = 0$ считать $a_{i+1}\overline{a_i} = a_i$.

18*. Найти две последние цифры чисел: а) 9^{9^9}; b) $7^{7^{\cdot^{\cdot^{\cdot^7}}}}$.

19*. Доказать, что $p^{p+2} + (p+2)^p \equiv 0\ (mod\ 2p+2)$, где $p > 2$.

20*. Доказать, что числа

$$-\frac{p-1}{2}, -\frac{p-3}{2}, ..., -1, 0, 1, ..., \frac{p-3}{2}, \frac{p-1}{2}$$

попарно несравнимы по модулю p > 2.

21*. Доказать, что $2^{3^n} \equiv -1\ (mod\ 3^{n+1})$, $n \in \boldsymbol{N}$

22*. Доказать, что числа вида $N = 3^{2^{4n+1}} + 2$ и вида $M = 2^{3^{4n+1}} + 3$ ($n \in \boldsymbol{N}$) являются составными.

23*. Доказать, что если даны два сравнения

$$\left.\begin{aligned} ac &\equiv bd \\ a &\equiv b \end{aligned}\right\} (mod\ m)$$

и $(a, m) = 1$, то можно почтенно первое сравнение разделить на второе и написать $c \equiv d\ (mod\ m)$.

24. Известно, что $a^{100} \equiv 2\ (mod\ 73)$ и $a^{101} \equiv 69\ (mod\ 73)$. Найти остаток от деления числа a на 73.

25*. Дано, что выражение $\frac{11a+2b}{19} \in \boldsymbol{Z}$. Доказать, что $\frac{18a+5b}{19} \in \boldsymbol{Z}$.

26. Доказать, что уравнения $2^x + 7^y = 19^z$ и $2^x + 5^y = 19^z$ не имеют решения в натуральных числах.

27. Доказать, что при $p > 2$ (p – простое число)

$$1^{2k+1} + 2^{2k+1} + 3^{2k+1} + ... + (p-1)^{2k+1} \equiv 0\ (mod\ p).$$

§2. Классы вычетов. Теоремы Эйлера и Ферма

Совокупность целых чисел, дающих при делении на натуральное число m (модуль) один и тот же остаток r, образует *класс чисел* по этому модулю m. Все числа данного класса в общем виде записываются так: $mk+r$, где $k \in \boldsymbol{Z}$. Число всех классов равно m.

Любое число класса называется *вычетом* по данному модулю m (по отношению ко всем числам того же класса).

Совокупность любых чисел, взятых из каждого класса по одному, называется *полной системой вычетов* по данному модулю m.

Обычно в качестве полной системы вычетов употребляется полная система наименьших неотрицательных вычетов по данному модулю m, т.е. совокупность чисел: 0, 1, 2,..., m-1.

Иногда употребляется и *полная система наименьших по абсолютной величине неположительных вычетов* по данному модулю m, т.е. числа: -(m-1), -(m-2),..., -2, -1, 0. Часто употребляется также *полная система абсолютно наименьших*

вычетов по модулю m. Например, для $m = 7$ этой системой будут числа: -3, -2, -1, 0, 1, 2, 3; для $m = 8$ – числа: -3, -2, -1, 0, 1, 2, 3, 4 или –4, -3, -2, -1, 0, 1, 2, 3.

Совокупность чисел, взятых из полной системы вычетов и взаимно простых с модулем m, называется *приведенной системой вычетов* по модулю m. Число чисел, составляющих приведенную систему вычетов, равно $\varphi(m)$.

Используются те же три вида приведенной системы вычетов, что и полной системы: *приведенная система наименьших положительных вычетов, приведенная система наименьших по абсолютной величине отрицательных вычетов и приведенная система абсолютно наименьших вычетов.*

Совокупность целых чисел $x_1, x_2,..., x_s$ тогда и только тогда является полной системой вычетов по модулю m, когда $s = m$ и $x_i \equiv x_j \pmod m$ при $i \neq j$. Чтобы значения линейной формы $ax + b$, где $(a, m) = 1$, пробегали полную систему вычетов по модулю m, необходимо и достаточно, чтобы соответствующие значения x пробегали полную систему вычетов по модулю m.

Совокупность чисел $x_1, x_2,..., x_s$ тогда и только тогда является приведенной системой вычетов по модулю m, когда $s = \varphi(m)$, $x_i \equiv x_j \pmod m$ при $i \neq j$ и $(x_i, m) = 1$. Чтобы значения формы ax, где $(a, m) = 1$, пробегали приведенную систему вычетов по модулю m, необходимо и достаточно, чтобы соответствующие значения x пробегали приведенную систему вычетов по модулю m.

При $m > 1$ и $(a, m) = 1$ имеет место сравнение:

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

где $\varphi(m)$ – функция Эйлера (*теорема Эйлера*).

При p простом и $(a, p) = 1$ имеет место сравнение:

$$a^{p-1)} \equiv 1 \pmod p \text{ (теорема Ферма)}.$$

Класс вычетов по модулю m, содержащий целое число a, обозначим через $a \bmod m$. Следовательно,

$$a \bmod m = a + m\boldsymbol{Z} = \{a + km \mid k \in \boldsymbol{Z}\}.$$

Обозначим через $\boldsymbol{Z}/m\boldsymbol{Z}$ множество всех классов вычетов по модулю m:

$$\boldsymbol{Z}/m\boldsymbol{Z} = \{0 \bmod m,\ 1 \bmod m,..., (m\text{-}1) \bmod m\}.$$

На этом множестве введем операции сложения и умножения следующими равенствами:

$$a \bmod m + b \bmod m = (a + b) \bmod m,$$

$$(a \bmod m) \cdot (b \bmod m) = ab \bmod m.$$

(Сравнить с задачей 12, §1, гл. V, задачей 112, §4, гл. V).

$(\boldsymbol{Z}/m\boldsymbol{Z}, +)$ – абелева группа, причем она является фактор группой группы $\boldsymbol{Z}$ по подгруппе $m\boldsymbol{Z}$ и называется *аддитивной группой классов вычетов по модулю m.*

$(Z/mZ, +, \cdot)$ – является коммутативным кольцом с единицей и называется *кольцом классов вычетов по модулю m.*

Если $(a, m) = 1$, класс $a \bmod m$ называется *классом вычетов, взаимно простых с модулем m.*

Множество классов вычетов по модулю m, взаимно простых с m, образует относительно умножения абелеву группу, которая называется *мультипликативной группой классов вычетов, взаимно простых с модулем.*

Вычет a называется *обратным* вычету b по модулю m, если $ab \equiv 1 \pmod m$. Вычеты a и b называются также взаимно обратными по модулю m.

П р и м е р 1. Написать все три вида полной системы вычетов по модулю 10.

Решение. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 – полная система наименьших неотрицательных вычетов по модулю 10.

-9, -8, -7, -6, -5, -4, -3, -2, -1, 0 – полная система наименьших по абсолютной величине неположительных вычетов по модулю 10.

-4, -3, -2, -1, 0, 1, 2, 3, 4, 5 или –5, -4, -3, -2, -1, 0, 1, 2, 3, 4 – полные системы абсолютно наименьших вычетов по модулю 10. ■

П р и м е р 2. Написать все три вида приведенной системы вычетов по модулю 10.

Решение. 1, 3, 7, 9 – приведенная система наименьших неотрицательных вычетов по модулю 10.

-9, -7, -3, -1 – приведенная система наименьших по абсолютной величине неположительных вычетов по модулю 10.

-3, -1, 1, 3 приведенная система абсолютно наименьших вычетов по модулю 10. ■

П р и м е р 3. По какому модулю числа 20, -4, 22, 18, -1 составляют полную систему вычетов?

Решение. Так как по модулю 5 данные числа сравнимы соответственно с 0, 1, 2, 3, 4, то искомый модуль равен 5. ■

П р и м е р 4. Доказать, что система чисел 3^1, 3^2, 3^3, 3^4, 3^5, 3^6 составляет приведенную систему вычетов по модулю 7.

Решение. Составим наименьшие положительные вычеты указанных чисел:

3, 2, 6, 4, 5, 1, так как $3^2 \equiv 2$ (*mod* 7), $3^3 \equiv 6$ (*mod* 7), $3^4 \equiv 4$ (*mod*7), $3^5 \equiv 5$ (*mod* 7), $3^6 \equiv 1$ (*mod* 7). ■

П р и м е р 5. Найти остаток от деления 383^{175} на 45.

Решение. Так как $383 \equiv 23$ (*mod* 45), то $383^{175} \equiv 23^{175}$ (*mod* 45). Далее, так как $\varphi(45) = 24$ и (23, 45) = 1, то по теореме Эйлера:

$23^{24} \equiv 1$ (*mod* 45). Следовательно,

$23^{175} = 23^{24\bullet 7 + 7} = (23^{24})^7 \cdot 23^7 \equiv 1^7 \cdot 23^7$ (*mod* 45).

Но $23^7 = (23^2)^3 \cdot 23 \equiv 34^3 \cdot 23 = 34^2 \cdot 34 \cdot 23 \equiv 1156 \cdot 782 \equiv 31 \cdot 17 = 527 \equiv 32$ (*mod* 45).

Таким образом, $383^{175} \equiv 32$ (*mod* 45). Искомый остаток равен 32. ■

П р и м е р 6. Доказать, что при любом целом значении x : $x^7 \equiv x$ (*mod* 42).

Решение. Имеем $x^7 \equiv x$ (*mod* 7). Остается доказать, что $x^7 \equiv x$ (*mod* 2 и 3), для чего можно испытать полную систему остатков по модулям 2 и 3, т.е. 0, 1, 2.

П р и м е р 7. Найти остаток от деления сотой степени целого числа на 125.

Решение. Если (a, 5) = 1, то по теореме Эйлера:

$a^{\varphi(125)} = a^{100} \equiv 1$ (*mod* 125).

Если же (a, 5) = 5, то $a^{100} \equiv 0$ (*mod* 125).

Следовательно, если (a, 5) = 1, то искомый остаток равен 1. Если же (a, 5) = 5, то a^{125} делится на 125. ■

П р и м е р 8. Найти остаток от деления $2^{\varphi(m)-1}$ на нечетное число m.

Решение. Пусть $2^{\varphi(m)-1} \equiv r$ *(mod m)*, где $0 \le r < m$. Тогда $2^{\varphi(m)} \equiv 2r \equiv 1$ *(mod m)* или $r = \frac{1+mq}{2}$, где $q \in \boldsymbol{Z}$. Условию $0 \le r < m$ удовлетворяет единственное значение $\frac{1+mq}{2}$ при $q = 1$, откуда $r = \frac{1+m}{2}$. ■

П р и м е р 9. Проверить, что для составного числа 341 имеет место сравнение $2^{341} \equiv 2 \ (mod\ 341)$.

Решение. Число 341 – составное, 341 = 11· 31. Легко проверить, что $2^5 \equiv 1 \ (mod\ 31)$ и $2^{10} \equiv 1 \ (mod\ 31)$.

По теореме Ферма $2^{10} \equiv 1 \ (mod\ 11)$. Так как 11 и 13 взаимно просты, то отсюда следует $2^{10} \equiv 1 \ (mod\ 11\cdot 31)$, т. е. $2^{10} \equiv 1 \ (mod\ 341)$. Следовательно, $2^{340} \equiv 1 \ (mod\ 341)$ и $2^{341} \equiv 2 \ (mod\ 341)$. ■

П р и м е р 10. Составное число n, такое, что для каждого целого числа a выполняется сравнение $a^n \equiv a \ (mod\ n)$, называется *абсолютно псевдопростым.* Доказать, что число 561 абсолютно псевдопростое.

Решение. Имеем 561 = 3·11·17. По теореме Ферма для каждого целого числа a, взаимно простого c 561, выполняются сравнения: $a^2 \equiv 1 \ (mod\ 3)$, $a^{10} \equiv 11 \ (mod\ 11)$, $a^{16} \equiv 17 \ (mod\ 17)$. Так как числа 3, 11, 17 попарно взаимно просты и [2, 10, 16] = 80, то из этих сравнений вытекают сравнения:

$a^{80} \equiv 1 \ (mod\ 561)$, $a^{560} \equiv 1 \ (mod\ 561)$. Следовательно, число 561 абсолютно псевдопростое. ■

У П Р А Ж Н Е Н И Я

28. Записать в виде сравнений все классы по модулю 10.

29. Записать все классы по модулю 10 при помощи формулы $x = 10q + r$, $0 \le r < 10$.

