МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г. Локтионова
«__» ____мая_____2016 г.

СИСТЕМЫ СРАВНЕНИЙ

Методические указания по выполнению практической работы для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2016

УДК 511.17

Составитель: М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *М.О. Таныгин*

Системы сравнений: методические указания по выполнению практической работы / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2016. 16 с. Библиогр.: с. 16.

Содержат основные сведения о системах сравнений и правилах их решения. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Цель лабораторной работы – научиться решать системы сравнений.

2. ЗАДАНИЕ

Ознакомиться с теоретическим материалом. Решить систему сравнения одним из описанных способов. Оформить отчет.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Решить систему сравнений согласно варианту задания.
4. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Решение системы сравнений.
4. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Системой сравнений первой степени с одним неизвестным называется система сравнений вида

$$\begin{cases} a_1 \cdot x \equiv c_1 (\mathrm{mod}\, m_1) \\ a_2 \cdot x \equiv c_2 (\mathrm{mod}\, m_2) \\ \dots \\ a_n \cdot x \equiv c_n (\mathrm{mod}\, m_n) \end{cases}$$

Предположим, что каждое из этих сравнений имеет решение. Тогда, разрешив каждое сравнение относительно x, систему сравнений можно привести к следующему виду

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1) \\ x \equiv c_2 (\mathrm{mod}\, m_2) \\ \dots \\ x \equiv c_n (\mathrm{mod}\, m_n) \end{cases}$$

Рассмотрим систему сравнений 1-й степени с одним неизвестным

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\, m_1) \\ x \equiv c_2 (\mathrm{mod}\, m_2) \end{cases}$$

5.1. Условие разрешимости системы.

Пусть d – наибольший общий делитель, M - наименьшее общее кратное m_1 и m_2, тогда, если разность $(c_2\text{-}c_1)$ не делится нацело на d, то система не имеет решений, а если $(c_2 - c_1) \subset d$, то система имеет единственное решение, представляющее класс по модулю M. Если m_1 и m_2 взаимно просты, то d=1, $M= m_1m_2$. А следовательно для таких модулей система всегда имеет одно решение, представляющее собой класс по модулю m_1m_2.

Пример 1.

Исследовать системы сравнений:

а) $\begin{cases} x \equiv 3(\mathrm{mod}7) \\ x \equiv 6(\mathrm{mod}12) \end{cases}$ б) $\begin{cases} x \equiv 8(\mathrm{mod}15) \\ x \equiv 4(\mathrm{mod}35) \end{cases}$

и решить их в случае совместности.

Решение.

а) Поскольку (7,12)=1, система имеет решение. Из первого сравнения системы запишем x в виде x=9+7t, подставим данное выражение во вторую систему и найдем t , решив вторую систему:

$9 + 7t \equiv 6 \pmod{12}$, $7t \equiv -3 \pmod{12}$, $7t \equiv -3 + 24 \pmod{12}$, $t \equiv 3 \pmod{12}$,

$t = 3 + 12y$.

Подставляя это значение t в выражение для x, имеем:

$x = 9 + 7(3 + 12y) = 30 + 84y$; $x \equiv 30 \pmod{84}$.

б) Поскольку (15,35)=5 и разность чисел 8 и 4 не делится на 5, то система не имеет решения.

Пример 2.

Исследовать систему сравнений

$$\begin{cases} 7x \equiv 10 \pmod{13} \\ 2x \equiv 2 \pmod{6} \end{cases}$$

и решить ее в случае совместности.

Решение.

Так как (13,6)=1, система имеет решение. Заметим, что второе сравнение системы имеет два решения, потому что обе части сравнения и модуль имеют НОД равный 2. Следовательно, данная система распадается на две системы сравнений:

$$\begin{cases} 7x \equiv 10 \pmod{13} \\ x \equiv 1 \pmod{6} \end{cases} \text{ и } \begin{cases} 7x \equiv 10 \pmod{13} \\ x \equiv 4 \pmod{6} \end{cases}$$

Решим первую систему. Для этого запишем x в виде x=1+6t, подставим данное выражение в первое сравнение и найдем t:

$7 + 42t \equiv 10 \pmod{13}$, $3t \equiv 3 \pmod{13}$, $t \equiv 1 \pmod{13}$, $t = 1 + 13y$.

