Практическое занятие 1

Основы модулярной арифметики, проверка простоты и факторизация чисел

Цель работы: освоение и программная реализация принципов, методов и алгоритмов решения вспомогательных задач криптографии.

Задание 1.1. Найти наибольший общий делитель НОД(a,b) двух чисел $a \in Z$, $b \in N$ методом Евклида.

Алгоритм и расчетные формулы метода Евклида:

$$r_{j-2} = q_j r_{j-1} + r_j,\ q_j = \left[\frac{r_{j-2}}{r_{j-1}}\right],\ j = 0,1,2\ldots, \text{ где } r_{-2} = a, r_{-1} = b.$$

Решением задачи является последний ненулевой остаток $r_j > 0$.

Пример. Найти НОД$(1547,560)$. Решение приведено в табл. 1.3.

Таблица 1.3 – Выполнение алгоритма Евклида для примера

шаг	кратность	разложение	остаток
$j=1$	$q_1 = \left[\frac{a}{b}\right] = \left[\frac{1547}{560}\right] = 2$	$a = q_1 b + r_0$: $1547 = 2 \cdot 560 + 427$	$r_0 = 427$
$j=2$	$q_2 = \left[\frac{b}{r_0}\right] = \left[\frac{560}{427}\right] = 1$	$b = q_2 r_0 + r_1$: $560 = 1 \cdot 427 + 133$	$r_1 = 133$
$j=3$	$q_3 = \left[\frac{r_0}{r_1}\right] = \left[\frac{427}{133}\right] = 3$	$r_0 = q_3 r_1 + r_2$: $427 = 3 \cdot 133 + 28$	$r_2 = 28$
$j=4$	$q_4 = \left[\frac{r_1}{r_2}\right] = \left[\frac{133}{28}\right] = 4$	$r_1 = q_4 r_2 + r_3$: $133 = 4 \cdot 28 + 21$	$r_3 = 21$
$j=5$	$q_5 = \left[\frac{r_2}{r_3}\right] = \left[\frac{28}{21}\right] = 1$	$r_2 = q_5 r_3 + r_4$: $28 = 1 \cdot 21 + 7$	$r_4 = 7$
$j=6$	$q_6 = \left[\frac{r_3}{r_4}\right] = \left[\frac{21}{7}\right] = 3$	$r_3 = q_6 r_4 + r_5$: $21 = 3 \cdot 7 + 0$	$r_5 = 0$

Получено: $r_5 = 0$, следовательно, выполнение алгоритма окончено. Решением является предшествующий (ненулевой) остаток $r_4 = 7$: НОД$(1547,560) = 7$.

Задание 1.2. Найти результат преобразования методом, основанным на теореме Эйлера.

Функция Эйлера: $\varphi(n)=\left|\left\{0\le b<n \middle| НОД(b,n)=1\right\}\right|$ обладает следующими ключевыми свойствами:

1) $\varphi(1)=1$;

2) для любого простого p: $\varphi(p)=p-1$;

3) для любого простого p в степени α: $\varphi\left(p^{\alpha}\right)=p^{\alpha}-p^{\alpha-1}$;

4) $\forall m,n\in N \mid НОД(m,n)=1: \varphi(m\cdot n)=\varphi(m)\cdot\varphi(n)$.

Используется теорема Эйлера:

$$\forall a,m\in N \mid НОД(a,m)=1: a^{\varphi(m)}\equiv 1(\mathrm{mod}\, m),$$

и следствие из нее: если НОД$(a,m)=1$ и n' – наименьший неотрицательный вычет n по модулю $\varphi(m)$, то $a^{n}\equiv a^{n'}(\mathrm{mod}\, m)$.

Пример. Провести преобразование: $5^{17}\bmod 7$

Решение. $a=5; n=17; m=7$. При этом 7 – простое число.

Находим $\varphi(m)=\varphi(7)=7-1=6$;

$n'=17\bmod(6)=(2\cdot 6+5)\bmod(6)=5$;

$5^{17}\bmod 7=5^{5}\bmod 7=3125\bmod 7=(446\cdot 7+3)\bmod 7=3$.

Задание 1.3. Найти обратное значение числа по модулю:

– при помощи определения кратности k («по определению»);

– с использованием функции Эйлера.

Сравнить полученные результаты и оценить трудоемкость.