30. Указать все классы вычетов: a) взаимно простых с модулем 10; b) имеющих с модулем 10 НОД равный 2; c) имеющих с модулем 10 НОД равный 5; d) имеющих с модулем 10 НОД равный 10.

31. Написать все три вида как полной, так и приведенной системы вычетов по модулям: a) $m = 9$; b) $m = 8$; c) $p = 7$; d) $m = 12$.

32*. Показать, что числа 25, -20, 16, 46, -21, 18, 37, -17 составляют полную систему вычетов по модулю 8.

33. Показать, что числа 32, -9, 15, 42, -18, 30, 6 составляют полную систему вычетов по модулю p =7.

34. Показать, что числа 21, 2, -18, 28, -19, 40, -22, -2, 15 составляют полную систему вычетов по модулю 9.

35. Показать, что числа 24, 18, -19, 37, 28, -23, -32, 5, 41, -35, -33 составляют полную систему вычетов по модулю 11.

36. Показать, что числа 19, 23, 25, -19 составляют приведенную систему вычетов по модулю 12.

37. Показать, что числа 11, -1, 17, -19 составляют приведенную систему вычетов по модулю 8.

38*. Найти наименьшие неотрицательные, наименьшие по абсолютной величине неположительные и абсолютно наименьшие вычеты чисел 24, 14, 25, 37, -8, -19, -40 по модулю 6. Ко скольким различным классам принадлежат данные числа по данному модулю? Какие числа из данных принадлежат к одному и тому же классу по данному модулю?

39. Условие предыдущей задачи применить к числам 17, -14, 19, -49, -22, 21, -29 по модулю 8.

40. Найти наименьшие неотрицательные, наименьшие по абсолютной величине неположительные и абсолютно наименьшие вычеты числа 100 по модулям: 5, 7, 11, 25, 120, 200.

41. Условие предыдущей задачи применить к числу 50 по модулям: 3, 8, 12, 25, 70, 100.

42*. Доказать, что любые m последовательных целых чисел составляют полную систему вычетов по модулю m.

43*. Найти хотя бы одну полную систему вычетов вида $3x - 1$ по модулю 10.

44. Найти хотя бы одну полную систему вычетов вида $5x$ по модулю 4.

45. Доказать, что система чисел 5, 5^2, 5^3, 5^4, 5^5, 5^6 является приведенной системой вычетов по модулю 7.

46. Доказать, что аддитивная группа $\boldsymbol{Z/mZ}$ классов вычетов по модулю m является циклической.

47. Доказать, что группа $(\boldsymbol{Z/mZ}, +)$ является аддитивной группой кольца классов вычетов по модулю m.

48. Доказать, что если a и b взаимно обратны, то $a \bmod m \cdot b \bmod m = 1 \bmod m$, т.е. классы вычетов $a \bmod m$ и $b \bmod m$ также взаимно обратны по модулю m.

49. Доказать, что группа обратимых элементов кольца классов вычетов по модулю m совпадает с мультипликативной группой классов вычетов, взаимно простых с модулем m.

50. Доказать, что кольцо классов по модулю m является полем в том и только в том случае, когда m – простое число.

51*. Доказать, что цифра единиц 12–й степени натурального числа, каноническое разложение которого не содержит множителей 2 и 5, есть 1.

52*. Проверить теорему Эйлера: a) при $a = 5$, $m = 24$; b) при $a = 2$, $m = 33$; c) при $a = 3$, $m = 18$; d) при $a = 3$, $m = 24$.

53*. Пользуясь теоремами Эйлера и Ферма, составить сравнения по модулям: a) 6; b) 5; c) 8; d) 7. Выписать значения a и классы чисел, удовлетворяющих каждому сравнению.

54*. Доказать, что: a) $a^{12} - 1$ делится на 7, если $(a, 7) = 1$; b) $a^{12} - b^{12}$ делится на 65, если $(a, 65) = (b, 65) = 1$.

55. Доказать, что число вида $a^{p-1} + p - 1$, где $a \not\equiv 0 \ (mod\ p)$, является составным.

56*. Доказать, что $\sum_{i=1}^{p-1} i^{k(p-1)} + 1 \equiv 0 \ (mod\ p)$.

57. Доказать, что $\left(\sum_{i=1}^{n} a_i\right)^p \equiv \sum_{i=1}^{n} a_i{}^p \pmod p$

58. Доказать, что $a^{n(p-1)+1} \equiv a \ (mod\ p)$.

59. Найти остатки от деления: a) 109^{345} на 14; b) 439^{291} на 60; c) 293^{275} на 48.

60. Найти остатки от деления: a) $3^{80} + 7^{80}$ на 11; b) $3^{100} + 5^{100}$ на 7; c) $2^{100} + 3^{100}$ на 5; d) $5^{70} + 7^{50}$ на 12.

61. Найти последние три цифры числа 243^{402}.

62*. Доказать, что наименьшее натуральное значение x, удовлетворяющее сравнению $a^x \equiv 1 \ (mod\ m)$, где $(a, m) = 1$, является делителем числа $\varphi(m)$.

63*. Доказать, что $a^{561} \equiv a \ (mod\ 1)$.

64*. Доказать, что сравнению $x^{(p-1)m} + x^{(p-1)n} \equiv 0 \ (mod\ p)$ может удовлетворять только значение x, кратное $p > 2$.

65*. Доказать, что натуральное число m, не делящееся ни на 2, ни на 3, ни на 5, является делителем $\varphi(m)$-значного числа вида 11...1.

66. Доказать, что: а) $a^{560} \equiv 1 \ (mod\ 561)$, где $(a, 561) = 1$; b) $2^{1093 \cdot 1092} \equiv 1 \ (mod\ 1093^2)$.

67*. Доказать, что если $a^p \equiv \pm 1 (mod\ p)$, то тогда и $a^p \equiv \pm 1 (mod\ p^2)$ (p – простое число).

68*. Если p и q – неравные между собой простые числа, то $p^{q-1} + q^{p-1} \equiv 1 (mod\ pq)$.

69*. Доказать, что при любом целом значении x, имеет место сравнение: $x^{13} \equiv x \ (mod\ 2730)$.

70*. Доказать, что если $\sum_{i=1}^{n} a_i \equiv 0 \ (mod\ 30)$, то $\sum_{i=1}^{n} a_i^{\,5} \equiv 0 \ (mod\ 30)$.

71*. Доказать, что если $m > 1$- нечетное число, то $2^{\varphi(m)-1}$ дает при делении на m остаток, равный $m - \left[\frac{m}{2}\right]$.

72*. Показать, чо если $(a, 10) = 1$, то $a^{100n+1} \equiv a \ (mod\ 1000)$, где $n \in \boldsymbol{N}$.

73*. Показать, что $2^{19 \cdot 73-1} \equiv 1 \ (mod\ 19 \cdot 73)$.

74*. Доказать, что $p_1^{P_2-1} + p_2^{P_1-1} \equiv 1 \ (mod\ p_1 p_2)$, где p_1 и p_2 – различные простые числа.

75*. Доказать, что если $2p + 1$ ($p \neq 3$) – число простое, то $4p + 1 \equiv 0 \ (mod\ 3)$.

76*. Доказать, что если $(a, m) = 1$ и $\alpha_1 \equiv \alpha_2 \ (mod\ \varphi(m))$, то $a \equiv a^{\alpha_1} (mod\ m)$.

77*. Показать, что сравнение $a^{6m} + a^{6n} \equiv 0 \ (mod\ 7)$, где $m, n \in \boldsymbol{N}$, может иметь место только при а кратном 7.

78*. Показать, что если $(n, 6) = 1$, то $n^2 \equiv 1 \ (mod\ 24)$.

79*. Найти простое число p из условия:

$$5^{P^2} + 1 \equiv 0 \ (mod\ p^2).$$

80*. Показать, что произведение трех последовательных целых чисел, среднее из которых равно кубу некоторого целого числа, делится на 504.

81*. Показать. Что если при $p > 3$ числа p и $2p+1$ – простые, то $4p+1$ – число составное.

§ 3. Алгебраические сравнения с одним неизвестным. Сравнения первой степени.

Сравнением n-й степени с одним неизвестным называется сравнение вида:

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \equiv 0 \ (mod\ m),$$

где $a_0 \not\equiv 0 \ (mod\ m)$, $a_i \in \boldsymbol{Z}$, $i = \overline{0, n}$ – целое неотрицательное число.

Решить сравнение – значит найти все значения x, удовлетворяющие сравнению.

Если данному сравнению удовлетворяет какое-либо значение $x = \alpha$, то этому сравнению удовлетворяют и все числа, сравнимые с α по модулю m: $x \equiv \alpha \pmod m$, или, что то же, $x = mk + \alpha$, т.е. все числа, составляющие *один класс вычетов* по модулю m, которому принадлежит α. Каждый класс составляет одно решение. Следовательно, *решить сравнение* – значит найти *классы чисел,* удовлетворяющих сравнению.

Так как числа, взятые из каждого класса по одному, составляют полную систему вычетов, то найти классы чисел, удовлетворяющих данному сравнению, это значит найти соответствующие им вычеты полной системы, удовлетворяющие сравнению. Обычно в качестве α берутся *наименьшие неотрицательные* или *абсолютно наименьшие вычеты* по данному модулю m. Таким образом, *сколько вычетов из этой системы удовлетворяют сравнению, столько решений имеет сравнение.*

Два сравнения по одному и тому же модулю с одним и тем же неизвестным x называются *равносильными*, если им удовлетворяют одни и те же значения x.

Сравнение, равносильное данному, получается в результате следующих преобразований:

a) прибавления к частям данного сравнения одного и того же числа;

b) прибавления к любой части сравнения числа, кратного модулю;

c) умножения (деления) частей данного сравнения на число, взаимно простое с модулем;

d) деление частей сравнения и модуля на одно и то же число.

П р и м е р 1. Решить сравнения:

a) $x^3 - 2x + 6 \equiv 0 \pmod{11}$;

b) $x^4 + 2x^3 + 6 \equiv 0 \pmod 8$;

c) $x^4 - x^3 - x^2 + 5x - 2 \equiv 0 \pmod 6$.

Решение. a) Непосредственная проверка показывает, что в полной системе наименьших по абсолютной величине вычетов

-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5

сравнению удовлетворяет только одно число 5. Решение записываем в виде $x \equiv 5 \pmod{11}$.

b) В полной системе вычетов -3, -2, -1, 0, 1, 2, 3, 4 ни одно число не удовлетворяет сравнению и, следовательно, сравнение не имеет решений.

c) В полной системе вычетов -2, -1, 0, 1, 2, 3 сравнению удовлетворяют два числа: -1 и 2. Сравнение имеет два решения:
$x \equiv -1 \pmod 6$ и $x \equiv 2 \pmod 6$.

Сравнение по модулю-делителю данного модуля является сравнением-следствием данного сравнения. ■

П р и м е р 2. Решить сравнение $x^2 - 5x + 6 \equiv 0 \pmod 9$.

Решение. Достаточно рассмотреть сравнение-следствие $x^2 - 5x + 6 \equiv 0 \pmod 3$ или $x^2 + x \equiv 0 \pmod 3$ или $x(x + 1) \equiv 0 \pmod 3$, откуда $x \equiv 0,2 \pmod 3$ или $x = 3q$; $3q + 2$.

Подставим $x = 3q$ в исходное сравнение:

$9q^2 - 15q + 6 \equiv 0 \pmod 9$, отсюда $3q \equiv 3 \pmod 9$, т.е. $q \equiv 1 \pmod 3$ или $q = 1 + 3t$, откуда $x = 3 + 9t$ или $x \equiv 3 \pmod 9$.

При $x = 3q + 2$ исходное сравнение дает:

$9q^2 + 12q + 4 - 15q - 10 + 6 \equiv 0$ (*mod* 9) или $3q \equiv 0$ (*mod* 9) или $q \equiv 0$ (*mod* 3), т.е. $q = 3t$, откуда $x = 9t + 2$ или $x \equiv 2$ (*mod* 9).

Таким образом, данное сравнение имеет два решения: $x \equiv 2; 3$ (*mod* 9). ■

П р и м е р 3. Путем перехода к равносильному сравнению решить следующее сравнение: $13x \equiv 5$ (*mod* 47).

