Тема 4. АРИФМЕТИЧНІ ОСНОВИ КРИПТОГРАФІЇ (ч. 1)

1. Алгоритм ділення з остачею та основна властивість конгруентності

Множину всіх натуральних чисел 1, 2, 3, … будемо позначати через N, а через Z – множину цілих чисел 0, ±1, ±2, …

Нехай a, b – елементи Z, $a\neq 0$.

Означення. Кажуть, що $b|a$ (b ділить a), якщо існує таке ціле c, що $a=bc$.

Властивості:

1. $b|a$, $b|c \Rightarrow b|a\pm c$.
2. $b|a \Rightarrow b|ac$, $c \in Z$.
3. $a|b$, $b|a \Leftrightarrow a=\pm b$.

Теорема про ділення з остачею. Нехай a – ціле, b – натуральне. Тоді існують такі однозначно визначені q, $r \in Z$, $0\leq r<b$, що $a=bq+r$.

Іншими словами, будь яке ціле a подається через натуральне b єдиним способом, тобто $a=bq+r$, де, ціле $\boldsymbol{q}$ – називається ***неповною часткою***, $\boldsymbol{b}$ називається ***модулем***, $\boldsymbol{0 \leq r < b}$ – називається ***остачею від ділення або лишком*** числа a за модулем b.

Теорема залишається справедливою для будь-якого цілого $b\neq 0$ при умові, що обмеження $r< b$ замінюється на $r < |b|$.

Операція знаходження остачі r від ділення цілого числа a на натуральне b позначається як $r=a \bmod b$.

Операція знаходження неповної частки q від ділення цілого числа a на натуральне число b позначається як $q=a \operatorname{div} b$.

Неповну частку q та остачу r можна знайти за допомогою алгоритму:

1) Нехай $q=0$.
2) Обчислюємо $r=a-bq$.
3) Якщо умова $0 \leq r < b$ виявилась істинною, то виконання алгоритму закінчено; інакше – виконання алгоритму продовжимо.
4) Якщо $a>0$, то $q:=q+1$, якщо $a<0$ то $q:=q-1$

5) Повернемось до пункту 2.

Приклад 1.

Знайдемо q і r для чисел $a=43$ та $b=11$. Виконаємо звичайне ділення: $a/b = 43/11 \approx 3.9091$. Заокруглимо отриманий дріб до цілого в меншу сторону: отримаємо $q=3$. Тепер за формулою $r = a-bq = 43 – 11\cdot3 = 10$.

Приклад 2.

Знайдемо q і r для чисел $a=44$ та $b=11$. Виконаємо звичайне ділення: $a/b = 44/11 = 4$. Заокруглимо отриманий дріб до цілого в меншу сторону: отримаємо $q=4$. Тепер за формулою $r = a-bq = 44 – 11\cdot4 = 0$.

Приклад 3.

Знайдемо q і r для чисел $a=-64$ та $b=14$. Виконаємо звичайне ділення: $a/b =-64/14 \approx -4.5714$. Заокруглимо отриманий дріб до цілого в меншу сторону: отримаємо $q=-5$. Тепер за формулою $r = a-bq = -64 – 14\cdot(-5) =6$.

При остачі $r = 0$, кажуть, що:

- ✓ a ділиться на b *(націло або без остачі)*,
- ✓ b ділить a,
- ✓ b є дільник числа a,
- ✓ a є кратним числу b.

Означення. Якщо двом цілим a і b відповідає одна й та ж остача r, то вони називаються ***конгруентними за модулем*** c, тобто $a \equiv b \pmod c$. ***(або порівнюваними за модулем*** c*).*

Або по іншому

Означення. Цілі числа a і b називаються ***конгруентними за модулем*** $c \in N$, якщо вони дають одну і ту ж остачу при діленні на c. Пишуть $a \equiv b \pmod c$.

Основна властивість. $a \equiv b \pmod c$ тоді і тільки тоді, коли $(a-b)$ ділиться на c.

Це випливає з теореми про ділення з остачею для a і b:

$a = q_1\cdot c+r$, $b = q_2\cdot c+r$, де q_1, q_2 – цілі, $0 \le r < |c|$. Тоді $(a-b) = (q_1 - q_2)\cdot c$ ділиться на c.

Приклад 4.

Відомо, що $r = 17 \bmod 5 = 2$ ($a = 17, b = 5, a/b = 17/5 = 3.4, q=3$, тоді $r = a-bq = 17-5\cdot4=17-15=2$) і $r = 32 \bmod 5 = 2$. Отже, можна записати, що $32 \equiv 17(\text{mod } 5)$.