Подставляя это значение t в выражение для x, имеем:

$x = 1 + 6(1 + 13y) = 7 + 78y$; $x \equiv 7 \pmod{78}$.

Решим вторую систему:

$x = 4 + 6t$, $28 + 42t \equiv 10 \pmod{13}$, $3t \equiv -18 \pmod{13}$, $t \equiv -6 \pmod{13}$,

$t \equiv 7 \pmod{13}$,

$t = 7 + 13y$, $x = 4 + 6(7 + 13y) = 46 + 78y$; $x \equiv 46 \pmod{78}$.

Таким образом, данная система сравнений имеет два решения:

$x \equiv 7 \pmod{78}$ и $x \equiv 46 \pmod{78}$.

Дана система сравнений:

$$\begin{cases} a_1 \cdot x \equiv b_1 \pmod{m_1} \\ a_2 \cdot x \equiv b_2 \pmod{m_2} \end{cases}$$

где $(m_1,m_2)=(a_1,m_1)=(a_2,m_2)=1$.

Эту систему сравнений можно заменить эквивалентной ей системой:

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\ m_1) \\ x \equiv c_2 (\mathrm{mod}\ m_2) \end{cases}$$

где первое и второе из сравнений этой системы является соответственно решениями исходной системы сравнений.

От полученной системы перейдем к системе

$$\begin{cases} m_2 \cdot x \equiv c_1 (\mathrm{mod}\ m_1 \cdot m_2) \\ m_1 \cdot x \equiv c_2 (\mathrm{mod}\ m_1 \cdot m_2) \end{cases}$$

эквивалентной данной и имеющей единственное решение по модулю $m_1 \cdot m_2$. При решении системы сравнений рассмотренным способом в случае попарно взаимно простых модулей нет необходимости заменять исходную систему системой

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\ m_1) \\ x \equiv c_2 (\mathrm{mod}\ m_2) \end{cases}$$

Пример 3.

Решить систему сравнений:

$$\begin{cases} 5x \equiv 7 (\mathrm{mod} 11) \\ 2x \equiv 3 (\mathrm{mod} 5) \end{cases}$$

Решение.

Так как (5,11)=(5,11)=(2,5)=1, то каждое сравнение системы имеет единственное решение, а сама система имеет единственное решение по модулю 55.

От данной системы переходим к системе сравнений

$$\begin{cases} 25x \equiv 35 (\mathrm{mod} 55) \\ 22x \equiv 33 (\mathrm{mod} 55) \end{cases}$$

и, вычитая из первого второе сравнение, получаем сравнение $3x \equiv 2 (\mathrm{mod} 55)$, решение которого $x \equiv 19 (\mathrm{mod} 55)$ является решением исходной системы.

5.2. Решение сложных систем сравнения.

Система сравнений

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\ m_1) \\ x \equiv c_2 (\mathrm{mod}\ m_2) \\ \quad\quad ... \\ x \equiv c_n (\mathrm{mod}\ m_n) \end{cases}$$

либо совсем не имеет решений, либо имеет решение, представляющее собой класс по модулю, равному наименьшему кратному чисел:

$$m_1, m_2, \dots, m_n.$$

Найти решение подобной системы можно, решив сначала первые два сравнения, добавив потом последовательно третье и т. д., пока не будет исчерпана вся система.

Пример 4.

Решить систему сравнений:

$$\begin{cases} x \equiv 1(\mathrm{mod}2) \\ x \equiv 3(\mathrm{mod}7) \\ x \equiv 5(\mathrm{mod}10) \end{cases}$$

Решение.

Решаем сначала систему, состоящую из двух первых сравнений:

$$x=1+2t\equiv3(\mathrm{mod}7),\ 2t\equiv2(\mathrm{mod}7),\ t\equiv1(\mathrm{mod}7),\ t=1+7y,$$
$$x=1+2(1+7y)=3+14y;\ x\equiv3(\mathrm{mod}14).$$

Таким образом, данная система эквивалентна системе:

$$\begin{cases} x \equiv 3(\mathrm{mod}14) \\ x \equiv 5(\mathrm{mod}10) \end{cases}$$

Здесь (10,14)=2 и 2|14-10|, так что система совместна. Решаем ее:

$$x=3+14t\equiv5(\mathrm{mod}10),\ 14t\equiv2(\mathrm{mod}10),\ 7t\equiv1(\mathrm{mod}5),\ 7t\equiv21(\mathrm{mod}5),$$
$$t\equiv3(\mathrm{mod}5),$$
$$t=3+5y,\ x=3+14(3+5y)=45+70y;\ x\equiv45(\mathrm{mod}70).$$

5.3. Китайская теорема об остатках.

