МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра «Интеллектуальные информационные технологии»

ТЕОРЕТИКО-ЧИСЛОВЫЕ АЛГОРИТМЫ В КРИПТОГРАФИИ

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

Брест 2012

УДК 347 77/681.3

В методических указаниях приведены необходимые теоретические сведения по теории чисел, а также математические алгоритмы, используемые для реализации криптографических протоколов, и множество примеров, что упрощает подготовку студентов к практическим занятиям. Методические указания предназначены для использования студентами специальности 1-40 03 01 «Искусственный интеллект» в ходе выполнения лабораторных работ и для изучения теоретического материала на практических занятиях по дисциплине «Криптографические методы защиты информации».

Составитель: Хацкевич М.В., старший преподаватель

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Для современного этапа научно-технического развития характерен стремительный рост потоков передаваемой информации. В связи с этим возникает острая необходмость в совершенствовании традиционных телекоммуникационных систем и создании новых, более совершенных, способных увеличить быстродействие используемых технических устройств, повысить безопасность и обеспечить экономичность самого процесса обмена информацией.

Информация превратилась в объект, на защиту которого направлены основные усилия и ресурсы многомиллионной армии математиков, программистов, радиофизиков и инженеров. Методы защиты информации динамически развиваются, усложняются и постепенно оформляются в отдельную отрасль информационно-коммуникационных технологий.

Криптографию в настоящее время следует рассматривать как дисциплину, на основе которой могут разрабатываться или уже созданы реальные законченные приложения, обеспечивающие защиту информации.

Математической основой большинства современных методов защиты информации является алгебраическая теория чисел. Поэтому в данном пособии приведены основы теории чисел.

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 (2004, 1941).

Решение.

2004 = 1941· 1 + 63

1941 = 63 · 30 + 51

53 = 51 · 1 + 12

51= 12 · 4 + 3

12 = 3 · 4

Итак (2004, 1941) = 3.

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

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

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:

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

и наши пресловутые u и v из **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 1не 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 α_1, α_2, ..., α_k кратности их вхождения в a, получим каноническое разложение числа, а на сомножители: $a = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_k^{a_k}$.

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:

$m = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_k^{a_k}$, 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:

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

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

$$\begin{aligned} m &= aq_0 + a_1 && (1) \\ a &= a_1 q_1 + a_2 && (2) \\ a_1 &= a_2 q_2 + a_3 && (3) \\ &\cdots\cdots\cdots\cdots && \\ a_{k-2} &= a_{k-1} q_{k-1} + a_k && (k) \\ a_{k-1} &= a_k q_k + 0 && (k+1) \end{aligned}$$

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

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

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 · 1 + 452
533 = 452 · 1 + 81
452 = 81 · 5 + 47
81 = 47 · 1 + 34
47 = 34 · 1 + 13
34 = 13 · 2 + 8
13 = 8 · 1 + 5
8 = 5 · 1 + 3
5 = 3 · 1 + 2
3 = 2 · 1 + 1
2 = 1 · 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 подходящих дробей основан на простой идее представления подходящей 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:

$$P_n = q_n P_{n-1} + P_{n-2} \text{ при условии, что } P_{-2} = 0, P_{-1} = 1;$$
$$Q_n = q_n Q_{n-1} + Q_{n-2} \text{ при условии, что } Q_{-2} = 1, Q_{-1} = 0.$$

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 $-11 = 13 + 8 \cdot (-3)$.
3) $63 \equiv 0(\mathrm{mod}\ 21)$ означает, что $63 = 0 + 21 \cdot 3$.

2.2 ОСНОВНЫЕ СВОЙСТВА СРАВНЕНИЙ

Основные свойства сравнений:

Свойство 1. Сравнения по одинаковому модулю можно почленно складывать.

Доказательство. Пусть $a_1 \equiv b_1(mod\ m)$, $a_2 \equiv b_2(mod\ m)$. 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 $a_1 + a_2 \equiv b_1 + b_2\ (mod\ m)$.

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

Доказательство.

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

$$a \equiv c - b(\mathrm{mod} m)$$

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

Доказательство.

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

$$a + mk \equiv b(\mathrm{mod} m)$$

Свойство 4. Сравнения по одинаковому модулю можно почленно перемножать.

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

Доказательство.

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

$$a_1 a_2 = b_1 b_2 + m(b_1 t_2 + b_2 t_1 + mt_1 t_2) \Rightarrow a_1 a_2 \equiv b_1 b_2(\mathrm{mod} m)$$

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 $a \equiv b(mod\ m)$, $a = a_1 d$, $b = b_1 d$. 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 $a_1 \equiv b_1\ (mod\ m)$.

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

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

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 $37 \equiv 2(\mathrm{mod}\ 7)$, $16 \equiv 2(\mathrm{mod}\ 7)$, $23 \equiv 2(\mathrm{mod}\ 7)$.

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

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

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 рис. 1.1.

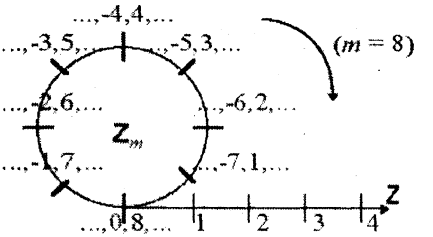

Рисунок 1.1 – Классы эквивалентности m = 8

На рис. 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 несравнимых 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 несравнимые 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 также пробегает приведенную систему вычетов по модулю m.

