МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

КАФЕДРА «ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

ТЕОРИЯ СРАВНЕНИЙ

Методические указания к выполнению лабораторных работ
по дисциплине
«Криптографические методы защиты информации»
для студентов специальности
1 – 40 03 01 «Искусственный интеллект»

Брест 2019

УДК 347 77/681.3
ББК 67.403.3 73/32.97

В методических указаниях приведены необходимые теоретические сведения по теории сравнений. Методические указания содержат информацию о свойствах сравнений, способах решения сравнений первой степени с одним неизвестным и решения сравнений произвольной степени с одним неизвестным. Содержатся основные вспомогательные алгоритмы для решения сравнений первой степени с одним неизвестным и произвольной степени с одним неизвестным.

Методические указания предназначены для использования студентами специальности 1-40 03 01 «Искусственный интеллект» в ходе выполнения лабораторных работ по дисциплине «Криптографические методы защиты информации».

Составитель: Хацкевич М. В., старший преподаватель кафедры ИИТ

Рецензент: Худяков А. П., доцент кафедры прикладной математики и информатики Учреждения образования «Брестский государственный университет» им. А.С. Пушкина, к.ф-м.н, доцент.

Учреждение образования

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Вместе с возникновением в криптографии новых понятий и методов расширился и круг применения теории чисел в криптографии. В дополнение к элементарной и аналитической теории чисел все более широко используется алгебраическая теория чисел (тесты на простоту с применением сумм Гаусса и Якоби, криптосистемы, основанные на квадратичных полях, решето числового поля) и арифметическая алгебраическая геометрия (факторизация при помощи эллиптических кривых, криптосистемы, основанные на эллиптических и гиперэллиптических кривых и абелевых многообразиях).

Важнейшим разделом теории чисел в современной криптографии является теория сравнений.

Цель разработки методических указаний к выполнению лабораторных работ по дисциплине «Криптографические методы защиты информации» – ознакомить студентов с основами математического аппарата, используемого в современной криптографии.

Материал изложен в соответствии с учебной программой для специальности 1 – 40 03 01 «Искусственный интеллект».

В криптографии важную роль играют простые числа. Теория чисел, или высшая арифметика, — раздел математики, первоначально изучавший свойства целых чисел. В методических указаниях рассмотрены алгоритмы нахождения наибольшего общего делителя и представления наибольшего общего делителя двух чисел в виде линейной комбинации этих чисел. Приведен алгоритм формирования непрерывных дробей, который очень часто применяется в криптографии. Описаны важнейшие функции теории чисел, в том числе широко используемая в криптографии функция Эйлера.

Приведена широко используемая в современной криптографии Китайская теорема об остатках. Рассмотрены алгоритмы решения сравнений первой степени с одним неизвестным и сравнений произвольной степени с одним неизвестным.

Изучение дисциплины «Криптографические методы защиты информации» предполагает проведение лабораторных занятий. В связи с этим в методических указаниях приведены практические примеры. Решение и изучение предлагаемых в методических указаниях упражнений поможет более глубокому усвоению изложенного материала.

1 МАТЕМАТИЧЕСКИЕ ОСНОВЫ

1.1 ОСНОВНЫЕ ПОНЯТИЯ

***Определение* 1.** Говорят, что *a* делится на *b*, если $a = bq$ и $q \in z$. При этом *a* называют кратным числа *b*, а *b*- делителем числа a.

Теорема 1 (о делении с остатком). Всякое целое *a* можно представить с помощью положительного целого числа *b* равенством вида $a = bq + r$, $0 \le r < b$.

Число *q* называется *неполным частным*, а число *r*-остатком от деления *a* на *b*.

***Определение* 2.** Всякое целое, делящее одновременно целые *a*, *b*, называется их *общим делителем*.

Определение 3. Наибольший из общих делителей чисел a и b называется общим наибольшим делителем и обозначается символом (a,b). Если (a,b)=1,то целые a и b называют взаимно простыми.

Теорема 2. Если a = bq + c , то (a,b)=(b, c). Для отыскания (a,b) при a > b применяется алгоритм Евклида, основанный на теореме 2.

Множество целых чисел {..., –3, –2, –1, 0, 1, 2 , 3,...}.обозначим через **Z**.

Алгоритм Евклида состоит в получении равенств вида: a > b; a, b $\in$**Z** .

$a=bq_0+r_1$	$0<r_1<b$
$b=r_1q_1+r_2$	$0<r_2<r_1$
$r=r_2q_2+r_3$	$0<r_3<r_2$
.....	.....
$r_{n-2}=r_{n-1}q_{n-1}+r_n$	$0<r_n<r_{n-1}$
$r_{n-1}=r_nq_n$	$r_{n+1}=0$

Тогда (a,b)= r_n - последнему не равному нулю остатку алгоритма Евклида.

Пример. Найти с помощью алгоритма Евклида (432, 111).

Решение. Согласно алгоритму Евклида получаем цепочку равенств:

$432=111\cdot3+99$

$111=99\cdot1+12$

$99=12\cdot8+3$

$12=3\cdot4$

Таким образом, наибольший общий делитель чисел 111 и 432 – это 3.

Ответ: НОД(111, 432)=3.

Совокупность делителей *a* и *b* совпадает с совокупностью делителей (*a* , *b*). Алгоритм Евклида дает практический способ нахождения чисел *u* и *v* из **Z**

$r_n = au + bv = (a, b)$.

Действительно, из цепочки равенств имеем:

$$r_n = r_{n-2} - r_{n-1} q_n = r_{n-2} - (r_{n-3} - r_{n-2} q_{n-1}) q_n = \ldots$$

(идем по цепочке равенств снизу вверх, выражая из каждого следующего равенства остаток и подставляя его в получившееся уже к этому моменту выражение)

$$\ldots = au + bv = (a, b).$$

Пример. Пусть *a* = 525, *b* = 231 ,необходимо найти (a,b).

Запишем в виде цепочки равенств:

$$525 = 231 \cdot 2 + 63$$
$$231 = 63 \cdot 3 + 42$$
$$63 = 42 \cdot 1 + 21$$
$$42 = 21 \cdot 2$$

Таким образом, (525, 231) = 21. Линейное представление наибольшего общего делителя (обратный ход алгоритма Евклида):

$21 = 63 - 42\cdot 1 = 63 - (231 - 63\cdot 3)\cdot 1 = 525 - 231\cdot 2 - (231 - (525 - 231\cdot 2)\cdot 3) = 525\cdot 4 - 231\cdot 9$

и наши пресловутые u и v из $\mathbf{Z}$ равны, соответственно, 4 и - 9.

Определение 4. Всякое целое, большее 1, имеющее только два положительных делителя, именно 1 и самого себя, называется простым. Заметим, что 1 не является простым числом. Среди первых 100 чисел простыми являются следующие 25 чисел: 2, 3, 5, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67,71, 73, 79, 83, 89, 97.

Теорема 3. Простых чисел бесконечно много.