Решение. Прибавим к правой части 47:

$13x \equiv 52$ (*mod* 47). Теперь разделим обе части сравнения на 13. Тогда получим: $x \equiv 4$ (*mod* 47). ■

Сравнение первой степени в общем виде записывается так:

$$ax \equiv b \ (mod\ m).$$

При решении сравнения первой степени могут быть три случая:

a) Если $(a, m) = 1$, то сравнение имеет одно и только одно решение.

b) Если $(a, m) = d > 1$, но свободный член b не делится на d, то сравнение не имеет решений.

c) Если $(a, m) = d > 1$ и b делится на d, то сравнение имеет d решений, которые находятся по формулам:

$$x \equiv \alpha;\ \alpha + \frac{m}{d},\ \alpha + \frac{2m}{d},\ldots,\ \alpha + \frac{(d-1)m}{d} \ (mod\ m),$$

где α - значение x, удовлетворяющее сравнению

$$\frac{a}{d}x \equiv \frac{b}{d}(mod\ \frac{m}{d}).$$

Способы нахождения решения сравнения

$$ax \equiv b \ (mod\ m)$$

рассматриваются только для случая а), когда $(a, m) = 1$, так как третий случай сводится к первому после сокращения на d.

Применяются следующие *три способа решения:*

a) решение находится путем непосредственных испытаний наименьших неотрицательных или абсолютно наименьших вычетов по модулю m;

b) *способ Эйлера*. Решение находится по формуле

$$x \equiv ba^{\varphi(m)-1} \ (mod\ m),$$

где $\varphi(m)$ – функция Эйлера;

c) при помощи конечных непрерывных дробей по формуле

$$x \equiv (-1)^n\, b\, P_{n-1} \ (mod\ m),$$

где P_{n-1} – числитель предпоследней подходящей дроби при разложении $\frac{m}{a}$ в непрерывную дробь.

Иногда сравнение первой степени легко решается при помощи преобразований (см. пример 3).

П р и м е р 4. Решить сравнение способом Эйлера:

$$9x \equiv 8 \ (mod\ 34).$$

Решение. Так как $(9, 34) = 1$, то данное сравнение имеет единственное решение.

Имеем $\varphi(34) = 16$ и мы получаем:

$$x \equiv 8\cdot 9^{15} \equiv 8\cdot 3^{30} \equiv 8\cdot 3^{14} \equiv 8\cdot (2187)^2 \equiv 8\cdot 11^2 \equiv 16 \ (mod\ 34).$$ ■

П р и м е р 5. Решить сравнение при помощи непрерывных дробей:

$$285x \equiv 177 \ (mod\ 924).$$

Решение. Так как (285, 924) = 3 и 177 = 59·3, то данное сравнение имеет три решения.

Разделим обе части сравнения и модуль на 3:

$$95x \equiv 59 \ (mod\ 308).$$

Разложим $\frac{308}{95}$ в непрерывную дробь: $\frac{308}{95} = (3, 4, 7, 1, 2)$. Отсюда

q_i		3	4	7	1	2
P_i	1	3	13	94	107	308

Таким образом, $P_{n-1} = P_4 = 107$, следовательно,

$$x \equiv (-1)^4 \cdot 107 \cdot 59 \ (mod\ 308),$$

Откуда $x \equiv 153$ (*mod* 308).

Тогда решения исходного сравнения представляются в виде:

$$x \equiv 153; 461; 769 \ (mod\ 924). \blacksquare$$

Рассмотрим *применение* сравнений первой степени к решению *неопределенных уравнений первой степени с двумя неизвестными*.

Пусть требуется решить неопределенное уравнение

$$ax + by = c; \quad a, b, c \in \boldsymbol{Z}.$$

Если $(a, b) = 1$, то уравнение имеет целые решения, которые в общем виде записываются так:

$$x = x_1 + bt,$$
$$y = y_1 - at$$

или при отрицательном b удобно брать:

$$x = x_1 - bt,$$
$$y = y_1 + at.$$

В этих формулах решения x_1 и y_1 – пара частных целых значений x и y, удовлетворяющих уравнению, $a\ t \in \boldsymbol{Z}$.

Если $(a, b) = d > 1$ и c не делится на d, то уравнение $ax + by = c$ не имеет решений в целых числах.

Из теории неопределенных уравнений первой степени известны несколько способов нахождения пары частных значений неизвестных, удовлетворяющих уравнению.

При помощи сравнений эта пара частных значений находится так: исходя из уравнения $ax + by = c$, записывается сравнение $ax \equiv c\ (mod\ b)$, где b берется со знаком плюс, значение x, удовлетворяющее сравнению, берется в качестве x_1, а значение y_1 обычно находится непосредственно из уравнения после подстановки в него найденного значения x_1.

П р и м е р 6. Решить в целых числах уравнение:

$$39x - 22y = 10.$$

Решение. Из уравнения имеем сравнение:

$$39x \equiv 10 \ (mod\ 22)$$

или $17x \equiv 10$ (*mod* 22), откуда $x_1 = 20$. Подстановкой в уравнение находим $y_1 = 35$. Общим решением будет:

$$\begin{cases} x = 20 + 22t, \\ y = 35 + 39t. \end{cases}$$ ■

П р и м е р 7. Определить день рождения, зная сумму S произведений числа месяца на 12 и номера месяца на 31, например, для $S = 299$.

Решение. Пусть x – число, а y – номер месяца рождения. Тогда получим уравнение

$$12x + 31y = 299.$$

Отсюда $12x \equiv 299 \pmod{31}$ или $12x \equiv 20 \pmod{31}$. Решая это сравнение получим, что $x_1 = 12$. Подставляя в уравнение получим $y_1 = 5$. Следовательно, днем рождения является 12 мая. ■

У П Р А Ж Н Е Н И Я

82. Непосредственным испытанием наименьших неотрицательных вычетов найти решения сравнений:

a) $5x^2 - 15x + 22 \equiv 0 \pmod{3}$; b) $x^2 + 2x + 2 \equiv 0 \pmod{5}$; c) $3x \equiv 1 \pmod{5}$;

d) $8x \equiv 3 \pmod{14}$; e) $x^3 - 2 \equiv 0 \pmod{5}$; f) $x^2 - 2x + 1 \equiv 0 \pmod{4}$;

g) $27x^2 - 13x + 11 \equiv 0 \pmod{5}$.

83. Непосредственным испытанием абсолютно наименьших вычетов решить следующие сравнения, предварительно упростив их на основании свойств сравнений:

a) $12x \equiv 1 \pmod{7}$; b) $8x \equiv 1 \pmod{5}$; c) $3x \equiv 13 \pmod{11}$; d) $6x \equiv 3 \pmod{7}$;

e) $6x + 5 \equiv 1 \pmod{7}$; f) $90x^{20} + 46x^2 - 52x + 46 \equiv 0 \pmod{15}$.

84. Показать, что следующие сравнения не имеют решений:

a) $2x - 3 \equiv 0 \pmod{6}$; b) $x^2 - 2x + 3 \equiv 0 \pmod{4}$; c) $x^3 + x + 4 \equiv 0 \pmod{5}$;

d) $x^4 + 2 \equiv 0 \pmod{5}$; e) $x^5 - 2x^3 + 13x - 1 \equiv 0 \pmod{4}$.

85. Показать, что следующим сравнениям удовлетворяют любые целые значения неизвестного:

a) $x^2 - x + 6 \equiv 0 \pmod{2}$; b) $x(x^2 - 1) \equiv 0 \pmod{6}$;

c) $x^4 + 2x^3 - x^2 - 2x \equiv 0 \pmod{4}$; d) $x^p - x \equiv 0 \pmod{p}$.

86. Путем преобразований решить сравнения:

a) $2x \equiv 7 \pmod{15}$; b) $5x \equiv 2 \pmod{8}$; c) $7x \equiv 2 \pmod{13}$;

d) $3x \equiv 23 \pmod{37}$; e) $27x \equiv 14 \pmod{25}$; f) $13x \equiv 10 \pmod{11}$;

g) $5x \equiv 3 \pmod{11}$; h) $7x \equiv 5 \pmod{24}$.

87. При каких целых значениях x трехчлен $5x^2 + x + 4$ делится на 10?

88. Решить сравнение $x^2 - 4x + 3 \equiv 0 \pmod{6}$, используя необходимое условие $x^2 - 4x + 3 \equiv 0 \pmod{2}$.

89. Решить сравнение $x^{\varphi(30)} \equiv 1 \pmod{30}$.

90. Сколько решений имеет сравнение $x^{\varphi(m)} \equiv 1 \pmod{m}$?

91*. Показать, что если $(n, m) = 1$, то сравнение n-й степени $x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{m}$ можно, путем введения нового неизвестного y, привести к сравнению той же степени $y^n + b_2 y^{n-2} + \ldots + b_n \equiv 0 \pmod{m}$, у которого отсутствует член $(n - 1)$-й степени.

92*. Пользуясь предыдущей задачей, привести сравнение $x^3 + 5x^2 + 6x - 8 \equiv 0 \pmod{13}$ к трехчленному виду: $y^3 + py + q \equiv 0 \pmod{13}$.

93. Решить способом Эйлера следующие сравнения:

a) $5x \equiv 7 \pmod{10}$; b) $3x \equiv 8 \pmod{13}$; c) $7x \equiv 5 \pmod{17}$;
d) $13x \equiv 3 \pmod{19}$; e) $27x \equiv 7 \pmod{58}$.

94. Решить при помощи непрерывных дробей следующие сравнения:

a) $7x \equiv 4 \pmod{19}$; b) $143x \equiv 41 \pmod{221}$; c) $13x \equiv 178 \pmod{153}$;
d) $67x \equiv 64 \pmod{183}$; e) $89x \equiv 86 \pmod{241}$; f) $213x \equiv 137 \pmod{516}$;
g) $111x \equiv 81 \pmod{447}$; h) $186x \equiv 374 \pmod{422}$; i) $129x \equiv 321 \pmod{471}$.

95. Решить одним из способов следующие сравнения:

a) $12x \equiv 9 \pmod{18}$;
b) $20x \equiv 10 \pmod{25}$;
c) $-50x \equiv 67 \pmod{177}$;
d) $-73x \equiv 60 \pmod{311}$;
e) $-53x \equiv 84 \pmod{219}$;
f) $90x + 18 \equiv 0 \pmod{138}$;
g) $78x \equiv 42 \pmod{51}$.

Правильность ответов проверить подстановкой.

96*. Составить сравнение первой степени по модулю 21: a) имеющее одно решение; b) имеющее 3 и 7 решений; c) имеющее 2, 10, 15 решений.

97. Определить день и месяц рождения, зная, что сумма произведений числа месяца на 12 и номера месяца на 31 равна 198.

98*. Приписать справа к числу 523 такое трехзначное число, чтобы полученное шестизначное число делилось на 7, 8 и 9.

99. Приписать справа к числу 629 такое трехзначное число, чтобы полученное шестизначное число делилось на 5, 8 и 11.

100. Приписать справа к числу 723 такое двузначное число, чтобы полученное пятизначное число при делении на 31 давало в остатке число 7.

101. Решить в целых числах уравнения:

a) $3x + 4y = 13$;
b) $8x - 13y = 63$;
c) $43x + 37y = 21$;
d) $45x - 37y = 25$;
e) $81x - 48y = 33$;
f) $26x + 3y = 13$;
g) $53x + 17y = 25$;
h) $47x - 105y = 4$;
i) $18x - 33y = 112$;
j) $11x + 16y = 156$;
k) $12x - 37y = -3$;
l) $23x + 15y = 19$.

102. Для перевозки зерна имеются мешки по 60 кг и по 80 кг. Сколько нужно тех и других мешков для перевозки 440 кг зерна?

103. Сколько билетов по 30 сумов и 50 сумов можно купить на 1490 сумов?

104. На прямой $ax + by = c$ найти количество целых точек, лежащих между точками с абсциссами a_1 и a_2:

a) $8x - 13y + 6 = 0$; $a_1 = -100$; $a_2 = 150$;
b) $7x + 29y = 584$; $a_1 = -20$, $a_2 = 160$;
c) $90x - 74y = 50$; $a_1 = -100$, $a_2 = 200$.

105*. При каких наименьших натуральных значениях a и b уравнение $ax - by = 31$ имеет решение $x = 5$, $y = 9$?

106*. Доказать, что число внутренних целых точек отрезка с целыми концами $A(x_1, y_1)$, $B(x_2, y_2)$ равно $d - 1$, где $d = (y_1 - y_2, x_1 - x_2)$.

107. Через сколько целых точек проходит треугольник с вершинами: A (2, 1), B (20, 7), C (8, 15)?

