МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

Кафедра прикладной математики

Т.М. ОТРЫВАНКИНА

АЛГОРИТМЫ КОМПЬЮТЕРНОЙ АЛГЕБРЫ

ПРАКТИКУМ

Рекомендовано к изданию Редакционно-издательским советом
государственного образовательного учреждения
высшего профессионального образования
«Оренбургский государственный университет»

Оренбург 2007

УДК 512 (076.5)
ББК 22.14я73
О 86

Рецензент
доктор физико-математических наук, профессор В.А. Молчанов

Отрыванкина Т.М.
О86 Алгоритмы компьютерной алгебры: практикум / Т.М. Отрыванкина. – Оренбург: ГОУ ОГУ, 2007. – 26 с.

Практикум предназначен для студентов очной формы обучения специальности 010501 Прикладная математика и информатика. Он содержит ряд типовых задач по дисциплине блока ДС.00 «Алгоритмы компьютерной алгебры», решения таких задач и ответы к ним. Методическая разработка поможет в организации самостоятельной работы студентов при изучении дисциплины, будет полезна при подготовке к контрольным работам, к проверке остаточных знаний.

ББК 22.14я73

Содержание

Введение

Цель написания данной учебно-методической разработки – предоставить варианты заданий по спецкурсу «Алгоритмы компьютерной алгебры» с решениями и ответами для использования в организации самостоятельной работы студентов, для помощи студентам в подготовке к самостоятельным и контрольным работам, к контролю остаточных знаний по дисциплине. Предлагаемые задания связаны:

а) с вычислением НОД двух целых чисел,

б) решением линейных диофантовых уравнений от двух переменных,

в) возведением числа в степень в конечном поле,

г) вычислением мультипликативного обратного в конечном поле,

д) применением греко-китайской теоремы об остатках к решению систем линейных сравнений,

е) восстановлением целого числа по остаткам, определением знака целого числа, представленного вектором остатков,

ж) вычислением символов Лежандра и Якоби,

з) поиском квадратичных вычетов.

Практикум содержит краткие теоретические сведения по указанному кругу вопросов, примеры задач с решениями, четыре варианта заданий, аналогичных разобранным, таблицу правильных ответов к ним и решения практически всех предложенных задач.

В результате работы с методическим руководством студент сможет повторить некоторые сведения из теории чисел и прикладной алгебры и расширить знания в этой области, обретя необходимые навыки решения ряда базовых задач курса.

1 Основные теоретические сведения

1Алгоритм Евклида.
Для вычисления НОД(a,b), $b\neq0$, выполняются действия:

$a=bq_1+r_1,\ 0\le r_1<|b|,$
$b=r_1q_2+r_2,$
$r_1=r_2q_3+r_3,$
$\ldots,$
$r_{m-2}=r_{m-1}q_m+r_m,$
$r_{m-1}=r_mq_{m+1},\ 0\le, r_i<r_{i-1},\ i=2,\ \ldots,\ m.$

Тогда НОД(a,b)$=r_m$.

2Расширенный алгоритм Евклида (РАЕ).
Для вычисления НОД(a,b), $b\neq0$, и получения его линейного представления НОД(a,b) $= ax+by$, $x,\ y\in\boldsymbol{Z}$, вычисляем по формулам

$$a_i = a_{i-2} - a_{i-1}q_{i-1},$$
$$x_i = x_{i-2} - x_{i-1}q_{i-1},$$
$$y_i = y_{i-2} - y_{i-1}q_{i-1},$$
$$q_i=[a_{i-1}/a_i],i\ge2$$

при $a_0=a,\ x_0=1,\ y_0=0,\ a_1=b,\ x_1=0,\ y_1=1,\ q_1=[a_0/a_1]$ значения $a_i,\ x_i,\ y_i$ до тех пор, пока не получим некоторое $a_{m+1}=0$. Тогда НОД(a,b) $=a_m= ax_m+by_m$.
Вычисления удобно проводить, оформляя таблицу

i	a_i	x_i	y_i	q_i
0	a	1	0	-
1	b	0	1	$[a_0/a_1]$
2	$a_2 = a_0 - a_1 q_1$	$x_2 =x_0 - x_1 q_1$	$y_2 = y_0 - y_1 q_1$	$[a_1/a_2]$
3	$a_3 = a_1 - a_2 q_2$	$x_3 =x_1 - x_2 q_2$	$y_3 = y_1 - y_2 q_2$	$[a_2/a_3]$
...	...	...	...	...
$m+1$	0			

3Диофантово уравнение $ax+by=c$ имеет решение, если c делится на d=НОД(a,b), в частности, если a и b взаимно просты. В этом случае решений в $\boldsymbol{Z}$ бесконечно много, они имеют вид

$$\left(x_0 - \frac{b}{d}k, y_0 + \frac{a}{d}k \right), k\in \boldsymbol{Z},$$

где ($x_0,\ y_0$) – некоторое частное решение данного уравнения.
Частное решение можно получить, применив РАЕ для поиска d=НОД(a,b):
$d = ax_m+by_m \Rightarrow d\cdot(c/d) = a\cdot(c/d)x_m+b\cdot(c/d)y_m \Rightarrow x_0=(c/d)x_m,\ y_0=(c/d)y_m.$

4В арифметике остатков, т.е. в кольце $\boldsymbol{Z_n}$, то одной из центральных задач является решение уравнения (сравнения)

$$ax=b(mod\ n)\ (\ ax\equiv b(mod\ n)\ ).$$

Нетрудно установить, что:

– Если НОД(a, n)=1, то существует ровно одно решение этого уравнения $x=b\cdot c(mod\ n)$, где c удовлетворяет равенству $a\cdot c=1(mod\ n)$.