Теорема 4. Всякое целое, большее единицы, разлагается на произведение простых сомножителей и притом единственным способом. Обозначая буквами $p_1, p_2, ..., p_k$ различные простые сомножители, а буквами $\alpha_1,\alpha_2, ...,\alpha_K$ кратности их вхождения в а, получим каноническое разложение числа а на сомножители: $a = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot ....\cdot p_k^{\alpha_k}$.

Определение 5. Функция $\varphi(m)$, определенная на множестве натуральных чисел, называется функцией Эйлера, если значение $\varphi(m)$ равно числу натуральных чисел, не превышающих m и взаимно простых с m, а $\varphi(1) = 1$.

Если m >1 имеет разложение на простые множители вида:

$m = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot ....\cdot p_k^{\alpha_k}$, то

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right).$$

Теорема 5. (Эйлер). Пусть m>1 , (a,m)=1 , $\varphi(m)$ – функция Эйлера. Тогда:

$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m)$.

Пример. Вычислить $\varphi(180)$.

Решение. $180 = 2^2\cdot 3^3\cdot 5$.Следовательно

$$\varphi(180) = 180\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 180\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} = 48.$$

Теорема 6 (Ферма). Пусть p – простое число, p не делит a . Тогда:

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p) .$$

Следствие 1. Без всяких ограничений на $a \in \mathbf{Z}$,

$$a^p \equiv a (\mathrm{mod}\ p) .$$

Следствие 2. $(a+b)^p \equiv a^p + b^p (\mathrm{mod}\ p)$.

Пример. Доказать, что $1^{18}+2^{18}+3^{18}+4^{18}+5^{18}+6^{18} \equiv -1 (\mathrm{mod}\ 7)$.

Доказательство. Числа 1, 2, 3, 4, 5, 6 взаимно просты с 7. По теореме Ферма имеем:

$$\begin{cases} 1^6 \equiv 1 (\mathrm{mod}\, 7) \\ 2^6 \equiv 1 (\mathrm{mod}\, 7) \\ \quad\vdots \\ 6^6 \equiv 1 (\mathrm{mod}\, 7) \end{cases}$$

Возведем эти сравнения в куб и сложим:

$1^{18}+2^{18}+3^{18}+4^{18}+5^{18}+6^{18} \equiv 6 (\mathrm{mod}\ 7) \equiv -1 (\mathrm{mod} 7)$.

1.2 РАЗЛОЖЕНИЕ ЧИСЕЛ В ЦЕПНЫЕ ДРОБИ

Пусть $a > 0$, $m > 0$ и $(a,m) = 1$. Применяя к дроби $\frac{m}{a}$ алгоритм Евклида, имеем:

$$m = aq_0 + a_1 \quad (1)$$
$$a = a_1q_1 + a_2 \quad (2)$$
$$a_1 = a_2q_2 + a_3 \quad (3)$$
$$\dots\dots\dots\dots$$
$$a_{k-2} = a_{k-1}q_{k-1} + a_k \quad (k)$$
$$a_{k-1} = a_kq_k + 0 \quad (k+1)$$

Из равенства (1) имеем $\frac{m}{a} = q_0 + \frac{a_1}{a} = q_0 + \frac{1}{a}$.

Из равенства (2) имеем $\frac{a}{a_1} = q_1 + \frac{a_2}{a_1} = q_1 + \frac{1}{\frac{a_1}{a_2}}$.

Откуда

$$\frac{m}{a} = q_0 + \frac{1}{q_1 + \frac{1}{\frac{a_1}{a_2}}} \quad (1.1)$$

Из равенства (3) имеем $\frac{a_1}{a_2} = q_2 + \frac{a_3}{a_2} = q_2 + \frac{1}{\frac{a_2}{a_3}}$.

Подставляя $\frac{a_1}{a_2}$ в равенство (1.1), имеем

$$\frac{m}{a} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{a_2}{a_3}}}.$$

Продолжая этот процесс для оставшихся равенств, получим

$$\frac{m}{a} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}}.$$

Правую часть этого равенства называют конечной цепной дробью и обозначают ее $[q_0,q_1,q_2,...,q_k]$. Итак, получили разложение числа $\frac{m}{a}$ в конечную цепную дробь

$$\frac{m}{a}=[q_0,q_1,q_2,...,q_k].$$

Пример. Разложить $\frac{105}{38}$ в цепную дробь.

Решение. Применяя к числу $\frac{105}{38}$ алгоритм Евклида, получим:

$$105 = 38 \cdot \underline{2} + 29$$
$$38 = 29 \cdot \underline{1} + 9$$
$$29 = 9 \cdot \underline{3} + 2$$
$$9 = 2 \cdot \underline{4} + 1$$
$$2 = 1 \cdot \underline{2}$$

Неполные частные подчеркнуты, теперь для написания ответа нужно аккуратно расположить их подряд на «этажах» цепной дроби перед знаками плюс:

$$\frac{105}{38}=2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{4+\frac{1}{2}}}}.$$

Итак, получили разложение числа $\frac{105}{38}$ в конечную цепную дробь

$$\frac{105}{38}=[2,1,3,4,2].$$

1.3 ПОДХОДЯЩИЕ ДРОБИ И ИХ ВЫЧИСЛЕНИЕ

Дроби вида $\delta_0=q_0,\delta_1=q_0+\frac{1}{q_1},\delta_2=q_0+\cfrac{1}{q_1+\frac{1}{q_2}},.....$ называются подходящими дробями

к цепной дроби $[q_0,q_1,q_2,...,q_K]=\frac{m}{a}$.

Пример, разложение числа $\frac{985}{533}$ в конечную цепную дробь.

Применяя к числу $\frac{985}{533}$ алгоритм Евклида, получим:

$985 = 533 \cdot \underline{1} + 452$
$533 = 452 \cdot \underline{1} + 81$
$452 = 81 \cdot \underline{5} + 47$
$81 = 47 \cdot \underline{1} + 34$

$47 = 34 \cdot \underline{1} + 13$
$34 = 13 \cdot \underline{2} + 8$
$13 = 8 \cdot \underline{1} + 5$
$8 = 5 \cdot \underline{1} + 3$
$5 = 3 \cdot \underline{1} + 2$
$3 = 2 \cdot \underline{1} + 1$
$2 = 1 \cdot \underline{2}$

Тогда, разложение числа $\frac{985}{533}$ в конечную цепную дробь $\frac{985}{533} = [1,1,5,1,1,2,1,1,1,1,2]$.