Лемма 3. Пусть $m_1, m_2, ..., m_k$ – попарно взаимно просты и $m_1 m_2 ... m_k = M_1 m_1 = M_2 m_2 = ... = M_k m_k$, где $M_j = m_1 ... m_{j-1} m_{j+1} ... m_k$
1) Если $x_1, x_2, ..., x_k$ пробегают полные системы вычетов по модулям $m_1, m_2, ..., m_k$ соответственно, то значения линейной формы $M_1x_1 + M_2x_2 + ...+ M_kx_k$ пробегают полную систему вычетов по модулю $m = m_1 m_2 ... m_k$.
2) Если $\xi_1, \xi_2, ..., \xi_k$ пробегают приведенные системы вычетов по модулям $m_1, m_2, ..., m_k$ соответственно, то значения линейной формы $M_1 \xi_1 + M_2 \xi_2 + ... + M_k \xi_k$ пробегают приведенную систему вычетов по модулю $m = m_1 m_2 ... m_k$.

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

3 ТЕОРИЯ 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:

$x \equiv 2(mod\ 7)$ 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

Рассмотрим сравнения первой степени вида ax ≡ b(mod m).

Приведем два способа решения этого уравнения.

Слагаемое mQ_{n-1}, кратное m, можно выкинуть из левой части сравнения.

Получаем:

$-aP_{n-1} \equiv (-1)^n (mod\ m)$ т.е.

$aP_{n-1} \equiv (-1)^{n-1} (mod\ m)$ т.е.

$a[(-1)^{n-1} P_{n-1} b] \equiv b(mod\ m)$.

Единственное решение исходного сравнения: $x \equiv (-1)^{n-1} P_{n-1} b(mod\ m)$

Пример. Решить сравнение 111x ≡ 75(mod 322).

Решение. (111, 322) = 1. Включаем алгоритм Евклида:

$322 = 11 \cdot \underline{2} + 100$

$111 = 100 \cdot \underline{1} + 11$

$100 = 11 \cdot \underline{9} + 1$

$11 = 1 \cdot \underline{11}$

В равенствах подчеркнуты неполные частные. Значит, $n = 4$, а соответствующая цепная дробь:

$$\frac{m}{a} = \frac{322}{111} = 2 + \cfrac{1}{1 + \cfrac{1}{9 + \cfrac{1}{11}}}$$

Посчитаем числители подходящих дробей, составив для этого стандартную таблицу 3.1.

Таблица 3.1 – Числители подходящих дробей

	0	2	1	9	11
P_n	1	2	3	29	322

Числитель предпоследней подходящей дроби равен 29, следовательно, готовая формула дает ответ: $x \equiv (-1)^3 \cdot 29\ 75 \equiv -2175 \equiv 79 (mod\ 322)$.

Вывод. Дано сравнение $ax \equiv b(mod\ m)$, где a и m взаимно просты. Необходимо с помощью алгоритма Евклида найти u, $v \in \mathbf{Z}$ такие, что $au + vm = 1$, если затем умножить это равенство на b: $aub + vmb = b$, откуда немедленно следует: $aub \equiv b(mod\ m)$.

Действительно, $ax \equiv b(mod\ m)$ бывает тогда и только тогда, когда $ax - b$ делится на m нацело, т.е. $ax - b = t \cdot m$, $t \in \mathbf{Z}$, откуда $b = ax - t \cdot m$, а правая часть последнего равенства кратна d.

Пусть $b = db_1$, $a = da_1$, $m = dm_1$. Тогда обе части сравнения $xa_1 d \equiv b_1 d (mod m_1 d)$ и его модуль поделим на d:

$$xa_1 \equiv b_1 (mod\ m_1),$$

где уже $(a_1, m_1) = 1$. Согласно случаю 1 этого пункта, такое сравнение имеет единственное решение x_0:

$$x \equiv x_0 (mod\ m_1). \qquad (3.1)$$

По исходному модулю m числа (3.1) образуют столько решений исходного сравнения, сколько чисел вида (3.1) содержится в полной системе вычетов: 0, 1, 2, ..., $m-2$, $m-1$. Очевидно, что из чисел $x = x_0 + t \cdot m$ в полную систему наименьших неотрицательных вычетов попадают только x_0, $x_0 + m_1$, $x_0 + 2m_1$, ..., $x_0 + (d-1)m_1$, т.е. всего d чисел. Значит, у исходного сравнения имеется d решений.

Теорема 7. Пусть $(a,m) = d$. Если b не делится на d, сравнение $ax \equiv b(mod\ m)$ не имеет решений. Если b кратно d, сравнение $ax \equiv b(mod\ m)$ имеет d штук решений.

Пример. Решить сравнение $111x \equiv 75(mod\ 321)$.

Решение. $(111,321)=3$, поэтому поделим сравнение и его модуль на 3:

$$37x \equiv 25(mod 107) \text{ и уже } (37,107) = 1.$$

Включаем алгоритм Евклида (подчеркнуты неполные частные):

$$107 = 37 \cdot \underline{2} + 33$$
$$37 = 33 \cdot \underline{1} + 4$$
$$33 = 4 \cdot \underline{8} + 1$$
$$4 = 1 \cdot \underline{4}$$

Имеем $n = 4$, и цепная дробь такова:

$$\frac{m}{a} = \frac{107}{37} = 2 + \cfrac{1}{1 + \cfrac{1}{8 + \cfrac{1}{4}}}$$

Таблица для нахождения числителей подходящих дробей:

Таблица 3.2 – Числители подходящих дробей

q_n	0	2	1	8	4
P_n	1	2	3	26	107

Значит, $x \equiv (-1)^3 \cdot 26 \cdot 25 \equiv -650(mod\ 107) \equiv -8(mod\ 107) \equiv 99(mod\ 107)$.

Три решения исходного сравнения: $x \equiv 99(mod\ 321)$, $x \equiv 206(mod\ 321)$, $x \equiv 313(mod\ 321)$, и других решений нет.