Если натуральные числа $a_1, a_2, .., a_n$ попарно взаимно просты, то для любых целых $r_1, r_2, .., r_n$ таких, что $0 \le r_i < a_i$ при всех $i \in \{1,2,..n\}$ найдётся число N, которое при делении на a_i даёт остаток r_i при всех $i \in \{1,2,..n\}$. Более того, если найдутся два таких числа N_1 и N_2, то $N_1 \equiv N_2(\mathrm{mod}\ a_1 \cdot a_2 \cdot .. \cdot a_n)$.

Первое упоминание утверждения китайской теоремы об остатках встречается в книге “Математическое руководство Сунь Цзы” китайского математика Сунь Цзы, о котором не известно ничего, кроме того, что он является автором этой книги; годы его

жизни устанавливались историками науки на основе анализа текста.

Задача 26 главы 3. Предположим, что имеется неизвестное количество объектов. Разбив их на тройки, получаем в остатке 2, разбив на пятерки — 3, разбив на семерки — 2. Сколько имеется объектов?

После решения этой конкретной задачи, в книге приводится алгоритм решения и общей — при произвольных остатках: «Умножь число остатков при делении на тройки на 70, добавь к полученному произведение числа остатков при делении на пятерки на 21, и затем добавь произведение числа остатков при делении на семерки на 15. Если результат равен 106 или более — вычти кратное 105.»

Эти рассуждения фактически соответствуют представлению решения системы формулой.

Некоторые специалисты полагают, что алгоритм решения системы сравнений позволял китайским генералам пересчитывать армию без особых усилий последовательностью однотипных распоряжений:

«В колонну по 7становись!»

По выполнении команды, подсчитывалось количество солдат, стоящих в последнем ряду. Затем производились аналогичные подсчеты по результатам выполнения команд:

«В колонну по 11становись!»

«В колонну по 13становись!»

«В колонну по 17становись!»

В соответствии с утверждением теоремы, по четырем остаткам однозначно восстанавливается число солдат, если оно не превосходит 17017=7·11·13·17.

Пусть m_1, m_2,…,m_n – попарно взаимно простые числа, $M=m_1\cdot m_2\cdot\ldots\cdot m_n$; y_1, y_2,…,y_n подобраны так, что:

$$\frac{M}{m_1}y_1 \equiv 1(\mathrm{mod}\, m_1), \frac{M}{m_2}y_2 \equiv 1(\mathrm{mod}\, m_2), .., \frac{M}{m_n}y_n \equiv 1(\mathrm{mod}\, m_n)$$

$$x_0 = \frac{M}{m_1}y_1c_1 + \frac{M}{m_2}y_2c_2 + .. + \frac{M}{m_n}y_nc_n$$

Тогда решение системы:

$$\begin{cases} x \equiv c_1 (\mathrm{mod}\ m_1) \\ x \equiv c_2 (\mathrm{mod}\ m_2) \\ \quad\quad ... \\ x \equiv c_n (\mathrm{mod}\ m_n) \end{cases}$$

будет иметь вид $x \equiv x_0 (\mathrm{mod}\ M)$.

Пример 5.

$$\begin{cases} x \equiv 7 (\mathrm{mod} 11) \\ x \equiv -5 (\mathrm{mod} 13) \\ x \equiv 8 (\mathrm{mod} 14) \end{cases}$$

Решение.

Находим:

$$13 \cdot 14 y_1 \equiv 1 (\mathrm{mod} 11), \quad 6 y_1 \equiv 1 (\mathrm{mod} 11), \quad y_1 = 2$$
$$11 \cdot 14 y_2 \equiv 1 (\mathrm{mod} 13), \quad 11 y_2 \equiv 1 (\mathrm{mod} 13), \quad y_2 = 11$$
$$11 \cdot 13 y_3 \equiv 1 (\mathrm{mod} 14), \quad 3 y_3 \equiv 1 (\mathrm{mod} 14), \quad y_3 = 5$$

$x=13\cdot14\cdot2\cdot7-11\cdot14\cdot11\cdot5+11\cdot13\cdot5\cdot8\equiv-202(\mathrm{mod}11\cdot13\cdot14);$