Подходящими дробями к цепной дроби [1,1,5,1,1,2,1,1,1,1,2] являются

$$\delta_0 = 1 = \frac{1}{1}, \delta_1 = 1 + \frac{1}{1} = \frac{2}{1}, \delta_2 = 1 + \frac{1}{1 + \frac{1}{5}}, \delta_3 = 1 + \frac{1}{1 + \frac{1}{5 + \frac{1}{1}}}, \ldots\ldots\ldots,$$

$$\delta_{10} = 1 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{2}}}}}}}}}}$$

Вывод рекуррентной формулы вычисления подходящей дробей основан на простой идее представления подходящих дроби δ_k в виде $\frac{P_k}{Q_k}$.

$$\delta_0 = q_0 = \frac{q_0}{1} = \frac{P_0}{Q_0} = \infty; (P_0 = q_0; Q_0 = 1)$$

$$\delta_1 = q_0 + \frac{1}{q_1} = \frac{q_0 + \frac{1}{q_1}}{1} = \frac{q_1 q_0 + 1}{q_1 \cdot 1 + 0} = \frac{q_1 P_0 + P_{-1}}{q_1 Q_0 + Q_{-1}} = \frac{P_1}{Q_1}; (P_{-1} = 1; Q_{-1} = 0)$$

$$\delta_2 = q_0 + \frac{1}{q_1 + \frac{1}{q_2}} = \frac{\left(q_1 + \frac{1}{q_2}\right) q_0 + 1}{\left(q_1 + \frac{1}{q_2}\right) \cdot 1 + 0} = \frac{\left(q_1 + \frac{1}{q_2}\right) \cdot P_0 + P_{-1}}{\left(q_1 + \frac{1}{q_2}\right) \cdot Q_0 + Q_{-1}} =$$

$$= \frac{q_1 \cdot P_0 q_2 + P_0 + q_2 P_{-1}}{q_1 \cdot Q_0 q_2 + Q_0 + q_2 Q_{-1}} = \frac{q_2 (q_1 P_0 + P_{-1}) + P_0}{q_2 (q_1 Q_0 + Q_{-1}) + Q_0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2}$$

и так далее и вообще при $n \geq 0$ имеем

$$\delta_n = \frac{q_n P_{n-1} + P_{n-2}}{q_n Q_{n-1} + Q_{n-2}} = \frac{P_n}{Q_n}, \text{где } P_{-1} = 1,\ Q_{-1} = 0.$$

При $n = 0$ имеем $\delta_0 = \frac{q_0 P_{-1} + P_{-2}}{q_0 Q_{-1} + Q_{-2}} = \frac{q_0 + P_{-2}}{0 + Q_{-2}}$, но $\delta_0 = q_0$, поэтому еще и : $P_{-2} = 0, Q_{-2} = 1$.

Таким образом, при $n \geq 0$ числители и знаменатели подходящих дробей к цепной дроби $\frac{m}{a} = [q_0, q_1, q_2, ..., q_k]$ вычисляются по формулам:

$P_n = q_n P_{n-1} + P_{n-2}$ при условии, что $P_{-2} = 0, P_{-1} = 1$,

$Q_n = q_n Q_{n-1} + Q_{n-2}$ при условии, что $Q_{-2} = 1, Q_{-1} = 0$.

Вычисления оформим в виде таблицы 1.1:

Таблица 1.1 – Вычисления числителей и знаменателей подходящих дробей

n	-2	-1	0	1	2	....	k-1	k
q_n	*	*	q_0	q_1	q_2	...	Q_{k-1}	Q_{k-2}
P_n	0	1	P_0	P_1	P_2	...	P_{k-1}	P_{k-2}
Q_n	1	0	Q_0	Q_1	Q_2	...	Q_{k-1}	Q_{k-2}

* – пустая клетка.

Из определения подходящей дроби следует, что $q_k = \frac{P_k}{Q_k} = \frac{m}{a}$. Так как $(a,m) = 1$, то $P_k = m, Q_k = a$.

Можно показать, что $P_k \cdot Q_{k-1} - P_{k-1} \cdot Q_k = (-1)^{k-1}$. Умножая это равенство на $(-1)^{k-1}$, получим:

$$(-1)^{k-1} \cdot P_k \cdot Q_{k-1} - P_{k-1} \cdot (-1)^{k-1} \cdot Q_k = (-1)^{2k-2} = 1 \qquad (1.2)$$

Пример. Найти подходящие дроби к цепной дроби $\frac{985}{533} = [1,1,5,1,1,2,1,1,1,1,2]$.

Решение. Вычисление $\{P_n\}$ и $\{Q_n\}$ сведем в таблицу 1.2.

Таблица 1.2 – Вычисления числителей и знаменателей подходящих дробей

n	-2	-1	0	1	2	3	4	5	6	7	8	9	10
q_n	*	*	1	1	5	1	1	2	1	1	1	1	2
P_n	0	1	1	2	11	13	24	61	85	146	231	377	985
Q_n	1	0	1	1	6	7	13	33	46	79	125	204	533

2 СРАВНЕНИЯ И ИХ СВОЙСТВА

2.1 ОСНОВНЫЕ ПОНЯТИЯ

Определение **5.** Если a и b – два целых числа и их разность $(a - b)$ делится на целое положительное число m, то говорят, что a сравнимо с b по модулю m, и при этом пишут $a \equiv b (\mathrm{mod} m)$.

Исходя из определения, запись $a \equiv b (\mathrm{mod} m)$ означает, что $a - b = mk$ или $a = b + mk$, $k \in Z$.

Если представить b в виде $b = mq1 + r$, $0 \le r < m$, то $a = mq1 + r + mk = m(q1 + k) + r$. Таким образом, при делении чисел a и b на модуль m получаем один и тот же остаток r.

Примеры. 1) $47 \equiv 11 (\mathrm{mod}\ 9)$ означает, что $47 = 11 + 9 \cdot 4$;

2) $-11 \equiv 13 (\mathrm{mod} 8)$ означает, что $-11 = 13 + 8 \cdot (-3)$.

2.2 ОСНОВНЫЕ СВОЙСТВА СРАВНЕНИЙ

Основные свойства сравнений:

Свойство 1. Сравнения по одинаковому модулю можно почленно складывать.

Доказательство. Пусть $a_1 \equiv b_1 (\mathrm{mod}\ m)$, $a_2 \equiv b_2 (\mathrm{mod}\ m)$. Это означает, что $a_1 = b_1 + mt_1$, $a_2 = b_2 + mt_2$. После сложения последних двух равенств получим $a_1 + a_2 = b_1 + b_2 + m(t_1 + t_2)$, что означает $a_1 + a_2 \equiv b_1 + b_2 (\mathrm{mod}\ m)$.

Свойство 2. Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, изменив его знак на обратный.

Доказательство.

$$\frac{\begin{cases} a + b \equiv c (\mathrm{mod}\ m) \\ -b \equiv -b (\mathrm{mod}\ m) \end{cases} +}{a \equiv c - b (\mathrm{mod}\ m)}$$

Свойство 3. К любой части сравнения можно прибавить любое число, кратное модулю.

Доказательство.

$$\frac{\begin{cases} a \equiv b (\mathrm{mod}\ m) \\ mk \equiv 0 (\mathrm{mod}\ m) \end{cases} +}{a + mk \equiv b (\mathrm{mod}\ m)}$$

Свойство 4. Сравнения по одинаковому модулю можно почленно перемножать.