108. При каких целых значениях x следующие функции принимают целочисленные значения:

a) $f(x) = \frac{9x-1}{7}$; b) $F(x) = \frac{7x-1}{15}$?

109*. На фабрику прибыло 500 т хлопка в 18 вагонах. В вагонах было по 15, 20 и 30 т хлопка. Сколько вагонов было по 15, сколько по 20 и сколько по 30 т?

§4. Системы сравнений первой степени

Система сравнений первой степени с одним и тем же неизвестным, но с разными модулями, записывается следующим образом:

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\cdots\cdots\cdots\cdots \\ a_n x &\equiv b_n \pmod{m_n} \end{aligned}\right\} \qquad (1)$$

Общий способ состоит в том, что сначала находится решение $x \equiv \alpha \pmod{m_1}$ первого сравнения, где α - наименьший неотрицательный или абсолютно наименьший вычет по модулю m_1 и берется класс чисел

$$x = m_1 t + \alpha, \qquad (2)$$

удовлетворяющих первому сравнению. (Если первое сравнение не имеет решения, то не имеет решений и вся система).

Затем это значение x подставляется во второе сравнение, что дает

$$a_2(m_1 t + \alpha) \equiv b_2 \pmod{m_2} \qquad (3)$$

Откуда находится t опять в виде класса чисел

$$t = m_2 t_1 + \beta$$

и подставляется в равенство (2). (Если сравнение (3) не имеет решения, то и вся система не имеет решения).

В результате получается значение x в виде класса чисел, удовлетворяющих первым двум сравнениям системы. Дальше это значение x подставляется в третье сравнение системы, так же находится t_1, затем находится x и подставляется в четвертое сравнение и т.д.

Отметим, что можно следовать и несколько другим путем: сначала решается каждое из сравнений системы и представляется в виде:

$$\left.\begin{aligned} x &\equiv \alpha_1 \pmod{m_1} \\ x &\equiv \alpha_2 \pmod{m_2} \\ &\cdots\cdots\cdots\cdots \\ x &\equiv \alpha_n \pmod{m_n} \end{aligned}\right\} \qquad (4)$$

а затем поступают описанным выше способом.

Если для сравнений $a_i x \equiv b_i \pmod{m_i}$ $(i = 1, \overline{n})$ системы (1) $(a_i, m_i) = d_i$ и $d_i | b_i$, то сокращая члены и модуль каждого i-го сравнения на d_i, получим систему:

$$\left.\begin{aligned}
&\frac{a_1}{d_1}x \equiv \frac{b_1}{d_1}\left(mod\,\frac{m_1}{d_1}\right)\\
&\frac{a_2}{d_2}x \equiv \frac{b_2}{d_2}\left(mod\,\frac{m_2}{d_2}\right)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&\frac{a_n}{d_n}x \equiv \frac{b_n}{d_n}\left(mod\,\frac{m_n}{d_n}\right)
\end{aligned}\right\} \qquad (5)$$

эквивалентную системе (1).

Сравнения этой системы можно решить относительно x и свести решение системы (5) к решению системы:

$$\left.\begin{aligned}
&x \equiv \alpha_1\left(mod\,\frac{m_1}{d_1}\right)\\
&x \equiv \alpha_2\left(mod\,\frac{m_2}{d_2}\right)\\
&\cdots\cdots\cdots\cdots\cdots\\
&x \equiv \alpha_n\left(mod\,\frac{m_n}{d_n}\right)
\end{aligned}\right\} \qquad (6)$$

Если в системе (4) модули $m_1, m_2,..., m_n$ *попарно взаимно просты*, т.е. $(m_i, m_j) = 1$ при $i \neq j$, то решение ее можно находить не указанным выше способом, а по формуле

$$x_0 = \frac{M}{m_1}y_1\alpha_1 + \frac{M}{m_2}y_2\alpha_2 + ... + \frac{M}{m_n}y_n\alpha_n, \qquad (7)$$

где $M = [m_1, m_2,..., m_n]$ и $y_1, y_2,..., y_n$ есть решения сравнений:

$$\frac{M}{m_i}y_i = 1(mod\ m_i),\ i = \overline{1,n}.$$

Решением системы будет:

$x \equiv x_0\ (mod\ M)$.

Этим способом можно решать и систему (6), если модули $\frac{m_1}{d_1}, \frac{m_2}{d_2},...,\frac{m_n}{d_n}$ попарно взаимно просты.

П р и м е р 1. Решить систему сравнений:

$$\left.\begin{aligned}
&x \equiv 13(mod\ 16)\\
&x \equiv 3(mod\ 10)\\
&x \equiv 9(mod\ 14)
\end{aligned}\right\}$$

Решение. Из первого сравнения имеем:

$$x = 16t + 13.$$

Подставляем во второе сравнение:

$$16t + 13 \equiv 3\ (mod\ 10), \quad \text{или} \quad 16t + 13 \equiv 0\ (mod\ 10),$$

откуда $8t \equiv 0\ (mod\ 5)$, или $16t \equiv 0\ (mod\ 5)$.

Следовательно, $t = 5t_1$.

Подставим $t = 5t_1$ в $x = 16t + 13$:

$x = 16 \cdot 5t_1 + 13 = 80t_1 + 13$.

Найденное значение x подставляем в третье сравнение системы:

$80t_1 + 13 \equiv 9 \ (mod\ 14)$, или $80t_1 \equiv -4 \ (mod\ 14)$, или

$80t_1 \equiv 10 \ (mod\ 14)$, или $40t_1 \equiv 5 \ (mod\ 7)$, или

$8t_1 \equiv 1 \ (mod\ 7)$, откуда $t_1 \equiv 1 \ (mod\ 7)$, т.е. $t_1 = 7t_2 + 1$.

Подставляя $t_1 = 7t_2 + 1$ в $x = 80t_1 + 13$, находим:

$x = 80\ (70t_2 + 1) + 13 = 560t_2 + 93$.

Таким образом, $x \equiv 93 \ (\text{mod } 560)$. ■

Проверка: 93 – 13 делится на 16; 93 – 13 делится на 10; 93 – 9 делится на 14.

Замечание. Решая сравнение $16t \equiv 0 \ (mod\ 10)$, мы получили сравнение $8t \equiv 0 \ (mod\ 5)$, и решение его $t \equiv 0 \ (mod\ 5)$, или $t = 5t_1$, которое привело к решению $x = 80t_1 + 13$. Но сравнение $16t \equiv 0 \ (mod\ 10)$ имеет еще второе решение $t \equiv 5 \ (mod\ 10)$, или $t = 10t_1 + 5$ (т.к. $d = (16, 10) = 2$), которое при подстановке в равенство $x = 16t + 13$ дает решение $x = 16(10t_1 + 5) + 13 = 160t_1 + 93$. Но $93 \equiv 13 \ (mod\ 80)$, т.е. числа 93 и 13 принадлежат одному классу по модулю 80, поэтому мы не находим решение системы соответствующее этому значению.

Из замечания (пример 1) следует, что: если какое-либо сравнение системы или сравнение относительно t_1 имеет d решений по некоторому модулю m, то для решения системы достаточно ограничиться только решением равносильного ему сравнения по модулю m/d.

П р и м е р 2. Решить систему сравнений:

$$\left.\begin{aligned} 7x &\equiv 3 \ (mod\ 11) \\ 15x &\equiv 5 \ (mod\ 35) \\ 3x &\equiv 2 \ (mod\ 5) \end{aligned}\right\}$$

Решение. Решая каждое сравнение, заменяем эту систему эквивалентной ей системой сравнений:

$$\left.\begin{aligned} x &\equiv 2 \ (mod\ 11) \\ x &\equiv 5 \ (mod\ 7) \\ x &\equiv 4 \ (mod\ 5) \end{aligned}\right\}$$

Модули сравнений этой системы попарно взаимно просты, поэтому решение ее можно найти по формуле (7).

Находим: $M = [11, 7, 5] = 385$,

$$\frac{M}{m_1} = 35, \quad \frac{M}{m_2} = 55, \quad \frac{M}{m_3} = 77 .$$

Составляем сравнения:

$$35y_1 \equiv 1 \ (mod\ 11),\ 55y_2 \equiv 1 \ (mod\ 7),\ 77y_3 \equiv 1 \ (mod\ 5),$$

откуда $y_1 = 6$, $y_2 = -1$, $y_3 = 3$.

Теперь по формуле (7) находим:

$$x_0 = 35 \cdot 6 \cdot 2 + 55 \cdot (-1) \cdot 5 + 77 \cdot 3 \cdot 4 = 1069 \equiv 299 \ (mod\ 385).$$

Таким образом, $x \equiv 299 \ (mod\ 385)$. ■

П р и м е р 3. Решить систему сравнений:

$$\left.\begin{aligned} 5x &\equiv 7 \pmod 9 \\ 4x &\equiv 3 \pmod 7 \\ 3x &\equiv 8 \pmod{12} \end{aligned}\right\}$$

Решение. Из данной системы сравнений видим, что в третьем сравнении (3, 12) = 3, но 8 не делится 3, поэтому оно неразрешимо; следовательно, не решая систему, можно сказать, что она не имеет решения.

П р и м е р 4. Решить систему сравнений:

$$\left.\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 2 \\ x &\equiv -1 \pmod 6 \end{aligned}\right\}$$

Решение. Первые два сравнения равносильны, соответственно, сравнениям $x \equiv -1 \pmod 3$ и $x \equiv -1 \pmod 2$ и могут быть отброшены как следствия третьего сравнения системы. Таким образом, третье сравнение системы является ее решением, т.е. $x \equiv -1 \equiv 5 \pmod 6$. ■

П р и м е р 5. Найти все целые числа, которые при делении на 2, на 3, на 4, на 5, на 6 и на 7 дают, соответственно, остатки 1, 2, 3, 4, 5 и 0.

Решение. Задача приводит к системе:

$$\left.\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 5 \pmod 6 \\ x &\equiv 0 \pmod 7 \end{aligned}\right\}$$

Сравнение $x \equiv 1 \pmod 2$ или $x \equiv 3 \pmod 2$ может быть сразу же отображено как следствие сравнения $x \equiv 3 \pmod 4$. Аналогичное соображение позволяет отбросить сравнение $x \equiv 2 \pmod 3$.

Таким образом, получим систему:

$$\left.\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 5 \pmod 6 \\ x &\equiv 0 \pmod 7 \end{aligned}\right\}$$

Решая эту систему, получим: $x \equiv 119 \pmod{420}$. ■

П р и м е р 6. Найти значения a, при которых имеет решение система:

$$\left.\begin{aligned} x &\equiv 5 \pmod{18} \\ x &\equiv 8 \pmod{21} \\ x &\equiv a \pmod{35} \end{aligned}\right\}$$

Решение. Из первого сравнения имеем

$$x = 18t + 5.$$

Подставляем x во второе сравнение и находим t:

$18t + 5 \equiv 8 \pmod{21}$, или $18t \equiv 3 \pmod{21}$, или $6t \equiv 1 \pmod 7$, $t \equiv 6 \pmod 7$.

Удобнее взять $t \equiv -1 \pmod 7$, откуда $t = 7t_1 - 1$. Тогда

$$x = 16\,(7t_1 - 1) = 5 = 126t_1 - 13.$$

Это значение x подставляем в третье сравнение системы:

$$126t_1 - 13 \equiv a \ (mod\ 35), \text{ т.е. } 21t_1 \equiv a = 13 \ (mod\ 35).$$

Так как (21, 35) = 7, то для разрешимости последнего сравнения необходимо, чтобы, $a + 13 \equiv 0 \ (mod\ 7)$, или $a \equiv 1 \ (mod\ 7)$.

Таким образом, исходная система имеет решения при $a \equiv 1 \ (mod\ 7)$. ■

П р и м е р 7. Число, записываемое в десятичной системе счисления как 4*x*87*y*6, делится на 56. Найти это число.

Решение. Из условия имеем систему сравнений:

$$\left.\begin{array}{l} 4x87y \equiv 0 (mod\ 8) \\ 4x87y6 \equiv 0 (mod\ 7) \end{array}\right\}$$

Из первого сравнения по признаку делимости на 8 следует, что 7*y*6 делится на 8, что будет при $y = 3$ и $y = 7$.

Подставляя во второе сравнение, получаем:

4x8736 ≡ 0 (*mod* 7),

4x8776 ≡ 0 (*mod* 7).