Приклад 5.

Відомо, що $r = 45 \bmod 7 = 3$ і $r = 24 \bmod 7 = 3$. Отже, можна записати, що $45 \equiv 24(\text{mod } 7)$.

Основна властивість конгруентності. Із конгруентності $a \equiv c(\text{mod } b)$ випливає рівність $a=c+bq$, де q – ціле. Це означає, що a і c відрізняються між собою на цілу кількість модулів b, тобто $a - c$ ділиться на b.

Приклад 6.

Оскільки $32 = 17 + 5\times3$, або $17=32+ 5\times (-3)$, або $r = (32 -17)\bmod 5 = 0$, або $r = (17 - 32)\bmod 5 = 0$. Відомо, що $32 \equiv 17(\text{mod } 5)$.

Приклад 7.

Оскільки $45 = 24 +7\times3$, або $24 = 45 +7 \times(-3)$, або $r = (45 - 24)\bmod 7 = 0$, або $r = (24 - 45)\bmod 7 = 0$. Відомо, що $45 \equiv 24(\text{mod } 7)$. [8]

2. Властивості конгруентностей по відношенню до арифметичних операцій

Припустимо, що $a_1 \equiv c_1 (\text{mod } b)$ і $a_2 \equiv c_2 (\text{mod } b)$. Тоді справедливі наступні конгруентності:

1) $(a_1 + a_2) \equiv (c_1 + c_2) (\text{mod } b)$ – суми конгруентних чисел конгруентні за тим же модулем;

2) $(a_1 \cdot a_2) \equiv (c_1 \cdot c_2) (\text{mod } b)$ – добутки конгруентних чисел конгруентні за тим же модулем;

3) $a_1^k = c_1^k (\text{mod } b)$ – степені конгруентних чисел конгруентні за тим же модулем.

Наведемо приклади виконання вказаних властивостей для наступних даних: відомо, що $27 \equiv 12 (\text{mod } 5)$ – їм відповідає остача 2; відомо також, що $34 \equiv 14 (\text{mod } 5)$ – їм відповідає остача 4.

Приклад 7.

Тоді $(27 + 34) \equiv (12 + 14)(mod\ 5) \rightarrow 61 \equiv 26(mod\ 5)$ – їм відповідає остача 1. Також і $(27 + 14) \equiv (12 + 34)(mod\ 5) \rightarrow 41 \equiv 46(mod\ 5)$ – їм теж відповідає остача 1.

Приклад 8.

Тоді $(27 \times 34) \equiv (12 \times 14)(mod\ 5) \rightarrow 918 \equiv 168(mod\ 5)$ – їм відповідає остача 3. Також і $(27 \times 14) \equiv (12 \times 34)(mod\ 5) \rightarrow 378 \equiv 408(mod\ 5)$ – їм теж відповідає остача 3.

Приклад 9.

Тоді $27^2 \equiv 12^2\ (mod\ 5) \rightarrow 729 \equiv 144(mod\ 5)$ – їм відповідає остача 4. Також і $27^3 \equiv 12^3\ (mod\ 5) \rightarrow 19683 \equiv 1728(mod\ 5)$ – їм відповідає остача 3.

На наведених властивостях конгруентностей по відношенню до арифметичних операцій базуються правила спрощеного обчислення ***остачі.***

Правило 1. Остачу для суми знайти простіше, якщо попередньо знайти остачі для кожного з доданків, тобто $(a+c)\ mod\ b = ((a\ mod\ b)+(c\ mod\ b))\ mod\ b$.

Приклад 10.

Пряме знаходження остачі для суми $(14+8)\ mod\ 5 = 22\ mod\ 5 = 2$. За правилом: $(14+8)\ mod\ 5 = (14\ mod\ 5 + 8\ mod\ 5)\ mod\ 5 = (4+3)\ mod\ 5 = 7\ mod\ 5 = 2$. Висновок: завдяки правилу проміжні результати не перевищують подвоєного модуля.

Правило 2. Остачу для добутку знайти простіше, якщо попередньо знайти остачі для кожного із співмножників, тобто $(a \cdot c)\ mod\ b = ((a\ mod\ b) \cdot (c\ mod\ b))\ mod\ b$.

Приклад 11.

