Тема 6. АРИФМЕТИЧНІ ОСНОВИ КРИПТОГРАФІЇ (ч. 2)

1. Набори лишків

Числа, конгруентні за модулем *m* утворюють *клас лишків* за модулем *m*. Усі числа з одного класу мають одну і ту же остачу *r* від ділення на *m*. Будь-яке число *a* з класу лишків називається лишком за модулем *m*. Відповідний клас позначається через $\bar{a}$. Оскільки відношення $a \equiv b(mod\ m)$ є відношенням еквівалентності, маємо розбиття цілих чисел на класи залишків. Всього є *m* класів лишків за модулем *m*: ($\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}$). Взявши з кожного класу по одному лишку отримаємо повний набір (систему) лишків.

m цілих чисел від 0 до *m-1* – це повний набір лишків.

Властивість 1. Будь-які *m* чисел, попарно непорівнювані за модулем *m* утворюють повний набір лишків.

Властивість 2. Якщо $НСД(a,m)=1$ і *x* пробігає повний набір лишків за модулем *m*, то $ax+b$, де *b* − будь-яке ціле, також пробігає повний набір лишків за модулем *m*.

Згідно властивості $a \equiv b(mod\ m) \Rightarrow НСД(a,m)=НСД(b,m)$ числа одного класу лишків мають з модулем *m* один і той же спільний дільник.

Розглянемо ті класи, для яких цей дільник рівний 1. Взявши з одного такого класу по одному лишку отримаємо *зведений набір лишків* (систему лишків).

Приклад 1.

Зведений набір за модулем *42* буде: 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.

Означення. Набір лишків, взаємно простих з модулем *m*, взятий із повного їх набору, називається *зведеним набором лишків за модулем m.*

Зведений набір лишків за модулем простого числа *m* містить *m-1* елементів і становить *{1,2,…, m-1}*.

Приклад 2.

Модуль *m=10*. *Повний набір лишків* становить $r \in \{1,2,\ldots, 9\}$. Відповідний *зведений набір лишків* містить елементи, взаємно прості з 10, і становить *{1,3, 7, 9}*. Таким чином, із повного набору лишків виключено елемент 0, елементи *2*, *4*, *6* і *8*, які мають з модулем *m=10* спільний дільник 2, а також елемент 5, який є дільником модуля.

Означення. Набором лишків цілого числа *a* за модулем *m* називається сукупність усіх різних остач від ділення чисел $a \cdot q$ на модуль *m*, де *q* послідовно приймає всі значення від *0* до *m-1*.

Приклад 3.

Набір лишків числа *a=5* за модулем *m=6* такий: *{0,5,4,3,2,1}*.

q	0	1	2	3	4	5
$a \cdot q$	0	5	10	15	20	25
$a \cdot q \bmod m$	0	5	4	3	2	1

Приклад 4.

Набір лишків числа *a=10* за модулем *m=6* такий: *{0,4,2}*

Q	0	1	2	3	4	5
$a \cdot q$	0	10	20	30	40	50
$a \cdot q \bmod m$	0	4	2	0	4	2

Отже, довжина набору лишків *(кількість)* цілого числа *a* за модулем *m* максимальна і рівна *m* у разі, якщо числа *a* і *m* взаємно прості.

Означення. Дано просте число *p*. Ціле число *g* називається *первісним коренем* за простим модулем *p*, якщо послідовність яка складається із *p-1* елементів $g^0 \bmod m = 1$, $g^1 \bmod p$, $g^2 \bmod p$, ... , $g^{p-2} \bmod p$ містить всі елементи зведеного набору лишків за модулем *p*, тобто *{1,2,…,p-1}*.

Оскільки зведений набір лишків за модулем простого числа *p* містить *p-1* елементів і така ж кількість елементів у вказаній послідовності, то це означає, що всі елементи цієї послідовності мають бути попарно різні і перший елемент послідовності – завжди рівний одиниці.

При побудові послідовності черговий елемент $g^k \ mod \ p$ доцільно отримувати шляхом домножування вже обчисленого попереднього елемента $g^{k-1} \ mod \ p$ на $g \ mod \ p$.