По определению обратные числа по модулю означают, что $a\cdot b\equiv 1(\mathrm{mod}\, m)$. Обратное число $b\equiv a^{-1}(\mathrm{mod}\, m)$ гарантированно

существует, если НОД$(a,m)=1$ (a и m – взаимно простые). При этом выполнено диофантово уравнение: $a\cdot b-k\cdot m=1$, где k – кратность m в числе $a\cdot b$. Внимание: число k должно быть получено *целым* числом.

Пример: найти $x=9^{-1}(\mathrm{mod}\,5)$.

Решение «по определению». Получаем уравнение $9\cdot x-k\cdot 5=1$;

$$x=(1+k\cdot 5):9.$$

Производим последовательный перебор возможных кратностей k как чисел последовательности натуральных чисел $\{1,2,3,4,....\}$ до тех пор, пока не получим x как *целое* число. В данном примере при $k=7$ получено целое число $x=4$.

Итак, получено $9^{-1}(\mathrm{mod}\,5)=4$.

Проверка: $9\cdot 4-7\cdot 5=36-35=1$.

Решение по теореме Эйлера: $a^{\varphi(m)}\equiv 1(\mathrm{mod}\,m)$. Домножим левую и правую части этого уравнения на $a^{-1}(\mathrm{mod}\,m)$. Получаем правило нахождения числа, обратного по модулю (в кольце), *с использованием функции Эйлера:*

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

Пример тот же: $x=9^{-1}(\mathrm{mod}\,5)$.

Решение: $a=9, m=5$. НОД$(9,5)=1$, $m=5$ – простое число.

Находим $\varphi(m)=\varphi(5)=5-1=4$;

$x=9^{4-1}(\mathrm{mod}\,5)=729(\mathrm{mod}\,5)=(145\cdot 5+4)(\mathrm{mod}\,5)=4$, т.е. $b=x=4$.

Получен тот же результат без перебора неподходящих вариантов k. Если в дальнейшем потребуется k как коэффициент диофантова уравнения, его можно будет определить из уравнения $a\cdot b-k\cdot m=1$.

Задание 1.4. Найти результат преобразования методом цепочек.

При больших значениях чисел $a^{n'}$ (задание 1.2) или $a^{\varphi(m)-1}$ (задание 1.3) определение вычетов по $(\mathrm{mod}\, m)$ может быть проведено с использованием метода цепочек модулярной арифметики:

$$(a \pm b) \bmod m = \big((a \bmod m) \pm (b \bmod m)\big) \bmod m;$$

$$(a * b) \bmod m = \big((a \bmod m) * (b \bmod m)\big) \bmod m;$$

$$\big(a * (b \pm c)\big) \bmod m = \big(((a * b) \bmod m) \pm ((a * c) \bmod m)\big) \bmod m.$$

Пример 1. Пусть требуется представить в форме цепочки $a^8 (\mathrm{mod}\, m)$. Степень четная, более того $8 = 2^3$.

Цепочка преобразований

$$(((a^2 (\mathrm{mod}\, m)^2 \bmod m)^2 \bmod m.$$

При использовании сложных чисел в выражении $a^n (\mathrm{mod}\, m)$ как в качестве a, так и в качестве степени n (n' или $(\varphi(m)-1)$) может быть использована факторизация чисел (разложение их на простые сомножители).

Пример 2. Найти методом цепочек $a^n (\mathrm{mod}\, m) = 15^{63} (\mathrm{mod}\, 7)$.

Решение. $a = 15 = 3 \cdot 5$; $n = 63 = 3^2 \cdot 7$.

$$15^{63} (\mathrm{mod}\, 7) = ((3^{63} \bmod 7) \cdot (5^{63} \bmod 7)) \bmod 7 = (A \cdot B) \bmod 7;$$

$$A = 3^{63} \bmod 7 = 3^{3 \cdot 3 \cdot 7} \bmod 7 = ((3^3 \bmod 7)^3 \bmod 7)^7 \bmod 7;$$

$$3^3 \bmod 7 = 27 \bmod 7 = (3 \cdot 7 + 6) \bmod 7 = 6;$$

$$6^3 \bmod 7 = 216 \bmod 7 = (30 \cdot 7 + 6) \bmod 7 = 6;$$

$$6^7 \bmod 7 = 6^{2 \cdot 2 + 3} \bmod 7 = ((6^{2 \cdot 2} \bmod 7) \cdot (6^3 \bmod 7)) \bmod 7;$$

$$6^{2 \cdot 2} \bmod 7 = (6^2 \bmod 7)^2 \bmod 7;\ 6^2 \bmod 7 = 36 \bmod 7 = (5 \cdot 7 + 1) \bmod 7 = 1;$$

$$1^2 \bmod 7 = 1;\ 6^7 \bmod 7 = (1 \cdot 6) \bmod 7 = 6;\ A = 6.$$

Аналогичными действиями для $5^{63} \bmod 7$ получаем $B = 6$.