$x\equiv1800(\mathrm{mod}2002).$

Пример 6.

$$\begin{cases} x \equiv 11 (\mathrm{mod} 8) \\ x \equiv 11 (\mathrm{mod} 9) \\ x \equiv 12 (\mathrm{mod} 7) \end{cases}$$

Способ 1. С помощью расширенного алгоритма Евклида.

$$3 \cdot 9 \cdot 7 \cdot x_1 \equiv 3 (\mathrm{mod} 8)$$
$$63 x_1 \equiv 1 (\mathrm{mod} 8)$$

Находим мультипликативно обратный элемент к 63 по модулю 8.

	63 | 8	
	-- | 7	
8	7	
--	1	
7	1=(63,8)=d	
--	7	
0		

i	Остатки	Частные	x_i	y_i
-1	63	-	1	0
0	8	-	0	1
1	7	7	1-0*7=1	0-1*7=-7
2	1=d	1	0-1*1=-1	1-(-7)*1=8
3	0	7	-	-

$$d = 1 = 63 \cdot (-1) + 8 \cdot 8$$
$$U = -1; x \equiv -1(mod8) = 7 \ (т.к \ -1 = 8 \cdot (-1) + 7)$$
$$2 \cdot 8 \cdot 7 \cdot x_2 \equiv 2(mod9)$$
$$56x_2 \equiv 1(mod9)$$

```
                56 | 9
                -- | 6
            9  | 2
            -- | 4
        2  | 1=(56,9)=d
        -- | 2
        0
```

i	Остатки	Частные	x_i	y_i
-1	56	-	1	0
0	9	-	0	1
1	2	6	1-0*6=1	0-1*6=-6
2	1=d	4	0-1*4=-4=U	1-(-6)*4=25
3	0	2	-	-

$$x_2 \equiv -4(mod9) = 5 \ (т.к \ -4 = 9 \cdot (-1) + 5)$$
$$5 \cdot 8 \cdot 9 \cdot x_3 \equiv 5(mod7)$$
$$72x_3 \equiv 5(mod7)$$

```
                72 | 7
                -- | 10
            7  | 2
            -- | 3
        2  | 1=(72,7)=d
        -- | 2
        0
```

i	Остатки	Частные	x_i	y_i
-1	72	-	1	0
0	7	-	0	1
1	2	10	1-0*10=1	0-1*10=-10
2	1=d	3	0-1*3=-3=U	1-(-10)*3=31
3	0	2	-	-

$$x_3 \equiv -3(\mathrm{mod}7) = 4 \ (\text{т.к } -3 = 7 \cdot (-1) + 4)$$

$$x = (93 \cdot 63 \cdot 7 + 2 \cdot 56 \cdot 5 + 5 \cdot 72 \cdot 4)\big(\mathrm{mod}(7 \cdot 8 \cdot 9)\big)$$

$$x = 3323(\mathrm{mod}504) = 299$$

Проверка. $299(\mathrm{mod}8) = 3;\ \ 299(\mathrm{mod}9) = 2;\ \ 299(\mathrm{mod}7) = 5;$

Способ 2. Способ Эйлера.

В данном примере его применение неэффективно, т.к. приводит к большим числам.

$$\begin{cases} 63x_1 \equiv 1(\mathrm{mod}8) \\ 56x_2 \equiv 1(\mathrm{mod}9) \\ 72x_3 \equiv 5(\mathrm{mod}7) \end{cases}$$

$$\varphi(8) = 4; U = 64^{4-1} = 250047; x_1 = 250047(\mathrm{mod}8) = 7$$

$$\varphi(9) = 6; U = 56^{6-1} = 550731776; x_2 = 550731776(\mathrm{mod}9) = 5$$

$$\varphi(7) = 6; U = 72^{6-1} = 51934917632; x_3 = 51934917632(\mathrm{mod}7) = 4$$

6. ПРАКТИЧЕСКИЕ ЗАДАНИЯ

1. $\begin{cases} x \equiv 13 (\mathrm{mod}\, 18) \\ x \equiv 19 (\mathrm{mod}\, 29) \\ x \equiv 12 (\mathrm{mod}\, 17) \end{cases}$ 2. $\begin{cases} x \equiv 21 (\mathrm{mod}\, 13) \\ x \equiv 12 (\mathrm{mod}\, 37) \\ x \equiv 11 (\mathrm{mod}\, 21) \end{cases}$