Пряме знаходження остачі для добутку $(7 \cdot 8)\ mod\ 5 = 56\ mod\ 5 = 1$. За правилом: $(7 \cdot 8)\ mod\ 5 = ((7\ mod\ 5) \cdot (8\ mod\ 5))\ mod\ 5 = (2 \cdot 3)\ mod\ 5 = 6\ mod\ 5 = 1$. Висновок: завдяки правилу проміжні результати не перевищують квадрата модуля.

Правило 3. Остачу для степеня знайти простіше, якщо попередньо знайти остачу для основи, тобто $a^k\ mod\ b = (a\ mod\ b)^k\ mod\ b$.

Приклад 12.

Пряме знаходження остачі для степеня $5^4 \bmod 3 = 625 \bmod 3 = 1$. За правилом: $5^4 \bmod 3 = (5 \bmod 3)^4 \bmod 3 = 2^4 \bmod 3 = 16 \bmod 3 = 1$.

Висновок: завдяки правилу проміжний результат не перевищує k-го степеня модуля. При цьому використовуючи послідовне множення замість піднесення до степеня можна досягнути неперевищення квадрата модуля.

Таким чином, завдяки наведеним правилам виникає можливість обмеження величин проміжних результатів виконуваних операцій, що важливо з точки зору алгоритмізації та програмування. [8]

3. Найбільший спільний дільник (НСД)

Означення. Будь-яке ціле число, на яке діляться a і b називається їх *спільним дільником.*

Означення. Найбільший із спільних дільників натуральних чисел a і b називається *найбільшим спільним дільником* і позначається *НСД(a,b).*

Теорема. Для довільних двох цілих чисел, серед яких принаймні одне ненульове, існує *НСД* і він єдиний.

Лема 1. $НСД(a,0) = a$ для $a \neq 0$.

Лема 2. Для довільних цілих a і $b \neq 0$ із $a = bq + r$, (q – частка, r - остача) $\Rightarrow НСД(a,b) = НСД(b,r)$.

Ці дві леми лежать в основі алгоритму Евкліда знаходження НСД. Виконаємо наступне ділення з остачею:

$a = bq_1 + r_1,\ 0 \le r_1 < b,$

$b = r_1 q_2 + r_2,\ 0 \le r_2 < r_1,$

$r_1 = r_2 q_3 + r_3,\ 0 \le r_3 < r_1,$

…

$r_{n-2} = r_{n-1} q_n + r_n,\ 0 \le r_n < r_{n-1},$

$r_{n-1} = r_n q_{n+1}.$

$НСД(a,b) = НСД(b,r_1) = НСД(r_1,r_2) = \ldots = НСД(r_{n-1},r_n) = НСД(r_n,0) = r_n.$

Остання рівність виконується за лемою (1), а всі попередні за лемою (2). Таким чином, НСД двох чисел дорівнює останній відмінній від нуля остачі в алгоритмі Евкліда.

Алгоритм Евкліда скінченний, бо $|b| > r_1 > r_2 > \ldots > r_k > r_{k+1} > \ldots$ а числа r_i – невід'ємні цілі, тому на якомусь кроці обов'язково отримаємо $r_{n-1} = 0$.

Отже, остання не рівна нулю остача одночасно є найбільшим спільним дільником.

Приклад 13.

Застосуємо алгоритм Евкліда для знаходження НСД (175, 77). 175 = 77·2 + 21, 77 = 21·3 + 14, 21 = 14·1 + 7, 14 = 7·2. Остання додатна остача = 7, тому НСД (175, 77)=7.

Словесний опис алгоритму Евкліда для пошуку НСД заданих чисел a і b.

1. якщо *a>b,* то *a* замінити на *a mod b* інакше *b* замінити на *b mod a;*
2. якщо *a=0* або *b=0,* то обчислити *НСД=a+b* і закінчити алгоритм;
3. повернутись до пункту 1.

Приклад 14.

Таблиця виконання алгоритму при *a=140, b=12.*

a>b	A	B	a=0 або b=0
	140	12	
Так	8		Ні
Ні		4	Ні
Так	0		Так

НСД=0+4=4, тобто НСД(140,12)=4

Поняття найбільшого спільного дільника можна ввести і для декількох чисел $a_1, a_2, \ldots, a_n$. Його позначають НСД($a_1, a_2, \ldots, a_n$).

НСД декількох чисел можна обчислювати послідовно. Наприклад, НСД(a_1, a_2, a_3)=НСД(НСД(a_1, a_2), a_3). [8]