$$15^{63} (\mathrm{mod}\, 7) = A \cdot B \bmod 7 = (6 \cdot 6) \bmod 7 = 36 \bmod 7 = (5 \cdot 7 + 1) \bmod 7 = 1.$$

В прикладной криптографии (при использовании двоичного кода представления целых чисел) особое значение имеет возможность построения на основе метода цепочек алгоритма повторного возведения в квадрат, который реализуется при выполнении заданий лабораторного практикума.

Обозначим промежуточный результат вычисления a. В конце работы алгоритма a примет значение наименьшего неотрицательного вычета $b^n (\mathrm{mod}\, m)$. Пусть $n = n_0 \cdot 2^0 + n_1 \cdot 2^1 + n_2 \cdot 2^2 + \ldots + n_{k-1} \cdot 2^{k-1}$, где n_j, $j = 0, 1, 2, \ldots, k-1$ – цифры двоичной записи числа n. Каждое n_j равно либо 1, либо 0. Принимаем начальное значение $a = 1$. Первые шаги алгоритма метода повторного возведения в квадрат представлены в табл. 1.6.

Таблица 1.6 – Первые шаги алгоритма метода

$j = 0$	$b_0 = b (\mathrm{mod}\, m)$	при $n_0 = 1 \Rightarrow a = b_0$
$j = 1$	$b_1 = b^2 (\mathrm{mod}\, m)$	при $n_1 = 1 \Rightarrow a = (a \cdot b_1) \bmod m$
$j = 2$	$b_2 = b_1^2 (\mathrm{mod}\, m)$	при $n_2 = 1 \Rightarrow a = (a \cdot b_2) \bmod m$
$j = 3$	$b_3 = b_2^2 (\mathrm{mod}\, m)$	при $n_3 = 1 \Rightarrow a = (a \cdot b_3) \bmod m$

Алгоритм продолжается для всех $j = 0, 1, 2, \ldots, k-1$. При $n_j = 0$ достигнутое значение a не меняется. На j-том шаге, получим $b_j = b^{2^j} (\mathrm{mod}\, m)$. Если $n_j = 1$, то есть – когда 2^j входит в двоичное представление числа n, поэтому используем b_j как множитель для вычисления нового значения a и не делаем этого при $n_j = 0$. После выполнения шагов по всем j, получим искомое $a = b^n (\mathrm{mod}\, m)$.

Пример 3. Найти $5^{17} \bmod 7$ методом повторного возведения в квадрат.

Получение бинарного («двоичного») представления числа 17 показано в табл. 1.7. Строки таблицы заполняются справа–налево.

Таблица 1.7 – Построение двоичного представления числа 17

Четное число без остатка					16
Делим на 2	1	2	4	8	17
Остаток (бинарное представление числа)	1	0	0	0	1
Позиция (разряд)	4	3	2	1	0

Проверка: $n = 1 \cdot 2^0 + 1 \cdot 2^4 = 1 + 16 = 17$.

Процедура «повторного возведения в квадрат» для определения $5^{17} \bmod 7$ представлена в табл. 1.8.

Таблица 1.8 – «Повторное возведение в квадрат» для $5^{17} \bmod 7$

j	n_j	b_j	a_j
0	1	$b_0 = 5 (\bmod 7) = 5$	$a = b_0 = 5$
1	0	$b_1 = 5^2 (\bmod 7) = 25 \bmod 7 =$ $= (3 \cdot 7 + 4) \bmod 7 = 4$	$a = a = 5$
2	0	$b_2 = 4^2 (\bmod 7) = 16 \bmod 7 =$ $= (2 \cdot 7 + 2) 16 \bmod 7 = 2$	$a = a = 5$
3	0	$b_3 = 2^2 (\bmod 7) = 4 \bmod 7 = 4$	$a = a = 5$
4	1	$b_4 = 4^2 (\bmod 7) = 16 \bmod 7 =$ $= (2 \cdot 7 + 2) \bmod 7 = 2$	$a = (a \cdot b_4) \bmod m = (5 \cdot 2) \bmod 7 =$ $= 10 \bmod 7 = (7 + 3) \bmod 7 = 3$

Ответ: $5^{17} \bmod 7 = 3$. Результат совпадает с ответом примера, представленного в задании 1.2.