МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВПО «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

М. И. Черемисина

ИЗБРАННЫЕ ВОПРОСЫ АЛГЕБРЫ И ТЕОРИИ ЧИСЕЛ

Сравнения. Цепные дроби. Квадратичные вычеты

Учебно-методическое пособие

Оренбург
Издательство ОГПУ
2016

УДК 512 (075.8)
ББК 22.14я73
Ч46

Рецензенты

И. В. Прояева, кандидат физико-математических наук, доцент кафедры алгебры, геометрии и истории математики ОГПУ

Н. А. Мунасыпов, кандидат физико-математических наук, доцент кафедры математического анализа и методики преподавания математики ОГПУ

Черемисина, М. И.

Ч46 **Избранные вопросы алгебры и теории чисел. Сравнения. Цепные дроби. Квадратичные вычеты** : учебно-методическое пособие / М. И. Черемисина ; Мин-во образования и науки Рос. Федерации, ФГБОУ ВПО «Оренб. гос. пед. ун-т». — Оренбург : Изд-во ОГПУ, 2016. — 28 с. ISBN 978-5-85859-625-7.

Учебно-методическое пособие посвящено ряду важных разделов алгебры и теории чисел и сочетает обучающие и контролирующие функции. Методические указания к выполнению каждого типа заданий позволяют студентам лучше ориентироваться в теоретическом материале и способствуют наиболее рациональному выбору решения каждой задачи. Издание окажется полезным студентам высших учебных заведений и колледжей (в первую очередь педагогических), учителям математики и учащимся старших классов средних школ.

УДК 512 (075.8)
ББК 22.14я73

ISBN 978-5-85859-625-7

ОГЛАВЛЕНИЕ

Введение

Учебно-методическое пособие посвящено важным разделам алгебры и теории чисел: «Сравнения по простому и составному модулям», «Цепные дроби». Изложенный в пособии материал поможет студентам физико-математических факультетов в изучении следующих разделов:

1. Сравнения с одной неизвестной. Равносильность сравнений.
2. Системы сравнений.
3. Сравнения по составному модулю.
4. Цепные дроби. Периодические цепные дроби.
5. Квадратичные вычеты. Символ Лежандра. Критерий Эйлера.

Пособие сочетает обучающие и контролирующие функции. В связи с этим даются не только варианты контрольных работ (7 вариантов по 10 задач), но и предложен образец выполнения контрольной работы с подробным теоретическим обоснованием. Методические указания к выполнению каждого типа заданий позволяют студентам лучше ориентироваться в теоретическом материале и способствуют наиболее рациональному выбору решения каждой задачи.

Издание окажется полезным студентам высших учебных заведений и колледжей (в первую очередь педагогических), учителям математики и учащимся старших классов средних школ.

1. Сравнения с одной неизвестной. Равносильность сравнений

Определение. *Сравнением с неизвестной величиной x называется сравнение*

$$f(x) \equiv 0 \pmod{m},$$

где $f(x) = C_0x^n + C_1x^{n-1} + ... + C_n$ *— многочлен с целыми коэффициентами.*

Определение. *Решением сравнения* $f(x) \equiv 0 \pmod{m}$ *называется класс по модулю m, состоящий из чисел, удовлетворяющих этому сравнению.*

Чтобы решить сравнение $f(x) \equiv 0 \pmod{m}$, можно взять любую полную систему вычетов по модулю m: $x_1, x_2, ..., x_m$, вычислить $f(x_1), f(x_2), ..., f(x_m)$ и отобрать те x_i, при которых $f(x_i)$ делятся на m. Соответствующие классы $\overline{x_i}$ дадут все решения этого сравнения. Обычно в качестве $x_1, x_2, ..., x_m$ берут полную систему наименьших по абсолютной величине вычетов.

Примеры. Найти все решения следующих сравнений:

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

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 $x \equiv 5 \pmod{11}$.

2) $x^4 + 2x^3 + 6 \equiv 0 \pmod{8}$.

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

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

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 $x \equiv 2 \pmod{6}$.

С теоретической точки зрения задача решения сравнений вида $f(x) \equiv 0 \pmod{m}$ проста, на практике указанный прием испытания вычетов при больших модулях оказывается затруднительным, так как приводит к большому ко-

личеству испытаний. Например, для решения сравнения $9x^3+13x^2-2x+17\equiv 0 \pmod{625}$ надо проверить 625 вычетов.

Существуют способы, позволяющие найти число решений сравнения, а в ряде случаев и все решения значительно быстрее.

Определение. *Два сравнения:* $f_1(x)\equiv\varphi_1(x) \pmod m$ *и* $f_2(x)\equiv\varphi_2(x) \pmod m$ *— называются равносильными (эквивалентными), если множество чисел, удовлетворяющих одному из них, совпадает с множеством чисел, удовлетворяющих другому сравнению.*

Теоремы равносильности сравнений позволяют производить упрощение сравнений: все коэффициенты сравнения $f(x)\equiv 0 \pmod m$ можно заменить соответствующими вычетами, обычно наименьшими неотрицательными или абсолютно наименьшими вычетами по модулю m.

Пример. Решить сравнение:

$$21x^3+17x^2+9x+30\equiv 0 \pmod 7.$$

Решение. $21\equiv 0 \pmod 7$, $17\equiv 0 \pmod 7$, $9\equiv 2 \pmod 7$, $30\equiv 2 \pmod 7$.

Данное сравнение можно заменить более простым равносильным ему сравнением: $3x^2+2x+2\equiv 0 \pmod 7$. Проверяя теперь вычеты полной системы абсолютно наименьших вычетов 0, 1, 2, 3, –3, –2, –1, находим решения данного сравнения: классы $x\equiv 1 \pmod 7$ и $x\equiv 3 \pmod 7$.

Заметим, что равносильные сравнения не обязательно должны иметь одну и ту же степень. Например: $3x-1\equiv 0 \pmod 2$ и $3x^3+4x^2+x-2\equiv 0 \pmod 2$ — равносильные сравнения, хотя имеют разные степени. Если модуль $m = p$ — простое число, то для понижения степени сравнения можно воспользоваться теоремой Ферма:

$$x^p \equiv x \pmod p.$$

Пример. Заменить сравнение

$$2x^8+6x^7-x^6+2x^5+3x^4-x^3+4x^2+8x-1\equiv 0 \pmod 5$$

равносильным сравнением более низкой степени.