Свойство 5. Обе части сравнения можно возвести в одну и ту же степень.

Доказательство.

$$\frac{\begin{cases} a_1 \equiv b_1 (\mathrm{mod}\ m) \Leftrightarrow a_1 = b_1 + mt_1 \\ a_2 \equiv b_2 (\mathrm{mod}\ m) \Leftrightarrow a_2 = b_2 + mt_2 \end{cases} \times}{a_1 a_2 = b_1 b_2 + m(b_1 t_2 + b_2 t_1 + mt_1 t_2) \Rightarrow a_1 a_2 \equiv b_1 b_2 (\mathrm{mod}\ m)}$$

Как следствие из вышеперечисленных свойств получаем

Свойство 6. Если

$a_0 \equiv b_0 (\mathrm{mod}\ m)$, $a_1 \equiv b_1 (\mathrm{mod}\ m)$, ..., $a_n \equiv b_n (\mathrm{mod}\ m)$, $x \equiv y (\mathrm{mod}\ m)$, то

$a_0 x^n + a_1 x^{n-1} + ... + a_n \equiv b_0 y^n + b_1 y^{n-1} + ... + b_n (\mathrm{mod}\ m)$

Свойство 7. Обе части сравнения можно разделить на их общий делитель, взаимно простой с модулем.

Доказательство. Пусть $a \equiv b (\mathrm{mod}\ m)$, $a = a_1 d$, $b = b_1 d$. Тогда $(a_1 - b_1) \cdot d$ делится на m. Поскольку d и m взаимно просты, то на m делится именно $(a_1 - b_1)$, что означает $a_1 \equiv b_1 (\mathrm{mod}\ m)$.

Свойство 8. Обе части сравнения и его модуль можно умножить на одно и то же целое число или разделить на их общий делитель.

Доказательство. $a \equiv b (\mathrm{mod}\ m) \Leftrightarrow a = b + mt \Leftrightarrow ak = bk + mkt \Leftrightarrow ak \equiv bk (\mathrm{mod}\ mk)$.

Свойство 9. Если сравнение $a \equiv b$ имеет место по нескольким разным модулям, то оно имеет место и по модулю, равному наименьшему общему кратному этих модулей.

Доказательство. Если $a \equiv b(mod\ m_1)$ и $a \equiv b(mod\ m_2)$, то a-b делится на m_1 и на m_2, значит a-b делится на наименьшее общее кратное m_1 и m_2.

Свойство 10. Если сравнение имеет место по модулю m, то оно имеет место и по модулю d, равному любому делителю числа m.

Доказательство очевидно следует из транзитивности отношения делимости: если $a \equiv b(mod\ m)$, то a-b делится на m, значит a-b делится на d, где $d|m$.

Свойство 11. Если одна часть сравнения и модуль делятся на некоторое число, то и другая часть сравнения должна делиться на то же число.

Доказательство. $a \equiv b(mod\ m) \Leftrightarrow a=b+mt$

Пример. Доказать, что при любом натуральном n число $37^{n+2}+16^{n+1}+23^n$ делится на 7.

Решение. Очевидно, что $37 \equiv 2(\text{mod } 7)$, $16 \equiv 2(\text{mod } 7)$, $23 \equiv 2(\text{mod } 7)$

Возведем первое сравнение в степень n+2, второе – в степень n+1, третье – в степень n и сложим:

$$\begin{array}{l} 37^{n+2} \equiv 2^{n+2}(\text{mod } 7), \\ 16^{n+1} \equiv 2^{n+1}(\text{mod } 7), \quad + \\ \hline 37^{n+2}+16^{n+1}+23^n \equiv 2^n \bullet 7(\text{mod } 7) \end{array}$$

т.е. $37^{n+2}+16^{n+1}+23^n$ делится на 7.

2.3 ПОЛНАЯ И ПРИВЕДЕННАЯ СИСТЕМЫ ВЫЧЕТОВ

Отношение $\equiv_m$ сравнимости по произвольному модулю m есть отношение эквивалентности на множестве целых чисел. Это отношение эквивалентности индуцирует разбиение множества целых чисел на классы эквивалентных между собой элементов, т. е. в один класс объединяются числа, дающие при делении на m одинаковые остатки. Число классов эквивалентности $\equiv_m$ ("индекс эквивалентности $\equiv_m$") в точности равно m.

Т. е. сравнимость a с b по модулю m означает, что a и b представляют один и тот же элемент в кольце Z_m.

Процесс собирания целых чисел в классы сравнимых между собой по модулю m (классы эквивалентности $\equiv_m$) поясняет следующая картинка:

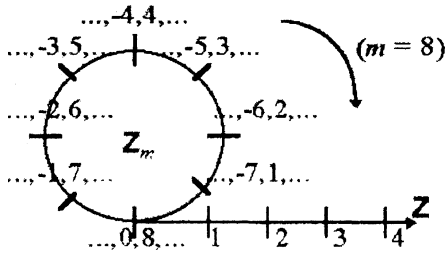

Рисунок 1.1 – Классы эквивалентности m=8

На рисунке 1.1 изображен процесс формирования цепочки целых чисел на «кольцо» с m делениями, при этом на одно деление автоматически попадают сравнимые между собой числа.

Определение 6. Любое число из класса эквивалентности $\equiv_m$ будем называть вычетом по модулю m . Совокупность вычетов, взятых по одному из каждого класса эквивалентности $\equiv_m$, называется полной системой вычетов по модулю m (в полной системе вычетов, таким образом, всего m штук чисел). Непосредственно сами остатки при делении на m называются наименьшими неотрицательными вычетами и, конечно, образуют полную систему вычетов по модулю m . Вычет ρ называется абсолютно наименьшим, если $|\rho|$ наименьший среди модулей вычетов данного класса.

Пример : Пусть m = 5 . Тогда: 0, 1, 2, 3, 4 - наименьшие неотрицательные вычеты;
-2, -1, 0, 1, 2 - абсолютно наименьшие вычеты.
Обе приведенные совокупности чисел образуют полные системы вычетов по модулю 5

Лемма 1.

1)Любые m штук попарно не сравнимых по модулю m чисел образуют полную систему вычетов по модулю m .

2)Если a и m взаимно просты, а x пробегает полную систему вычетов по модулю m , то значения линейной формы ax+b , где b - любое целое число, тоже пробегают полную систему вычетов по модулю m .

Определение 7. Приведенной системой вычетов по модулю m называется совокупность всех вычетов из полной системы, взаимно простых с модулем m .

Приведенную систему обычно выбирают из наименьших неотрицательных вычетов. Ясно, что приведенная система вычетов по модулю m содержит $\varphi(m)$ штук вычетов, где $\varphi(m)$– функция Эйлера – число чисел, меньших m и взаимно простых с m .

Пример. Пусть m = 42. Тогда приведенная система вычетов суть:

1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.

