Теория на числата

Модулна аритметика

Определение 1: Две цели числа **a** и **b**, се наричат сходни (или съответни) по модул **n**, ако **n** е делител на **(a-b).**
Означава се по следния начин: **a≡b (mod n).**
Числото **n** се нарича модул на сходство (съответствие).

Определение 2: Целите числа при модул **n**, означава се със **Zn,** е множеството {0, 1, 2, … ,n-1}. Операциите събиране, изваждане и умножение в **Zn** се изпълняват по модул **n.**

Пример: Z_{25} = {0, 1, 2, …, 24}.
В Z_{25} 13+16 = 4, тъй като 13+16 = 29 ≡ 4 (mod 25).

Определение 3: Операцията деление в **Zn** се свежда до умножение, т.е. **b/a (mod n) = b.a^{-1}(mod n).**
Числото **a^{-1}** се нарича обратен множител на **a** при модул **n** и представлява цяло число **x**, такова че **a.x=1 (mod n)**.

Модулна аритметика

В сила са комутативният, асоциативният и дистрибутивният закони.
Също така, редуцирайки всеки междинен резултат по модул **n**, се получава същия резултат, който се получава за цялото изчисление и след това редуцирано по модул **n**.

(a+b) mod n = ((a mod n) + (b mod n)) mod n
(a-b) mod n = ((a mod n) - (b mod n)) mod n
(a.b) mod n = ((a mod n) . (b mod n)) mod n
(a.(b+c)) mod n = (((a.b) mod n) + ((a.c) mod n)) mod n

Пример: В Z_{25} 140+165 = ((140 mod 25)+(165 mod 25)) mod 25 =
= (15+15) mod 25 = 30 mod 25 = **5**
(140+165) mod 25 = 305 mod 25 = **5**

Степенуване

Изчисляване на степен на число

a^x(mod n)

1/ Директно изчисление

Пример: Да се изчисли 7^5=? в Z_{11} .

7^5(mod 11) = 7.49.49 (mod 11) = 7.5.5 (mod 11) = 7.3 (mod 11) = **10**

2/ Метод *"повдигни на квадрат и умножи"*
Използва се двоичното представяне на **x**.

Пример: Да се изчисли 7^5=? в Z_{11} . **x** = $5_{10} = 101_2$

$7^{(1)} = 1^2.7 \pmod{11} = 7 \pmod{11} = 7$

$7^{(10)} = 7^2.1 \pmod{11} = 49 \pmod{11} = 5$

$7^{(101)} = 5^2.7 \pmod{11} = 3.7 \pmod{11} = \mathbf{10}$

Степенуване

Задача1: Изчислете 7^{22}=? в Z_{11}.

$x = 22_{10} = 10110_2$

$7^{(1)} = 1^2.7 \pmod{11} = 7 \pmod{11} = 7$
$7^{(10)} = 7^2.1 \pmod{11} = 49 \pmod{11} = 5$
$7^{(101)} = 5^2.7 \pmod{11} = 3.7 \pmod{11} = 10$
$7^{(1011)} = 10^2.7 \pmod{11} = 1.7 \pmod{11} = 7$
$7^{(10110)} = 7^2.1 \pmod{11} = 49 \pmod{11} = \mathbf{5}$

Отговор: $\mathbf{7^{22} \pmod{11} = 5}$

Задача2: Изчислете $5^{26} \pmod{12} = ?$

Отговор: $\mathbf{5^{26} \pmod{12} = 1}$

Обратен множител

Разширен алгоритъм на Евклид

Пример1: Да се намери 3^{-1} в Z_7 / т.е. $3^{-1} \pmod{7} = ?$ /

7 : 3 = 2 (1) -> 7 = 2.3 + 1 -> 1 = 7 - 2.3
3 : 1 = 3 (0)

$-2 \pmod{7} = -2 + 7 = \mathbf{5}$

$3^{-1} \pmod{7} = 5$ Проверка: $3.5 \pmod{7} = 15 \pmod{7} = 1$

Пример2: Да се намери 2^{-1} в Z_{11} / т.е. $2^{-1} \pmod{11} = ?$ /

11 : 2 = 5 (1) -> 11 = 5.2 + 1 -> 1 = 11 - 5.2
2 : 1 = 2 (0)