Так как $x^5 \equiv x \pmod 5$, то $x^6 \equiv x^2 \pmod 5$, $x^7 \equiv x^3 \pmod 5$, $x^8 \equiv x^4 \pmod 5$, то данное сравнение равносильно сравнению:

$$2x^4 + 6x^3 - x^2 + 2x + 3x^4 - x^3 + 4x^2 + 8x - 1 \equiv 0 \pmod 5,$$

т.е. сравнению:

$$5x^4 + 5x^3 + 3x^2 + 10x - 1 \equiv 0 \pmod 5,$$

или, что то же самое, $3x^2 - 1 \equiv 0 \pmod 5$.

2. Системы сравнений

Рассмотрим систему сравнений вида:

$$\begin{cases} f_1(x) \equiv 0 \pmod{m_1}, \\ f_2(x) \equiv 0 \pmod{m_2}, \\ \qquad\qquad f_i(x) \in Z[x]. \\ \ldots \\ f_s(x) \equiv 0 \pmod{m_s}. \end{cases} \qquad (1)$$

Определение. *Решением системы сравнений* (1) *называется класс чисел по* $\bmod M = [m_1, m_2, \ldots, m_s]$, *удовлетворяющих всем сравнениям системы* (1). *Следовательно, число решений* (1) *равно числу классов по* $\bmod M$, *удовлетворяющих системе сравнений* (1).

Рассмотрим систему сравнений с одним неизвестным первой степени.

Рассмотрим систему вида:

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ x \equiv c_2 \pmod{m_2}. \end{cases} \qquad (2)$$

***Теорема* 1.** *Пусть* $(m_1, m_2) = d$; $[m_1, m_2] = M$. *Тогда если* $(c_2 - c_1) \not\vdots d$, *то система* (2) *не имеет решения; если* $(c_2 - c_1) \vdots d$, *то система* (2) *имеет единственное решение — класс чисел по* $\bmod M$.

Замечание. Если $(m_1, m_2) = 1$, то $M = m_1 \cdot m_2$, тогда система (2) всегда имеет одно решение — класс по $\bmod m_1 \cdot m_2$.

***Теорема* 2.** *Система*

$$\begin{cases} x \equiv c_1 \pmod{m_1}, \\ \ldots, \\ x \equiv c_s \pmod{m_s} \end{cases} \qquad (3)$$

либо не имеет решений, либо имеет одно решение.

Если система (3) имеет решение, то его можно найти, решив сначала первые два сравнения, добавив потом последовательно третье, и т.д., пока не будет исчерпана вся система.

***Теорема* 3.** *Если* $m_1, m_2, \ldots, m_s$ *— попарно взаимно простые числа, то система* (3) *совместна и имеет одно решение — класс по* $M = m_1 \cdot m_2 \cdot \ldots \cdot m_s$.

Для нахождения решения системы сравнений первой степени с взаимно простыми модулями можно воспользоваться теоремой:

***Теорема* 4.** *Пусть* $m_1, m_2, \ldots, m_s$ *— попарно взаимно простые числа,* $M = m_1 \cdot m_2 \cdot \ldots \cdot m_s$, $y_1, y_2, \ldots, y_s$ *подобраны так, что*

$$\frac{M}{m_1} y_1 \equiv 1 \pmod{m_1}, \quad \frac{M}{m_2} y_2 \equiv 1 \pmod{m_2}, \ \ldots, \ \frac{M}{m_s} y_s \equiv 1 \pmod{m_s}.$$

Тогда решение системы (3) *имеет вид:* $x \equiv x_0 \pmod{M}$, *где*

$$x_0 = \frac{M}{m_1} y_1 c_1 + \frac{M}{m_2} y_2 c_2 + \ldots + \frac{M}{m_s} y_s c_s .$$

Пример. Решить систему сравнений: $\begin{cases} x = 6 \pmod{17}, \\ x = 4 \pmod{11}, \\ x = -3 \pmod{8}. \end{cases}$

Согласно теореме 4,

$11 \cdot 8 \cdot y_1 \equiv 1 \pmod{17}, \quad 3y_1 \equiv 1 \pmod{17}, \quad y_1 = 6,$

$17 \cdot 8 \cdot y_2 \equiv 1 \pmod{11}, \rightarrow \ 4y_2 \equiv 1 \pmod{11}, \rightarrow \ y_2 = 3,$

$17 \cdot 11 \cdot y_3 \equiv 1 \pmod{8} \quad 3y_3 \equiv 1 \pmod{8} \quad y_3 = 3,$

$x_0 = 11 \cdot 8 \cdot 6 \cdot 6 + 17 \cdot 8 \cdot 3 \cdot 4 + 17 \cdot 11 \cdot 3 \cdot (-3) \equiv 3117 \equiv$

$\equiv 125 \pmod{17 \cdot 11 \cdot 8},$

$x \equiv 125 \pmod{1496}$ — искомое решение системы.

Рассмотрим систему сравнений первой степени общего вида:

$$\begin{cases} a_1 x = b_1 \pmod{m_1}, \\ a_2 x = b_2 \pmod{m_2}, \\ \ldots \\ a_s x = b_s \pmod{m_s}. \end{cases} \qquad (4)$$

Если хотя бы при одном i ($i = \overline{1, S}$) для $(a_i, m_i) = d_i$, $b_i \not\vdots d_i$, то система несовместна. Если же для всех i $b_i \vdots d_i$, то каждое сравнение можно решить относительно x и заменить систему (4) эквивалентной ей системой

$$\begin{cases} x \equiv c_1 \pmod{\dfrac{m_1}{d_1}}, \\ x \equiv c_2 \pmod{\dfrac{m_2}{d_2}}, \\ \ldots \\ x \equiv c_s \pmod{\dfrac{m_s}{d_s}}. \end{cases} \qquad (5)$$

Решение системы (5) есть класс по

$$\text{mod } M = \left[\frac{m_1}{d_1}, \frac{m_2}{d_2}, \ldots, \frac{m_s}{d_s} \right].$$

Пример. Решить систему сравнений:

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

Решая каждое сравнение системы в отдельности, получим эквивалентную ей систему сравнений:

$$\begin{cases} x \equiv 2 \pmod{11}, \\ x \equiv 5 \pmod{7}, \\ x \equiv 4 \pmod{5}, \end{cases} \quad \begin{cases} 7 \cdot 5 y_1 \equiv 1 \pmod{11}, \\ 11 \cdot 5 y_2 \equiv 1 \pmod{7}, \\ 7 \cdot 11 y_3 \equiv 1 \pmod{5}, \end{cases} \quad \rightarrow \quad \begin{array}{l} y_1 = 6, \\ y_2 = -1, \\ y_3 = 3, \end{array}$$

$$x_0 = 7 \cdot 5 \cdot 6 \cdot 2 + 11 \cdot 5 \cdot 5 \cdot (-1) + 7 \cdot 11 \cdot 4 \cdot 3 \equiv 299 \pmod{11 \cdot 7 \cdot 5}.$$

$x \equiv 299 \pmod{385}$ или $x \equiv -86 \pmod{385}$ — искомое решение системы.