Теорема 8. Пусть $m>1$, $(a,m) = 1$. Тогда сравнение $ax \equiv b(mod\ m)$ имеет решение:

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

Доказательство. По теореме Эйлера имеем: $a^{\varphi(m)} \equiv 1(mod\ m)$, следовательно,

$$a \cdot ba^{\varphi(m)-1} \equiv b(mod\ m).$$

Пример. Решить сравнение $7x \equiv 3(mod\ 10)$. Вычисляем:

$$\varphi(10) = 4;\ x \equiv 3 \cdot 7^{4-1}\ (mod\ 10) \equiv 1029(mod\ 10) \equiv 9(mod\ 10).$$

Данный способ решения сравнений может потребовать возведения числа a в довольно большую степень, что довольно трудоемко.

Теорема 9. Пусть p – простое число, $0<a<p$. Тогда сравнение $ax \equiv b(mod\ p)$ имеет решение:

$$x \equiv b \cdot (-1)^{a-1} \cdot \frac{(p-1)(p-2)\ldots(p-a+1)}{1 \cdot 2 \cdot 3 \cdot \ldots \cdot (a-1) \cdot a} (\mathrm{mod}\, p) \equiv b \cdot (-1)^{a-1} \cdot \frac{(p-1)!}{(a!) \cdot (p-a)!} (\mathrm{mod}\, p) \equiv$$

$$\equiv b \cdot (-1)^{a-1} \cdot \frac{p!}{p \cdot (a!) \cdot (p-a)!} (\mathrm{mod}\, p) \equiv b \cdot (-1)^{a-1} \cdot \frac{1}{p} \cdot C_p^a (\mathrm{mod}\, p),$$

где C_p^a – биномиальный коэффициент.

Пример. Решить сравнение $7x \equiv 2(mod\ 11)$. Вычисляем:

$$C_{11}^7 = \frac{11!}{(7!) \cdot (11-7)!} = \frac{8 \cdot 9 \cdot 10 \cdot 11}{2 \cdot 3 \cdot 4} = 2 \cdot 3 \cdot 5 \cdot 11 = 330;$$

$$x \equiv 2 \cdot (-1)^6 \cdot \frac{1}{11} \cdot 330 \equiv 60 \equiv 5(\mathrm{mod}\, 11)$$

3.2 ВЫЧИСЛЕНИЕ ОБРАТНЫХ ПО МОДУЛЮ ВЕЛИЧИН

Определение. Целое число a является обратным числу b по модулю n, если выполняется сравнение: $ab \equiv 1\ (\mathrm{mod}\ m)$.

1. Проверять путем поочередной подстановки чисел натурального ряда в формулу, пока не будет найдено число a, удовлетворяющее сравнению $ab \equiv 1\ (\mathrm{mod}\ m)$.

2. Используя функцию Эйлера $\varphi(m)$, можно вычислить

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

3. С помощью расширенного алгоритма Евклида.

В этом случае при решении сравнения $a \cdot x \equiv 1$ mod m найти

$$x \equiv a^{-1} \cdot 1 (\mathrm{mod}\, m).$$

Используя алгоритм Евклида и подходящие дроби, найдем

$$x \equiv \underbrace{((-1)^{k-1} P_{k-1})}_{a^{-1}} \cdot b (\mathrm{mod}\, m)$$, в нашем случае b = 1, отсюда:

$$x \equiv \underbrace{((-1)^{k-1} P_{k-1})}_{a^{-1}} \cdot 1 (\mathrm{mod}\, m),$$

где P_{k-1} – знаменатель предпоследней подходящей дроби разложения в непрерывную дробь.

Получаем формулу для поиска обратного значения по модулю:

$$a^{-1} \equiv ((-1)^{k-1} P_{k-1}) (\mathrm{mod}\, m).$$

Непрерывная дробь имеет вид: $\frac{m}{a} = [q_0, q_1, q_2, ..., q_k]$, где q_i – частное в цепочке следующих равенств:

$$m = aq_0 + a_1,$$
$$a = a_1q_1 + a_2,$$
$$a_1 = a_2q_2 + a_3,$$
$$\ldots\ldots\ldots\ldots$$
$$a_{k-2} = a_{k-1}q_{k-1} + a_k,$$
$$a_{k-1} = a_kq_k + 0,$$

где *ri* – остатки от деления.

Поскольку остатки от деления *ri* в алгоритме Евклида представляют собой строго убывающую последовательность натуральных чисел, то обеспечивается сходимость представленного алгоритма. При этом получается, что *rk* – общий делитель чисел *a* и *m*. Любой общий делитель чисел *a* и *m* делит и *rk*. Таким образом, *rk* = (*a*, *m*).

Последовательности {*Pm*} и {*Qm*} числителей и знаменателей подходящих дробей в непрерывной дроби определяются рекуррентно:

P – 2 = 0, *P* – 1 = 1, *Pm* = *qmPm* – 1+ *Pm* – 2 для $m \geq 0$,

Q – 2 = 1, *Q* – 1 = 0, *Qm* = *qmQm* – 1 + *Qm* – 2 для $m \geq 0$.

Для решения более сложных сравнений

$$a \cdot x \equiv b(\text{mod } m),\ b \neq 1$$

используют следующий прием. Сначала решают сравнение $a \cdot y \equiv 1\ (\text{mod } m)$, т.е. определяют $y \equiv a^{-1}(\text{mod } m)$, а затем находят

$$x \equiv a^{-1}\, b(\text{mod } m) \equiv y \cdot b(\text{mod } m).$$

3.3 СИСТЕМА СРАВНЕНИЙ ПЕРВОЙ СТЕПЕНИ (КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ)

Теорема 11. **(Китайская теорема об остатках).** Пусть дана простейшая система сравнений первой степени:

$$\begin{cases} x \equiv b_1(\text{mod}\, m_1) \\ x \equiv b_2(\text{mod}\, m_2) \\ \quad\vdots \\ x \equiv b_k(\text{mod}\, m_k) \end{cases}, \qquad (3.2)$$

где $m_1, m_2, \ldots, m_k$ попарно взаимно просты.