Представим полученные сравнения в виде:

$400000 + 10000x + 8736 \equiv 0 \ (mod\ 7)$,

$400000 + 10000x + 8776 \equiv 0 \ (mod\ 7)$, или $4x \equiv 1 \ (mod\ 7)$, $4x \equiv 3 \ (mod\ 7)$.

Первое сравнение имеет решение $x \equiv 2 \ (mod\ 7)$, или $x = 7t+2$, откуда при $t=0$ получаем $x_1=2$ и при $t=1$ будет $x_2=9$. При других t значения x не пригодны.

Второе сравнение имеет решение $x \equiv 6 \ (mod\ 7)$, или $x = 7t + 6$, откуда получаем единственное значение $x_3 = 6$. Подставляя полученные значения x, получаем числа: 428736, 498736, 468776. ■

П р и м е р 8. Решить сравнение сведением его к системе сравнений по парно взаимно простым модулям:

$$x^3 + 2x + 3 \equiv 0 \ (mod\ 15) .$$

Решение. Данное сравнение равносильно системе:

$$\left.\begin{array}{l} x^3 + 2x + 3 \equiv 0 (mod\ 5) \\ x^3 + 2x + 3 \equiv 0 (mod\ 3). \end{array}\right\}$$

Второе сравнение этой системы равносильно сравнению $(x - 1)x(x + 1) \equiv 0 \ (mod\ 3)$ и, следовательно, является тождественным. Задача сводится к решению сравнения

$$x^3 + 2x + 3 \equiv 0 \ (mod\ 5),$$

откуда $x \equiv 2; 4 \ (mod\ 5)$.

По данному модулю 15 имеем: $x \equiv 2; 7; 12; 4; 9; 14 \ (mod\ 15)$. ■

П р и м е р 9. Через какие целые точки проходит линия:

$$15y = 2x^3 - 5x^2 + 4x + 11, \text{ где } -2 < x < 8 \text{ ?}$$

Решение. Имеем $2x^3 - 5x^2 + 4x + 11 \equiv 0 \ (mod\ 15)$ или

$$2x^3 - 5x^2 + 4x + 11 \equiv 0 \ (mod\ 5)$$

$$2x^3 - 5x^2 + 4x + 11 \equiv 0 \ (mod\ 3).$$

Первое сравнение системы имеет решения $x \equiv 2; 4 \ (mod\ 5)$, а второе $x \equiv 1; 2 \ (mod\ 3)$.

Решая системы:

$$\left\{\begin{array}{l} x \equiv 2 (mod\ 5) \\ x \equiv 1 (mod\ 3) \end{array}\right. \quad \left\{\begin{array}{l} x \equiv 2 (mod\ 5) \\ x \equiv 2 (mod\ 3) \end{array}\right. \quad \left\{\begin{array}{l} x \equiv 4 (mod\ 5) \\ x \equiv 1 (mod\ 3) \end{array}\right. \quad \left\{\begin{array}{l} x \equiv 4 (mod\ 5). \\ x \equiv 2 (mod\ 3), \end{array}\right.$$

находим $x \equiv 7; 2; 4; 14 \ (mod\ 15)$.

Указанным в условии границам удовлетворяют $x = 7; 2; 4; -1$. Соответствующие значения y находятся по данному уравнению. ■

П р и м ер 10. Решить систему сравнений:

$$\begin{cases} 9y \equiv 15 \\ 7x - 3y \equiv 1 \end{cases} (mod\ 12),$$

Решение. Решая первое сравнение получаем:

$3y \equiv 5 \ (mod\ 4)$, или $3y \equiv 9 \ (mod\ 4)$, или $y \equiv 3 \ (mod\ 4)$.

По модулю 12 имеем: $y \equiv 3; 7; 11 \ (mod\ 12)$.

Отсюда имеем три системы:

$$\begin{cases} 7x \equiv 1 + 3y \\ y \equiv 3 \end{cases} (mod\ 12), \quad \begin{cases} 7x \equiv 1 + 3y \\ y \equiv 7 \end{cases} (mod\ 12), \quad \begin{cases} 7x \equiv 1 + 3y \\ y \equiv 11 \end{cases} (mod\ 12)$$

или

$$\begin{cases} x \equiv 10 \\ y \equiv 3 \end{cases} (mod\ 12), \quad \begin{cases} x \equiv 10 \\ y \equiv 7 \end{cases} (mod\ 12), \quad \begin{cases} x \equiv 10 \\ y \equiv 11. \end{cases} (mod\ 12). \ ■$$

П р и м е р 11. Решить систему сравнений:

$$\begin{cases} x + 2y \equiv 3 \\ 4x + y \equiv 2 \end{cases} (mod\ 5).$$

Решение. Умножая части второго сравнения на 2 и затем, почленно вычитая, получаем $7x \equiv 1 \ (mod\ 5)$, откуда $x \equiv 3 \ (mod\ 5)$. Умножение частей первого сравнения на 4 и почленное вычитание даст $y \equiv 0 \ (mod\ 5)$. Проверка показывает, что

$$\begin{cases} x \equiv 3 \\ y \equiv 2 \end{cases} (mod\ 5)$$

является решением системы. ■

У П Р А Ж Н Е Н И Я

110. Решить системы сравнений:

a) $\left.\begin{array}{l} x \equiv 4 \ (mod\ 5) \\ x \equiv 1 \ (mod\ 12) \\ x \equiv 7 \ (mod\ 14) \end{array}\right\}$;

b) $\left.\begin{array}{l} x \equiv 1 \ (mod\ 25) \\ x \equiv 2 \ (mod\ 4) \\ x \equiv 3 \ (mod\ 7) \\ x \equiv 4 \ (mod\ 9) \end{array}\right\}$;

c) $\left.\begin{array}{l} 2x \equiv 7 \ (mod\ 13) \\ 5x \equiv 8 \ (mod\ 17) \\ 3x \equiv 7 \ (mod\ 31) \\ 14x \equiv 35 \ (mod\ 19) \end{array}\right\}$;

d) $\left.\begin{array}{l} 4x \equiv 7 \ (mod\ 13) \\ x \equiv 2 \ (mod\ 17) \\ 5x \equiv 3 \ (mod\ 9) \\ 8x \equiv 4 \ (mod\ 14) \end{array}\right\}$;

e) $\left.\begin{array}{l} 3x \equiv 7 \ (mod\ 10) \\ 2x \equiv 5 \ (mod\ 15) \\ 7x \equiv 5 \ (mod\ 12) \end{array}\right\}$;

f) $\left.\begin{array}{l} 4x \equiv 1 \ (mod\ 9) \\ 5x \equiv 3 \ (mod\ 7) \\ 4x \equiv 5 \ (mod\ 12) \end{array}\right\}$;

g) $\left.\begin{array}{l} 5x \equiv 1 \ (mod\ 12) \\ 5x \equiv 2 \ (mod\ 8) \\ 7x \equiv 3 \ (mod\ 11) \end{array}\right\}$;

h) $\left.\begin{array}{l} 3x \equiv 1 \ (mod\ 10) \\ 4x \equiv 3 \ (mod\ 5) \\ 2x \equiv 7 \ (mod\ 9) \end{array}\right\}$;

i) $\left.\begin{array}{l} 3x \equiv 5 \ (mod\ 7) \\ 2x \equiv 3 \ (mod\ 5) \\ 3x \equiv 3 \ (mod\ 9) \end{array}\right\}$;

j) $\left.\begin{array}{l} 5x \equiv 200 \ (mod\ 251) \\ 11x \equiv 192 \ (mod\ 401) \\ 3x \equiv -15 \ (mod\ 907) \end{array}\right\}$.

111. Найти все натуральные числа, дающие в остатке 1 при делении на 2, на 3, на 4 и делящиеся на 5 без остатка.

112. Между числами 200 и 500 найти все целые числа, которые при делении на 4, 5, 7 дают, соответственно, остатки 3, 4, 5.

113*. Найти целые точки прямых $4x - 7y = 9$, $2x + 9y = 15$ и $5x - 13y = 12$, лежащие на одном перпендикуляре к оси абсцисс.

114. Решить системы сравнений:

a) $\left.\begin{array}{l} x \equiv a \ (mod\ 6) \\ x \equiv 1 \ (mod\ 8) \end{array}\right\}$;

b) $\left.\begin{array}{l} x \equiv 2 \ (mod\ 6) \\ x \equiv a \ (mod\ 8) \end{array}\right\}$;

c) $\left.\begin{array}{l} x \equiv 5 \ (mod\ 18) \\ x \equiv 8 \ (mod\ 21) \\ x \equiv a \ (mod\ 35) \end{array}\right\}$;

d) $\left.\begin{array}{l} x \equiv a \ (mod\ 7) \\ x \equiv b \ (mod\ 5) \\ x \equiv c \ (mod\ 3) \end{array}\right\}$.

115. Найти значения a, при которых имеют решение системы:

a) $\left.\begin{array}{l} x \equiv a \ (mod\ 6) \\ x \equiv 1 \ (mod\ 10) \\ x \equiv 2 \ (mod\ 21) \\ x \equiv 3 \ (mod\ 11) \end{array}\right\}$;

b) $\left.\begin{array}{l} x \equiv 3 \ (mod\ 11) \\ x \equiv 11 (mod\ 20) \\ x \equiv 1 \ (mod\ 15) \\ x \equiv a \ (mod\ 18) \end{array}\right\}$;

c) $\left.\begin{array}{l} 2x \equiv a \ (mod\ 4) \\ 3x \equiv 4 \ (mod\ 10) \end{array}\right\}$.

116*. Число N, записываемое в десятичной системе счисления как $xyz138$, делится на 7, а $138xyz$ при делении на 13 дает остаток 6 и $x1y3z8$ при делении на 11 дает остаток 5. Найти число N.

117*. Зная, что число $13xy45z$ делится на 792, найти x, y, z.

118*. Найти трехзначные числа, обладающие тем свойством, что, приписав к каждому из них справа следующее за ним, получим точный квадрат.

119*. Некоторое целое число при делении на 7 дает в остатке 3, его квадрат при делении на 7^2 дает в остатке 44; наконец, его куб при делении на 7^3 дает в остатке 111. Найти это число.

120. Следующие сравнения решить сведением их к системам попарно взаимно простым модулям:

a) $13x \equiv 32 \pmod{28}$; b) $245x \equiv 405 \pmod{475}$; c) $78x \equiv 49 \pmod{77}$;

d) $56x \equiv 81 \pmod{45}$; e) $x^2 \equiv -1 \pmod{20}$; g) $x^2 \equiv -1 \pmod{85}$.

121. Через какие целые точки проходит линия:

$$14y = 3x^3 - 4x^2 + 11x + 4, \text{ где } -7 < x < 7?$$

122. Решить системы сравнений:

a) $\begin{cases} x + 3y \equiv 5 \pmod 7 \\ 4x \equiv 5 \end{cases}$; b) $\begin{cases} x \equiv 2 \pmod 4 \\ x - 2y \equiv 1 \end{cases}$;

c) $\begin{cases} 9y \equiv 15 \pmod{12} \\ 3x - 7y \equiv 1 \end{cases}$; d) $\begin{cases} 3x - 5y \equiv 1 \pmod{12} \\ 9y \equiv 15 \end{cases}$;

e) $\begin{cases} x + 2y \equiv 0 \pmod 5 \\ 3x + 2y \equiv 2 \end{cases}$; f) $\begin{cases} 3x + 4y \equiv 29 \pmod{143} \\ 2x - 9y \equiv -84 \end{cases}$;

g) $\begin{cases} x + 2y \equiv 4 \pmod 5 \\ 3x + y \equiv 2 \end{cases}$; h) $\begin{cases} 4x - y \equiv 2 \pmod 6 \\ 2x + 2y \equiv 0 \end{cases}$.

123. Решить в целых числах системы уравнений:

a) $\left.\begin{array}{l} x + 2y + 5z = 1 \\ 3x + y + 5z = 3 \end{array}\right\}$; b) $\left.\begin{array}{l} x - y - 3z = 1 \\ x + y - 2z = 1 \end{array}\right\}$.

124. Найти все целые числа x и y, такие, чтобы числа вида

$\dfrac{3x - y + 1}{7}$ и $\dfrac{2x + 3y - 1}{7}$ также были целыми.

ОТВЕТЫ К ГЛ. VIII СРАВНЕНИЯ

§ 1.