Лемма 2.

1) Любые $\varphi(m)$ чисел, попарно не сравнимые по модулю m и взаимно простые с модулем, образуют приведенную систему вычетов по модулю m .

2) Если $(a,m) = 1$ и x пробегает приведенную систему вычетов по модулю m , то ax так же пробегает приведенную систему вычетов по модулю m .

Лемма 3. Пусть $m_1, m_2, \ldots, m_k$ – попарно взаимно просты и $m_1 m_2 \ldots m_k = M_1 m_1 = M_2 m_2 = \ldots = M_k m_k$, где $M_j = m_1 \ldots m_{j-1} m_{j+1} \ldots m_k$

1) Если $x_1, x_2, \ldots, x_k$ пробегают полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ соответственно, то значения линейной формы $M_1 x_1 + M_2 x_2 + \ldots + M_k x_k$ пробегают полную систему вычетов по модулю $m = m_1 m_2 \ldots m_k$.

2) Если $\xi_1, \xi_2, \ldots, \xi_k$ пробегают приведенные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ соответственно, то значения линейной формы $M_1 \xi_1 + M_2 \xi_2 + \ldots + M_k \xi_k$ пробегают приведенную систему вычетов по модулю $m = m_1 m_2 \ldots m_k$.

Лемма 4. Пусть $x_1, x_2, \ldots, x_k$,x пробегают полные, а $\xi_1, \xi_2, \ldots, \xi_k$, ξ– пробегают приведенные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ и $m = m_1 m_2 \ldots m_k$ соответственно, где $(m_i, m_j) = 1$ при $i \neq j$. Тогда дроби $\{x_1/m_1 + x_2/m_2 + \ldots + x_k/m_k\}$ совпадают с дробями $\{x/m\}$, а дроби $\{\xi_1/m_1 + \xi_2/m_2 + \ldots + \xi_k/m_k\}$ совпадают с дробями $\{\xi/m\}$.

3 РЕШЕНИЕ СРАВНЕНИЙ

Рассмотрим сравнения с одним неизвестным вида: $f(x) \equiv 0 (mod\ m)$,
где $f(x)=a_0 x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n$ – многочлен с целыми коэффициентами.

Если m не делит a_0, то говорят, что n – степень сравнения. Если какое-нибудь число x подходит в сравнение, то в это же сравнение подойдет и любое другое число, сравнимое с x по $mod\ m$.

Решить сравнение – значит найти все те x, которые удовлетворяют данному сравнению, при этом весь класс чисел по mod m считается за одно решение.

Таким образом, число решений сравнения есть число вычетов из полной системы, которые этому сравнению удовлетворяют.

Пример. Дано сравнение: $x^5 + x + 1 \equiv 0 (mod\ 7)$.

Из чисел: 0, 1, 2, 3, 4, 5, 6, этому сравнению удовлетворяют два: $x_1 = 2$, $x_2 = 4$. Это означает, что у данного сравнения два решения:

$$x \equiv 2 (mod\ 7) \text{ и } x \equiv 4 (mod\ 7).$$

Сравнения называются равносильными, если они имеют одинаковые решения. Сравнение любой степени всегда решается, хотя бы, например, перебором всех вычетов по $mod\ m$. Перебор и подстановка всех вычетов - долгий процесс (особенно, при больших m и n), но существуют специально разработанные алгоритмы, исполняя которые, можно всегда найти все решения данного сравнения любой степени.

3.1 СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ С ОДНИМ НЕИЗВЕСТНЫМ

Пусть a и b – целые числа. Обозначим через целое m модуль для вычисления сравнений. Тогда выражение

$ax \equiv b \bmod m$

называется сравнением первой степени с одним неизвестным. Решить сравнение – значит найти все значения x, которые удовлетворяют данному сравнению.

Теорема. Если (a, m) = d, т. е. число a и модуль m имеют общий делитель d, причем число d не делит b, то сравнение $ax \equiv b \bmod m$ не имеет решений.

Согласно этой теореме решение сравнения $ax \equiv b \bmod m$ существует только в случае, если d|b. Тогда имеем $a = a_1 d$, $b = b_1 d$, $m = m_1 d$, а исходное сравнение можно записать в виде $a_1 dx - b_1 d \bmod m_1 d$.

Используя свойство сравнения, последнее соотношение можно заменить эквивалентным

$a_1 x \equiv b_1 \bmod m_1$,

где $(a_1, m_1) = 1$.

Поэтому, не ограничивая общности, изучать сравнение $ax \equiv b \bmod m$ можно, предполагая, что коэффициент при неизвестном и модуль являются взаимно простыми числами, т. е. НОД (a, m) = 1.

Теорема. Если (a, m) = 1, т. е. числа a и m взаимно просты, то сравнение $ax \equiv b \bmod m$ имеет одно и только одно решение.

Теорема. Если наибольший общий делитель (a, m) чисел a и m равен d и d делит b, то сравнение $ax \equiv b \pmod m$ имеет d решений.

Пример. Решите сравнение

$1287x \equiv 447 \pmod{516}$.

Решение:

1) Заменим коэффициенты сравнения $1287x \equiv 447 \pmod{516}$ соответствующими наименьшими положительными вычетами по модулю 516, получим:

$255x \equiv 447 \pmod{516}$.

2) Если наибольший общий делитель (a, m) чисел a и m равен d и d делит b, то сравнение $ax \equiv b \pmod{m}$ имеет d решений.

Если же d не делит b, то сравнение $ax \equiv b \pmod{m}$ не имеет решений.

Для сравнения $255x \equiv 447 \pmod{516}$ имеем $d = (a, m) = (255, 516) = 3$.

Поскольку $d = 3$ делит $b = 447$, то сравнение $255x \equiv 447 \pmod{516}$, а значит, и сравнение $1287x \equiv 447 \pmod{516}$ имеет 3 решения.

3) Разделим обе части сравнения $255x \equiv 447 \pmod{516}$ и его модуль на $d = 3$, получим: $85x \equiv 149 \pmod{172}$.

Рассмотрим два способа решения сравнения $ax \equiv b \pmod{m}$, где $(a, m) = 1$.

Первый способ:

Решение x_0 находим по формуле

$$x_0 \equiv (-1)^{n-1} P_{n-1} b \pmod{m},$$

где P_{n-1} – числитель предпоследней подходящей дроби для числа $\frac{m}{a}$, разложенного в непрерывную (цепную) дробь.

