4) Мультипликативная группа вычетов по модулю *n*.

Несколько сложнее определяется мультипликативная группа вычетов по модулю *n*. Элементы этой группы образуют множество Z*n , состоящее из элементов Zn , взаимно простых с *n*. Понятие взаимной простоты имеет следующий смысл:
если k – целое число, то НОД(*a*,*n*) = 1 равносильно НОД(*a*+*kn*,*n*) =1.

Теорема 7.

Система $(Z_n^*, \cdot_n)$ *является конечной абелевой группой.*

Доказательство.

Проверим, что любой элемент имеет обратный в смысле групповой операции. (Нейтральным элементом является класс *C1*). Чтобы найти обратный к элементу *a*, рассмотрим тройку (*d*,*x*,*y*), выдаваемую процедурой *Extended-Euclid*(*a*,*n*). Поскольку $a \in Z_n^*$, числа *a* и *n* взаимно просты и *d*= НОД(*a*,*b*) = 1, поэтому $ax + ny = 1$ и $ax \equiv 1 (\mathrm{mod}\, n)$, таким образом, элемент $[x]_n$ является обратным к $[a]_n$ в группе $(Z_n^*, \cdot_n)$.

Единственность обратного можно доказать (как и для любой группы) следующим образом: если x и x' обратны к a, то $(x \oplus a) \oplus x' = e \oplus x' = x'$, а переставив скобки по ассоциативности, получим $x(a \oplus x') = x \oplus e = x$, ч.т.д.

В дальнейшем мы для простоты будем обозначать сложение и умножение по модулю обычными знаками + и · (иногда опуская знак умножения), а аддитивную и мультипликативную группы вычетов по модулю n будем обозначать Zn и Z^*n (не упоминая групповую операцию). Элемент, обратный (относительно операции умножения) к a, мы будем обозначать $a^{-1} \bmod n$. Как обычно, частное a/b в Z^*_n определяется как $ab^{-1} (\bmod n)$. Например, в Z^*_{15} имеем $7^{-1} \equiv 13 \pmod{15}$, поскольку $7 \cdot 13 \equiv 91 \equiv 1 (\bmod 15)$, откуда $4/7 \equiv 4 \cdot 13 \equiv 7 (\bmod 15)$.

5) Количество обратимых элементов в кольце вычетов.

Количество обратимых элементов в кольце вычетов Z_n , т.е. число элементов в Z_n^* , обозначается $\varphi(n)$. Функция φ называется φ - **функцией Эйлера**.

Можно доказать такую формулу для функции Эйлера:

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_s}\right) \qquad (3)$$

где $p_1,\ldots,p_s$ – список всех простых делителей числа n. Можно пояснить эту формулу так: случайное число t взаимно просто с n, если оно не делится на p_1 (вероятность чего есть $(1-1/p_1)$), не делится на p_2 (вероятность $(1-1/p_2)$) и т.д., а события эти независимы.

Например, $\varphi(45) = 45(1-1/3)(1-1/5) = 24$ поскольку простыми делителями числа 45 являются числа 3 и 5. Для простого числа имеем

$$\varphi(p) = p - 1 \qquad (4)$$

т.к. все числа 1,2,…, p -1 взаимно просты с p. Если число n составное, то $\varphi(n) < n - 1$

6) Подгруппы.

Пусть $(S,\oplus)$ является группой, а $S' \subseteq S$ Если $(S',\oplus)$ тоже является группой, то $(S',\oplus)$ называют **подгруппой** группы $(S,\oplus)$. Например, четные числа образуют подгруппу целых чисел (с операцией сложения).

Теорема 8 (Лагранж).

Если $(S',\oplus)$ *является подгруппой конечной группы* $(S,\oplus)$, *то* $|S'|$ *делит* $|S|$.

Доказательство.

Можно найти в учебниках алгебры (группа S разбивается на непересекающиеся классы вида $x \oplus S'$, каждый из которых содержит $|S'|$ элементов).

Подгруппа S' группы S, не совпадающая со всей группой, называется **собственной** подгруппой.

Следствие 8.1.

Если S' является собственной подгруппой конечной группы S, то $|S'| \leq |S/2|$.