Далее $m_1 m_2 \ldots m_k = M_s m_s$; $M_s M_s^{\nabla} \equiv 1 (\text{mod } m_s)$.

Число M_s^{∇} всегда можно подобрать (с помощью алгоритма Евклида), т.к. $(m_s, M_s) = 1$; $x_0 = M_1 M_1^{\nabla} b_1 + M_2 M_2^{\nabla} b_2 + \ldots + M_k M_k^{\nabla} b_k$. Тогда система (3.2) равносильна одному сравнению

$$x \equiv x_0 (\text{mod } m_1 m_2 \ldots m_k),$$

т.е. $x \equiv x_0 (\text{mod } m_1 m_2 \ldots m_k)$ и есть решение системы сравнений (3.2).

Пример. Найти число, которое при делении на 4 дает в остатке 1, при делении на 5 дает в остатке 3, а при делении на 7 дает в остатке 2.Составим систему сравнений первой степени:

$$\begin{cases} x \equiv 1(\text{mod}\, 4) \\ x \equiv 3(\text{mod}\, 5) \\ x \equiv 2(\text{mod}\, 7) \end{cases}$$

Решение.
$b_1 = 1; b_2 = 3; b_3 = 2;$ $m_1 m_2 m_3$, т.е. $M_1 = 35, M_2 = 28, M_3 = 20.$
Далее:
$35 \cdot 3 \equiv 1 (\mathrm{mod}\ 4)$,
$28 \cdot 2 \equiv 1 (\mathrm{mod}\ 5)$,
$20 \cdot 6 \equiv 1 (\mathrm{mod}\ 7)$,
т.е. $M_1^{\nabla} = 3$, $M_2^{\nabla} = 2$, $M_3^{\nabla} = 6$. Значит $x_0 = 35 \cdot 3 \cdot 1 + 28 \cdot 2 \cdot 3 + 20 \cdot 6 \cdot 2 = 513$.
По теореме 10, получим ответ:
$x \equiv 513 (\mathrm{mod}\ 140) \equiv 93 (\mathrm{mod}\ 140)$, т.е. наименьшее положительное число равно 93.
Лемма 5. Если $b_1, b_2, \ldots, b_k$ пробегают полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$ соответственно, то x_0 пробегает полную систему вычетов по модулю $m_1 m_2 \ldots m_k$.

3.4 СРАВНЕНИЯ ЛЮБОЙ СТЕПЕНИ ПО ПРОСТОМУ МОДУЛЮ

Рассмотрим сравнения вида $f(x) \equiv 0 (\mathrm{mod}\ p)$, где p – простое число,
$f(x) = ax^n + a_1 x^{n-1} + \ldots + a_n$ – многочлен с целыми коэффициентами.
Лемма 6. Произвольное сравнение $f(x) \equiv 0 (\mathrm{mod}\ p)$, где p – простое число, равносильно некоторому сравнению степени не выше $p - 1$.
Доказательство. Разделим $f(x)$ на многочлен $x^p - x$ (такой многочлен иногда называют "многочлен деления круга") с остатком: $f(x) = (x^p - x) \cdot Q(x) + R(x)$, где, как известно, степень остатка $R(x)$ не превосходит $p-1$. Но ведь, по теореме Ферма, $x^p - x \equiv 0 (\mathrm{mod}\ p)$. Это означает, что $f(x) \equiv R(x) (\mathrm{mod}\ p)$, а исходное сравнение равносильно сравнению $R(x) \equiv 0 (\mathrm{mod}\ p)$.
С помощью данной теоремы можно свести решение сравнения высокой степени к решению сравнения меньшей степени.
Лемма 7. Если сравнение $ax^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 (\mathrm{mod}\ p)$ степени n по простому модулю p имеет более n различных решений, то все коэффициенты $a, a_1, \ldots, a_n$ кратны p.
Вывод. Всякое нетривиальное сравнение по $mod\ p$ равносильно сравнению степени не выше $p-1$ и имеет не более $p - 1$ решений.
Теорема 12.(Вильсон) Сравнение $(p - 1)! + 1 \equiv 0 (\mathrm{mod}\ p)$ выполняется тогда и только тогда, когда p – простое число.
Доказательство. Пусть p – простое число. Если $p = 2$, то, очевидно, $1! + 1 \equiv 0 (\mathrm{mod}\ 2)$.
Если $p > 2$, то рассмотрим сравнение:

$$[(x - 1)(x - 2)\ldots(x - (p - 1))] - (x^{p-1} - 1) \equiv 0 (\mathrm{mod}\ p).$$

Ясно, что это сравнение степени не выше $p - 2$, но оно имеет $p - 1$ решение: $1, 2, 3, \ldots, p-1$, т.к. при подстановке любого из этих чисел слагаемое в квадратных скобках обращается в ноль, а (x^{p-1}) сравнимо с нулем по теореме Ферма (x и p взаимно просты, т.к. $x<p$).
Это означает, что все коэффициенты выписанного сравнения кратны p, в частности, на p делится его свободный член, равный $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p - 1) + 1$.
Если p – не простое, то найдется делитель d числа p, $1<d<p$. Тогда $(p - 1)!$ делится на d, поэтому $(p - 1)! + 1$ не может делиться на d и, значит, не может делиться также и на p.
Следовательно, сравнение $(p - 1)! + 1 \equiv 0 (\mathrm{mod}\ 2)$ не выполняется.
Пример. $1 \cdot 2 \cdot 3 \cdot \ldots \cdot 10 + 1 = 3628800 + 1 = 3628801$ – делится на 11 (вспомните признак делимости на 11 – если сумма цифр в десятичной записи числа на четных позициях совпадает с суммой цифр на нечетных позициях, то число кратно 11).
Пример-задача. Доказать: если простое число p представимо в виде $4n+1$, то существует такое число x, что $x^2 + 1$ делится на p.