Пример. Разложим число $\frac{172}{85}$ в непрерывную дробь и найдем числитель предпоследней подходящей дроби:

$$\frac{172}{85} = 2 + \frac{2}{85} = 2 + \frac{1}{42 + \frac{1}{2}} = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}.$$

Найдем числители подходящих дробей по рекуррентной формуле

$P_{i+1} = q_i P_i + P_{i-1}$,

где $P_0 = 1$, $P_1 = q_1$, где $i = 1, \ldots, n - 1$:

i	0	1	2	3
q_i		2	42	2
P_i	1	2	85	172

Получим, что $n = 3$, $P_{n-1} = P_2 = 85$ и решение сравнения (2) имеет вид:

$x_0 \equiv (-1)^{n-1} P_{n-1} b \pmod{m} \equiv (-1)^{3-1} \cdot 85 \cdot 149 \pmod{172} \equiv \equiv 85 \cdot (-23) \pmod{172} \equiv -1955 \pmod{172} \equiv 109 \pmod{172}$.

Второй способ:

По теореме Эйлера для чисел a и m, удовлетворяющих условию $(a, m) = 1$, выполняется сравнение $a^{\varphi(m)} \equiv 1 \pmod{m}$, где $\varphi(m)$ - функция Эйлера.

Теорема. Если $(a, m) = 1$, т. е числа a и b взаимно простые, то решением сравнения $ax \equiv b \bmod m$ является класс $x \equiv b a^{\varphi(m)-1} \bmod m$, где $\varphi(m)$ – значение функции Эйлера для модуля m.

Найдем $\varphi(172)$. Поскольку $172 = 22 \cdot 43$, то по свойствам функции Эйлера

$\varphi(172) = \varphi(2^2) \cdot \varphi(43) = (2^2 - 2^1) \cdot (43 - 1) = 2 \cdot 42 = 84$

$x_0 \equiv 149 \cdot 858^{4-1} \pmod{172} \equiv -23 \cdot 85^{2 \cdot 41+1} \pmod{172} \equiv -23 \cdot 85 \cdot (85^2)^{41} \pmod{172} \equiv$

$\equiv -1955 \cdot (25 \cdot 289)^{41} \pmod{172} \equiv 109 \cdot (25 \cdot (-55))^{41} \pmod{172} \equiv 109 \cdot 1^{41} \pmod{172} \equiv 109 \pmod{172}$

Результат решения сравнения:
Итак, $x_0 \equiv 109 \pmod{172}$ является решением сравнения $85x \equiv 149 \pmod{172}$.
Все решения сравнения $255x \equiv 447 \pmod{516}$, а также сравнения
$1287x \equiv 447 \pmod{516}$, находят по формуле
$x = x_0 + 172 \cdot k$, где $k = 0, 1, ..., d - 1$.
В нашем случае $k = 0, 1, 2$, значит,
$x \equiv 109; 281; 453 \pmod{516}$.
Ответ: $x \equiv 109; 281; 453 \pmod{516}$

3.2 РЕШЕНИЕ СИСТЕМ СРАВНЕНИЙ ПЕРВОЙ СТЕПЕНИ С ОДНИМ НЕИЗВЕСТНЫМ

Пример. Решите систему сравнений

$$\begin{cases} 13x \equiv (\mathrm{mod}\, 24) \\ 8x \equiv 5 (\mathrm{mod}\, 75) \end{cases} \quad (3.1)$$

Решение. Решив каждое из сравнений системы (3.1) отдельно, получим систему

$$\begin{cases} x \equiv 19 (\mathrm{mod}\, 24) \\ x \equiv 10 (\mathrm{mod}\, 75) \end{cases} \quad (3.2)$$

Используя каноническое разложение модулей $24 = 2^3 \cdot 3$, $75 = 3 \cdot 5^2$, получим что система (3.2) равносильна системе:

$$\begin{cases} x \equiv 19 (\mathrm{mod}\, 8), \\ x \equiv 19 (\mathrm{mod}\, 3), \\ x \equiv 10 (\mathrm{mod}\, 25), \\ x \equiv 10 (\mathrm{mod}\, 3) \end{cases}$$

или

$$\begin{cases} x \equiv 3 (\mathrm{mod}\, 8), \\ x \equiv 1 (\mathrm{mod}\, 3), \\ x \equiv 10 (\mathrm{mod}\, 25), \\ x \equiv 1 (\mathrm{mod}\, 3) \end{cases}$$

Второе и четвертое сравнения системы одинаковые, поэтому удалим одно из них.
Получим систему, у которой модули всех сравнений попарно взаимно просты

$$\begin{cases} x \equiv 3 (\mathrm{mod}\, 8) \\ x \equiv 1 (\mathrm{mod}\, 3) \\ x \equiv 10 (\mathrm{mod}\, 25) \end{cases} \quad (3.3)$$

Для решения системы (3.3)воспользуемся формулой, следующей из китайской теоремы об остатках. Для системы сравнений

$$\begin{cases} x \equiv b_1 (\mathrm{mod}\, m_1) \\ x \equiv b_2 (\mathrm{mod}\, m_2) \\ \dots \\ x \equiv b_n (\mathrm{mod}\, m_n) \end{cases},$$

где числа $m_1, m_2, \dots, m_n$ попарно взаимно просты, решение находится по следующей формуле

$$x \equiv M_1 M'_1 b_1 + M_2 M'_2 b_2 + \dots + M_n M'_n b_n (\mathrm{mod}\, m),$$

где $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$, $M_i = \frac{m}{m_i}$,

где M'_i – некоторое решение сравнения;
$M_i x \equiv 1 \pmod{m_i}$, $i = 1, \ldots, n$.

Для системы (3.3) имеем $m = 8 \cdot 3 \cdot 25 = 600$, $M_1 = \frac{8 \cdot 3 \cdot 25}{8} = 75$, $M_2 = \frac{8 \cdot 3 \cdot 25}{3} = 200$,

$M_3 = \frac{8 \cdot 3 \cdot 25}{25} = 24$.

Найдем M'_i, $i = 1, 2, 3$:
$75x \equiv 1 \pmod 8 \Leftrightarrow 3x \equiv 1 \pmod 8 \Leftrightarrow x \equiv 3 \pmod 8 \Rightarrow M'_1 = 3$,
$200x \equiv 1 \pmod 3 \Leftrightarrow 2x \equiv 1 \pmod 3 \Leftrightarrow x \equiv 2 \pmod 3 \Rightarrow M'_2 = 2$,
$24x \equiv 1 \pmod{25} \Leftrightarrow x \equiv -1 \pmod{25} \Rightarrow M'_3 = -1$.
Подставим значения M_i, M'_i, b_i в формулу :
$x \equiv M_1 M'_1 b_1 + M_2 M'_2 b_2 + \ldots + M_3 M'_3 b_3 \pmod m$ и получим:
$x \equiv 75 \cdot 3 \cdot 3 + 200 \cdot 2 \cdot 1 + 24 \cdot (-1) \cdot 10 = = 675 + 400 - 240 = 835 \equiv 235 \pmod{600}$.
Ответ: $x \equiv 235 \pmod{600}$.

3.3 СРАВНЕНИЯ ПРОИЗВОЛЬНОЙ СТЕПЕНИ С ОДНИМ НЕИЗВЕСТНЫМ

Сравнения произвольной степени с одним неизвестным $f(x) \equiv 0 \pmod m$.