Это (очевидное) следствие теоремы Лагранжа используется при анализе вероятностного алгоритма Шиллера – Рабина (проверка простоты).

7) Подгруппа, порожденная элементом группы.

Пусть a – некоторый элемент конечной группы S. Рассмотрим последовательность элементов $a, a \oplus a, a \oplus a \oplus a, \ldots$ По аналогии со степенями (групповая операция соответствует умножению) будем писать

$$a^{(0)} = e, a^{(1)} = a, a^{(2)} = a \oplus a, a^{(3)} = a \oplus a \oplus a$$

и т.д.

Легко видеть, что

$$a^{(i)} \oplus a^{(j)} = a^{(i+j)},$$

в частности $a^{(i)} \oplus a = a^{(i+1)}$. Аналогичное утверждение можно сформулировать и для «отрицательных степеней»,

в частности

$$a^{(i)} \oplus a^{(-1)} = a^{(i-1)}.$$

Если группа S конечна, то последовательность $e, a, a \oplus a, a \oplus a \oplus a, \ldots$ будет периодической (следующий элемент определяется предыдущим, поэтому раз повторившись, элементы будут повторяться по циклу). Таким образом, последовательность имеет вид $e = a^{(0)}, a^{(1)}, \ldots, a^{(t-1)}, a^{(t)} = e, \ldots$ (дальше все повторяется) и содержит t различных элементов, где t – наименьшее положительное число, для которого $a^{(t)} = e$. Это число называется **порядком** элемента a и обозначается $ord(a)$.

Указанные t элементов образуют подгруппу, т. к. групповая операция соответствует сложению «показателей степени». Эта подгруппа называется **порожденной элементом** a и обозначается $\langle a \rangle$ или, если мы хотим явно указать групповую операцию,($\langle a \rangle, \oplus$). Элемент a называют **образующей** подгруппы $\langle a \rangle$; говорят, что он **порождает** эту подгруппу.

Например, элемент a=2 группы Z_6 порождает подгруппу, состоящую из элементов 0,2,4.

Вот несколько подгрупп группы Z_6 , порожденных различными элементами: $\langle 0\rangle = \{0\}, \langle 1\rangle = \{0,1,2,3,4,5\}, \langle 2\rangle = \{0,2,4\}$. Аналогичный пример для мультипликативной группы Z_7^* : здесь $\langle 1\rangle = \{1\}, \langle 2\rangle = \{1,2,4\}, \langle 3\rangle = \{1,2,3,4,5,6\}$

Из сказанного вытекает Теорема 9.

Теорема 9.

Пусть $(S,\oplus)$ *- конечная группа. Если* $a \in S$ *, то число элементов в подгруппе, порождаемой a, совпадает с порядком a (т.е.* $|\langle a \rangle| = ord(a)$ *).*

Следствие 9.1.

Последовательность $a^{(1)}, a^{(2)}, ..$ *имеет период* $t=ord(a)$;
иначе говоря $a^{(i)} = a^{(j)}$, *тогда и только тогда, когда* $i \equiv j (\mathrm{mod}\, t)$.

Периодичность позволяет продолжить последовательность в обе стороны, определив $a^{(i)}$ как $a^{(i \bmod t)}$ при всяком целом i, в том числе и отрицательном.

Следствие 9.2.

В конечной группе $(S,\oplus)$ *единицей* e *для всякого* $a \in S$ *выполняется равенство* $a^{(|S|)} = e$.

Доказательство. *По теореме Лагранжа ord(a) делит* $|S|$, *откуда* $|S| \equiv 0(\mathrm{mod}\, t)$, *где* $t = ord(a)$, *ч.т.д.*

8) Решение линейных диофантовых уравнений.

Нас будут интересовать целочисленные решения уравнения $ax \equiv b(\mathrm{mod}\, n)$ (5) (здесь a, b и n – целые числа; такие уравнения называют «линейными диофантовыми уравнениями»). Ясно, что здесь важен лишь остаток от деления x на n, так что решением (5) естественно называть не целое число, а элемент группы Z_n, (класс чисел, дающих один и тот же остаток при делении на n). Таким образом, можно сформулировать задачу так: есть элементы $a, b \in Z_n$, мы ищем все $x \in Z_n$, для которых $ax \equiv b(\mathrm{mod}\, n)$.