Рассмотрим еще один способ решения. Пусть дана система (4) и первое сравнение системы имеет решение, тогда решение первого сравнения можно записать в виде:

$$x = x_1 + \frac{m_1}{d_1} \cdot y \ \ (y \in Z) \ \ (*), \quad d_1 = (a_1,\, m_1)\,.$$

Подставим это решение (*) во второе сравнение системы:

$$a_2\left(x_1 + \frac{m_1}{d_1}\, y\right) \equiv b_2 \pmod{m_2}\,,$$

получим сравнение:

$$\underbrace{\frac{a_2 m_1}{d_1}}_{a'_2} \cdot y \equiv \underbrace{b_2 - a_2 x_1}_{b'_2} \pmod{m_2} \Rightarrow a'_2 y \equiv b'_2 \pmod{m_2} \ \text{—}$$

оно или не имеет решения, или имеет решение относительно y.

Пусть $y = y_0 + \frac{m_2}{d_2} \cdot z \ \ (z \in Z)$, где $d_2 = (a'_2,\, m_2)$, подставим решение относительно y в выражение (*):

$$x = x_1 + \frac{m_1}{d_1} \cdot \left(y_0 + \frac{m_2}{d_2} z\right) = \underbrace{x_1 + \frac{m_1}{d_1}\, y_0}_{x_2} + \frac{m_1}{d_1}\frac{m_2}{d_2} z\,,$$

то есть $x = x_2 + \frac{m_1}{d_1}\frac{m_2}{d_2} \cdot z \ \ (z \in Z)$ есть решение первых двух сравнений системы, его подставим в третье сравнение системы (4) и т. д.

Продолжая этот процесс, на каком-то шаге придем к неразрешимому сравнению или получим решение вида:

$$x = x_s + \frac{m_1}{d_1}\frac{m_2 \ldots m_s}{d_2 \ldots m_s} \cdot t \ \ (t \in Z) \ \text{—}$$

решение системы (4), можно записать: $x \equiv x_s\left(\frac{m_1}{d_1}\frac{m_2 \ldots\, m_s}{d_2 \ldots\, d_s}\right)$.

Замечание: если $(a_i,\, m_i) = 1$, $i = \overline{1,\, S}$, и $m_1, m_2, \ldots, m_s$ — попарно взаимно простые, то система (4) разрешима и имеет решение: $x = x_s + m_1 m_2 \ldots m_s \cdot t \ \ (t \in Z)$.

Пример. Решим системы сравнений:

а) $\begin{cases} 3x \equiv 1 \pmod 5, \\ 5x \equiv 4 \pmod 7. \end{cases}$ Решение первого сравнения $x \equiv 2 \pmod 5 \to x = 2 + 5y$, $y \in Z$, подставим во второе срав-

нение и получим: $10+25y\equiv 4 \pmod 7$ или $4y\equiv 1 \pmod 7 \Rightarrow y\equiv 2 \pmod 7$, т. е. $y=2+7t$, $t\in Z$. Значит, $x=2+5(2+7t)=12+35t$, $t\in Z$, т.е. $x\equiv 12 \pmod{35}$ — искомое решение системы.

б) $\begin{cases} 2x\equiv 31 \pmod{35}, \\ 4x\equiv 7 \pmod{25}, \\ 5x\equiv 18 \pmod{21}. \end{cases}$

Решая каждое сравнение в отдельности, получим следующую систему:

$$\begin{cases} x\equiv -2 \pmod{35}, \\ x\equiv 8 \pmod{25}, \\ x\equiv 12 \pmod{21}. \end{cases}$$

Первому сравнению удовлетворяют $x=-2+35t$, t — любое целое. Найдем, при каких значениях t верно второе сравнение:

$-2+35t\equiv 8 \pmod{25} \Rightarrow 35t\equiv 10 \pmod{25} \Rightarrow$

$t\equiv 1 \pmod 5 \Rightarrow t=1+5n,$

n — любое целое число.

Получили, что решениями системы первых двух сравнений являются:

$$x=-2+35(1+5n)=33+175n.$$

Найдем, при каких значениях n эти значения x удовлетворяют и третьему сравнению:

$33+175n\equiv 12 \pmod{21}$, $175n\equiv -21 \pmod{21}$,

$7n\equiv 0 \pmod{21} \Rightarrow n\equiv 0 \pmod 3 \Rightarrow n=3k$,

где k — любое целое число.

Итак, $x=33+175n=33+175(3k)=33+525k$ или $x\equiv 33 \pmod{525}$. Эти значения x являются решением системы.

3. Сравнения по составному модулю

Рассмотрим сравнения по составному модулю и приведение их к сравнениям по простому модулю. Рассмотрим $f(x)$ с целыми коэффициентами.

Теорема. *Если* $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$ — *каноническое представление* m, *то сравнение* $f(x) \equiv 0 \pmod{m}$ (1) *эквивалентно системе сравнений:*

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}}, \\ \ldots, \\ f(x) \equiv 0 \pmod{p_s^{\alpha_s}}. \end{cases} \qquad (2)$$

Для нахождения решений системы сравнений (2) решают каждое из сравнений системы. Если хотя бы одно не имеет решений, то система сравнений (2) несовместна, следовательно, сравнение (1) не имеет решений. Если каждое из сравнений (2) имеет хотя бы одно решение, то находим их в виде:

$$\begin{cases} x \equiv a_1 \pmod{p_1^{\alpha_1}}, \\ \ldots, \\ x \equiv a_s \pmod{p_s^{\alpha_s}}. \end{cases} \qquad (3)$$

Значения x, удовлетворяющие всем этим сравнениям с взаимно простыми модулями, существуют и образуют класс по $\bmod m$ — решение системы (2) и (1).