Пусть $m = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ – каноническое разложение числа $m > 0$.
Тогда сравнение

$$f(x) \equiv 0 \pmod m \qquad (3.4)$$

равносильно системе сравнений

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{a_1}} \\ f(x) \equiv 0 \pmod{p_2^{a_2}} \\ \ldots \\ f(x) \equiv 0 \pmod{p_k^{a_k}} \end{cases}$$

Таким образом, решение сравнения (3.4) сводится к решению нескольких сравнений вида

$$f(x) \equiv 0 \pmod{p^\alpha}. \qquad (3.5)$$

Из решений $x \equiv x1 \pmod p$ сравнения $f(x) \equiv 0 \pmod p$ выбираем решения сравнения (3.5) вида

$$x \equiv x_\alpha + p^\alpha t_\alpha,\ t_\alpha \in Z$$

или

$$x \equiv x_\alpha \pmod{p^\alpha}.$$

Эти решения определяются последовательно для $s = 2, 3, \ldots, \alpha$ в виде $x_s + p^s t_s$,
где t_s – решение сравнения

$$f(x_{s-1}) + f'(x_{s-1}) p^{s-1} t \equiv 0 \pmod{p^s}$$

или

$$\frac{f(x_{s-1})}{p^{s-1}} + f'(x_{s-1}) t \equiv 0 \pmod p. \qquad (3.6)$$

Поскольку x_{s-1} является решением сравнения $f(x) \equiv 0 \pmod{p^{s-1}}$, то $\frac{f(x_{s-1})}{p^{s-1}}$ является целым числом. Если p не делит $f'(x_{s-1})$, то сравнение (3.6) имеет единственное решение.

Если $p \mid f'(x_{s-1})$, то сравнение (3.6) имеет p решений при условии $p \mid \frac{f(x_{s-1})}{p^{s-1}}$, иначе сравнение (3.6) не имеет решений.

Пример. Решите сравнение $5x^3 + 4x^2 + 8x + 18 \equiv 0 \pmod{135}$.

Решение.

Шаг 1. Обозначим $f(x) = 5x^3 + 4x^2 + 8x + 18$. Поскольку $135 = 5 \cdot 3^3$, то данное сравнение равносильно системе

$$\begin{cases} f(x) \equiv 0 \pmod{27} \\ f(x) \equiv 0 \pmod{5} \end{cases} \quad (3.7)$$

Шаг 2. Решим сравнение по модулю 5. Рассмотрим полную систему абсолютно наименьших вычетов по модулю 5. Заменим коэффициенты многочлена f(x) на соответствующие абсолютно наименьшие вычеты по модулю 5:

$f(x) = 5x^3 + 4x^2 + 8x + 18 \equiv -x^2 - 2x - 2 \pmod 5$.

Итак,

$f(-2) = -(-2)^2 - 2 \cdot (-2) - 2 = -2 \not\equiv 0 \pmod 5$, ($\not\equiv$ означает не сравнимо)

$f(-1) = -(-1)^2 - 2 \cdot (-1) - 2 = -1 \not\equiv 0 \pmod 5$,

$f(0) = -0^2 - 2 \cdot 0 - 2 = -2 \not\equiv 0 \pmod 5$,

$f(1) = -1^2 - 2 \cdot 1 - 2 = -5 \equiv 0 \pmod 5$,

$f(2) = -2^2 - 2 \cdot 2 - 2 = -10 \equiv 0 \pmod 5$.

Сравнение $f(x) \equiv 0 \pmod 5$ имеет два решения

$x \equiv 1; 2 \pmod 5$.

Шаг 3. Далее, для решения сравнения $f(x) \equiv 0 \pmod{27}$ найдем сначала решения сравнения $f(x) \equiv 0 \pmod 3$. Из них выберем решения сравнения $f(x) \equiv 0 \pmod 9$, а затем из решений сравнения по модулю 9 найдем решения сравнения $f(x) \equiv 0 \pmod{27}$.

Модуль 3. Все вычисления производятся по модулю 3.

$f(x) = 5x^3 + 4x^2 + 8x + 18 \equiv 2x^3 + x^2 + 2x \pmod 3$,

$f'(x) = 15x^2 + 8x + 8 \equiv 2x + 2 \pmod 3$.

Имеем

$f(0) = 2 \cdot 0^3 + 0^2 + 2 \cdot 0 \equiv 0 \pmod 3$,

$f(1) = 2 \cdot 1^3 + 1^2 + 2 \cdot 1 = 2 \not\equiv 0 \pmod 3$,

$f(2) = 2 \cdot 2^3 + 2^2 + 2 \cdot 2 = 24 \equiv 0 \pmod 3$.

Получили, что сравнение $f(x) \equiv 0 \pmod 3$ имеет два решения $x \equiv 0 \pmod 3$, $x \equiv 2 \pmod 3$. Если $f(x) \equiv 0 \pmod 9$ имеет решения, то эти решения имеют вид $0 + 3t$ или $2 + 3t$ для некоторого $t \in Z$.

Модуль 9. Все вычисления производятся по модулю 9.

$f(x) = 5x^3 + 4x^2 + 8x + 18$,

$f'(x) = 15x^2 + 8x + 8$.

Используем формулу (3.6) при s = 2:

$f(x_1) + f'(x_1)pt \equiv 0 \pmod{p^2}$

или

$$\frac{f(x_1)}{p} + f'(x_1)t \equiv 0 \pmod p. \quad (3.8)$$

1) Рассмотрим $x_1 \equiv 0 \pmod 3$, т.е. $x_1 = 0 + 3t$. Имеем
$f(x_1) = f(0) = 5 \cdot 0^3 + 4 \cdot 0^2 + 8 \cdot 0 + 18 = 18 \equiv 0 \pmod 9$,
$f'(x_1) = f'(0) = 15 \cdot 0^2 + 8 \cdot 0 + 8 = 8 \equiv -1 \pmod 9$.

По формуле (3.8) получим $\frac{0}{3} + (-1) \cdot t \equiv 0 \pmod 3$ или $t \equiv 0 \pmod 3$.

Поэтому $t_1 = 0$ и $x_2 = x_1 + 3t_1 = 0 + 3 \cdot 0 = 0$ является решением сравнения $f(x) \equiv 0 \pmod 9$.

2) Те же действия выполним для $x_1 \equiv 2 \pmod 3$, т.е. $x_1 = 2 + 3t$. Имеем
$f(x_1) = f(2) = 5 \cdot 2^3 + 4 \cdot 2^2 + 8 \cdot 2 + 18 = 90 \equiv 0 \pmod 9$,
$f'(x_1) = f'(2) = 15 \cdot 2^2 + 8 \cdot 2 + 8 = 84 \equiv 3 \pmod 9$,

По формуле (3.8) получим $\frac{0}{3} + 3 \cdot t \equiv 0 \pmod 3$ или $0 \equiv 0 \pmod 3$. Поэтому

$t_1 = 0; 1; 2$ и числа $x_2 = x_1 + 3t_1 = 2 + 3t_1 = 2; 5; 8$ являются решениями сравнения $f(x) \equiv 0 \pmod 9$.