Решение. Пусть $p = 4n + 1$ – простое число. По теореме Вильсона $(4n)! + 1$ делится на p. Заменим в выражении $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (4n) + 1$ все множители большие $(p - 1)/2 = 2n$ через разности числа p и чисел меньших $(p-1)/2 = 2n$. Получим:

$(p-1)! + 1 = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2n \cdot (p - 2n)(p - 2n + 1) \cdot \ldots \cdot (p-1) =$

$= (1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2n)[A \cdot p + (-1)^{2n} \cdot 2n \cdot (2n - 1) \cdot \ldots \cdot 2 \cdot 1] + 1 = A_1 p + (1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2n)^2) + 1.$

Так как это число делится на p, то и сумма $(1 \cdot 2 \cdot 3 \cdot \ldots \cdot 2n)^2 + 1$ делится на p, т.е. $x = (2n)! = ((p-1)/2)!$.

3.5 СРАВНЕНИЯ ЛЮБОЙ СТЕПЕНИ ПО СОСТАВНОМУ МОДУЛЮ

Теорема 13. Если числа $m_1, m_2, \ldots, m_k$ попарно взаимно просты, то сравнение $f(x) \equiv 0 (\mathrm{mod}\ m_1 m_2 \ldots m_k)$ равносильно системе сравнений:

$$\begin{cases} f(x) \equiv 0 (\mathrm{mod}\, m_1) \\ f(x) \equiv 0 (\mathrm{mod}\, m_2) \\ \vdots \\ f(x) \equiv 0 (\mathrm{mod}\, m_k) \end{cases}$$

При этом, если $T_1, T_2, \ldots, T_k$ – числа решений отдельных сравнений этой системы по соответствующим модулям, то число решений T исходного сравнения равно $T_1 T_2 \ldots T_k$.

Доказательство. Первое утверждение теоремы (о равносильности системы и сравнения) очевидно, т.к. если $a \equiv b \pmod m$, то $a \equiv b \pmod d$, где d делит m.

Если же $a \equiv b \pmod{m_1}$ и $a \equiv b \pmod{m_2}$, то $a \equiv b \pmod{НОК(m_1, m_2)}$, где

$НОК(m_1, m_2)$ – наименьшее общее кратное m_1 и m_2. (Вспомните простейшие свойства сравнений).

Второе утверждение теоремы (о числе решений сравнения):

Каждое сравнение $f(x) \equiv 0 (\mathrm{mod}\ m_s)$ выполняется тогда и только тогда, когда выполняется одно из T_s штук сравнений вида $x \equiv b_s (\mathrm{mod}\ m_s)$, где b_s пробегает вычеты решений сравнения $f(x) \equiv 0 (\mathrm{mod}\ m_s)$. Всего различных комбинаций таких простейших сравнений

$$\begin{cases} x \equiv b_1 (\mathrm{mod}\, m_1) \\ x \equiv b_2 (\mathrm{mod}\, m_2) \\ \vdots \\ x \equiv b_k (\mathrm{mod}\, m_k) \end{cases}$$

$T_1 T_2 \ldots T_k$ штук. Все эти комбинации приводят к различным классам вычетов по $\mathrm{mod}(m_1 m_2 \ldots m_k)$.

Итак, решение сравнения $f(x) \equiv 0 (\mathrm{mod}\, p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k})$ сводится к решению сравнений вида $f(x) \equiv 0 (\mathrm{mod}\, p^a)$. Решение последнего сравнения, в свою очередь, сводится к решению некоторого сравнения $g(x) \equiv 0 (\mathrm{mod} p)$ с другим многочленом в левой части, но уже с простым модулем, а приводит нас в рамки предыдущего пункта.

3.5.1 Процесс сведения решения сравнения $f(x) \equiv 0 (\mathrm{mod}\, p^a)$ к решению сравнения $g(x) \equiv 0 (\mathrm{mod}\, p)$.

Выполнение сравнения $f(x) \equiv 0 \pmod{p^a}$ влечет, что x подходит в сравнение $f(x) \equiv 0 (\mathrm{mod}\ p)$. Пусть $x \equiv x_1 \pmod p$ – какое-нибудь решение сравнения $f(x) \equiv 0 (\mathrm{mod}\ p)$. Это означает, что

$$x = x_1 + p \cdot t_1, \text{ где } t_1 \in \mathbf{Z}.$$

Вставим это x в сравнение $f(x) \equiv 0 (\mathrm{mod}\ p^2)$. Получим сравнение

$$f(x_1 + p \cdot t_1) \equiv 0 (\mathrm{mod}\ p^2),$$

которое тоже выполняется.