Если некоторые из сравнений (2) имеют больше чем по одному решению, то получим несколько систем вида (3), а именно, если $f(x) \equiv 0 \pmod{p_1^{\alpha_1}}$ имеет k_1 решений, $f(x) \equiv 0 \pmod{p_2^{\alpha_2}}$ — k_2 решений, ..., $f(x) \equiv 0 \pmod{p_s^{\alpha_s}}$ имеет k_s решений, то можно составить $k_1 \cdot k_2 \cdot \ldots \cdot k_s$ систем вида (3), каждая из которых дает одно решение системы (2) и тогда (2) и (1) имеют $k_1 \cdot k_2 \cdot \ldots \cdot k_s$ решений.

Мы доказали ***теорему***: *число решений сравнения* (1) *равно* $k_1 \cdot k_2 \cdot \ldots \cdot k_s$, *где* k_1, ..., k_s *соответственно равны числу решений каждого из сравнений системы* (2).

Пример. Найти решение сравнения:

$$x^2 - 3x + 23 \equiv 0 \pmod{63}.$$

$x^2 - 3x + 23 \equiv 0 \pmod{63}$ эквивалентно

$$\begin{cases} x^2 - 3x + 23 \equiv 0 \pmod 7, \\ x^2 - 3x + 23 \equiv 0 \pmod 9, \end{cases}$$

$x^2 - 3x + 23 \equiv 0 \pmod 7 \Leftrightarrow x^2 - 3x + 2 \equiv 0 \pmod 7$;

$\begin{matrix} x \equiv 1 \pmod 7, \\ x \equiv 2 \pmod 7 \end{matrix}$ — два решения первого сравнения;

$x^2 - 3x + 23 \equiv 0 \pmod 9 \Leftrightarrow x^2 - 3x + 5 \equiv 0 \pmod 9$;

$\begin{matrix} x \equiv 4 \pmod 9, \\ x \equiv 8 \pmod 9 \end{matrix}$ — два решения второго сравнения.

Решаем 4 системы:

(1) $\begin{cases} x \equiv 1 \pmod 7, \\ x \equiv 4 \pmod 9; \end{cases}$

(2) $\begin{cases} x \equiv 1 \pmod 7, \\ x \equiv 8 \pmod 9; \end{cases}$

(3) $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv 4 \pmod 9; \end{cases}$

(4) $\begin{cases} x \equiv 2 \pmod 7, \\ x \equiv 8 \pmod 9. \end{cases}$

Получим следующие решения систем:

(1) $x \equiv 22 \pmod{63}$;

(2) $x \equiv 8 \pmod{63}$;

(3) $x \equiv 58 \pmod{63}$;

(4) $x \equiv 44 \pmod{63}$.

Итак, исходное сравнение $x^2 - 3x + 23 \equiv 0 \pmod{63}$ имеет четыре решения — классы $\overline{8}$, $\overline{22}$, $\overline{44}$, $\overline{58}$ по модулю 63.

Рассмотрим сравнения по $\bmod p^2$, p — простое. Нахождение решений таких сравнений сводится к решению сравнений по простому модулю.

Теорема. *В каждом классе* $\overline{a}$ *по простому* $\bmod p$, *удовлетворяющем сравнению* $f(x) \equiv 0 \pmod p$, *таком что*

$f'(a) \not\equiv p$, *числа, удовлетворяющие сравнению* $f(x) \equiv 0 \pmod{p^k}$ $(k \geq 1)$, *образуют класс по* $\bmod p^k$.

Воспользуемся выводами из теоремы:

1. Для того чтобы, зная решение $x \equiv b \pmod{p^k}$ сравнения $f(x) \equiv 0 \pmod{p^k}$, причем $f'(b) \not\equiv p$, найти решение $x \equiv \gamma \pmod{p^{k+1}}$ сравнения $f(x) \equiv 0 \pmod{p^{k+1}}$, надо взять

$$\gamma = b + p^k \cdot t_0, \qquad (*)$$

где t_0 удовлетворяет сравнению

$$f'(b) \cdot t + \frac{f(b)}{p^k} \equiv 0 \pmod{p}. \qquad (**)$$

2. Теорема дает возможность для каждого решения $\overline{a}$ сравнения $f(x) \equiv 0 \pmod{p}$, причем $f'(a) \not\equiv p$, найти последовательно решения сравнений

$$f(x) \equiv 0 \pmod{p^2}, \ldots, f(x) \equiv 0 \pmod{p^\alpha}$$

при любом α.

Пример. Решить сравнение:

$x^3 - 2x^2 - 30x + 41 \equiv 0 \pmod{125}$.

Пусть

$$f(x) = x^3 - 2x^2 - 30x + 41,\ 125 = 5^3.$$

Решаем сначала: $f(x) \equiv 0 \pmod{5}$; его решение:

$$x \equiv 1 \pmod{5} \rightarrow \underline{b = 1}.$$

Составляем сравнение (**):

$$f'(1) \cdot t + \frac{f(1)}{5} \equiv 0 \pmod{5} \Rightarrow -31t + 2 \equiv 0 \pmod{5} \rightarrow$$

$$4t \equiv 3 \pmod{5},$$

$$\underline{t \equiv 2 \pmod{5}}.$$

Возьмем $t_0 = 2$ и найдем решение сравнения $f(x) \equiv 0 \pmod{p^2}$, т.е.

$$f(x) \equiv 0 \pmod{25},$$

в виде $x \equiv \gamma$, т. е.

$$x \equiv 1 + 5 \cdot 2 \pmod{25},\ \underline{x \equiv 11 \pmod{25}}.$$

Составляем сравнение (**):

$$f'(11)\cdot t+\frac{f(11)}{25}\equiv 0 \pmod 5,$$

то есть

$289t+32\equiv 0 \pmod 5$, $4t+2\equiv 0 \pmod 5 \to t\equiv 2 \pmod 5$,

в качестве $t'_0 = 2$.

Решение сравнения $f(x)\equiv 0 \pmod{125}$ имеет вид:

$$x\equiv 11+25\cdot 2 \pmod{125} \to x\equiv 61 \pmod{125}.$$

Ответ: $x\equiv 61 \pmod{125}$.