3. $\begin{cases} x \equiv 11 (\mathrm{mod}\, 15) \\ x \equiv 36 (\mathrm{mod}\, 19) \\ x \equiv 24 (\mathrm{mod}\, 37) \end{cases}$ 4. $\begin{cases} x \equiv 23 (\mathrm{mod}\, 28) \\ x \equiv 27 (\mathrm{mod}\, 31) \\ x \equiv 15 (\mathrm{mod}\, 17) \end{cases}$

5. $\begin{cases} x \equiv 21 (\mathrm{mod}\, 25) \\ x \equiv 11 (\mathrm{mod}\, 19) \\ x \equiv 32 (\mathrm{mod}\, 17) \end{cases}$ 6. $\begin{cases} x \equiv 37 (\mathrm{mod}\, 24) \\ x \equiv 22 (\mathrm{mod}\, 29) \\ x \equiv 25 (\mathrm{mod}\, 13) \end{cases}$

7. $\begin{cases} x \equiv 21 (\mathrm{mod}\, 23) \\ x \equiv 11 (\mathrm{mod}\, 29) \\ x \equiv 12 (\mathrm{mod}\, 17) \end{cases}$ 8. $\begin{cases} x \equiv 27 (\mathrm{mod}\, 31) \\ x \equiv 32 (\mathrm{mod}\, 19) \\ x \equiv 29 (\mathrm{mod}\, 15) \end{cases}$

9. $\begin{cases} x \equiv 21 (\mathrm{mod}\, 37) \\ x \equiv 31 (\mathrm{mod}\, 19) \\ x \equiv 17 (\mathrm{mod}\, 21) \end{cases}$ 10. $\begin{cases} x \equiv 13 (\mathrm{mod}\, 22) \\ x \equiv 41 (\mathrm{mod}\, 29) \\ x \equiv 15 (\mathrm{mod}\, 17) \end{cases}$

11. $\begin{cases} x \equiv 31 (\mathrm{mod}\, 21) \\ x \equiv 17 (\mathrm{mod}\, 29) \\ x \equiv 19 (\mathrm{mod}\, 20) \end{cases}$ 12. $\begin{cases} x \equiv 13 (\mathrm{mod}\, 25) \\ x \equiv 32 (\mathrm{mod}\, 19) \\ x \equiv 25 (\mathrm{mod}\, 27) \end{cases}$

13. $\begin{cases} x \equiv 11 (\mathrm{mod}\, 17) \\ x \equiv 31 (\mathrm{mod}\, 19) \\ x \equiv 23 (\mathrm{mod}\, 27) \end{cases}$ 14. $\begin{cases} x \equiv 13 (\mathrm{mod}\, 28) \\ x \equiv 21 (\mathrm{mod}\, 23) \\ x \equiv 29 (\mathrm{mod}\, 17) \end{cases}$

15. $\begin{cases} x \equiv 21 (\mathrm{mod}\, 28) \\ x \equiv 24 (\mathrm{mod}\, 13) \\ x \equiv 19 (\mathrm{mod}\, 31) \end{cases}$ 16. $\begin{cases} x \equiv 27 (\mathrm{mod}\, 31) \\ x \equiv 31 (\mathrm{mod}\, 19) \\ x \equiv 36 (\mathrm{mod}\, 21) \end{cases}$

17. $\begin{cases} x \equiv 19 (\mathrm{mod}\, 23) \\ x \equiv 21 (\mathrm{mod}\, 29) \\ x \equiv 29 (\mathrm{mod}\, 17) \end{cases}$ 18. $\begin{cases} x \equiv 32 (\mathrm{mod}\, 17) \\ x \equiv 33 (\mathrm{mod}\, 19) \\ x \equiv 15 (\mathrm{mod}\, 37) \end{cases}$

19. $\begin{cases} x \equiv 11 (\mathrm{mod}\, 26) \\ x \equiv 31 (\mathrm{mod}\, 19) \\ x \equiv 24 (\mathrm{mod}\, 27) \end{cases}$ 20. $\begin{cases} x \equiv 23 (\mathrm{mod}\, 28) \\ x \equiv 21 (\mathrm{mod}\, 29) \\ x \equiv 31 (\mathrm{mod}\, 17) \end{cases}$