Разложим далее левую часть полученного сравнения по формуле Тейлора по степеням $(x - x_1)$:

$$f(x) = f(x_1) + \frac{f'(x_1)}{1!}(x - x_1) + \frac{f''(x_1)}{2!}(x - x_1)^2 + \ldots$$

Но, $x = x_1 + p \cdot t_1$, следовательно:

$$f(x_1 + p \cdot t_1) = f(x_1) + \frac{f'(x_1)}{1!} p \cdot t_1 + \frac{f''(x_1)}{2!} p^2 \cdot t_1^2 + \ldots$$

Число $\dfrac{f^{(k)}(x_1)}{k!}$ всегда целое, т.к. $f(x_1 + p\, t_1)$ – многочлен с целыми коэффициентами. Теперь в сравнении

$$f(x_1 + p \cdot t_1) \equiv 0 (\mathrm{mod}\ p^2)$$

можно слева отбросить члены, кратные p^2:

$$f(x_1) + \frac{f'(x_1)}{1!} p \cdot t_1 \equiv 0 (\mathrm{mod}\ p^2).$$

Разделим последнее сравнение и его модуль на p:

$$\frac{f(x_1)}{p} + \frac{f'(x_1)}{1!} \cdot t_1 \equiv 0 (\mathrm{mod}\ p).$$

Заметим, что $\dfrac{f(x_1)}{p}$ – целое число, т.к. $f(x_1) \equiv 0 (\mathrm{mod}\ p)$. Далее ограничимся случаем, когда значение производной $f'(x_1)$ не делится на p. В этом случае имеется всего одно решение сравнения первой степени:

$$\frac{f(x_1)}{p} + \frac{f'(x_1)}{1!} \cdot t_1 \equiv 0 (\mathrm{mod}\ p),$$

относительно t_1:

$$t_1 \equiv t_1^{\nabla} (\mathrm{mod}\ p).$$

Это означает, что $t_1 = t_1^{\nabla} + p \cdot t_2$, где $t_2 \in \mathbf{Z}$, и

$$x = x_1 + p \cdot t_1 = \underbrace{x_1 + p \cdot t_1^{\nabla}}_{x_2} + p^2 t_2 = x_2 + p^2 t_2$$

Снова вставим это $x = x_2 + p^2 t_2$ в сравнение $f(x) \equiv 0 (\mathrm{mod}\ p^3)$ (но теперь это сравнение уже по $\mathrm{mod} p^3$), разложим его левую часть по формуле Тейлора по степеням $(x - x_2)$ и отбросим члены, кратные p^3:

$$f(x_2) + (f'(x_2)/1!) \cdot p^2 t_2 \equiv 0 (\mathrm{mod} p^3).$$

Делим это сравнение и его модуль на p^2:

$$f(x_2)/p^2 + f'(x_2) \cdot t_2 \equiv 0 (\mathrm{mod} p).$$

Опять-таки $f(x_2)/p^2$ – целое число, ведь число t_1^{∇} такое, что $f(x_1 + p \cdot t_1^{\nabla}) \equiv 0 (\mathrm{mod} p^2)$. Кроме того, $x_2 \equiv x_1 (\mathrm{mod}\ p)$, значит, $f'(x_2) \equiv f'(x_1) (\mathrm{mod}\ p)$, т.е. $f'(x_2)$, как и $f'(x_1)$, не делится на p. Имеем единственное решение сравнения первой степени $f(x_2)/p^2 + f'(x_2) \cdot t_2) \equiv 0 (\mathrm{mod}\ p)$ относительно t_2:

$$t_2 \equiv t_2^{\nabla} (\mathrm{mod}\ p).$$

Это означает, что $t_2 = t_2^{\nabla} + p \cdot t_3$, где $t_3 \in \mathbf{Z}$, и $x = \underbrace{x_2 + p^2 \cdot t_2^{\nabla}}_{x_3} + p^3 t_3 = x_3 + p^3 t_3$,

и процесс продолжается дальше и дальше, аналогично предыдущим шагам, до достижения степени p^a, в которой стоит простое число p в модуле исходного сравнения $f(x) \equiv 0(\mathrm{mod}\ p^a)$.

Вывод. *Всякое решение* $x \equiv x_1 (\mathrm{mod}\ p)$ *сравнения* $f(x) \equiv 0(\mathrm{mod}\ p)$, *при условии* $p / f''(x_1)$, *дает одно решение сравнения* $f(x) \equiv 0(\mathrm{mod}\ p^a)$ *вида* $x \equiv x_a + p^a t_a$, т.е. $x \equiv x_a (\mathrm{mod}\ p^a)$.

Пример. Решить сравнение $x^4 + 7x + 4 \equiv 0(\mathrm{mod}27)$.

Решение. $27 = 3^3$. Далее, перебором полной системы вычетов по mod3 найдем, что сравнение $x^4 + 7x + 4 \equiv 0(\mathrm{mod}3)$ имеет всего одно решение $x \equiv 1(\mathrm{mod}3)$.

Далее:

$$f'(x) = (4x^3 + 7)\big|_{x \equiv 1} \equiv 2(\mathrm{mod}3),$$

т.е. не делится на $p = 3$. Далее:

$x_1 = 1 + 3 \cdot t_1$

$f(1) + f'(1)\, 3 \cdot t_1 \equiv 0(\mathrm{mod}3^2)$

Ищем t_1:

$3 + 3 t_1 \cdot 2 \equiv 0(\mathrm{mod}9)$,

после деления на $p = 3$:

$1 + 2 t_1 \equiv 0(\mathrm{mod}3)$,

$t_1 \equiv 1(\mathrm{mod}3)$ – единственное решение.

Далее:

$t_1 = 1 + 3 t_2$,

$x = 1 + 3 t_1 = 4 + 9 t_2$,

$f(4) + 9 \cdot t_2 \cdot f'(4) \equiv 0(\mathrm{mod}\ p^3 = 27)$,

$18 + 9 \cdot 20 \cdot t_2 \equiv 0(\mathrm{mod}27)$,

и, после деления на $p^2 = 9$, ищем t_2:

$2 + 20 t_2 \equiv 0(\mathrm{mod}3)$,

$t_2 \equiv 2(\mathrm{mod}3)$,

$t_2 = 2 + 3 t_3$,

откуда

$$x = 4 + 9 \cdot (2 + 3 t_3) = 22 + 27 t_3.$$

Значит, единственным решением исходного сравнения является $x \equiv 22(\mathrm{mod}27)$.