Приклад 5.

Число $g=3$ є первісним коренем за простим модулем $p=5$.

$3^0 \ mod \ 5$	$1 \cdot 3 \ mod \ 5$	$3 \cdot 3 \ mod \ 5$	$4 \cdot 3 \ mod \ 5$
1	3	4	2

Приклад 6.

Число $g=4$ не є первісним коренем за простим модулем $p=5$.

$4^0 \ mod \ 5$	$1 \cdot 4 \ mod \ 5$	$4 \cdot 4 \ mod \ 5$	$1 \cdot 4 \ mod \ 5$
1	4	1	4

В нижньому рядку бачимо повторення елементів. Це означає що 4 не є первісним коренем за простим модулем $p=5$. [8]

2. Дискретне піднесення до степеня

Означення. Дискретне піднесення до степеня являє собою обчислення цілочисельної функції $x=g^y mod \ p$, де модуль p – натуральне число, y – ціле невід'ємне число, $1 \leq g \leq p$.

Сучасна інтерпретація «індійського піднесення до степеня» відома під назвою *дискретне піднесення до степеня бінарним методом.*

Ефективність бінарного методу визначається різким скороченням кількості виконуваних множень.

Бінарний метод базується на тому, що будь-який показник степеня може бути розкладений за степенями двійки.

Приклад 7.

Розглянемо дискретне піднесення до степеня $7^{50} \ mod \ 11$. Розкладаємо показник степеня за степенями двійки: $50_{10} = 110010_2 = 1 \cdot 2^5+1 \cdot 2^4+0 \cdot 2^3+0 \cdot 2^2+1 \cdot 2^1+0 \cdot 2^0 = 32+16+2$.

Звідси отримуємо: $7^{50} = 7^{32} \cdot 7^{16} \cdot 7^2$

Це показує, що кожен наступний проміжний результат може бути отриманим шляхом множення самого на себе попереднього результату.

Зокрема, щоб отримати 7^{32} потрібно перемножити $7^{16} \cdot 7^{16}$. За рахунок цього як раз і скорочується кількість потрібних операцій множення.

Реальний процес дискретного піднесення до степеня $7^{50} \ mod \ 11$ можна представити у вигляді наступної таблиці:

Показник	Основа	Результат =1 (коли «Показник» mod 2=1)
50	$7^1 \bmod 11 = 7$	
25	$7^2 \bmod 11 = 5$	$1 \cdot 5 \bmod 11 = 5$
12	$7^4 \bmod 11 = 5^2 \bmod 11 = 3$	
6	$7^8 \bmod 11 = 3^2 \bmod 11 = 9$	
3	$7^{16} \bmod 11 = 9^2 \bmod 11 = 4$	$5 \cdot 4 \bmod 11 = 9$
1	$7^{32} \bmod 11 = 4^2 \bmod 11 = 5$	$9 \cdot 5 \bmod 11 = 1$
0		

Зміст таблиці циклічного процесу дискретного піднесення до степеня наступний:

- ✓ стовпчик «Показник» містить результати поступового цілочисельного ділення на 2 даного показника степеня 50; ознакою завершення процесу є нульове значення показника степеня;
- ✓ в стовпчику «Основа» здійснюється множення попереднього результату самого на себе за заданим модулем, починаючи із заданого значення 7;
- ✓ в стовпчику «Результат» здійснюється накопичення потрібного результату шляхом множення попереднього його значення на поточне значення основи в ті моменти, коли показник є непарним; початкове значення результату вважається рівним одиниці.

Особливо добре ефективність бінарного методу видно на великих числах.[8]

3. Функція Ейлера. Теорема Ейлера. Теорема Ферма

Означення. Число класів залишків у зведеному наборі залишків позначають через $\phi(m)$ і ***називають функцією Ейлера.*** Функція Ейлера визначена для всіх натуральних чисел і являє собою кількість взаємно простих з a натуральних чисел, що не перевищують a.

Приклад 8.