1. По модулю 1. **2**. а); в); с); **3**. *Решение*. Если $a = mq + r$, то $a - r = mq$ и $a \equiv r \pmod{m}$. **4**. а) $x = 3q$; в) $x = 1+2q$. **5**. Делители числа $2p$. **6**. Делители числа 8. **7**. *Решение*. Если n нечетное число, тогда n-1 и n+1- последовательные четные числа. Если одно из них кратно 2, то другое по меньшей мере кратно 4, поэтому: $(n-1)(n+1) = n^2 - 1 \equiv 0 \pmod 8$, или $n^2 \equiv 1 \pmod 8$. **8**. *Решение.* Умножим обе части данного сравнения на 4: $400a + 40b + 4c \equiv 0 \pmod{21}$, но $400a \equiv a \pmod{21}$, $40b \equiv -2 \pmod{21}$, $4c \equiv 4 \pmod{21}$. Сложим эти три сравнения: $400a + 40b + 4c \equiv a - 2b + 4c \pmod{21}$. Отсюда $a - 2b + 4c \equiv 0 \pmod{21}$. **10.** *Решение.* Так как $11\cdot31 - 1 = 340 = 5\cdot68$ и так как $2^5 \equiv -1 \pmod{11}$, то возводя члены этого сравнения в 68-ю степень, получим: $(2^5)^{68} = 2^{340} = 2^{11\bullet31-1} \equiv 1 \pmod{11}$. Далее, так как $2^5 \equiv 1 \pmod{31}$, то $(2^5)^{68} = 2^{11\bullet31-1} \equiv 1 \pmod{31}$. Отсюда $2^{11\bullet31-1} \equiv 1 \pmod{11\cdot31}$. Умножая члены этого сравнения на 2, получим искомое сравнение. **11.** *Решение.* При $x = 3n + 1$ делимое равно $1+3\cdot27^n + 9\cdot729^n$. По данному модулю $27^n \equiv 729^n \equiv 1$, поэтому $1 + 3\cdot27^n + 9\cdot729^n \equiv 1 + 3 + 9 = 13$. **14.** 4. **15.** *Решение.* По условию $a = b + p^n q$ ($q = 0, \pm1, \pm2, ...$). Возводя обе части этого равенства в степень p, получим $a^p = b^p + p^{n+1} \cdot \alpha$ ($\alpha = 0, \pm1, \pm2, ...$). **17.** *Указание.* Из левой части сравнения $a_4 \cdot 10^4 + a_3a_2\cdot10^2 + a_1a_0 \equiv 0 \pmod{33}$ вычесть число $999a_4 + 99a_3a_2$ кратное модулю. **18.** *Решение*. а) Так как $9^{10} \equiv 1 \pmod{100}$, то $9^{10q+r} \equiv 9^r \pmod{100}$. Так как $9^9 \equiv 9 \pmod{10}$, то $9^{9^9} \equiv 9^9 \equiv 89 \pmod{100}$. Искомыми цифрами являются 8 и 9; b) Так как $7^4 = 2401 \equiv 1 \pmod{100}$, то и $7^{100} \equiv 1 \pmod{100}$, откуда $7^{9^{9^9}} \equiv 7^{100q+89} \equiv 7^{89} \pmod{100}$. Так как $7^{88} \equiv 1 \pmod{100}$, то $7^{89} \equiv 7 \pmod{100}$. Искомыми цифрами являются 0 и 7. **19.** *Решение*. Из $p \equiv p + 2 \equiv 1 \pmod 2$ следует $p^{p+2} + (p+2)^p \equiv 0 \pmod 2$, а из $p \equiv -1 \pmod{p+1}$, $p + 2 \equiv 1 \pmod{p+1}$ следует $p^{p+2} + +(p+2)^p \equiv 0 \pmod{p+1}$. **20.** *Указание.* За исключением нуля даны числа вида $\pm\frac{p-x}{2}\left(x = 1, 2, ..., p-2\right)$. Сравнения

$$\pm\frac{p-x}{2} \equiv 0 \pmod p, \quad \frac{p-x_1}{2} \equiv \pm\frac{p-x_2}{2} \equiv 0 \pmod p,$$

приводят, соответственно, к неверным сравнениям $x \equiv p \pmod p$, $x_1 \equiv \pm x_2 \pmod p$. **21.** *Решение.* Применим метод математической индукции. При $n = 1$ сравнение верно. Пусть сравнение верно для n. Покажем, что оно верно и для $n + 1$.

Действительно, $2^{3^{n+1}}+1=\left(2^{3^n}\right)^3+1=\left(2^{3^n}+1\right)\left(2^{2\cdot 3^n}-2^3+1\right)\equiv 0\left(mod\ 3^{n+2}\right)$, так как $2^{3^n}+1)\equiv 0$ ($mod\ 3^{n+1}$) по предположению и $2^{2\bullet 3}$ - 2^3 +1) ≡ 0 (*mod* 3) в силу того, что 2 ≡ - 1(*mod* 3). **22.** а) *Решение.* $2^{4n+1}=2\cdot 4^{2n}\equiv 2(mod\ 5)$, так как 4 ≡ - 1(*mod* 5). Таким образом, $2^{4n+1}=2+5k$, где $k\in \boldsymbol{N}$, и $N=3^{2+5k}+2=$ $9\cdot 243^k+2\equiv 0$ (*mod* 11), так как 243 ≡ 1(*mod* 11). Итак, 11| N и $N>11$. Значит, N – составное число. b**)** **Решение.** $3^{4n+1}=3\cdot 9^{2n}\equiv 3(mod\ 10)$, так как 9 ≡ -1(*mod* 10). Значит, $3^{4n+1}=3+10k$, где $k\in \boldsymbol{N}$, и $M=2^{3+10k}+3=8\cdot 32^{2k}+3\equiv 0$ (*mod* 11), так как 32 ≡ -1(*mod* 11). Из того, что $M>11$ и 11| M, следует, что M – составное число. **23.** *Решение.* Предварительно покажем, что если *(a, m) = k,* то и *(b, m) = k.* Из сравнения $a\equiv b\ (mod\ m)$ следует $a=mt+b$, или $b=a-mt$, откуда видно, что если *(a, m) = k*, то $k\mid b$. Таким образом, если *(a, m)* = 1, то и *(b, m)* = 1. Умножая второе сравнение из условия задачи на *c*, получим: $ac\equiv bc\ (mod\ m)$. Тогда $bc\equiv bd\ (mod\ m)$, откуда, имея в виду, что *(b, m)* = 1, получаем $c\equiv d\ (mod\ m)$. **24.** *Решение.* По условию, $a^{100}\equiv 2$ (*mod* 73); умножив обе части этого сравнения на *a*, получаем: $a^{101}\equiv 2a$ (*mod* 73); но, по условию, $a^{101}\equiv 69$ (*mod* 73). Из этих сравнений следует, что $2a\equiv 69$ (*mod* 73). Прибавим к правой части $73:2a\equiv 142\left(mod\ 73\right)$. Так как (2, 73) = 1, то, сокращая члены сравнения на 2, получим: $a\equiv 71(mod\ 73)$. Остаток равен 73. **25.** *Решение.* Из условия следует, что $11a+2b\equiv 0$ (*mod* 19). Умножим обе части сравнения на 12: $132a+24b\equiv 0$ (*mod* 19), откуда $18a+5b\equiv 0$ (*mod* 19).

27. Составим из чисел 1, 2, 3, ... , $\underbrace{\frac{p-1}{2}}\ \underbrace{\frac{p+2}{2}}\ldots, p-2, p-1$

следующие $\frac{p-1}{2}$сравнений: 1 ≡ -(*p*-1) (*mod p*), 2 ≡ -(*p*-2) (*mod p*),

... , $\frac{p-1}{2}\equiv -\frac{p+1}{2}(mod\ p)$. Возводя каждое из этих сравнений в

степень $2k+1$ и складывая, получим требуемое сравнение.

§2.

28. $x\equiv$ 0; 1; 2; ... ; 9 (*mod* 10). **30.** а) $x\equiv$ 1; 3; 7; 9 (*mod* 10); b) $x\equiv$ 2; 4; 6; 8 (*mod* 10); c) $x\equiv$ 5 (*mod* 10); d) $x\equiv$ 0 (*mod* 10). **31.** а) При m = 9. Полные системы вычетов: 0, 1, 2, 3, 4, 5, 6, 7, 8; -8, -7, -6, -5, -4, -3, -2, -1, 0; -4, -3, -2, -1, 0, 1, 2, 3, 4. Приведенные системы вычетов: 1, 2, 4, 5, 7, 8; -8, -7, -5, -4, -2, -1; -4, -2, -1, 1, 2, 4. b) При m = 8. Полные системы вычетов: 0, 1, 2, 3, 4, 5, 6, 7; -7, -6, -5, -4, -3, -2, -1, 0; -3, -2, -1, 0, 1, 2, 3, 4 или -4, -3, -2, -1, 0, 1, 2, 3. Приведенные системы вычетов: 1, 3, 5, 7; -7, -5, -3, -1; -3, -1, 1, 3.

32. *Решение*. По общему виду всех чисел данного класса находим:
25 = 8·3 + 1; -20 = 8(-3) + 4; 16 = 8·2 + 0; 46 = 8·5 + 6; -21 = 8(-3) + 3; 18 = 8·2 + 2; 37 = 8·4 + 5; -17 = 8(-3) + 7. Полученные остатки все различны и составляют полную систему наименьших неотрицательных вычетов 0, 1, 2, 4, 5, 6, 7, следовательно, и данные числа составляют полную систему вычетов (только не наименьших). Можно было бы найти неположительные остатки, наименьшие по абсолютной величине или абсолютно наименьшие. **38.** *Решение*. Деля каждое число

на 6, получаем соответственно остатки: 0, 2, 1, 1, 4, 5, 2. Вычитая из каждого найденного неотрицательного вычета, кроме вычета нуль, величину модуля 6, получим 0, -4, -5, -5, -2, -1, -4 – наименьшие по абсолютной величине неположительные вычеты. Абсолютно наименьшими вычетами будут 0, 2, 1, 1, -2, -1, 2. **40.** Наименьшие неотрицательные вычеты: 0, 2, 1, 0, 100, 100; неположительные вычеты, наименьшие по абсолютной величине: 0, -5, -10, 0, -20, -100; абсолютно наименьшие вычеты: 0, 2, 1, 0, -20, 100 или –100. **42.** *Указание*. Записать данные числа в виде $a + x$ ($x = 0, 1, 2, \ldots, m$-1), где a – произвольное целое число, и применить теорему о вычетах линейной формы. **43.** *Указание*. Можно воспользоваться значениями x, составляющими полную систему остатков по модулю 10. **51.** *Решение.* По условию $x^4 \equiv 1 (mod\ 10)$, откуда $x^{12} \equiv 1\ (mod\ 10)$. **52.** *Решение*. а**)** Так как $(5, 24) = 1$ и $\varphi(24) = 8$, то должно быть $5^8 \equiv 1\ (mod\ 24)$. Действительно, $5^8 = (5^2)^4 = 25^4 \equiv 1^4 = 1\ (mod\ 24)$; с) *Решение* Так как $(3, 18) = 3 > 1$, то теорема Эйлера не имеет места. Действительно, $\varphi(18) = 6$ и $3^6 = 3^4 \cdot 3^2 = 81 \cdot 9 \equiv 9 \cdot 9 = 81 \equiv 9\ (mod\ 18)$. **53.** *Решение*. а**)** Так как $\varphi(6) = 2$, то $a^2 \equiv 1\ (mod\ 6)$. Удовлетворяют значения $a = 1$ и $a = 5$, взаимно простые с модулем 6, или классы чисел $6k + 1$ и $6k + 5$. **54.** *Решение*. b) Имеем $a^{12} \equiv b^{12} \equiv 1\ (mod\ 13)$ и $a^4 \equiv b^4 \equiv 1\ (mod\ 5)$, откуда $a^{12} \equiv b^{12} \equiv 1\ (mod\ 5)$; следовательно, $a^{12} \equiv b^{12} \equiv 1\ (mod\ 65)$ или $a^{12} - b^{12}$ делится на 65. **56.** *Указание*. Сложить почленно сравнения $i^{k(p-1)} \equiv 1\ (mod\ p)$, $i = 1, p - 1$. **57.** *Указание*. Использовать сравнение $a^p \equiv a\ (mod\ p)$. **59.** a) 1; b) 19; c) 29. **60.** a) 2; b) 6; c) 2; d) 2. **61.** 049. **62.** *Решение*. Пусть $\varphi(m) = P_m(a) \cdot q + r$, где $q \geq 0$ и $0 \leq r \leq P_m(a) - 1$. Из $a\ P_m(a) \equiv 1\ (mod\ m)$ следует $a^{\varphi(m)} \equiv a^r \equiv 1\ (mod\ m)$, откуда $r = 0$. **63.** *Указание*. Применить предыдущую задачу. **64.** *Указание*. Если $(x, p) = 1$, то $x^{(p-1)m} + x^{(p-1)n} \equiv 2\ (mod\ p)$. **65.** *Указание*. Так как $(m, 10) = 1$, то $10^{\varphi(m)} \equiv 1\ (mod\ m)$ или $10^{\varphi(m)} - 1 = 99\ldots9 \equiv 0\ (mod\ m)$. Так как $(9, m) = 1$, то части полученного сравнения можно разделить на 9. **66.** b) *Указание.* 1093 – простое число. **67.** *Решение*. Пусть $a^{p-1} - 1 = (a - 1)(a^{p-1} + a^{p-2} + \ldots + a + 1) \equiv 0\ (mod\ p)$. Так как $a^p \equiv a\ (mod\ p)$, поэтому $a^p - 1 \equiv a - 1 (mod\ p)$. Итак, если $a^p - 1 \equiv 0\ (mod\ p)$, то и $a - 1 \equiv 0\ (mod\ p)$. Из последнего сравнения имеем: $a^{p-1} \equiv 1\ (mod\ p)$, $a^{p-2} \equiv 1\ (mod\ p)$, $\ldots$, $a \equiv 1\ (mod\ p)$, $1 \equiv 1\ (mod\ p)$. Складывая эти сравнения, получим: $a^{p-1} + a^{p-2} + \ldots + a + 1 \equiv p \equiv 0\ (mod\ p)$ и, следовательно, $a^p - 1 \equiv 0\ (mod\ p^2)$. Аналогично находим, что если $a^p + 1 \equiv 0\ (mod\ p)$, то $a^p + 1 \equiv 0\ (mod\ p^2)$. **68.** *Решение*. По теореме Ферма $p^{q-1} - 1 \equiv 0\ (mod\ q)$, откуда $p^{q-1} - 1 = qt_1$. Аналогично, $q^{p-1} - 1 \equiv 0\ (mod\ p)$, откуда $q^{p-1} - 1 = pt_2$. Перемножая полученные равенства получим искомое сравнение. **69.** *Решение*. $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$. Имеем $x^{13} \equiv x\ (mod\ 13)$. Справедливость сравнений $x^{13} \equiv x\ (mod\ 2, 3, 5$ и $7)$ вытекает из сравнения задачи 58.