Теорема 14. Пусть A, m, n – натуральные числа; $(A, m) = 1$, $x \equiv x_0 (\mathrm{mod}\ m)$ – одно из решений сравнения $x^n \equiv A (\mathrm{mod}\ m)$. Тогда все решения этого сравнения получаются умножением x_0 на вычеты решений сравнения $y^n \equiv 1(\mathrm{mod}\ m)$.

Доказательство. Перемножим сравнения:

$$\begin{array}{l} x_0^n \equiv A(\mathrm{mod}\, m) \\ \underline{y^n \equiv (\mathrm{mod}\, m)} \quad \times \\ (x_0 y)^n \equiv A(\mathrm{mod}\, m), \end{array}$$

откуда видно, что $x_0 y$ – решения сравнения $x^n \equiv A (\mathrm{mod}\ m)$.

Если теперь y_1 несравнимо с y_2 по модулю (mod m), то x_0y_1 несравнимо с x_0y_2 по модулю (mod m). Действительно, предположим, что $x_0 y_1 \equiv x_0 y_2 \pmod m$. Очевидно, что $(x_0, m)=1$, т.к. иначе было бы:

$$x_0 = d \cdot x_0^{\nabla},\ m = d \cdot m^{\nabla},$$
$$x_0 = d^n (x_0^{\nabla})^n \equiv A \pmod{d\, m^{\nabla}},$$

следовательно, d делит A и делит m, что противоречит взаимной простоте A и m. Значит, $(x_0, m) = 1$ и сравнение $x_0y_1 \equiv x_0y_2 \pmod m$ можно поделить на x_0: $y_1 \equiv y_2 \pmod m$ – а это противоречит исходному предположению. Таким образом, для разных y_1 и y_2 получаются разные решения.

Убедимся, что каждое решение сравнения $x^n \equiv A \pmod m$ получается именно таким способом. Имеем:

$$x^n \equiv A \pmod m$$
$$x_0^n \equiv A \pmod m,$$

следовательно, $x^n \equiv x_0^n \pmod m$. Возьмем число y такое, что $x \cdot y \equiv x_0 \pmod m$.

Тогда $y^n x_0^n \equiv x_0^n \pmod m$, т.е. $y^n \equiv 1 \pmod m$.

3.6 СРАВНЕНИЯ ВТОРОЙ СТЕПЕНИ. СИМВОЛ ЛЕЖАНДРА

Рассмотрим простейшее двучленное сравнение второй степени вида:

$$x^2 \equiv a \pmod p,$$

где a и p взаимно просты, а p – нечетное простое число.

Условие взаимной простоты $(a, p) = 1$ исключает из рассмотрения случай $a = 0$. Т.к. сравнение $x^2 \equiv a \pmod 2$ имеет решение при любых a, т.к. вместо a достаточно подставлять только 0 или 1, а числа 0 и 1 являются квадратами. Именно поэтому случай $p = 2$ не представляет особого интереса. (всякий элемент любого поля характеристики 2 является квадратом, т.к. отображение $x \to x^2$ есть автоморфизм такого поля).

Сравнение $x^2 \equiv 0 \pmod p$ всегда имеет решение $x = 0$. Итак, интерес представляет только ситуация с нечетным простым модулем и $a \neq 0$.

Определение. Если сравнение $x^2 \equiv a \pmod p$ имеет решения, то число a называется квадратичным вычетом по модулю p. В противном случае, число a называется квадратичным невычетом по модулю p.

Если a – квадрат некоторого числа по модулю p, то a – «квадратичный вычет», если же никакое число в квадрате не сравнимо с a по модулю p, то a – «квадратичный невычет».

Пример. Число 2 является квадратом по модулю 7, т.к. $4^2 \equiv 16 \equiv 2 \pmod 7$. Значит, 2 – квадратичный вычет. (Сравнение $x^2 \equiv 2 \pmod 7$ имеет еще и другое решение: $3^2 \equiv 9 \equiv 2 \pmod 7$.) Напротив, число 3 является квадратичным невычетом по модулю 7, т.к. сравнение $x^2 \equiv 3 \pmod 7$ решений не имеет, в чем нетрудно убедиться последовательным перебором полной системы вычетов: $x = 0,1,2,3,4,5,6$.

Наблюдение. Если a – квадратичный вычет по модулю p, то сравнение $x^2 \equiv a \pmod p$ имеет в точности два решения. Действительно, если a – квадратичный вычет по модулю p, то у сравнения $x^2 \equiv a \pmod p$ есть хотя бы одно решение $x \equiv x_1 \pmod p$. Тогда $x_2 = -x_1$ – тоже решение, ведь $(-x_1)^2 = x_1^2$. Эти два решения не сравнимы по модулю $p > 2$, так как из $x_1 \equiv -x_1 \pmod p$ следует $2x_1 \equiv 0 \pmod p$, т.е. (поскольку $p \neq 2$) $x_1 \equiv 0 \pmod p$, что невозможно, ибо $a \neq 0$.

Поскольку сравнение $x^2 \equiv a \pmod p$ есть сравнение второй степени по простому модулю, то больше двух решений оно иметь не может.

Наблюдение: Приведенная (т.е. без нуля) система вычетов

$$-\frac{p-1}{2},\ldots,-2,-1,1,2,\ldots,\frac{p-1}{2}$$

по модулю p состоит из $(p-1)/2$ квадратичных вычетов, сравнимых с числами $1^2, 2^2, \ldots, ((p-1)/2)^2$, и $(p-1)/2$ квадратичных невычетов, т.е. вычетов и невычетов поровну.