$\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(5) = 4, \phi(6) = 2.$

Для *m=10* взаємно простими з ним та меншими його є натуральні числа 1, 3, 7, 9. Отже, $\phi(10) = 4$.

Очевидні наступні властивості:

1. $\phi(p) = p - 1$
2. $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1),\ k \epsilon N$

Приклад 9.

При *p=3, k=4* отримуємо: $\phi(3^4) = 3^{4-1}(3-1) = 27 \cdot 2 = 54$, Дійсно, $\phi(3^4) = \phi(81) = 54$, оскільки для отримання числа елементів зведеного набору залишків по модулю 81 треба від числа елементів повного набору залишків 81 відняти 27 елементів, значення яких кратні трьом.

Лема. *(Мультиплікативність функції).* Якщо *НСД(a,b)=1* => $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

n= $p_1^{к1} * p_2^{к2} *_{...} * p_s^{кs}$, p_i – різні прості числа, $k_i \geq 1$ ($k_i \in N$), тоді $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_s}\right)$.

Приклад 10.

При *a=2, b=5* і *a·b = 2·5 = 10* маємо $\phi(2 \cdot 5) = \phi(2) \cdot \phi(5) = 1 \cdot 4 = 4$

З функцією Ейлера пов'язана його ж знаменита теорема.

Теорема Ейлера. Для взаємно простих цілого *x* та натурального *m* *(НСД(x,m)=1)* справедлива конгруенція $x^{\phi(m)} \equiv 1\ (mod\ m)$ або $x^{\phi(m)}\ mod\ m \equiv 1$.

Приклад 11.

Для *x=3, m=10* маємо $3^4 \equiv 1 (mod\ p)$, тобто $3^4\ mod\ 10 = 81\ mod\ 10 = 1$.

Наслідок з теореми Ейлера (відомий під назвою *мала теорема Ферма).*

Якщо *p* – просте число і *НСД(a, p) = 1*, то $a^{p-1} \equiv (mod\ p)$ або $a^{p-1}\ mod\ p = 1$

Висновок малої теореми Ферма випливає з того, що $\phi(p) = p - 1$.

Наслідок з малої теореми Ферма: $a^p \equiv a(mod\ p)$, тобто $a^p\ mod\ p = a\ mod\ p$, при всіх цілих *a*, в тому числі і кратних *p*.

Приклад 12.

Дано взаємно прості число $a = 10$ і просте число $p = 3$, тобто $НСД(10, 3) = 1$. Тоді у відповідності з малою теоремою Ферма маємо $10^2 \equiv 1(mod\ 3)$, тобто $10^{3-1}\ mod\ 3 = 10^2\ mod\ 3 = 100\ mod\ 3 = 1$. Одночасно, у відповідності із наслідком з малої теореми Ферма маємо $10^3\ mod\ 3 = 1$ і $10\ mod\ 3 = 1$. [8]

4. Діофантове рівняння

Відомо, що взаємно прості числа – це такі натуральні a і m для яких $НСД(a,m)=1$. Для такої пари взаємно простих чисел a і m завжди можна знайти такі цілі U, V що $aU+mV=1$ або $aU-mV=1$, $a>0$, $m>0$. Такі рівняння називаються діофантовими рівнянням першого степеня.

Для вирішення цієї задачі число $\alpha = \frac{a}{m}$ перетворюють у скінченний ланцюговий дріб за допомогою алгоритму Евкліда:

$a=m\cdot q_0 + a_1,$

$m=a_1\cdot q_1+a_2,$

$a_1=a_2\cdot q_2 + a_3,$

$a_2=a_3\cdot q_3 + a_4,$

...