4. Цепные дроби

4.1. Найти величину цепной дроби:

1) $\alpha = 1+\frac{1}{3}\Big/+\frac{1}{1}\Big/+\frac{1}{3}\Big/+\ldots$

2) $\alpha = 3+\frac{1}{3}\Big/+\frac{1}{3}\Big/+\frac{1}{1}\Big/+\frac{1}{3}\Big/+\ldots$

Решение

1) Согласно теореме: «Пусть разложение α в цепную дробь имеет вид $\alpha = a_0+\frac{1}{a_1}\Big/+\frac{1}{a_2}\Big/+\ldots$». Введем обозначение: $\alpha'_s = a_s+\frac{1}{a_{s+1}}\Big/+\ldots$ Тогда:

а) $\alpha = a_0+\frac{1}{a_1}\Big/+\ldots\frac{1}{a_{s-1}}\Big/+\frac{1}{a'_s}\Big/$ т. е. $\alpha'_s = \alpha_s$ является полным S-м частным;

б) $a_s = [\alpha_s]$ для всех S.

Получим:

$$\alpha = 1+\frac{1}{3}\Big/+\frac{1}{\alpha}\Big/ = 1+\frac{1}{3+\frac{1}{\alpha}} = 1+\frac{\alpha}{3\alpha+1} = \frac{4\alpha+1}{3\alpha+1};$$

$$\alpha = \frac{4\alpha+1}{3\alpha+1} \Rightarrow \begin{array}{l} 3\alpha^2+\alpha = 4\alpha+1, \\ 3\alpha^2-3\alpha-1 = 0, \end{array}$$

$D = 9 + 12 = 21$, $\alpha_{1,2} = \dfrac{3 \pm \sqrt{21}}{6}$, так как $\alpha > 0$, то $\alpha = \dfrac{3 + \sqrt{21}}{6}$.

2) При решении данной задачи используем приведенную выше теорему и следующую.

Теорема. *Пусть* $\alpha = a_0 + \dfrac{1}{a_1} + \dfrac{1}{a_2} + \ldots$, α_{S+1} — *полное частное в разложении* α, *тогда* $\alpha = \dfrac{P_S\,\alpha_{S+1} + P_{S-1}}{Q_S\,\alpha_{S+1} + Q_{S-1}}$ *и* $\alpha_{S+1} = \dfrac{P_{S-1} - \alpha Q_{S-1}}{\alpha Q_S - P_S}$, *где* P_S, Q_S, P_{S-1}, Q_{S-1} — *числители и знаменатели S-й и* $(S-1)$-*й подходящих дробей к* α.

$$\alpha = 3 + \frac{1}{3} + \frac{1}{3} + \frac{1}{1} + \frac{1}{\alpha}, \quad \alpha = \frac{P_3\alpha + P_2}{Q_3\alpha + Q_2}.$$

Определим P_2, Q_2, P_3, Q_3, по таблице:

n	–2	–1	0	1	2	3
			3	3	3	1
P_n	0	1	3	10	33	43
Q_n	1	0	1	3	10	13

$\alpha = \dfrac{43\alpha + 33}{13\alpha + 10}$, $13\alpha^2 + 10\alpha = 43\alpha + 33$, $13\alpha^2 - 33\alpha - 33 = 0$.

$D = 1089 + 1716 = 2805$, и так как $\alpha > 0$, то $\alpha = \dfrac{33 + \sqrt{2805}}{26}$.

4.2. Разложить в цепную дробь:

$\alpha = \dfrac{\sqrt{7} + 1}{2}$.

Решение. $\alpha = a_0 + \dfrac{1}{a_1} + \dfrac{1}{a_2} + \ldots$, где $a_i \in Z$, найдем последовательно следующим образом: $a_0 = [\alpha] = 1$.

Составим:

$$\alpha_1 = \frac{1}{\alpha - a_0} = \frac{1}{\frac{\sqrt{7}+1}{2} - 1} = \frac{2}{\sqrt{7}-1} = \frac{2\left(\sqrt{7}+1\right)}{7-1} = \frac{\sqrt{7}+1}{3};$$

$$a_1 = [\alpha_1] = 1;$$

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{\frac{\sqrt{7}+1}{3} - 1} = \frac{3}{\sqrt{7}-2} = \frac{3\left(\sqrt{7}+2\right)}{7-4} = \sqrt{7}+2;$$

$$a_2 = [\alpha_2] = 4;$$

$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{1}{\sqrt{7}+2-4} = \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{7-4} = \frac{\sqrt{7}+2}{3};$$

$$a_3 = [\alpha_3] = 1;$$

$$\alpha_4 = \frac{1}{\alpha_3 - a_3} = \frac{1}{\frac{\sqrt{7}+2}{3} - 1} = \frac{3}{\sqrt{7}-1} = \frac{3\left(\sqrt{7}+1\right)}{7-1} = \frac{\sqrt{7}+1}{2};$$

так как $\alpha_4 = \alpha$, то получим:

$$\frac{\sqrt{7}+1}{2} = 1 + \frac{1}{1}/ + \frac{1}{4}/ + \frac{1}{1}/ + \frac{1}{1}/ + \frac{1}{1}/ + \frac{1}{4}/ + \ldots$$

4.3. Найти величину периодической цепной дроби:

1) $\alpha = \left[\overline{1, 1, 2, 2}\right]$;

2) $\alpha = \left[0, 1, 1, 1, 1, \overline{2, 2, 2}\right]$.

Решение

1) $\alpha = \left[\overline{1, 1, 2, 2}\right] = 1 + \underline{\frac{1}{1}/ + \frac{1}{2}/ + \frac{1}{2}/ + \ldots}$

При нахождении величины α чисто периодической цепной дроби $\alpha = \underline{a_0 + \frac{1}{a_1}/ + \ldots + \frac{1}{a_{k-1}}/ + \ldots}$ удобно пользоваться формулой $\alpha = \frac{P_{k-1}\alpha + P_{k-2}}{Q_{k-1}\alpha + Q_{k-2}}$. Тогда α является положительным корнем квадратного уравнения

$$Q_{k-1}\alpha^2 + (Q_{k-2} - P_{k-1})\alpha - P_{k-2} = 0.$$

Вычислим P_n и Q_n:

			1	1	2	2	…
P_n	0	1	1	2	5	12	…
Q_n	1	0	1	1	3	7	…

$\alpha = \dfrac{12\alpha + 5}{7\alpha + 3}$, $7\alpha^2 + 3\alpha = 12\alpha + 5$, $7\alpha^2 - 9\alpha - 5 = 0$;

$D = 81 + 140 = 221$, $\alpha = \dfrac{9 + \sqrt{221}}{14}$.