21. $\begin{cases} x \equiv 17 (\mathrm{mod}\, 18) \\ x \equiv 19 (\mathrm{mod}\, 25) \\ x \equiv 31 (\mathrm{mod}\, 17) \end{cases}$ 22. $\begin{cases} x \equiv 30 (\mathrm{mod}\, 17) \\ x \equiv 22 (\mathrm{mod}\, 37) \\ x \equiv 19 (\mathrm{mod}\, 23) \end{cases}$

23. $\begin{cases} x \equiv 11 (\mathrm{mod}\, 25) \\ x \equiv 34 (\mathrm{mod}\, 19) \\ x \equiv 24 (\mathrm{mod}\, 33) \end{cases}$ 24. $\begin{cases} x \equiv 23 (\mathrm{mod}\, 27) \\ x \equiv 21 (\mathrm{mod}\, 31) \\ x \equiv 15 (\mathrm{mod}\, 19) \end{cases}$

25. $\begin{cases} x \equiv 21 (\mathrm{mod}\, 23) \\ x \equiv 13 (\mathrm{mod}\, 19) \\ x \equiv 33 (\mathrm{mod}\, 27) \end{cases}$ 26. $\begin{cases} x \equiv 37 (\mathrm{mod}\, 25) \\ x \equiv 21 (\mathrm{mod}\, 29) \\ x \equiv 28 (\mathrm{mod}\, 17) \end{cases}$

27. $\begin{cases} x \equiv 22 (\mathrm{mod}\, 23) \\ x \equiv 11 (\mathrm{mod}\, 28) \\ x \equiv 13 (\mathrm{mod}\, 17) \end{cases}$ 28. $\begin{cases} x \equiv 17 (\mathrm{mod}\, 21) \\ x \equiv 32 (\mathrm{mod}\, 19) \\ x \equiv 23 (\mathrm{mod}\, 25) \end{cases}$

29. $\begin{cases} x \equiv 21 (\mathrm{mod}\, 27) \\ x \equiv 33 (\mathrm{mod}\, 19) \\ x \equiv 16 (\mathrm{mod}\, 29) \end{cases}$ 30. $\begin{cases} x \equiv 13 (\mathrm{mod}\, 23) \\ x \equiv 41 (\mathrm{mod}\, 27) \\ x \equiv 15 (\mathrm{mod}\, 19) \end{cases}$

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Условия разрешимости системы сравнений.
2. Мультипликативно-обратные по модулю элементы.
3. Решение сравнений первой степени с помощью расширенного алгоритма Евклида.
4. Способ Эйлера решения сравнений первой степени.
5. Китайская теорема об остатках.

8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Александров В.А., Горшенин С.М. Задачник – практикум по теории чисел. М.: Учпедгиз, 1972.
2. Бухштаб А.А. Теория чисел. М.: Учпедгиз, 1960.
3. Виноградов И.М. Основы теории чисел. М.: Наука,1995.
4. Гайнов А.Т. Теория чисел. Изд - во НГУ, 1995.
5. Галочкин А.И., Нестеренко Н.В., Шидловский А.Б. Введение в теорию чисел. Изд - во МГУ, 1995.
6. Грибанов В.У., Титов Л.И. Сборник упражнений по теории чисел. М.:Просвещение, 1964.
7. Кудреватов Г.А. Сборник задач по теории чисел. М.: Просвещение,1970.
8. Ляпин С.Е., Баранова И.В., Борчугова З.Г. Сборник задач по элементарной математике. М.: Просвещение, 1973.
9. Окунев Л.Я. Краткий курс теории чисел. М.: Учпедгиз, 1956.
10. Пензин Ю.Г., Клейменов В.Ф. Сравнения. Учебно-методические разработки (тексты лекций). Изд-во ИГУ, 1998.
11. Серр Ж. Курс арифметики. М.: Мир, 1972.
12. И.М. Виноградов «Элементы высшей математики» М., «Высшая школа», 1999
13. Л.Я. Куликов, А.И. Москаленко, А.А. Фомин «Сборник задач по алгебре и теории чисел» М., «Просвещение», 1993
14. Ю.С. Харин, В.И. Берник, Г.В. Матвеев, С.В. Ажевич «Математические и компьютерные основы криптологии» Минск, «Новое знание», 2003