Криптографія:Теорія чисел. Алгебра.

Треба знати:

- ✔ Лишки, властивості
- ✔ Група, поле, кільце
- ✔ Алгоритм Евкліда знаходження НСД(a,b)
- ✔ Мала теорема Ферма
- ✔ Функція Ейлера

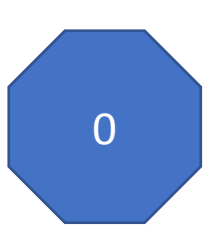
Лишки утворюють кільце – операції додавання/віднімання, множення/***ділення***?.

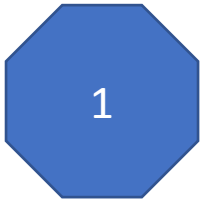
- $a \equiv b \bmod n \leftrightarrow a - b = kn$ $\quad a \bmod n = r, \quad 0 \leq r < n,$

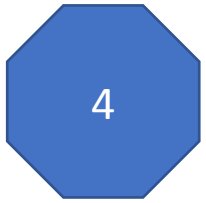
  $a = r + kn$

  17 mod 10 = 7 = -3, 7 mod 5 = 2 = - 3

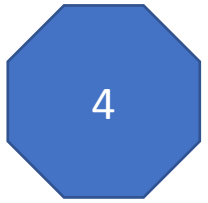
Класи лишків mod 5

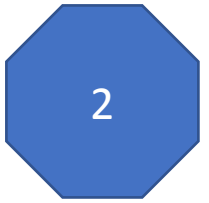


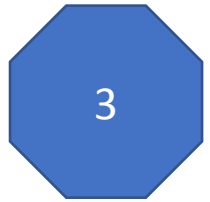




= { 4 + 5k }







Where is an error?

•

- $2 \times 3 = 6 \; mod \; 10$
- $2 \times 8 = 6 \; mod \; 10$

$2 \times 3 = 2 \times 8 \; mod \; 10$

Скорочуємо на 2

$3 = 8 \; mod \; 10$!?

$ax \equiv bx \; mod \; n \Rightarrow (a - b)x \equiv 0 \; mod \; n$

gcd(x,n)=1 a=b

Група

- **Групою зветься деяка множина елементів**

$G =< a, b, c\ldots >$ з бінарною операцією, яку називають “добутком” і яка задовольняє наступним умовам.

1. *Замкнутість відносно групової операції*. Для кожної упорядкованої пари елементів a, b із G існує добуток, який також належить G, $ab = c$ який визначається однозначно.

2. *Асоціативний закон*. Для будь яких елементів a, b, c із G

$$a(bc) = (ab)c.$$

3. *Існування одиниці*. В Gіснує елемент e, який зветься одиницею і для якого виконується умова: для будь якого елемента a виконується рівність $ea = ae = a$.

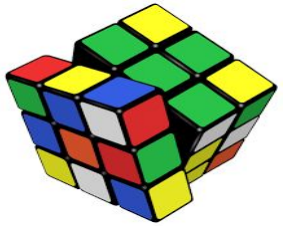
4. *Існування оберненого елемента*. Для будь якого елемента a із Gіснує обернений елемент, позначається a^{-1}, такий, що $a\,a^{-1} = a^{-1}a = e$.

GROUP

- ✓ $ab=c$
- ✓ $a(bc)=(ab)c$
- ✓ $\exists e \ \ \forall a \qquad ae=ea=a$
- ✓ $\forall a \ \ \exists \ a^{-1} \qquad a^{-1}a = e$

Приклади груп

- ✓Група підстановок
- ✓ Група натуральних чисел +/-
- ✓ Група раціональних чисел без 0 $*/\div$
- ✓ Кубик Рубік



- ✓Група точок еліптичної кривої
- ✓Група лишків (без 0) за ***простим модулем*** Z_p^* відносно множення. Довести!

$$Z_p^*$$

$Z_5^* = \{1, 2, 3, 4\}$

$1^{-1} = 1, \quad 2^{-1} = 3,$
$3^{-1} = 2, \quad 4^{-1} = 4$

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Розбиття групи по підгрупі.

- G – група, H – підгрупа

Розбиття групи G по підгрупі H.

S - змінна множина;

1. $S \leftarrow H$;

2. Якщо $S = G$ то *процес закінчено* інакше

2.1 Беремо будь-який елемент $x \in G \setminus S$. Утворюємо множину Hx;

2.2 $S \leftarrow S + H \cdot x$;

3. *перейти на крок* 2.

Теорема Лагранжа

- $$G = H + Hx_1 + Hx_2 + \cdots + Hx_k$$

$$|G| = n, |H| = m,$$

$$n = (k+1)m$$

Порядок підгрупи є дільником порядку групи.