– Если d=НОД(a, n)≠1 и $b \vdots d$, то уравнение имеет d решений $x=x_0 + k\cdot\frac{n}{d}$, $k=0, 1, \ldots, d-1$, где x_0 – решение сравнения $\frac{a}{d}x \equiv \frac{b}{d}\left(\mathrm{mod}\frac{n}{d}\right)$.

– В других случаях решений нет.

Решение уравнения $ax=b(mod\ n)$, таким образом, требует вычисления значения c, удовлетворяющего равенству $a\cdot c=1(mod\ n)$. Это число обозначают a^{-1} и оно существует, когда a и n взаимно просты. Если же n – простое число (обычно пишут, p), то $\boldsymbol{Z_n}$ является полем и в нем любой ненулевой элемент обладает мультипликативным обратным.

Для поиска мультипликативных обратных используются:

а) РАЕ;

б) следствие малой теоремы Ферма: если p – простое число, $a^{-1}=a^{p-2}$ в $\boldsymbol{Z_p}$;

в) бинарный («индийский») метод: пусть требуется вычислить a^k, запишем k в двоичной системе, заменим каждую 1 на буквы SM_a, а каждый 0 – на S, вычеркнем первое слева вхождение SM_a, а оставшуюся последовательность читаем, интерпретируя S как «возвести в квадрат и взять остаток по модулю р» и M_a – как «умножить на a и взять остаток по модулю р».

5*Греко-китайская теорема об остатках*. Пусть $m_1, m_2, \ldots, m_k$ – попарно взаимно простые целые числа, большие 1, и M= $m_1\cdot m_2\cdot \ldots \cdot m_k$. Тогда существует единственное неотрицательное решение по модулю M решение системы уравнений (сравнений)

$$\begin{cases} x \equiv a_1 (\mathrm{mod}\, m_1), \\ x \equiv a_2 (\mathrm{mod}\, m_2), \\ \ldots, \\ x \equiv a_k (\mathrm{mod}\, m_k). \end{cases}$$

В общем случае решение представляется в виде

(*) $x=q_1+q_2(m_1)+q_3(m_1m_2)+q_4(m_1m_2m_3)+\ldots+q_k(m_1m_2m_3\ldots m_{k-1})$,

где $0\le q_i < |m_i|$, q_1 – остаток от деления a_1 на m_1.

6Пусть дано представление $x=[a_1, a_2, a_3, \ldots, a_n]$ по вектору оснований $\beta=[m_1, m_2, m_3, \ldots, m_n]$. Необходимо определить знак числа x, который совпадает со знаком старшего члена q_n в выражении *(*)*. Для этого найдем:

1) $q_1= a_1$
2) $x'=(x-q_1)\ (m_1)^{-1}(mod[\ m_2, m_3, \ldots, m_n]\ )=[\ b_2, b_3, \ldots, b_n]$
3) $q_2= b_2$
4) $x''=(x'-q_2)\ (m_2)^{-1}(mod[\ m_3, \ldots, m_n]\ )=[\ c_3, \ldots, c_n]$
5) $q_3= c_3$
6) ...

2n-1) $q_n = \begin{cases} 0, \text{если } x > 0, \\ 1, \text{если } x < 0. \end{cases}$

[7]Лежандр в 1798 г. ввел символ $\left(\frac{a}{p}\right)$, который определил следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, a \equiv 0 (\mathrm{mod}\, p), \\ 1, \exists x : x^2 \equiv a (\mathrm{mod}\, p), a \bmod p \neq 0, \\ -1, \neg \exists x : x^2 \equiv a (\mathrm{mod}\, p), a \bmod p \neq 0. \end{cases}$$

Основные свойства символа Лежандра:

1) $a_1 \equiv a (\mathrm{mod}\, p) \Rightarrow \left(\frac{a_1}{p}\right) = \left(\frac{a}{p}\right)$

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

3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

4) Если НОД(a, p)=1, то $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$

5) $\left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

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

Квадратичный закон взаимности. Для любых простых нечетных чисел p и q

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

[8]Пусть p – нечетное простое число. Если сравнение $x^2 \equiv a (\mathrm{mod}\, p)$ имеет решение, что a называют квадратичным вычетом по модулю p. Сравнение имеет решение, если символ Лежандра $\left(\frac{a}{p}\right)$ равен 1. Найти решение можно, например, с помощью алгоритма Шэнкса:

7) Выбираем $n : \left(\frac{n}{p}\right) = -1$.

8) Пусть e, $q \in \boldsymbol{Z}$, q – нечетное: $p-1 = 2^e q$.

9) Положим $y=n^q(mod\ p)$, $r=e$, $x = a^{\frac{q-1}{2}} (\mathrm{mod}\ p)$.

10) Положим $b=ax^2(mod\ p)$, $x=ax(mod\ p)$.

11) Пока b≠1(mod p), делать:

а) найти наименьшее число $m : b^{2^m} = 1(\mathrm{mod}\ p)$,

б) положить $t = y^{2^{r-m-1}} (\mathrm{mod}\ p), y = t^2(\mathrm{mod}\ p)$, $r=m$,

в) положить $x = xt(\mathrm{mod}\ p), b = by(\mathrm{mod}\ p)$.

12) Вывести x

Полезно знать, что если p≡3(mod 4), то $x = a^{\frac{p+1}{4}} (\mathrm{mod}\ p)$.

[9]Пусть n – нечетное число, большее 2, и $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$. Символ Якоби $\left(\frac{a}{n}\right)$ определяется равенством $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdot \left(\frac{a}{p_2}\right)^{e_2} ... \left(\frac{a}{p_k}\right)^{e_k}$. В данном случае $\left(\frac{a}{n}\right) = 1$ не означает, что a является квадратичным вычетом по модулю n.