Напомним, что через $\langle a \rangle$ обозначается порождённая элементом a подгруппа (в данном случае подгруппа группы Z_n). По определению $\langle a \rangle = \{a^{(x)} : x > 0\} = \{ax \bmod n : x > 0\}$, поэтому уравнение (5) имеет хотя бы одно решение тогда и только тогда, когда $b \in \langle a \rangle$. Сколько элементов в $\langle |a| \rangle$? По теореме Лагранжа (Т8) это число является делителем n. В Z_n групповая операция – это сложение т.к. Z_n - аддитивная группа, поэтому

$$a^{(x)} = \underbrace{a + a + \ldots + a}_{x \quad раз} = xa \Rightarrow a^{(x)} = xa \ .$$

Теорема 10.

Пусть уравнение $ax \equiv b \pmod{n}$ *разрешимо и является* x_0 *его решением. Тогда уравнение имеет* d =НОД(a,n) *решений в* Z_n *, задаваемых формулой* $x_i = x_0 + i(n/d)$, *где* $i = 0,1,2,\ldots, n-1$.

Доказательство.

Начав с x_0 и двигаясь с шагом n/d, мы сделаем d шагов, прежде чем замкнем круг, т.к. $x_0 + n \equiv x_0 \pmod{n}$. Все пройденные числа будут решениями уравнения $ax \equiv b \pmod{n}$, так как при увеличении x на n/d произведение ax увеличивается на $n(a/d)$, т.е. на кратное n. Таким образом, мы перечислили все d решений.

$ax_0 = b$

$a(x_0 + n/d) = ax_0 + an/d = ax_0 + na/d = ax_0 + kn \equiv ax_0 \pmod{n} = b$

ч.т.д.

Следствие 10.1

Пусть $n > 1$. *Если* НОД(a, n) = 1, *то уравнение* $ax \equiv b \pmod{n}$ *имеет единственное решение* (*в* Z_n).

Случай b=1 особенно важен – при этом мы находим обратный к x элемент по модулю n, т.е. обратный в группе Z_n^* элемент.

Следствие 10.2

Пусть $n > 1$. *Если* НОД$(a, n) = 1$, *то уравнение*

$ax \equiv 1 \pmod{n}$ (6)

имеет единственное решение в Z_n.

При НОД$(a, n) > 1$ *это уравнение решений не имеет.*

Тем самым мы научились вычислять обратный элемент в группе Z_n^* за $O(\log n)$ арифметических операций.

9) Китайская теорема об остатках.

Около 100 г. до Р.Х. китайский математик Сун Цу решил такую задачу: найти число, дающее при делении на 3, 5 и 7 остатки 2, 3 и 2 соответственно (общий вид решения 23+105k при целых k). Поэтому утверждение об эквивалентности системы сравнений по взаимно простым модулям и сравнения по модулю произведения называют «китайской теоремой об остатках».

Пусть некоторое число n представлено в виде произведения попарно взаимно простых чисел $n_1 n_2 \cdot \ldots \cdot n_k$. Китайская теорема об остатках утверждает, что кольцо вычетов Z_n устроено как произведение колец вычетов $Z_{n1} \times Z_{n2} \times \ldots \times Z_{nk}$ (с покомпонентным сложением и умножением). Это соответствие полезно и с алгоритмической точки зрения, так как бывает проще выполнить операции во всех множествах Z_{ni}, чем непосредственно в Z_n.

10) Степени элемента.

Рассмотрим в мультипликативной группе вычетов Z_n^* последовательность степеней некоторого элемента a:

$$a^{(0)}, a^{(1)}, a^{(2)}, a^{(3)}, \ldots \qquad (7)$$

Мы начинаем счет с нуля, полагая $a^{(0)} \bmod n := 1$

i-й член последовательности степеней числа 3 по модулю 7 имеет вид:

i	0	1	2	3	4	5	6	7	8	9	10	11	...
$3^i \bmod 7$	1	3	2	6	4	5	1	3	2	6	4	5	...

а для степеней числа 2 по модулю 7 имеем:

i	0	1	2	3	4	5	6	7	8	9	10	11	...
$2^i \bmod 7$	1	2	4	1	2	4	1	2	4	1	2	4	...