2) $\alpha = \left\lfloor 0, 1, 1, 1, 1, \overline{2, 2, 2} \right\rfloor =$

$= 0 + \dfrac{1}{1} + \dfrac{1}{1} + \dfrac{1}{1} + \dfrac{1}{1} + \underline{\dfrac{1}{2} + \dfrac{1}{2} + \dfrac{1}{2}} + \ldots$

При вычислении величины α смешанной периодической цепной дроби вида $\alpha = a_0 + \dfrac{1}{a_1} + \ldots + \dfrac{1}{a_{S-1}} + \underline{\dfrac{1}{a_S} + \ldots + \dfrac{1}{a_{S+k-1}}} + \ldots$ удобней сначала найти величину α_S чисто периодической цепной дроби $\alpha_S = a_S + \underline{\dfrac{1}{a_{S+1}} + \ldots + \dfrac{1}{a_{S+k-1}}}$, а затем из соотношения $\alpha = \dfrac{P_{S-1}\alpha + P_{S-2}}{Q_{S-1}\alpha + Q_{S-2}}$ найти α. В данном случае $S = 5$, $k = 3$.

Вычислим: $\alpha_5 = 2 + \dfrac{1}{2} + \dfrac{1}{2} + \ldots$ $\alpha_5 = \dfrac{P_1\alpha_5 + P_0}{Q_1\alpha_5 + Q_0}$.

Вычислим: P_1, P_0, Q_1, Q_0:

			2	2	2
P_n	0	1	2	5	12
Q_n	1	0	1	2	5

$\alpha_5 = \dfrac{5\alpha_5 + 2}{2\alpha_5 + 1}$, $2\alpha_5^2 + \alpha_5 = 5\alpha_5 + 2$,

$2\alpha_5^2 - 4\alpha_5 - 2 = 0$, $\alpha_5^2 - 2\alpha_5 - 1 = 0$;

$\dfrac{D}{4} = 1 + 1 = 2$, $\alpha_5 = 1 + \sqrt{2}$. $\alpha = \dfrac{P_4\alpha_5 + P_3}{Q_4\alpha_5 + Q_3}$.

Вычислим: P_4, P_3, Q_4, Q_3:

			0	1	1	1	1
P_n	0	1	0	1	1	2	3
Q_n	1	0	1	1	2	3	5

$$\alpha = \frac{3(1+\sqrt{2})+2}{5(1+\sqrt{2})+3} = \frac{3\sqrt{2}+5}{5\sqrt{2}+8} = \frac{(3\sqrt{2}+5)(5\sqrt{2}-8)}{(5\sqrt{2}+8)(5\sqrt{2}-8)} =$$

$$= \frac{(30-40)+(25-24)\sqrt{2}}{50-64} = \frac{10-\sqrt{2}}{14}.$$

5. Квадратичные вычеты

5.1. С помощью символа Лежандра установить, имеет ли решения сравнение $x^2 = 68 \pmod{57}$.

Решение. Сравнение $x^2 \equiv a \pmod{p}$ имеет 2 решения, если символ Лежандра $\left(\frac{a}{p}\right) = 1$, и не имеет решений, если $\left(\frac{a}{p}\right) = -1$. При вычислении символа Лежандра используем его свойства:

1) $b \equiv a \pmod{p} \Leftrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

2) $\left(\frac{a^2}{p}\right) = 1$;

3) $\left(\frac{a_1 \cdot a_2 \cdot a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \ldots \left(\frac{a_n}{p}\right)$;

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

и закон взаимности:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \begin{cases} -1, & \text{если } p = 4n+3,\ q = 4n'+3; \\ 1, & \text{если } p \text{ или } q \text{ имеют вид } 4k+1. \end{cases}$$

Вычислим символ Лежандра:

$$\left(\frac{68}{57}\right)=\left(\frac{4\cdot 17}{57}\right)=\left(\frac{2^2}{57}\right)\cdot\left(\frac{17}{57}\right)=$$

$$=\left[\text{так как по 2)}\left(\frac{2^2}{57}\right)=1\right]=\left(\frac{17}{57}\right)=$$

$$=\left[\text{так как } 17=4\cdot 4+1\text{, то, по закону взаимности,}\right.$$

$$\left.\left(\frac{17}{57}\right)\cdot\left(\frac{57}{17}\right)=1\right]=\left(\frac{57}{17}\right)=\left[\text{так как } 57\equiv 6\ (\mathrm{mod}\ 17)\text{ по (1)}\right]$$

$$=\left(\frac{6}{17}\right)=\left(\frac{2}{17}\right)\cdot\left(\frac{3}{17}\right)=$$

$$=\left[\text{по 4)}\left(\frac{2}{17}\right)=(-1)^{\frac{17^2-1}{8}}=(-1)^{\frac{(17-1)(17+1)}{8}}=1\right]=$$

$$=\left(\frac{3}{17}\right)=\left(\frac{17}{3}\right)=\left[\text{так как } 17\equiv 2\ (\mathrm{mod}\ 3)\right]=\left(\frac{2}{3}\right)=(-1)^{\frac{3^2-1}{8}}=$$

$$=(-1)^1=-1.$$

Так как $\left(\frac{68}{57}\right)=-1$, то сравнение не имеет решений.

5.2. С помощью критерия Эйлера среди чисел 2, 3, 4, 5, 6, 7, 8 найти квадратичные вычеты по mod 11.

Решение. Критерий Эйлера. Число a, не делящееся на простое число p ($p>2$), является квадратичным вычетом по $\mathrm{mod}\ p \Leftrightarrow a^{\frac{p-1}{2}}\equiv 1\ (\mathrm{mod}\ p)$.

Выясним, с 1 или с –1 (в этом случае a является квадратичным невычетом по (mod p)) сравнимо $2^{\frac{11-1}{2}}$.

$2^{\frac{11-1}{2}}\equiv 2^5\equiv 32\equiv -1\ (\mathrm{mod}\ 11)$;

$3^{\frac{11-1}{2}}\equiv 3^5\equiv 3^2\cdot 3^2\cdot 3\equiv(-2)(-2)\cdot 3\equiv 12\equiv 1\ (\mathrm{mod}\ 11)$;

3 является квадратичным вычетом по mod 11.