Основные свойства символа Якоби:

1) $a_1 \equiv a(\mathrm{mod} n) \Rightarrow \left(\frac{a_1}{n}\right) = \left(\frac{a}{n}\right)$

2) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

4) Если НОД(a, n)=1, то $\left(\frac{a^2 b}{n}\right) = \left(\frac{b}{n}\right)$

5) $\left(\frac{1}{n}\right) = 1, \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$

6) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

Квадратичный закон взаимности. Для любых нечетных чисел p и q

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

[10]Чтобы решить квадратичное сравнение $x^2 \equiv a(mod\ n)$, где $n=pq$, p, q – простые числа, найдем y: $y^2 \equiv a(mod\ p)$, z: $z^2 \equiv a(mod\ q)$. Обозначим первое s_p, а второе – s_q, после чего решим систему $\begin{cases} x = s_p(\mathrm{mod}\ p) \\ x = s_q(\mathrm{mod}\ q) \end{cases}$ с помощью греко-китайской теоремы об остатках.

2 Примеры задач с решениями

1С помощью алгоритма Евклида найдите НОД(14638, 3198).

14638=3198·4+1846
3198=1846·1+1352
1846=1352·1+494
1352=494·2+364
494=364·1+130
364=130·2+104
130=104·1+26
104=26·4 $\Rightarrow$ НОД (14638,3198)=26

2Найдите НОД(9457, 3211) с помощью расширенного алгоритма Евклида.

a_i	x_i	y_i	q_i
9457	1	0	–
3211	0	1	2
3035	1	–2	1
176	–1	3	17
43	18	–53	4
4	–73	215	10
3	748	–2203	1
1	–821	2418	3
0			

1=9457·(-821)+3211·2418 – линейное представление НОД(9457, 3211)=1.

3Найдите x, y$\in$ **Z**, такие, что 34x-13y=8.

Рассмотрим уравнение 34x+13y=1:

34	1	0	–
13	0	1	2
8	1	–2	1
5	–1	3	1
3	2	–5	1
2	–3	8	1
1	5	–13	2
0			

Значит, 1=34·5-13·13, откуда 8=34·40-13·104 и пара (40,104) – частное решение исходного уравнения, а (40+13k, 104+34k), k$\in$ **Z**, – его общее решение.

4Найдите все x, y$\in$ **Z**, такие, что 12x+21y=1.

Множество решений является ∅, так как НОД(12,21)=3 не делит 1.

5Найдите $2^{47}(\mathrm{mod}\ 23)$.

$2^{47}(\mathrm{mod}\ 23)=(2^{22})^2\cdot 2^3(\mathrm{mod}\ 23)=8$.

6Вычислите $11^{-1}(\mathrm{mod}\ 29)$.

I способ – применение расширенного алгоритма Евклида:

a_i	y_i	q_i
29	0	–
11	1	2
7	–2	1
4	3	1
3	–5	1
1	8	3
0		

Значит, $11^{-1}(\mathrm{mod}\ 29)=8$.

II способ – «индийский» алгоритм
$11^{-1}(\mathrm{mod}\ 29)=11^{27}(\mathrm{mod}\ 29)$
$27=11011_2 \Rightarrow SM_{11}SM_{11}SSM_{11}SM_{11} \Rightarrow SM_{11}SSM_{11}SM_{11} \Rightarrow$
$\Rightarrow 11^{27}(\mathrm{mod}\ 29)=(((11^2\cdot 11)^2)^2\cdot 11)^2\cdot 11(\mathrm{mod}\ 29)=(((5\cdot 11)^2)^2\cdot 11)^2\cdot 11(\mathrm{mod}\ 29)=$
$=(((-3)^2)^2\cdot 11)^2\cdot 11(\mathrm{mod}\ 29)=(23\cdot 11)^2\cdot 11(\mathrm{mod}\ 29)=64\cdot 11(\mathrm{mod}\ 29)=8$

7Решите систему сравнений

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

Из первого сравнения $x=5k+2$, $k\in \mathbf{Z}$. Подстановкой во второе сравнение получим:
$5k+2\equiv 3(\mathrm{mod}\ 11)$,
$5k\equiv 1(\mathrm{mod}\ 11)$,
$k\equiv 9(\mathrm{mod}\ 11)$,
$k=11l+9$, $l\in \mathbf{Z}$.
Значит, $x=5k+2=5(11l+9)+2=55l+47$, $l\in \mathbf{Z}$ – решение первых двух сравнений системы. Подстановкой найденного значения в третье сравнение получим:
$55l+47\equiv 2(\mathrm{mod}\ 7)$,
$6l\equiv 4(\mathrm{mod}\ 7)$,
$3l\equiv 2(\mathrm{mod}\ 7)$,
$l\equiv 2\cdot 3^{-1}(\mathrm{mod}\ 7)$,

$l \equiv 3 \pmod 7$,
$l = 7m+3$, $m \in \mathbf{Z}$.
Значит, $x = 55l+47 = 55(7m+3)+47 = 385m+212$, $m \in \mathbf{Z}$.
Другими словами, $x \equiv 212 \pmod{385}$ или $x \equiv 212 \pmod{5 \cdot 11 \cdot 7}$.