11) Теорема 11 (Эйлер).

Если n>1 – целое число, то

$$a^{\varphi(n)} \equiv 1 \pmod{n} \qquad (8)$$

для всякого $a \in Z_n^*$, *где* $\varphi(n)$ *- фи-функция Эйлера.*

Без доказательства.

При простом n теорема превращается в «малую теорему Ферма».

12) Теорема 12 (малая теорема Ферма).

Если p – простое число, то

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p) \qquad (9)$$

для всякого $a \in Z_p^*$

Доказательство. Поскольку число p – простое,

$= \varphi(p)$, ч.т.д.

Следствие 12.1. Пусть p – простое число

$$\begin{cases} ax \equiv 1 (\mathrm{mod}\ p) \Rightarrow x = a^{-1} (\mathrm{mod}\ p) \\ a^{p-1} = 1 (\mathrm{mod}\ p) \Rightarrow a^{p-2} = a^{-1} (\mathrm{mod}\ p) \end{cases} \Rightarrow x = a^{p-2} (\mathrm{mod}\ p)$$

Следствие 12.2. Пусть p – простое число $a^{p-1} = 1 (\mathrm{mod}\ p) \Rightarrow a^{p} = a (\mathrm{mod}\ p)$, тогда теорема Ферма будет применима и к a=0.

13) Теорема 13 (Усиление теоремы Эйлера).

Пусть $n=pq$, где p и q – разные простые числа. Тогда для любого целого числа a и для любого натурального k справедливо тождество

$$a^{k\varphi(n)+1} \equiv a(\mathrm{mod}\, n).$$

Доказательство.

$$n = pq \Rightarrow \varphi(n) = n(1-\frac{1}{p})(1-\frac{1}{q}) = pq(1-\frac{1}{p})(1-\frac{1}{q}) = (p-1)(q-1)$$

$$a^{k\varphi(n)} = \left(a^{\varphi(n)}\right)^k = 1^k = 1(\mathrm{mod}\, n)$$

$$a^{k\varphi(n)} \cdot a = a(\mathrm{mod}\, n)$$

$$a^{k\varphi(n)+1} = a(\mathrm{mod}\, n)$$

ч.т.д.

14) Вычисление степеней повторным возведением в квадрат.

Возведение в степень по модулю играет важную роль при проверке чисел на простоту, а также в криптосистеме RSA. Как и для обычных чисел, повторное умножение – не самый быстрый способ; лучше воспользоваться алгоритмом **повторного возведения в квадрат**.

Пусть мы хотим вычислить $a^b \bmod n$, где a – вычет по модулю n, а b – целое неотрицательное число, имеющее в двоичной записи вид $(bk,bk\text{-}1,\ldots,b1,b0)$ (число знаков считаем равным $k + 1$; старшие разряды, как обычно, слева). Мы вычисляем $a^c \bmod n$ для некоторого c, которое возрастает и, в конце концов, становится равным b.

При умножении c на 2 число a^c возводится в квадрат, при увеличении c на 1 число a^c умножается на a. На каждом шаге двоичная запись c сдвигается на 1 влево, после чего, если надо(bi=1), последняя цифра двоичной записи меняется с 0 на 1. (Заметим, что переменная c фактически не используется и может быть опущена.)

Оценим время работы процедуры. Если три числа, являющиеся её исходными данными, имеют не более β битов, то число арифметических операций есть $O(\beta)$, а число битовых – $O(\beta^3)$.

Пример ($a = 7$, $b = 560$, $n=561$) показан на рисунке.

$b \equiv 2$ $\quad a^b = a^{2k} = ((a^2)^k \bmod n)^2 \bmod n$

$$a^b = a^{2k+1} = a^{2k} \cdot a = ((a^2)^k \bmod n)^2 \cdot a$$

Возведение в квадрат – это сдвиг на 1 влево степени числа.

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
d	7	49	157	526	160	241	298	166	67	1

Рис. Работа процедуры возведение в степень по модулю *n*
при $a = 7$, $b = 560 = (1000110000)$ и $n = 561$.
Показаны значения переменных после очередного исполнения тела цикла for.
Процедура возвращает ответ 1.