Мала Теорема Ферма

- Група C зветься *циклічною*, якщо існує такий елемент g, що будь який елемент a із C є деяка степінь g, $a = g^i$. Елемент g зветься *утворюючим* елементом групи.

Порядок елемента g

$\min m \quad g^m = e$, = *порядок підгрупи, що породжена g.*

МТФ:p –просте число, $0 < a < p$,

$$a^{p-1} \equiv 1 mod\ p$$

Мала Теорема Ферма. Приклади. Доведення.

$2^{3-1} \equiv 1 \mathrm{mod} 3$, $4^{7-1} \equiv 1 mod 7$,
$6^{11-1} \equiv 1\ mod\ 11$.

Доведення. Нехай $0 < a < p$,

$a1 \equiv r_1$, $a2 \equiv r_2, \ldots,$
$a(p-1) \equiv r_{p-1}$.

$a^{p-1}(p-1)! \equiv r_1\ r_2 \ldots\ r_{p-1}$,

$r_1\ r_2 \ldots\ r_{p-1} = (p-1)!$

Тест Ферма

- МТФ : $\forall a \quad 0 < a < p, a - random, a^{p-1} \equiv 1 \; mod \; p$

If $a^{p-1} \not\equiv 1 \; mod \; p$, p - не просте.

Числа Кармайкла (Carmichael)

n - составне

$\forall a \quad a^{n-1} \equiv 1 \; mod \; n$

приклад ТФ: 9 – просте?

$2^8 \equiv 4 \; mod \; 9$, Ні

Функція Ейлера. Теорема Ейлера.

Функція Ейлера

- $\varphi(n) =$ *кількість* a , $0 < a < n$, *НСД(a,n)* = 1.
- $\varphi(4) =$*2*, $\varphi(5) = 4$, $\varphi(6) =$ *2*
- $\varphi(15) =$ *8.*
- Z_n^* - група всіх *a* взаємно прості з *n*, *операція множення по модулю n.*
- $|Z_n^*| = \varphi(n)$,
- ТЕ:
- *НСД(a,n)* = 1, $a^{\varphi(n)} \equiv 1 \; mod \; n$

Lagrange
Eiler
Ferma

Ейлера

p – просте
$\varphi(p) = p - 1$

Homework

$15^{3^{1000}} \bmod 17 =$

Send to

ava.lectures@gmail.com

$$ax \equiv b \bmod n, x = ?$$

$3x = 2 \bmod 7, \quad x = 3$ *Алгоритм Евкліда НСД(а,в)*

$a = a_1 b + r_1, \quad 0 \le r_1 < b,$

$b = a_2 r_1 + r_2, \quad 0 \le r_2 < r_1,$

$r_1 = a_3 r_2 + r_3$

… … … … …

$r_k = a_{k+2} r_{k+1} + r_{k+2}, \quad 0 \le r_{k+2} < r_{k+1}$

… … … … … .

$r_n = a_{n+2} r_{n+1} + r_{n+2}, \quad 0 \le r_{n+2} < r_{n+1}$

$r_{n+1} = r_{n+3} r_{n+2}$

НСД$(a,в) = d = r_{k+2}$

Теорема 1.10. Нехай d = НСД (a, b). Існують цілі числа λ_1 і λ_2 такі, що $\lambda_1 a + \lambda_2 b = d$.

НСД$(a,в) = d = r_{k+2}$

- $d = r_{k+2} = r_k - q_{k+2} r_{k+1} =$

$r_k - q_{k+2}(r_{k-1} - q_{k+1} r_k) =$

$r_k(1 + q_{k+2} q_{k+1}) - q_{k+2} r_{k-1}.$

НСД$(a,в) = d = r_{k+2}$

Якщо $d = u\, r_i + v\, r_{i+1}$, то тоді

$$d = u\, r_i + v(r_{i-1} - q_{i+1} r_i)$$

$$= v\, r_{i-1} + (u - q_{i+1} v) r_i.$$

$$НСД(a,в) = d = r_{k+2}$$

- **Розширений алгоритм Евкліда.** (Рекурсивний варіант)
- *Extended - Euclid*(a, b)
- ВХІД: a, b
- РЕЗУЛЬТАТ: d = НСД(a, b), x, y такі, що $xa + yb = d$

1. Якщо $b = 0$, то *результат*$\leftarrow (a, 1, 0)$,
- інакше $(d_1, x_1, y_1) \leftarrow$ *Extended-Euclid* $(b,\ a \bmod b)$

1. $(d, x, y) \leftarrow (d_1, y_1, x_1 - y_1)$
2. *Результат* $\leftarrow (d, x, y)$


And this is not
the end of the story…