8Найдите знак числа (6,4,2,1) по вектору (7,5,3,2).
$x=(6,4,2,1)$, $\beta=(7,5,3,2)$.
$q_1=6$
$x_1=x-6=(0,-2,-4,-5)(\text{mod } \beta)=(0,3,2,1)(\text{mod } \beta)=(3,2,1)(\text{mod } \beta_1)$, где $\beta_1=(5,3,2)$.
$x_1 \cdot 7^{-1}(\text{mod } \beta_1)=(3,2,1)\cdot(3,1,1)=(9,2,1)=(4,2,1)$
$q_2=4$
$x_2=x_1-4=(0,-2,-3)=(0,1,1)=(1,1)(\text{mod } \beta_2)$, где $\beta_2=(3,2)$.
$x_2 \cdot 5^{-1}(\text{mod } \beta_2)=(1,1)\cdot(2,1)=(2,1)$
$q_3=2$
$x_3=x_2-2=(0,-1)=(0,1)=1(\text{mod } \beta_3)$, где $\beta_3=(2)$.
$x_3 \cdot 3^{-1}(\text{mod } \beta_3)=1\cdot 1=1$
$q_4=1 \Rightarrow$ x, представленное вектором (6,4,2,1), является отрицательным целым числом.

9Вычислите символ Лежандра $\left(\frac{17}{23}\right)$.

$$\left(\frac{17}{23}\right)=\left(\frac{23}{17}\right)(-1)^{11\cdot 8}=\left(\frac{6}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{3}{17}\right)=\left(\frac{2}{17}\right)\left(\frac{17}{3}\right)(-1)^{8\cdot 1}=\left(\frac{2}{17}\right)\left(\frac{2}{3}\right)=$$

$$(-1)^{\frac{17^2-1}{8}}(-1)^{\frac{3^2-1}{8}}=-1.$$

10Имеет ли решение сравнение $x^2 \equiv 17 \pmod{23}$? Если да, то какое?

Решений в данном случае нет, так как соответствующий символ Лежандра $\left(\frac{17}{23}\right)$ равен -1.

11Вычислите символ Якоби $\left(\frac{9}{32}\right)$.

$$\left(\frac{9}{32}\right)=\left(\frac{9}{2}\right)^5=\left(\frac{9}{2}\right)=\left(\frac{1}{2}\right)=1.$$

12Существует ли решение сравнения $x^2 \equiv 8 \pmod{33}$? Если да, то какое?

Если такой x существует, то он удовлетворяет системе $\begin{cases} x \equiv s_3 (\text{mod} 3), \\ x \equiv s_{11} (\text{mod} 11), \end{cases}$

где $s_3^2 \equiv 8 (\mathrm{mod}\ 3) \equiv 2 (\mathrm{mod}\ 3)$, а $s_{11}^2 \equiv 8 (\mathrm{mod}\ 11)$.

Подходящего значения s_3 не существует, т.к. $\left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$, более того, подходящего значения s_{11} – тоже. Таким образом, система, а вместе с ней и сравнение $x^2 \equiv 8 (\mathrm{mod}\ 33)$, решений не имеют.

3 Варианты заданий

Вариант 1

1С помощью алгоритма Евклида найдите НОД(8771, 3206).
Ответ: а) 77; б) 7; в) 42; г) 1; д) правильный ответ не указан.

2Найдите НОД(314, 918) с помощью расширенного алгоритма Евклида.
Ответ: а) 14; б) 38; в) 1; г) 2; д) правильный ответ не указан.

3Найдите x, y$\in$ **Z**, такие, что 34x+13y=8.
Ответ: а) (40, -104); б) (5, -13); в) (40+13k, -104+34k); г) правильный ответ не указан.

4Найдите все x, y$\in$ **Z**, такие, что 5x+12y=18.
Ответ: а) (-2, 5); б) (-36-12k, 90+5k); в) (90-12k, -36+5k); г) (90, -36); д) правильный ответ не указан.

5Найдите $5^{148} (\mathrm{mod}\ 37)$.
Ответ: а) 33; б) 5; в) 25; г) 1; д) правильный ответ не указан.

6Вычислите $16^{-1} (\mathrm{mod}\ 23)$.
Ответ: а) 16; б) 13; в) 128; г) -10.

7Решите систему сравнений

$$\begin{cases} x \equiv 2 (\mathrm{mod}\ 7), \\ x \equiv 3 (\mathrm{mod}\ 5), \\ x \equiv 4 (\mathrm{mod}\ 9). \end{cases}$$

8Найдите знак числа (6,3,1,1) по вектору (7,5,3,2).

9Вычислите символ Лежандра $\left(\frac{13}{17}\right)$.

Ответ: а) 1; б) -1; в) 0; г) 5.

10Имеет ли решение сравнение $x^2 \equiv 13 (\mathrm{mod}\ 17)$? Если да, то какое?

11Вычислите символ Якоби $\left(\frac{15}{28}\right)$.

Ответ: а) 1; б) -1; в) 0; г) 5.

12Существует ли решение сравнения $x^2 \equiv 11 (\mathrm{mod}\ 33)$? Если да, то какое?

Вариант 2

1С помощью алгоритма Евклида найдите НОД(1738, 4131).
Ответ: а) 13; б) 9; в) 23; г) 1; д) правильный ответ не указан.

2Найдите НОД(217, 413) с помощью расширенного алгоритма Евклида.
Ответ: а) 7; б) 13; в) 1; г) 11; д) правильный ответ не указан.

3Найдите x, y$\in$ **Z**, такие, что 5x+12y=18.
Ответ: а) (-2, 5); б) (-36-12k, 90+5k); в) (90-12k, -36+5k); г) (90, -36); д) правильный ответ не указан.

4Найдите все x, y$\in$ **Z**, такие, что 15x+36y=3.
Ответ: а) (5,-2); б) (-2,5); в) (5-12k, -2+5k); г) (-2-5k, 5+12k); д) правильный ответ не указан.

5Найдите $4^{53}(\mathrm{mod}\ 11)$.
Ответ: а) 16; б) 4; в) 1; г) 9; д) правильный ответ не указан.