$4^{\frac{11-1}{2}}\equiv 4^5\equiv 4^2\cdot 4^2\cdot 4\equiv 5\cdot 5\cdot 4\equiv 3\cdot 4\equiv 1\ (\mathrm{mod}\ 11)$;

4 — квадратичный вычет по mod 11.

$5^{\frac{11-1}{2}} \equiv 5^5 \equiv 5^2 \cdot 5^2 \cdot 5 \equiv 3 \cdot 3 \cdot 5 \equiv (-2) \cdot 5 \equiv -10 \equiv 1 \pmod{11}$;

5 — квадратичный вычет по mod 11.

$6^{\frac{11-1}{2}} \equiv 6^5 \equiv 6^2 \cdot 6^2 \cdot 6 \equiv 3 \cdot 3 \cdot 6 \equiv (-2) \cdot 6 \equiv -12 \equiv -1 \pmod{11}$;

$7^{\frac{11-1}{2}} \equiv 7^5 \equiv 7^2 \cdot 7^2 \cdot 7 \equiv 5 \cdot 5 \cdot 7 \equiv 5 \cdot 2 \equiv 10 \equiv -1 \pmod{11}$;

$8^{\frac{11-1}{2}} \equiv 8^5 \equiv 8^2 \cdot 8^2 \cdot 8 \equiv (-2) \cdot (-2) \cdot 8 \equiv 32 \equiv -1 \pmod{11}$.

Ответ: среди чисел 2, 3, 4, 5, 6, 7 числа 3, 4, 5 являются квадратичными вычетами по mod 11.

Задания для самостоятельного решения

Задание 1. Сведите сравнение к равносильному сравнению и затем решите его:

1) $6x^{23}+14x^{14}+3x^4-8x^3+x^2+3\equiv 0 \pmod{11}$.

2) $6x^9-5x^8+4x^7+x^3-2x^2+x-3\equiv 0 \pmod{7}$.

3) $5x^{24}+4x^{18}+4x^{16}+5x^{11}-13x^3-x^2+2x-7\equiv 0 \pmod{5}$.

4) $22x^{11}+4x^8-x^7+7x^6+14x^5+3x^2-6x+1\equiv 0 \pmod{7}$.

5) $4x^{23}+2x^{21}+x^{20}+6x^{19}+6x^{15}+2x^{13}+4x^8+2x^7+$
$+x^2+6x+2\equiv 0 \pmod{7}$.

6) $28x^{11}-2x^9+18x^8-x^7+14x^6+7x^5-13x^4+12x^3-x^2-$
$-34x+11\equiv 0 \pmod{3}$.

7) $13x^{10}+6x^9-5x^8+4x^7+15x^3-2x^2+41x-111\equiv 0 \pmod{5}$.

8) $23x^{33}-49x^{32}+14x^{27}-x^{17}+8x^{14}-2x^{13}+25x^{11}+$
$+12x^7-3x^4+4x^3-5x+1\equiv 0 \pmod{11}$.

9) $26x^{21}-20x^{20}-11x^{19}+x^{18}-4x^{16}+16x^{15}+74x^{11}+$
$+41x^{10}+2x^7+27x^6+10x^5-x^4+14x^3-6x^2-x+1\equiv 0 \pmod{5}$.

10) $9x^{14}-x^{12}+8x^{11}-9x^4+23x^3+47x^2-123x+$
$+211\equiv 0 \pmod{11}$.

Задание 2. Решите системы сравнений:

1) $\begin{cases} 3x\equiv 8 \pmod{20}, \\ 5x\equiv 8 \pmod{9}, \\ 4x\equiv 1 \pmod{21}. \end{cases}$

2) $\begin{cases} x\equiv 12 \pmod{13}, \\ x\equiv 10 \pmod{11}, \\ x\equiv 5 \pmod{12}. \end{cases}$

3) $\begin{cases} 8x\equiv 1 \pmod{13}, \\ 5x\equiv 7 \pmod{18}, \\ 2x\equiv 1 \pmod{9}. \end{cases}$

4) $\begin{cases} x \equiv 8 \pmod{13}, \\ x \equiv 9 \pmod{17}, \\ x \equiv 5 \pmod{11}. \end{cases}$

5) $\begin{cases} 3x \equiv 1 \pmod{25}, \\ 6x \equiv 3 \pmod{33}, \\ 4x \equiv 5 \pmod{9}. \end{cases}$

6) $\begin{cases} x \equiv 10 \pmod{11}, \\ x \equiv 9 \pmod{16}, \\ x \equiv 5 \pmod{7}. \end{cases}$

7) $\begin{cases} 2x \equiv 9 \pmod{15}, \\ 5x \equiv 4 \pmod{7}, \\ 7x \equiv 3 \pmod{9}. \end{cases}$

8) $\begin{cases} x \equiv 14 \pmod{19}, \\ x \equiv 5 \pmod{7}, \\ x \equiv 9 \pmod{10}. \end{cases}$

9) $\begin{cases} 5x \equiv 2 \pmod{12}, \\ 7x \equiv 2 \pmod{8}, \\ 3x \equiv 1 \pmod{5}. \end{cases}$

10) $\begin{cases} x \equiv 5 \pmod{9}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 1 \pmod{7}. \end{cases}$

Задание 3. Решите сравнения:

1) $x^4 - 33x^3 + 8x - 26 \equiv 0 \pmod{35}$.

2) $6x^3 - 7x - 11 \equiv 0 \pmod{125}$.

3) $x^5 - 3x^4 + 5x^3 + 9x^2 + 4x - 12 \equiv 0 \pmod{42}$.

4) $x^4 - 4x^3 + 2x^2 + x + 6 \equiv 0 \pmod{25}$.

5) $6x^3 - 3x^2 - 13x - 10 \equiv 0 \pmod{30}$.

6) $9x^2 + 29x + 62 \equiv 0 \pmod{64}$.

7) $3x^3 + 4x^2 - 7x - 6 \equiv 0 \pmod{15}$.

8) $4x^3 - 8x - 13 \equiv 0 \pmod{27}$.

9) $x^5 + x^4 - 3x^3 + x^2 + 2x - 2 \equiv 0 \pmod{77}$.

10) $x^3 + 3x^2 - 5x + 16 \equiv 0 \pmod{125}$.