$a_{k-2}=a_{k-1}\cdot q_{k-1} + a_k,$

$a_{k-1}=a_k\cdot q_k + 0.$

Ланцюговий дріб має вигляд: $\frac{a}{m} = [q_0\ ,\ q_1\ ,\ \dots\ ,\ q_k]$, а послідовності $\{P_n\}$ і $\{Q_n\}$ чисельників і знаменників підходящих дробів для ланцюгового дробу визначаються рекурентно:

$P_{-2} = 0;\ P_{-1} = 1;$

$Q_{-2} = 1;\ Q_{-1} = 1;$

При

$n\geq 0 \rightarrow P_n = q_n\cdot P_{n-1} + P_{n-2};$

$n\geq 0 \rightarrow Q_n = q_n\cdot Q_{n-1} + Q_{n-2}.$

Їх обчислення зручно оформляти у вигляді таблиці:

n	-2	-1	0	1	2	...	k-1	k
q_n			q_0	q_1	q_1	...	q_{k-1}	q_k
P_n	0	1	P_0	P_1	P_2	...	P_{k-1}	P_k
Q_n	1	0	Q_0	Q_1	Q_2	...	Q_{k-1}	Q_k

Але відомо, що $P_k \cdot Q_{k-1} - P_{k-1} \cdot Q_k = (-1)^{k-1}$ і $a/m = P_k/Q_k$.

Таким чином, $(-1)^{k-1} P_k \cdot Q_k - P_{k-1} \cdot (-1)^{k-1} Q_k = 1$. Так як $НСД\ (a,m)=1$, то $P_k = a$, $Q_k = m$ іншими словами: пара чисел U, V рівна $U = (-1)^{k-1} Q_{k-1}$ та $V = (-1)^{k-1} P_{k-1}$, є цілочисельним розв'язком діофантового рівняння.

Приклад 13.

Знайти розв'язки рівняння: $aU-mV=1$, при $a=211, m=79$.

n	-2	-1	0	1	2	3
q_n			2	1	2	26
P_n	0	1	2	3	8	211
Q_n	1	0	1	1	3	79

За формулою $a=m \cdot q_0 + a_1$, можна знайти q_0 та a_1

$211=79 \cdot q_0 + a_1$, $q_0 = 211\ div\ 79=2$, отже, $a_1=53$.

При $n = 0$, маємо:

$P_0 = q_0 \cdot P_{-1} + P_{-2} = 2 \cdot 1 + 0 = 2$;

$Q_0 = q_0 \cdot Q_{-1} + Q_{-2} = 2 \cdot 0 + 1 = 1$.

За формулою $m=a_1 \cdot q_1 + a_2$, можна знайти q_1 та a_2

$79 = 53 \cdot q_1 + a_2$, $q_1 = 79\ div\ 53 = 1$, тому $a_2=26$.

При $n = 1$, маємо:

$P_1 = q_1 \cdot P_0 + P_{-1} = 1 \cdot 2 + 1 = 3$;

$Q_1 = q_1 \cdot Q_0 + Q_{-1} = 1 \cdot 0 + 1 = 1$.

Користуючись формулою $a_1=a_2 \cdot q_2 + a_3$, знаходимо q_2 та a_3

$53 = 26 \cdot q_2 + a_2$, $q_2 = 53\ div\ 26 = 2$, тому $a_3=1$.

При $n = 2$, маємо:

$P_2 = q_2 \cdot P_1 + P_0 = 2 \cdot 3 + 2 = 8$;

$Q_2 = q_2 \cdot Q_1 + Q_0 = 2 \cdot 1 + 1 = 3.$

Далі за формулою $a_2 = a_3 \cdot q_3 + a_4$, знаходимо q_3 та a_4

$26 = 1 \cdot q_3 + a_4$, $q_3 = 26 \; div \; 1 = 26$, тому $a_4 = 0$.

При $n = 3$, маємо:

$P_3 = q_3 \cdot P_2 + P_1 = 26 \cdot 8 + 3 = 211$;

$Q_3 = q_3 \cdot Q_2 + Q_1 = 26 \cdot 3 + 1 = 79.$

Отже, при $k = 3$, $P_3 = a = 211$, $Q_3 = m = 79$. Тому знаходимо пару чисел U, V: $U = (-1)^2 \cdot Q_2 = 1 \cdot 3 = 3$ та $V = (-1)^2 \cdot P_2 = 1 \cdot 8 = 8$.

Перевірка, дійсно $3 \cdot 211 - 8 \cdot 79 = 633 - 632 = 1$.