6Вычислите $38^{-1}(\mathrm{mod}\ 41)$.
Ответ: а) -14; б) 27; в) 109; г) 1.

7Решите систему сравнений

$$\begin{cases} x \equiv 2(\mathrm{mod}\,3), \\ x \equiv 3(\mathrm{mod}\,5), \\ x \equiv 11(\mathrm{mod}\,13). \end{cases}$$

8Найдите знак числа (6,0,2,1) по вектору (7,5,3,2).

9Вычислите символ Лежандра $\left(\frac{15}{17}\right)$.
Ответ: а) 1; б) -1; в) 0; г) 2.

10Имеет ли решение сравнение $x^2\equiv 14(\mathrm{mod}17)$? Если да, то какое?

11Вычислите символ Якоби $\left(\frac{13}{25}\right)$.
Ответ: а) 1; б) -1; в) 0; г) 2.

12Существует ли решение сравнения $x^2\equiv 8(\mathrm{mod}\ 35)$? Если да, то какое?

Вариант 3

1С помощью алгоритма Евклида найдите НОД(3365, 1320).
Ответ: а) 5; б) 15; в) 65; г) 1; д) правильный ответ не указан.

2Найдите НОД(8771, 3206) с помощью расширенного алгоритма Евклида.
Ответ: а) 6; б) 23; в) 1; г) 12; д) правильный ответ не указан.

3Найдите x, y$\in$ **Z**, такие, что 12x+21y=1.
Ответ: а) (1, -1); б) $\varnothing$; в) (1+3k,-1+4k); г) правильный ответ не указан.

4Найдите все x, y$\in$ **Z**, такие, что 34x+13y=8.
Ответ: а) (40, -104); б) (5, -13); в) (40+13k, -104+34k); г) правильный ответ не указан.

5Найдите $2^{39} \pmod{29}$.
Ответ: а) 4; б) 2; в) 1; г) 39; д) правильный ответ не указан.

6Вычислите $21^{-1} \pmod{23}$.
Ответ: а) 17; б) 1; в) 11; г) -2.

7Решите систему сравнений

$$\begin{cases} x \equiv 5 \pmod{13}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}. \end{cases}$$

8Найдите знак числа (5,2,1,1) по вектору (7,5,3,2).

9Вычислите символ Лежандра $\left(\frac{15}{19}\right)$.
Ответ: а) 3; б) -1; в) 0; г) 1.

10Имеет ли решение сравнение $x^2 \equiv 15 \pmod{19}$? Если да, то какое?

11Вычислите символ Якоби $\left(\frac{11}{28}\right)$.
Ответ: а) 3; б) -1; в) 0; г) 1.

12Существует ли решение сравнения $x^2 \equiv 9 \pmod{42}$? Если да, то какое?

Вариант 4

1С помощью алгоритма Евклида найдите НОД(9457, 3211).
Ответ: а) 7; б) 47; в) 31; г) 1; д) правильный ответ не указан.

2Найдите НОД(3365, 1320) с помощью расширенного алгоритма Евклида.
Ответ: а) 1; б) 15; в) 5; г) 135; д) правильный ответ не указан.

3Найдите x, y$\in$ **Z**, такие, что 15x+36y=3.
Ответ: а) (5,-2); б) (-2,5); в) (5-12k, -2+5k); г) (-2-5k, 5+12k); д) правильный ответ не указан.

4Найдите все x, y$\in$ **Z**, такие, что 34x-13y=8.
Ответ: а) (40, 104); б) (5, 13); в) (40+13k, -104+34k); г) (40+13k, 104+34k); д) правильный ответ не указан.

5Найдите $3^{52}(\mathrm{mod}\ 17)$.
Ответ: а) 13; б) 3; в) 1; г) 81; д) правильный ответ не указан.

6Вычислите $9^{-1}(\mathrm{mod}\ 19)$.
Ответ: а) 1; б) 17; в) 36; г) -2 .

7Решите систему сравнений

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

8Найдите знак числа (6,2,2,1) по вектору (7,5,3,2).

9Вычислите символ Лежандра $\left(\frac{15}{23}\right)$.
Ответ: а) -1; б) 1; в) 0; г) -2.

10Имеет ли решение сравнение $x^2\equiv 15(\mathrm{mod}23)$? Если да, то какое?

11Вычислите символ Якоби $\left(\frac{9}{28}\right)$.
Ответ: а) -1; б) 1; в) 0; г) -2.

12Существует ли решение сравнения $x^2\equiv 7(\mathrm{mod}\ 35)$? Если да, то какое?

4 Таблица правильных ответов

№ задания	№ варианта			
	1	2	3	4
1	б	г	а	г
2	г	а	д	в
3	а	в,г	б	а,в
4	в	в	г	г
5	а	г	д	а
6	б	б	в	б
7	58(mod 315)	128(mod 195)	408(mod 455)	23(mod 105)
8	«+»	«–»	«–»	«–»
9	а	а	б	а
10	8 и 9	нет	нет	нет
11	а	а	г	б
12	нет	нет	3 и 39	нет

5 Решения

1.1 $8771=3206\cdot2+2359$,
$3206=2359\cdot1+847$,
$2359=847\cdot2+665$,
$847=665\cdot1+182$,
$665=182\cdot3+119$,
$182=119\cdot1+63$,
$119=63\cdot1+56$,
$63=56\cdot1+7$,
$56=7\cdot8 \Rightarrow$ НОД(8771, 3206)=7.

2.1 $4131=1738\cdot2+655$
$1738=655\cdot2+428$
$655=428\cdot1+227$
$428=227\cdot1+201$
$227=201\cdot1+26$
$201=26\cdot7+19$
$26=19\cdot1+7$
$19=7\cdot2+5$
$7=5\cdot1+2$
$5=2\cdot2+1$
$2=1\cdot2 \Rightarrow$ НОД (1738, 4131)=1.