Задание 4. Найдите величину цепной дроби:

1) $\alpha = 1 + \cfrac{1/}{2} + \cfrac{1/}{1} + \cfrac{1/}{2} + \ldots$

2) $\alpha = 2 + \cfrac{1/}{2} + \cfrac{1/}{2} + \cfrac{1/}{2} + \cfrac{1/}{1} + \cfrac{1/}{2} + \ldots$

3) $\alpha = 1 + \cfrac{1/}{5} + \cfrac{1/}{1} + \cfrac{1/}{5} + \ldots$

4) $\alpha = 3 + \cfrac{1/}{3} + \cfrac{1/}{1} + \cfrac{1/}{3} + \ldots$

5) $\alpha = 1 + \cfrac{1/}{7} + \cfrac{1/}{1} + \cfrac{1/}{7} + \ldots$

6) $\alpha = 2 + \cfrac{1/}{2} + \cfrac{1/}{2} + \cfrac{1/}{3} + \cfrac{1/}{2} + \ldots$

7) $\alpha = 1 + \cfrac{1/}{6} + \cfrac{1/}{1} + \cfrac{1/}{6} + \ldots$

8) $\alpha = 3 + \cfrac{1/}{3} + \cfrac{1/}{3} + \cfrac{1/}{2} + \cfrac{1/}{3} + \ldots$

9) $\alpha = 1 + \cfrac{1/}{8} + \cfrac{1/}{1} + \cfrac{1/}{8} + \ldots$

10) $\alpha = 2 + \cfrac{1/}{2} + \cfrac{1/}{2} + \cfrac{1/}{5} + \cfrac{1/}{2} + \ldots$

Задание 5. Разложите в цепную дробь:

1) $\dfrac{\sqrt{5}-1}{2}$.

2) $\dfrac{\sqrt{3}-2}{5}$.

3) $\dfrac{\sqrt{13}+2}{5}$.

4) $\frac{\sqrt{7}-1}{2}$.

5) $\frac{\sqrt{5}-2}{3}$.

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

7) $\frac{\sqrt{2}-1}{2}$.

8) $\frac{\sqrt{23}+1}{2}$.

9) $\frac{\sqrt{13}+1}{3}$.

10) $\frac{\sqrt{23}+1}{3}$.

Задание 6. Найдите величину периодической цепной дроби:

1) $[\overline{2, 3, 1}]$.

2) $[3, 4, \overline{5, 2, 1}]$.

3) $[\overline{3, 4, 5}]$.

4) $[1, 2, \overline{3, 4}]$.

5) $[\overline{0, 1, 1, 2}]$.

6) $[2, 3, \overline{1, 2, 3}]$.

7) $[\overline{1, 1, 1, 2}]$.

8) $[1, 0, \overline{1, 2, 5}]$.

9) $[\overline{2, 3, 1, 0}]$.

10) $[0, 1, 1, 2, \overline{3, 3, 3}]$.

Задание 7

1) С помощью символа Лежандра установите, имеет ли решения сравнение $x^2 \equiv 21 \pmod{587}$.

2) С помощью символа Лежандра установите, имеет ли решения сравнение $x^2 \equiv 240 \pmod{97}$.

3) С помощью символа Лежандра установите, имеет ли решения сравнение $x^2 \equiv 126 \pmod{59}$.

4) С помощью символа Лежандра установите, имеет ли решения сравнение $x^2 \equiv 124 \pmod{71}$.

5) С помощью символа Лежандра установите, имеет ли решения сравнение $x^2 \equiv 420 \pmod{571}$.

6) С помощью критерия Эйлера среди чисел 2, 3, ..., $p - 1$ найдите квадратичные вычеты по $\bmod p$ ($p = 5$).

7) С помощью критерия Эйлера среди чисел 2, 3, $p - 1$ найдите квадратичные вычеты по $\bmod p$ ($p = 7$).

8) С помощью критерия Эйлера среди чисел 2, 5, 6, 7, 10, 11, 12 найдите квадратичные вычеты по $\bmod p$ ($p = 13$).

9) С помощью критерия Эйлера среди чисел 2, 5, 6, 7, 10, 11, 12 найдите квадратичные вычеты по $\bmod p$ ($p = 17$).

10) С помощью критерия Эйлера среди чисел 2, 5, 6, 7, 10, 11, 12 найдите квадратичные вычеты по $\bmod p$ ($p = 19$):

Основная литература

1. Куликов, Л. Я. Алгебра и теория чисел / Л. Я. Куликов. М. : Высшая школа, 1979.

2. Казачек, Н. А. Алгебра и теория чисел / Н. А. Казачек [и др.] ; под общ. ред. Н. Я. Виленкина. М. : Просвещение, 1979.

3. Михелович, Ш. Х. Теория чисел / Ш. Х. Михелович. М. : Высшая школа, 1962.

4. Бухштаб, А. А. Теория чисел : учеб. пособие / А. А. Бухштаб. 3-е изд., стер. СПб. : Лань, 2008.

5. Кудреватов, Г. А. Сборник задач по теории чисел / Г. А. Кудреватов. М. : Просвещение, 1966.

6. Грибанов, В. У. Сборник упражнений по теории чисел / В. У. Грибанов, П. И. Титов. М. : Просвещение, 1964.

Дополнительная литература

1. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. М. : Просвещение, 1972.

2. Солнцев, Ю. К. Арифметика рациональных чисел / Ю. К. Солнцев [и др.]. 3-е изд. М. : Просвещение, 1971.

3. Солнцев, Ю. К. Контрольные работы и методические указания по арифметике рациональных чисел / Ю. К. Солнцев, Ю. И. Сопкин. М. : Учпедгиз, 1960.

4. Черемисина, М. И. Избранные вопросы алгебры и теории чисел. Ч. 1 / М. И. Черемисина. Оренбург, 2006.

Учебное издание

Черемисина Марина Ивановна

Избранные вопросы алгебры и теории чисел
Сравнения. Цепные дроби. Квадратичные вычеты

Учебно-методическое пособие

Редактор И. Н. Рожков
Компьютерная верстка Е. С. Рожковой

Подписано в печать 11.01.2016 г.
Усл. печ. л. 1,62
Тираж 100 экз. Заказ 1

ФГБОУ ВПО «Оренбургский государственный педагогический университет». 460014, г. Оренбург, ул. Советская, 19