70. *Решение*. $a_i^5 \equiv a_i\ (mod\ 30)$, так как $a_i^5 \equiv a_i\ (mod\ 2, 3, 5)$ (см. задачу 58). Таким образом, $\sum_{i=1}^{n} a_i^5 \equiv \sum_{i=1}^{n} a_i \equiv 0\ (mod\ 30)$. **71.** *Решение*. Имеем

$m - \left[\frac{m}{2}\right] = m - \frac{m-1}{2} = \frac{m+1}{2}$. Пусть при делении $2^{\varphi(m)-1} \equiv r\ (mod\ m)$. или $2^{\varphi(m)} - 1 \equiv 2r - 1 (mod\ m)$. Но по теореме Эйлера $2^{\varphi(m)-1} \equiv r\ (mod\ m)$. Следовательно, и $2r - 1 \equiv 0\ (mod\ m)$ что дает $2r - 1 = mt, r = \frac{mt+1}{2}$, $r = \frac{m+1}{2}$. **72.** *Решение*. По условию, $(a, 10) = 1$, но тогда $(a, 5) = 1$ и $(a, 2) = 1$. Имея в виду, что

1000 = 125·8, используем сравнения по модулю 125 и по модулю 8. Из решения примера 7: $a^{100} \equiv 1$ (*mod* 125). С другой стороны , по теореме Эйлера $a^4 \equiv 1$ (*mod* 8); возводя это сравнение в 25-ю степень, получим $a^{100} \equiv 1$ (*mod* 8). Отсюда $a^{100} \equiv 1$ (*mod* 1000). Возведя это сравнение в *n*-ю степень и затем умножая обе части сравнения на *a*, получим: $a^{100n+1} \equiv a$ (*mod* 1000). **73.** *Решение*. Так как 19·73 – 1 = 1386 = 18·77. По теореме Ферма $2^{18} \equiv 1$ (*mod* 19). Тогда $2^{18 \bullet 77} = 2^{19 \bullet 73 - 1} \equiv 1$ (*mod* 19). Так как $2^9 = 512 \equiv 1$ (*mod* 73), то $2^{9 \bullet 154} = 2^{19 \bullet 73-1} \equiv 1$ (*mod* 73). Отсюда $2^{19 \bullet 73 - 1} \equiv 1$ (*mod* 19·73). **74.** *Указание*. Перемножить почленно $p_1^{p_2-1} - 1 = p_2 \cdot q_1$ и $p_1^{p_1-1} - 1 = p_1 \cdot q_2$, где $q_1, q_2 \in \boldsymbol{Z}$. **75.** *Решение*. Так как (2*p* + 1, 3) = 1, то $(2p + 1)^2 \equiv 1$ (*mod* 3), откуда 4*p* + 1 ≡ 0 (*mod* 3). **76.** *Решение*. По условию $a^{\varphi(m)} \equiv 1 (mod\ m)$ и $\alpha_1 = \alpha_2 + \varphi(m) \cdot q$. Следовательно, $a^{\alpha_2 + \varphi(m) q} \equiv a^{\alpha_2} (mod\ m)$ или $a^{\alpha_1} \equiv a^{\alpha_2} (mod\ m)$. **77.** *Решение*. Если *a* не кратно 7, то (*a*, 7) = 1, тогда $a^6 \equiv 1$ (*mod* 7). Отсюда: $a^{6m} \equiv 1$ (*mod* 7) и $a^{6n} \equiv 1$ (*mod* 7). Складывая эти сравнения, получим: $a^{6m} + a^{6n} \equiv 2$ (*mod* 7). Отсюда следует требуемое. **78.** *Решение*. Если (*n*, 6) = 1, то (*n*, 2) = 1. Отсюда *n* – нечетное число, значит, (*n* – 1) (*n* + 1) делится на 8 как произведение двух последовательных четных чисел, т.е. $n^2 - 1 \equiv 0$ (*mod* 8), или $n^2 \equiv 1$ (*mod* 8). С другой стороны, из (*n*, 6) = 1 следует, что (*n*, 3) = 1. Поэтому $n^2 \equiv 1$ (*mod* 3). Из полученных сравнений следует, что $n^2 \equiv 1$ (*mod* 24). **79.** *Решение*. Легко проверить, что $p \neq 5$. Итак, $5^{p-1} \equiv 1$ (*mod p*), откуда $5^{p^2-1} \equiv 1$ (*mod p*) и $5^{p^2} + 1 \equiv 6$ (*mod* 6). Так как необходимо, чтобы 6 ≡ 0 (*mod p*), то значение *p* следует искать среди чисел 2 и 3. Проверка показывает, что *p* = 3. **80.** *Решение*. Необходимо доказать, что $(x^3 - 1)x^3(x^3 + 1) \equiv 0$ (*mod* 504), или, что то же $x^2(x^7 - x) \equiv 0$ (*mod* 7·8·9). Но $x^7 - x \equiv 0$ (*mod* 7) при любом $x \in \boldsymbol{Z}$, следовательно, и $(x^3 - 1)x^3(x^3 + 1) \equiv 0$ (*mod* 7). В то же время $(x^3 - 1)x^3(x^3 + 1) \equiv 0$ (*mod* 8), как при четном, так и при нечетном *x*, и так как $\varphi(9) = 6$, то $x^3(x^6 - 1) \equiv 0$ (*mod* 9). Отсюда: $(x^3 - 1)x^3(x^3 + 1) \equiv 0$ (*mod* 504). **81.** *Решение*. По условию, *p* и 2*p* + 1 – простые, поэтому $(2p + 1)^2 \equiv 1 (mod\ 3)$, $p^2 \equiv 1 (mod\ 3)$. Умножим второе сравнение на 4 и вычтем из первого, тогда 4*p* + 1 ≡ - 3 ≡ 0 (*mod* 3), т.е. 4*p* + 1 – составное число (делится на 3). **82.** a) $x_1 \equiv 1 (mod\ 3)$, $x_2 \equiv 2$ (*mod* 3); b) $x_1 \equiv 1 (mod\ 5)$, $x_2 \equiv 2$ (*mod* 5); c) $x \equiv 2$ (*mod* 5); d) решений нет; e) $x \equiv 3$ (*mod* 5); f) $x_1 \equiv 1 (mod\ 4)$, $x_2 \equiv 3$ (*mod* 4); g) $x_1 \equiv 1 (mod\ 5)$, $x_2 \equiv 3$ (*mod* 5). **83.** a) $x \equiv 3$ (*mod* 7); b) $x \equiv 2$ (*mod* 5); c) $x \equiv -3$ (*mod* 11); d) $x \equiv -3$ (*mod* 7); e) $x \equiv -1$ (*mod* 7); f) $x \equiv -4$ (*mod* 15). **86.** a) $x \equiv 11$ (*mod* 15); b) $x \equiv 2$ (*mod* 8); c) $x \equiv 4$ (*mod* 13); d) $x \equiv 20$ (*mod* 37); e) $x \equiv 7$ (*mod* 25); f) $x \equiv 5$ (*mod* 11); g) $x \equiv 5$ (*mod* 11); h) $x \equiv 11$ (*mod* 24). **91.** *Решение*. Введя подстановку $x = y + \alpha$, получаем: $(y + \alpha)^n + a_1(y + \alpha)^{n-1} + ... + a_n \equiv 0 (mod\ m)$. После преобразований будем иметь: $y^n + (n\alpha + a_1) y^{n-1} + ... + (\alpha^n + a_1\alpha^{n-1} + ... + a_n) \equiv 0 (mod\ m)$. Выбираем α такое, чтобы было $n\alpha + a_1 \equiv 0 (mod\ m)$. В результате член содержащий y^{n-1} исключается из сравнения и мы получаем сравнение: $y^n + b_1y^{n-2} + ... + b_n \equiv 0 (mod\ m)$. **92.** *Решение*. Составляем сравнение $n\alpha + a_1 \equiv 0 (mod\ m)$. Из условия имеем: $3\alpha + 5 \equiv 0$ (*mod* 13), его решение: $\alpha \equiv 7$ (*mod* 13), следовательно, для подстановки берем $x = y + 7$. Подставляя в сравнение, получаем: $(y + 7)^3 + 5(y + 7)^2 + 6(y + 7) - 8 = y^3 + 26y^2 + 223y + 622 \equiv y^3 + 2y - 2 \equiv 0$ (*mod* 13). **94.** a) Решения нет, так как (5, 10) = 5, но 7 не делится на 5. b) $x \equiv 7 (mod\ 13)$; c) $x \equiv 8$ (*mod* 17); d) $x \equiv 9$ (*mod* 19); e) $x \equiv 11$ (*mod* 58). **94.** a) $x \equiv 6 (mod\ 19)$; b) решения нет; c) $x \equiv 49$ (*mod* 153); d) $x \equiv 3$ (*mod* 183); e) $x \equiv 47$ (*mod*