3.1 $3365=1320\cdot2+725$
$1320=725\cdot1+595$
$725=595\cdot1+130$
$595=130\cdot4+75$
$130=75\cdot1+55$
$75=55\cdot1+20$
$55=20\cdot2+15$
$20=15\cdot1+5$
$15=5\cdot3 \Rightarrow$ НОД (3365,1320)=5

4.1 $9457=3211\cdot2+3035$
$3211=3035\cdot1+176$
$3035=176\cdot17+43$
$176=43\cdot4+4$
$43=4\cdot10+3$
$4=3\cdot1+1$
$3=1\cdot3 \Rightarrow$ НОД (9457,3211)=1

1.2

i	a_i	x_i	y_i	q_i
0	918	1	0	–
1	314	0	1	2
2	290	1	-2	1
3	24	-1	3	12
4	2	13	-38	12
5	0			

НОД (314,918)=2=314·(-38)+918·13

2.2

i	a_i	x_i	y_i	q_i
0	413	1	0	–
1	217	0	1	1
2	196	1	–1	1
3	21	–1	2	9
4	7	10	–19	3
5	0			

НОД(217, 413)=7=413·10+217·(-19)

3.2

i	a_i	x_i	y_i	q_i
0	8771	1	0	–
1	3206	0	1	2
2	2359	1	–2	1
3	847	–1	3	2
4	665	3	–8	1
5	182	–4	11	3
6	119	15	–41	1
7	63	–19	52	1
8	56	34	–93	1
9	7	–53	145	8
10	0			

НОД(8771, 3206)=7=8771·(–53)+3206·145

4.2

i	a_i	x_i	y_i	q_i
0	3365	1	0	–
1	1320	0	1	2
2	725	1	–2	1
3	595	–1	3	1
4	130	2	–5	4

5	75	–9	23	1
6	55	11	–28	1
7	20	–20	51	2
8	15	51	–130	1
9	5	–71	181	3
10	0			

НОД(3365, 1320)=5=3365·(-71)+1320·181

1.3

34	1	0	–
13	0	1	2
8	1	–2	1
5	–1	3	1
3	2	–5	1
2	–3	8	1
1	5	–13	2
0			

$34\cdot5+13\cdot(-13)=1 \Rightarrow 34\cdot40+13\cdot(-104)=8 \Rightarrow$ (40,–104) – частное решение, а (40–13k, –104+34k), $k\in\mathbf{Z}$, – общее решение уравнения.

2.3

12	1	0	–
5	0	1	2
2	1	–2	2
1	–2	5	2
0			

$1=5\cdot5+12\cdot(-2) \Rightarrow 18=5\cdot90+12\cdot(-36) \Rightarrow$ (90,–36) – частное решение, а (90–12k, –36+5k), $k\in\mathbf{Z}$, – общее решение уравнения.

4.3

$15x+36y=3 \Leftrightarrow 5x+12y=1$. См. 2.3. (5–12k, –2+5k), $k\in\mathbf{Z}$, – общее решение.

1.5 $5^{148}(\text{mod } 37)=(5^{36})\cdot5^4(\text{mod } 37)=5^4(\text{mod } 37)=33$

2.5 $4^{53}(\text{mod } 11)=(4^{10})^5\cdot4^3(\text{mod } 11)=4^3(\text{mod } 11)=9$

3.5 $2^{39}(\text{mod } 29)=(2^{28})\cdot2^{11}(\text{mod } 29)=2^{11}(\text{mod } 29)$
$11 \rightarrow 1011_2 \rightarrow SM_2SSM_2SM_2 \rightarrow SSM_2SM_2 \rightarrow 2^{11}(\text{mod } 29) = ((2^2)^2\cdot2)^2\cdot2(\text{mod } 29) =$
$= 3^2\cdot2(\text{mod } 29) =18$

4.5 $3^{52}(\text{mod } 17)=(3^{16})^3\cdot3^4(\text{mod } 17)=3^4(\text{mod } 17)=13$

1.6 $16^{-1}(\text{mod } 23)=4^{-2}(\text{mod } 23)=(4^{-1})^2(\text{mod } 23)=36(\text{mod } 23)=13$

2.6

41	0	–
38	1	1
3	–1	12
2	13	1
1	–14	2
0		

$38\cdot(-14)\equiv 1 \pmod{41} \Rightarrow 38^{-1} \pmod{41} = 27$

3.6 $21^{-1} \pmod{23} = 11$, так как

23	0	–
21	1	1
2	–1	10
1	11	2
0		

4.6

I способ – РАЕ:

i	a_i	y_i	q_i
0	19	0	–
1	9	1	2
2	1	–2	9
3	0		

$-2 \pmod{19} = 17 \pmod{19} \Rightarrow 9^{-1} = 17 \pmod{19}$

II способ:

$9^{-1} = 9^{17} \pmod{19}$

$17 = 10001_2 \rightarrow SM_9SSSSM_9 \rightarrow SSSSM_9 \rightarrow 9^{17} \pmod{19} = (((9^2)^2)^2)^2 \cdot 9 \pmod{19} =$

$= ((5^2)^2)^2 \cdot 9 \pmod{19} = (6^2)^2 \cdot 9 \pmod{19} = 17^2 \cdot 9 \pmod{19} = 36 \pmod{19} = 17$