3.6.1 Символ Лежандра $\left(\frac{a}{p}\right)$

Определение. Пусть a не кратно p. Тогда символ Лежандра определяется как:

$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{если a – квадратичный вычет по модулю p.} \\ -1, & \text{если a – квадратичный невычет по модулю p.} \end{cases}$

Теорема 15. (Критерий Эйлера) Пусть a не кратно p. Тогда:

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

Доказательство. По теореме Ферма, $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$, т.е.

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 (\mathrm{mod}\, p).$$

В левой части последнего сравнения в точности один сомножитель делится на p, ведь оба сомножителя на p делиться не могут, иначе их разность, равная двум, делилась бы на $p > 2$. Следовательно, имеет место одно и только одно из сравнений:

$$a^{(p-1)/2} \equiv 1 (\mathrm{mod}\ p),$$
$$a^{(p-1)/2} \equiv -1 (\mathrm{mod}\ p).$$

Но всякий квадратичный вычет a удовлетворяет при некотором x сравнению $a \equiv x^2 (\mathrm{mod}\ p)$ и, следовательно, удовлетворяет также получаемому из него почленным возведением в степень $(p-1)/2$ сравнению $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 (\mathrm{mod}\ p)$ (теорема Ферма).

При этом, квадратичными вычетами и исчерпываются все решения сравнения $a^{(p-1)/2} \equiv 1 (\mathrm{mod}\ p)$, т.к., будучи сравнением степени $(p-1)/2$, оно не может иметь более $(p-1)/2$ решений. Это означает, что квадратичные невычеты удовлетворяют сравнению $a^{(p-1)/2} \equiv -1 (\mathrm{mod}\ p)$.

Свойство $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\, p)$, даваемое критерием Эйлера, можно сразу принять за определение символа Лежандра, показав, предварительно, с помощью теоремы Ферма, что $a^{(p-1)/2} \equiv \pm 1 (\mathrm{mod}\ p)$.

Пример. Будет ли число 5 квадратом по модулю 7?

$$5^{(7-1)/2} = 5^3 = 125 = 18 \cdot 7 - 1 \equiv -1 (\mathrm{mod} 7),$$

т.е. сравнение $x^2 \equiv 5 (\mathrm{mod} 7)$ решений не имеет и 5 – квадратичный невычет по модулю 7.

3.6.2 Простейшие свойства символа Лежандра

Свойство 1. Если $a \equiv b (\mathrm{mod}\ p)$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Это свойство следует из того, что числа одного и того же класса по модулю p будут все одновременно квадратичными вычетами либо квадратичными невычетами.

Свойство 2. $(1/p) = 1$. Доказательство очевидно, ведь единица является квадратом.

Свойство 3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Доказательство этого свойства следует из критерия Эйлера при a = -1. Так как (p -1)/2 – четное, если p вида 4 n +1, и нечетное, если p вида 4 n +3, то число -1 является квадратичным вычетом по модулю p тогда и только тогда, когда p вида 4 n +1.

Свойство 4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

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

Свойство 4, очевидно, распространяется на любое конечное число сомножителей в числителе символа Лежандра, взаимно простых с p. Кроме того, из него следует

Свойство 5: $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$, т.е. в числителе символа Лежандра можно отбросить любой квадратный множитель. Действительно:

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right)\cdot 1 = \left(\frac{a}{p}\right) (\mathrm{mod}\, p).$$

3.6.2.1 Закон взаимности Гаусса

Теорема 16. **(Закон взаимности квадратичных вычетов)** Если p и q – нечетные простые числа, то

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

Другими словами, если хоть одно из чисел p или q вида 4n + 1, то p квадрат по модулю q тогда и только тогда, когда q квадрат по модулю p.

Если же оба числа p и q вида 4n + 3, то p квадрат по модулю q тогда и только тогда, когда q не является квадратом по модулю p.

ЛИТЕРАТУРА

1. Айерлэнд, К. Классическое введение в современную теорию чисел / К. Айерлэнд, М. Роузен. – М.: Мир, 1987.

2. Воронков, Б.Н. Методическое пособие по разработке средств защиты информации в вычислительных сетях / Б.Н. Воронков, В.И. Тупота. – Воронеж: ЛОП ВГУ, 2000.

3. Иванов, В.А. Криптографические методы защиты информации в компьютерных системах и сетях / В.А. Иванов. – М.: КУДИЦ – ОБРАЗ,2001.

4. Математические и компьютерные основы криптологии: учеб. пособие / Ю.С. Харин [и др.]. – Минск: Новое знание, 2003.

5. Основы криптографии: учеб. пособ. / А.П. Алферов [и др.]. – М.: Гелиос АРВ, 2001.

6. Питерсон, У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон. – М.: Мир, 1976.

7. Холл, М. Комбинаторика / М. Холл. – М.: Мир, 1970.

8. Diffie, W. New directions in cryptography / W. Diffie, M. Hellman // IEEE Trans. Inf. Theory, 1976. – Vol. 22, № 11.

9. Giblin, P.J. Primes and Programming: An Introduction to Number Theory with Computing / P.J. Giblin. – Cambridge: Cambridge University Press, 1993.

УЧЕБНОЕ ИЗДАНИЕ

Составитель: Хацкевич Мария Викторовна

ТЕОРЕТИКО-ЧИСЛОВЫЕ АЛГОРИТМЫ В КРИПТОГРАФИИ

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.В.
Компьютерная верстка: Кармаш Е.Л.
Корректор: Никитчик Е.В.

Подписано к печати 08.10.2012 г. Формат 60x84 1/16.
Усл. печ. лист. 1,4. Уч. изд. л. 1,5. Тираж 30 экз. Заказ № 1092
Отпечатано на ризографе учреждения образования
«Брестский государственный технический университет».
224017, г. Брест, ул. Московская, 267.