Модуль 27. Все вычисления производятся по модулю 27.
$f(x) = 5x^3 + 4x^2 + 8x + 18$,
$f'(x) = 15x^2 + 8x + 8$.
Используем формулу (3.6) при $s = 3$:
$f(x_2) + f'(x_2)p^2t \equiv 0 \pmod{p^3}$
или
$$\frac{f(x_2)}{p^2} + f'(x_2)t \equiv 0 \pmod p. \qquad (3.9)$$

Рассмотрим $x_2 \equiv 0; 2; 5; 8 \pmod 9$, т. е. $x_2 = 0 + 9t$, $x_2 = 2 + 9t$, $x_2 = 5 + 9t$, $x_2 = 8 + 9t$.

1) Для $x_2 = 0 + 9t$ имеем
$f(x_2) = f(0) = 5 \cdot 0^3 + 4 \cdot 0^2 + 8 \cdot 0 + 18 \equiv 18 \pmod{27}$,
$f'(x_2) = f'(0) = 15 \cdot 0^2 + 8 \cdot 0 + 8 \equiv 8 \pmod{27}$.

По формуле (3.9) получим $\frac{18}{9} + 8 \cdot t \equiv 0 \pmod 3$ или $t \equiv 2 \pmod 3$.

Поэтому $t_2 = 2$ и
$x_3 = x_2 + 9t_2 = 0 + 9 \cdot 2 = 18$
является решением сравнения $f(x) \equiv 0 \pmod{27}$.

2) Для $x_2 = 2 + 9t$ имеем
$f(x_2) = f(2) = 90 \equiv 9 \pmod{27}$,
$f'(x_2) = f'(2) = 84 \equiv 3 \pmod{27}$, $\frac{9}{9} + 3 \cdot t \equiv 0 \pmod 3$ или $1 \not\equiv 0 \pmod 3$.

Среди чисел вида $2 + 9t$ нет решений сравнения $f(x) \equiv 0 \pmod{27}$.

3) Для $x_2 = 5 + 9t$ имеем
$f(x_2) = f(5) = 783 \equiv 0 \pmod{27}$,
$f'(x_2) = f'(5) = 423 \equiv 18 \pmod{27}$, $\frac{0}{9} + 18t \equiv 0 \pmod 3$ или $0 \equiv 0 \pmod 3$.

Поэтому $t_2 = 0; 1; 2$ и $x_3 = 5 + 9t_2 = 5; 14; 23$
являются решениями сравнения $f(x) \equiv 0 \pmod{27}$.

4) Для $x_2 = 8 + 9t$ имеем

$f(x_2) = f(8) = 2898 \equiv 9 \pmod{27}$,

$f'(x_2) = f'(8) = 1032 \equiv 6 \pmod{27}$, $\frac{9}{9} + 6t \equiv 0 \pmod 3$ или $1 \not\equiv 0 \pmod 3$.

Среди чисел вида $8 + 9t$ нет решений сравнения $f(x) \equiv 0 \pmod{27}$.

Шаг 4. Итак, система (3.7) решена:

$$\begin{cases} x \equiv 1,2 \pmod 5 \\ x \equiv 5,14,18,23 \pmod{27} \end{cases}$$

В правой части сравнений находятся несколько значений, поэтому удобно рассматривать систему

$$\begin{cases} x \equiv b_1 \pmod 5 \\ x \equiv b_2 \pmod{27} \end{cases}, \text{ где } b_1 \in \{1,2\}, b_2 \in \{5,14,18,23\}$$

Воспользуемся формулой, следующей из китайской теоремы об остатках:

$m = 5 \cdot 27 = 135$,

$M_1 = \frac{m}{5} = 27$, $27x \equiv 1 \pmod 5 \Leftrightarrow x \equiv 3 \pmod 5 \Rightarrow M'_1 = 3$;

$M_2 = \frac{m}{27} = 5$, $5x \equiv 1 \pmod{27} \Leftrightarrow x \equiv 11 \pmod{27} \Rightarrow M'_2 = 11$;

$x \equiv M_1 \cdot M'_1 \cdot b_1 + M_2 \cdot M'_2 \cdot b_2 \pmod{135} \equiv 27 \cdot 3 \cdot b_1 + 5 \cdot 11 \cdot b_2 \pmod{135} \equiv$

$\equiv 81b_1 + 55b_2 \pmod{135}$.

Подставляя $b_1 = 1; 2$ и $b_2 = 5; 14; 18; 23$, получим все решения исходного сравнения

$x \equiv 32; 41; 72; 77; 86; 122; 126; 131 \pmod{135}$.

Ответ: $x \equiv 32; 41; 72; 77; 86; 122; 126; 131 \pmod{135}$.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003.

2. Виноградов, И. М. Основы теории чисел. — Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003.

3. Нестеренко, Ю. В. Теория чисел : учебник для студ. высш. учеб. заведений / Ю. В. Нестеренко. — М.: Издательский центр «Академия», 2008.

4. Оре, О. Приглашение в теорию чисел: пер. с англ. — Изд. 2-е, стереотипное. — М.: Едиториал УРСС, 2003.

5. Просветов, Г. И. Теория чисел: задачи и решения: учебно-практическое пособие. — М.: Издательство «Альфа-Пресс», 2010.

6. Ростовцев, А. Г. Алгебраические основы криптографии. — СПб.: Мир и Семья, 2000.

7. Ростовцев, А. Г. Введение в криптографию с открытым ключом / А. Г. Ростовцев, Е. Б. Маховенко. — СПб.: Мир и Семья, 2001.

8. Сизый, С. В. Лекции по теории чисел: учебное пособие для математических специальностей. Екатеринбург: Уральский государственный университет им. А. М. Горького, 1999.

9. Столингс, В. Криптография и защита сетей: принципы и практика. — 2-е изд. — М.: Издательский дом "Вильямс", 2001.

УЧЕБНОЕ ИЗДАНИЕ

Составитель:
Хацкевич Мария Викторовна

ТЕОРИЯ СРАВНЕНИЙ

Методические указания к выполнению лабораторных работ
по дисциплине
«Криптографические методы защиты информации»
для студентов специальности
1 – 40 03 01 «Искусственный интеллект»

Ответственный за выпуск: Хацкевич М.В.
Редактор: Боровикова Е.А.
Компьютерная вёрстка: Соколюк А.П.
Корректор: Никитчик Е.В.

Подписано в печать 21.03.2019 г. Формат 60x84 1/16. Бумага «Performer».
Гарнитура «Arial Narrow». Усл. печ. л.1,39. Уч. изд. л. 1,50. Заказ №1645. Тираж 20 экз.
Отпечатано на ризографе учреждения образования «Брестский государственный
технический университет». 224017, г. Брест, ул. Московская, 267.