$9^{-1} = 17 \pmod{19}$

1.7

$x = 7k+2$, $k \in \mathbf{Z}$

$7k+2 \equiv 3 \pmod{5}$

$7k \equiv 1 \pmod{5}$

$k \equiv 7^{-1} \pmod{5}$

$k \equiv 3 \pmod{5}$

$k = 5l+3$, $l \in \mathbf{Z}$

$x = 7k+2 = 7(5l+3)+2 = 23+35l$, $l \in \mathbf{Z}$

$23+35l \equiv 4 \pmod{9}$

$5+8l \equiv 4 \pmod{9}$

$8l \equiv 8 \pmod 9$
$l \equiv 1 \pmod 9$
$l = 9m+1,\ m \in \mathbf{Z}$
$x = 23+35l = 23+35(9m+1) = 58+415m,\ m \in \mathbf{Z}$
$x \equiv 58 \pmod{415}$

2.7
$x = 3k+2,\ k \in \mathbf{Z}$
$3k+2 \equiv 3 \pmod 5$
$3k \equiv 1 \pmod 5$
$k \equiv 2 \pmod 5 \Rightarrow k = 5l+2,\ l \in \mathbf{Z}$
$x = 3k+2 = 3(5l+2)+2 = 15l+8,\ l \in \mathbf{Z}$
$15l+8 \equiv 11 \pmod{13}$
$15l \equiv 3 \pmod{13}$
$2l \equiv 3 \pmod{13}$
$l \equiv 3 \cdot 2^{-1} \pmod{13} \equiv 8 \pmod{13} \Rightarrow l = 13m+8,\ m \in \mathbf{Z}$
$x = 15(13m+8)+8 = 128+195m,\ m \in \mathbf{Z}$
$x \equiv 128 \pmod{195}$

3.7
$x = 13k+5,\ k \in \mathbf{Z}$
$13k+5 \equiv 3 \pmod 5$
$13k \equiv 3 \pmod 5$
$3k \equiv 3 \pmod 5$
$k \equiv 1 \pmod 5 \Rightarrow k = 5l+1,\ l \in \mathbf{Z}$
$x = 13k+5 = 13(5l+1)+5 = 18+65l,\ l \in \mathbf{Z}$
$18+65l \equiv 2 \pmod 7$
$4+2l \equiv 2 \pmod 7$
$2l \equiv 5 \pmod 7$
$l \equiv 5 \cdot 2^{-1} \pmod 7$
$l \equiv 6 \pmod 7 \Rightarrow l = 7m+6,\ m \in \mathbf{Z}$
$x = 18+65l = 18+65(7m+6) = 408+455m,\ m \in \mathbf{Z}$
$x \equiv 408 \pmod{455}$

4.7
$x = 3k+2,\ k \in \mathbf{Z}$
$3k+2 \equiv 3 \pmod 5$
$3k \equiv 1 \pmod 5$
$k \equiv 2 \pmod 5 \Rightarrow k = 5l+2,\ l \in \mathbf{Z}$
$x = 3k+2 = 3(5l+2)+2 = 8+(3 \cdot 5)l$
$8+15l \equiv 2 \pmod 7$

$15l \equiv 1 \pmod 7$

$l \equiv 1 \pmod 7 \Rightarrow l = 7z+1,\ z \in \mathbf{Z}$

$x = 8+(3\cdot 5)l = 23+(3\cdot 5\cdot 7)z,\ z \in \mathbf{Z} \Rightarrow x \equiv 23 \pmod{3\cdot 5\cdot 7}$

1.8

$q_1 = 6$

$x' = x-6 = (0,2,1,1) = (2,1,1)$ по вектору $\beta_1 = (5,3,2)$

$7^{-1} \pmod{\beta_1} = (3,1,1)$

$x' \cdot 7^{-1} \pmod{\beta_1} = (1,1,1)$

$q_2 = 1$

$x'' = (1,1,1)-1 = (0,0,0) = 0 \Rightarrow x > 0$

2.8

$q_1 = 6$

$x' = x-6 = (0,-6,-4,-5) = (4,2,1)$ по вектору $\beta_1 = (5,3,2)$

$x' \cdot 7^{-1} \pmod{\beta_1} = (2,2,1)$

$q_2 = 2$

$x'' = x'-2 = (0,0,-1) = (0,0,1) = (0,1)$ по вектору $\beta_2 = (3,2)$

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

$x'' \cdot 5^{-1} \pmod{\beta_2} = (0,1)$

$q_3 = 0$

x1)=‴) по вектору $\beta_3 = (2)$

$3^{-1} \pmod{\beta_3} = (1)$

$x3^{-1} \cdot ‴ \pmod{\beta_3} = 1$

$q_4 = 1 \Rightarrow x < 0$

1.9

$$\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)\cdot(-1)^{6\cdot 8} = \left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{2}{13}\right) = 1$$

2.9

$$\left(\frac{15}{17}\right) = \left(\frac{3}{17}\right)\left(\frac{5}{17}\right) = \left(\frac{17}{3}\right)\left(\frac{17}{5}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1)^3 = 1$$

3.9

$$\left(\frac{15}{19}\right) = \left(\frac{3\cdot 5}{19}\right) = \left(\frac{3}{19}\right)\left(\frac{5}{19}\right) = \left(\frac{19}{3}\right)\cdot(-1)^{1\cdot 9}\left(\frac{19}{5}\right)(-1)^{2\cdot 9} = \left(\frac{1}{3}\right)(-1)\left(\frac{4}{5}\right)\cdot 1 = -1$$

4.9

$$\left(\frac{15}{23}\right) = \left(\frac{3}{23}\right)\left(\frac{5}{23}\right) = \left(\frac{2}{3}\right)(-1)^{1\cdot 11}\left(\frac{3}{5}\right)(-1)^{11\cdot 2} = \left(\frac{2}{3}\right)(-1)\left(\frac{5}{3}\right)(-1)^{2\cdot 1} = \left(\frac{2}{3}\right)^2(-1) = -1$$

1.10

Так как символ Лежандра $\left(\frac{13}{17}\right)$ равен 1, сравнение имеет решение. Подбором легко убедиться, что это значения 8 и 9. В общем случае необходимо воспользоваться одним из специальных алгоритмов, например, алгоритмом Шэнкса.