241). f) решений нет; g) $x \equiv 41, 190, 339$ (*mod* 447); h) $x \equiv 61, 248$ (*mod* 422); i) $x \equiv 39, 196, 353$ (*mod* 471). **95.** a) Решения нет; b) $x \equiv 3, 8, 13, 18, 23$ (*mod* 25); c) $x \equiv 73$ (*mod* 177); d) $x \equiv 29$ (*mod* 311); e) $x \equiv 48$ (*mod* 219); f) $x \equiv 9, 32, 55, 78, 101, 124$ (*mod* 138); g) $x \equiv 11, 28, 45$ (*mod* 51). **96.** *Решение*. a) $ax \equiv b$ (*mod* 21), где $(a, 21) = 1$, $b \in \boldsymbol{Z}$; b) для того чтобы сравнение $ax \equiv b$ (*mod* 21) имело, например, 3 решения, необходимо и достаточно, чтобы $(a, 21) = 3$ и b делилось бы на 3; c) такого сравнения составить нельзя. **97.** 1 июня. **98.** *Решение*. Обозначим приписываемое число через x, тогда $523 \cdot 10^3 + x \equiv 0$ (*mod* $7 \cdot 8 \cdot 9$), откуда $x \equiv -523000 \equiv -352 \equiv 152$ (*mod* 504), или класс чисел $x = 504t + 152$. Значение x будет трехзначным числом при $t = 0$ и $t = 1$. Получаем $x_1 = 152$, $x_2 = 656$. **99.** $x \equiv 200$ (*mod* 440), т.е. $x \equiv 200; 640$. **100.** $x \equiv 30$ (*mod* 31), т.е. $x = 30, 61, 42$. **101.** a) $x = 3 + 4t$, $y = 1 - 3t$; b) $x = 3 + 13t$, $y = -3 + 8t$; c) $x = 22 - 37t$, $y = -25 + 43t$; d) $x = 17 + 37t$, $y = 20 + 45t$; e) $x = 1 + 16t$, $y = 1 + 27t$; f) неразрешимо; g) $x = 4 + 17t$, $y = -11 - 53t$; h) $x = 47 + 105t$, $y = 21 + 47t$; i) неразрешимо; j) $x = 4 + 16t$, $y = 7 - 11t$; k) $x = 9 + 37t$, $e = 3 + 12t$; l) $x = -7 + 15t$, $y = 12 - 23t$. **102.** $x = 2 - 4t$, $y = 4 + 3t$. При $t = 0$ и $t = -1$ получаем требуемое. **103.** $x = 3 - 5t$, $y = 28 + 3t$. **104.** a) $x = -4 + 13t$, $-100 < -4 + 13t < 150$, $-7 \le t \le 11$; 19 точек; b) 7 точек; c) 8 точек. **105.** *Решение*. Имеем $5a - 9b = 31$ или $5a \equiv 31$ (*mod* 9). Наименьшее натуральное значение a, удовлетворяющее этому условию, есть $a = 8$. Соответствующее значение b есть $b = 1$. **106.** *Указание*. Следует из того, что угловой коэффициент прямой AB, т.е. $\frac{y_1 - y_2}{x_1 - x_2}$, есть сократимая дробь; случай, когда $x_1 = x_2$ очевиден. **107.** Согласно предыдущей задаче (учитывая еще вершины треугольника) искомое число целых точек равно $(18, 6) + (12, 8) + (6, 14) + 3 = 12$. **108.** a) $9x \equiv 1$ (*mod* 7), откуда $x = 4 + 7t$; b) $x = 13 + 15t$. **109.** *Решение*. По условию $15x + 20y + 30z = 500$ и $x + y + z = 18$, откуда $y + 3z = 46$, $y \equiv 1$ (*mod* 3) или $y = 1 + 3t$. Значит, $3z = 45 - 3t$ и $z = 15 - t$. Теперь имеем $x + 16 + 2t = 18$ или $x = 2 - 2t$. Натуральное решение имеем только при $t = 0$. Следовательно, $x = 2$, $y = 1$, $z = 15$.

§ 4.

110. a) $x \equiv 49$ (*mod* 420); b) $x \equiv 4126$ (*mod* 6300); c) $x \equiv 85056$ (*mod* 130169); d) $x \equiv 9573$ (*mod* 13923); e) решений нет; f) решений нет; g) решений нет; h) $x \equiv 17$ (*mod* 90); i) $x \equiv 4$ (*mod* 105); j) $x \equiv 7777777$ (*mod* 91290457). **111.** $x \equiv 25$ (*mod* 60). **112.** 299 и 439. **113.** *Указание.* Следует решить систему сравнений: $4x \equiv 9$ (*mod* 7); $2x \equiv 15$ (*mod* 9); $5x \equiv 12$ (*mod* 13), откуда $x \equiv 291$ (*mod* 819). Ординаты точек находятся с помощью данных уравнений прямых. **114.** a) $x \equiv 4a - 3$ (*mod* 24), где $a \equiv 1$ (*mod* 2); b) $x \equiv 8 - 3a$ (*mod* 24), где $a \equiv 0$ (*mod* 2); c) $x \equiv 36a - 175$ (*mod* 630), где $a \equiv 1$ (*mod* 7); d) $x \equiv 15a + 21b - 35c$ (*mod* 105). **115.** a) $a \equiv 5$ (*mod* 6); b) $a \equiv 1$ (*mod* 6); c) $a \equiv 0$ (*mod* 4). **116.** *Решение*. Из условия имеем систему сравнений: $xyz138 \equiv 0$ (*mod* 7), $138xyz \equiv 6$ (*mod* 13), $x1y3z8 \equiv 5$ (*mod* 11). Первое сравнение запишем в виде: $10^3xyz + 138 \equiv 0$ (*mod* 7). Тогда $3xyz \equiv 1$ (*mod* 7), откуда $xyz \equiv 5$ (*mod* 7). Аналогично поступим со вторым сравнением: $138000 + xyz \equiv 6$ (*mod* 113), откуда $xyz \equiv 1$ (*mod* 13). Решая систему сравнений: $xyz \equiv 1$ (*mod* 13), $xyz \equiv 5$ (*mod* 7) относительно xyz, получаем $xyz \equiv 40$ (*mod* 91), или $xyz = 91t + 40$. Полагая $t = 1, 2, 3,$

... , 10, находим: xyz = 131, 222, 313, ... , 950. Теперь третье сравнение системы представим в виде: $x\cdot10^5 + 10^4 + y\cdot10^3 + 3\cdot10^2 + z\cdot10 + 8 \equiv 5$ (*mod* 11), или после упрощений $x + y + z \equiv 7$ (*mod* 11), т.е. $x + y + z = 11t + 7$. Учитывая, что $0 < x + y + z < 27$, имеем: $x + y + z = 7$ и $x + y + z = 18$. Тогда из ряда чисел 131, 222, 313, ... , 950, находим два числа удовлетворяющие условию: 313138 и 495138. **117.** *Решение*. По условию $13xy45z \equiv 0$ (*mod* 792), но $792 = 8\cdot9\cdot11$, поэтому можно написать систему:

$$\left.\begin{array}{l} 13xy45z \equiv 0 \ (mod\ 8) \\ 13xy45z \equiv 0 \ (mod\ 9) \\ 13xy45z \equiv 0 \ (mod\ 11) \end{array}\right\}.$$

Из первого сравнения по признаку делимости на 8 имеем: $450 + z \equiv 0$ (*mod* 8), откуда $z \equiv 6$ (*mod* 8). Подставляя $z = 6$ во второе и третье сравнения, получаем систему:

$$\left.\begin{array}{l} 13xy456 \equiv 0 \ (mod\ 9) \\ 13xy456 \equiv 0 \ (mod\ 11) \end{array}\right\}$$

Из первого сравнения этой системы по признаку делимости на 9 имеем: $x + y + 19 \equiv 0$ (*mod* 9), или $x + y \equiv 0$ (*mod* 9). Второе сравнение системы представим в виде: $1300000 + x\cdot10^4 + y\cdot10^3 + 456 \equiv 0$ (*mod* 11), или после упрощения $x - y \equiv 8$ (*mod* 11). Тогда

$$\left.\begin{array}{l} x + y = 9t_1 + 8 \\ x - y = 11t_2 + 8 \end{array}\right\}$$

Теперь легко видеть, что $x = 8$ и $y = 0$. Таким образом, искомое число 1380456.

118. *Решение*. Обозначим через x искомое число. Тогда $x\cdot1000+(x+1)=1001x+1=N^2$, или $(N+1)(N-1)=7\cdot11\cdot13x$, откуда

$$x = \frac{(N+1)(N-1)}{7\cdot11\cdot13}.$$

Из этого равенства для определения N и x имеем ряд систем сравнений:

1) $\left.\begin{array}{l} N+1\equiv0 \ (mod\ 7) \\ N-1\equiv0 \ (mod\ 143) \end{array}\right\}$

Решая систему обычным путем, находим N=573, N^2=328329, x_1=328.

2) $\left.\begin{array}{l} N+1\equiv0 \ (mod\ 143) \\ N-1\equiv0 \ (mod\ 7) \end{array}\right\}$.

Откуда N=428, N^2=183184, x_2=183.

3) $\left.\begin{array}{l} N+1\equiv0 \ (mod\ 11) \\ N-1\equiv0 \ (mod\ 91) \end{array}\right\}$.

Откуда N=274, N^2=075076, но x=075 не является решением, как число двузначное.

4) $\left.\begin{array}{l} N+1\equiv0 \ (mod\ 91) \\ N-1\equiv0 \ (mod\ 11) \end{array}\right\}$

Получаем N=727, N^2=528529, x_3=528.

5) $\left.\begin{array}{l} N+1\equiv0 \ (mod\ 13) \\ N-1\equiv0 \ (mod\ 77) \end{array}\right\}$

N=155, N^2=024025, но x=025 не является решением, как число двузначное.

6) $\left.\begin{array}{l} N+1\equiv0 \ (mod\ 77) \\ N-1\equiv0 \ (mod\ 13) \end{array}\right\}$

Откуда N=846, N^2=715716, x_4=715.

119. Из условия получаем систему: $x\equiv 3\ (mod\ 7)$, $x^2\equiv 44\ (mod\ 7^2)$, $x^3\equiv 111\ (mod\ 7^3)$. Из первого сравнения имеем: $x=7t+3$. Подставляем найденное значение x во второе сравнение и решаем последнее относительно t: $(7t+3)^2=44\ (mod\ 7^2)$, или после упрощения, $42t\equiv 35\ (mod\ 7^2)$. Сокращая на 7, получаем $6t\equiv 5(mod\ 7)$, откуда $t\equiv 2\ (mod\ 7)$, т.е. $t=7t_1+2$. Подставим это значение t в равенство $x=7t+3$, тогда: $x=7(7t_1+2)+3=49t_1+17$. Теперь, подставляя x в третье сравнение системы, имеем: $(49t_1+17)^3\equiv 111(mod\ 7^3)$. После возведения в куб и упрощения находим: $t_1\equiv 0\ (mod\ 7)$, откуда $t_1=7t_2+0$. Подставляя это значение t_1 в равенство $x=49t_1+17$, окончательно получаем: $x\equiv(mod\ 7^3)$. **120.** a) $x\equiv 24\ (mod\ 28)$; b) $x\equiv 54\ (mod\ 95)$; c) $x\equiv 39\ (mod\ 77)$; d) $x\equiv -9\ (mod\ 45)$; e) решений нет; f)$x\equiv\pm 13;\ \pm 47\ (mod\ 85)$. **121.** (-6,-61), (-1,-1), (1,1), (6,41). **122.** a) $x\equiv y\equiv 3\ (mod\ 7)$; b) решений нет; c) решений нет; d) $x_1\equiv 0(mod\ 12)$, $y_1\equiv 7(mod\ 12)$ $x_2\equiv 4\ (mod\ 12)$, $y_2\equiv 7\ (mod\ 12)$; $x_3\equiv 8\ (mod\ 12)$, $y_3\equiv 7\ (mod\ 12)$. **123.** a) $x=k+5n$, $y=2k-2+10n$, $z=1-k-5n$, где k=0; 1; 2; 3; 4 и $n\in Z$; b) имеем систему сравнений $x-y\equiv 1\ (mod\ 3)$, $x+y\equiv 1(mod\ 2)$. Из первого сравнения $y\equiv x-1+3i\ (mod\ 6)$, где i=0; 1. Подстановка во второе сравнение системы дает $2x\equiv 2-3i\ (mod\ 2)$, откуда $3i\equiv 0\ (mod\ 2)$ и i=0. Следовательно, $x\equiv k(mod\ 6)$, $y\equiv k-1\ (mod\ 6)$, k=0; 1; 2; 3; 4; 5, или $x=k+6n$, $y=k-1+6m$, где $m,\ n\in Z$. Подставляя в уравнения, имеем $z=2n-2m=k-1+3n+3m$, откуда $n=1-k-5m$. Таким образом, решения данной системы уравнений имеют вид: $z=6-5k-30m$, $y=k-1+6m$, $x=2-2k-12m$, где k=0; 1; 2; 3; 4; 5 и $m\in Z$. **124.** *Указание*. Задачу можно решить при помощи системы сравнений:

$$\begin{cases} 3x - y + 1 \equiv 0\ (mod\ 7) \\ 2x + 3y - 1 \equiv 0\ (mod\ 7), \end{cases} \quad \text{откуда} \quad \begin{cases} x \equiv 3\ (mod\ 7) \\ y \equiv 5\ (mod\ 7). \end{cases}$$