Поясним его работу на примере решения сравнения $x^2 \equiv 15 \pmod{17}$.

Т.к. $\left(\frac{15}{17}\right) = 1$, решение существует: это пара x, 17–x из $\mathbf{Z}_{17}$.

$x_1=7$, $x_2=10$, что легко получить подбором.

Алгоритм Шэнкса даст тот же результат:

1) n=3, т.к. $\left(\frac{3}{17}\right) = -1$
2) $p-1=16=2^4 \cdot 1 \Rightarrow e=4$, q=1
3) $y=3 \pmod{17}$, r=4, $x=15^0 \pmod{17}=1 \pmod{17}$
4) $b=15 \pmod{17}$, $x=15 \pmod{17}$
5) $b \neq 1$: а) наименьшее m: $15^{2^m}=1 \pmod{17}$, m=3

   б) $t=3^{2^0}=3 \pmod{17}$, $y=9 \pmod{17}$, r=3

   в) $x=11 \pmod{17}$, $в=16 \pmod{17}$

$b \neq 1$: а) m: $16^{2^m}=1 \pmod{17}$, m=1

б) $t=9^2 \pmod{17}=13 \pmod{17}$, $y=16 \pmod{17}$, r=1

в) **$x=7 \pmod{17}$**, $b=1 \pmod{17}$.

2.10-4.10 соответствующие этим случаям символы Лежандра равны -1, значит, приведенные сравнения решений не имеют.

1.11

$$\left(\frac{15}{28}\right) = \left(\frac{15}{2}\right)\left(\frac{15}{2}\right)\left(\frac{15}{7}\right) = \left(\frac{15}{7}\right) = \left(\frac{1}{7}\right) = 1.$$

2.11

$$\left(\frac{13}{25}\right) = \left(\frac{13}{5}\right)^2 = 1.$$

3.11

$$\left(\frac{11}{28}\right) = \left(\frac{11}{2}\right)^2 \cdot \left(\frac{11}{7}\right) = \left(\frac{11}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2}{7}\right)^2 = 1.$$

4.11

$$\left(\frac{9}{28}\right)=\left(\frac{9}{2}\right)^2\cdot\left(\frac{9}{7}\right)=\left(\frac{9}{7}\right)=\left(\frac{2}{7}\right)=(-1)^6=1.$$

1.12

$x^2\equiv 11 \pmod{33} \Leftrightarrow \begin{cases} x\equiv y \pmod 3, \\ x\equiv z \pmod{11}, \end{cases}$ где $y^2\equiv 11 \pmod 3 \equiv 2 \pmod 3$, $z^2\equiv 11 \pmod{11} \equiv 0 \pmod{11}$. $\Rightarrow y\in\varnothing$, $z\equiv 0 \pmod{11} \Rightarrow x\in\varnothing$.

2.12

$x^2\equiv 8 \pmod{35} \Leftrightarrow \begin{cases} x\equiv y \pmod 5, \\ x\equiv z \pmod 7, \end{cases}$

где $y^2\equiv 8 \pmod 5 \equiv 3 \pmod 5$, $z^2\equiv 8 \pmod 7 \equiv 1 \pmod 7$.
$y\in\varnothing$, $z\equiv 1 \pmod{11}$ или $z\equiv 10 \pmod{11} \Rightarrow x\in\varnothing$.

3.12

$x^2\equiv 9 \pmod{42} \Leftrightarrow \begin{cases} x\equiv y \pmod 2, \\ x\equiv z \pmod 2, \\ x\equiv t \pmod 7, \end{cases}$ где $y^2\equiv 9 \pmod 2 \equiv 1 \pmod 2$, $z^2\equiv 9 \pmod 3 \equiv 0 \pmod 3$, $t^2\equiv 9 \pmod 7 \equiv 2 \pmod 7$. Значит, $y=1$, $z=0$, $t_1=3$, $t_2=4$. Таким образом,

$x^2\equiv 9 \pmod{42} \Leftrightarrow \left[\begin{array}{l} \begin{cases} x\equiv 1 \pmod 2, \\ x\equiv 0 \pmod 3, \\ x\equiv 3 \pmod 7, \end{cases} \\ \begin{cases} x\equiv 1 \pmod 2, \\ x\equiv 0 \pmod 3, \\ x\equiv 4 \pmod 7. \end{cases} \end{array}\right.$ Первая система имеет решение $x\equiv 3 \pmod{42}$,

вторая – $x\equiv 39 \pmod{42}$.

4.12

$x^2\equiv 7 \pmod{35} \Leftrightarrow \begin{cases} x\equiv y \pmod 5, \\ x\equiv z \pmod 7, \end{cases}$ где $y^2\equiv 7 \pmod 5 \equiv 2 \pmod 5$, $z^2\equiv 7 \pmod 7 \equiv 0 \pmod 7$. $y\in\varnothing$, так как символ Лежандра $\left(\frac{2}{5}\right)=-1$; $z=0$. $\Rightarrow x\in\varnothing$.

Список использованных источников

1**Акритас, А.** Основы компьютерной алгебры с приложениями/ А. Акритас. – М.: Мир, 1994.
2**Смарт, Н.** Криптография/ Н. Смарт. – М.: Техносфера, 2005.
3**Черемушкин, А.В.** Лекции по арифметическим алгоритмам в криптографии/ А.В. Черемушкин. – М.: МЦНМО, 2002.