$-5 \pmod{11} = -5 + 11 = \mathbf{6}$

$2^{-1} \pmod{11} = 6$ Проверка: $2.6 \pmod{11} = 12 \pmod{11} = 1$

Обратен множител

Разширен алгоритъм на Евклид

Пример3: Да се намери 7^{-1} в Z_{26} / т.е. $7^{-1} \pmod{26} = ?$ /

26 : 7 = 3 (5) -> 26 = 3.7 + 5 -> 5 = 26 - 3.7

7 : 5 = 1 (2) -> 7 = 1.5 + 2 -> 2 = 7 - 1.5

5 : 2 = 2 (1) -> 5 = 2.2 + 1 -> 1 = 5 - 2.2

2 : 1 = 2 (0) -> 2 = 2.1 + 0

$1 = 5 - 2.2 = 5 - 2.(7 - 1.5) = 5 - 2.7 + 2.5 =$

$= 3.5 - 2.7 = 3.(26 - 3.7) - 2.7 = 3.26 - 9.7 - 2.7 =$

$= 3.26 - 11.7$

$-11 \pmod{26} = -11 + 26 = \mathbf{15}$

$7^{-1} \pmod{26} = 15$ Проверка: $7.15 \pmod{26} = 105 \pmod{26} = 1$

Обратен множител

Малка теорема на Ферма

Ако **n** е просто число и $\mathbf{a} \in \mathbf{Z_n}$, то $\mathbf{a^{n-1} \equiv 1 \pmod{n}}$

тогава $\mathbf{a^{(n-1)}.a^{-1} \equiv 1.\ a^{-1} \pmod{n}}$

$\Rightarrow \mathbf{a^{(n-1)-1} \equiv a^{-1} \pmod{n}}$, т.е. $\mathbf{a^{-1} \equiv a^{n-2} \pmod{n}}$

Пример1: Да се намери 3^{-1} в Z_7 / т.е. $3^{-1} \pmod{7} = ?$ /

$3^{-1} = 3^{7-2} \pmod{7} = 3^5 \pmod{7} = 243 \pmod{7} = \mathbf{5}$

Пример2: Да се намери 2^{-1} в Z_{11} / т.е. $2^{-1} \pmod{11} = ?$ /

$2^{-1} = 2^{11-2} \pmod{11} = 2^9 \pmod{11} = 512 \pmod{11} = \mathbf{6}$

Обратен множител
Ойлерова теорема

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

тогава $\mathbf{a^{\varphi(n)}.a^{-1} \equiv 1.\ a^{-1} \pmod n}$

=> $\mathbf{a^{\varphi(n)-1} \equiv a^{-1} \pmod n}$, т.е. $\mathbf{a^{-1} \equiv a^{\varphi(n)-1} \pmod n}$

$\varphi(n)$ = ?

Ако $\mathbf{n = n_1.n_2.n_3...n_k}$, то $\mathbf{\varphi(n) = n.(1-1/n_1).(1-1/n_2)...(1-1/n_k)}$

Когато **n** е просто число **$\varphi(n)$ = n-1**

Пример: n=12, $\varphi(n)$ =?

$\varphi(12) = \varphi(2^2.3) = 12.(1-1/2).(1-1/3) = (12.1.2)/(2.3) =$ **4**

Задача3: n=36, $\varphi(n)$ =?

$\varphi(36) = \varphi(2^2.3^2) = 36.(1-1/2).(1-1/3) = (36.1.2)/(2.3) =$ **12**

Обратен множител
Ойлерова теорема

$\mathbf{a^{-1} \equiv a^{\varphi(n)-1} \pmod n}$

Пример3: Да се намери 7^{-1} в Z_{26} / т.е. $7^{-1} \pmod{26}$ =? /

$\varphi(n)$ = ?

$\varphi(26) = \varphi(2.13) = 26.(1-1/2).(1-1/13) = (26.1.12)/(2.13) =$ **12**

Тогава $7^{-1} = 7^{\varphi(26)-1} \pmod{26} = 7^{12-1} \pmod{26} = 7^{11} \pmod{26} = ?$

Задача4: Да се намери $13^{-1} \pmod{15}$ =?

$\varphi(15) = \varphi(3.5) = 15.(1-1/3).(1-1/5) = (15.2.4)/(3.5) =$ **8**

Тогава $13^{-1} = 13^{\varphi(15)-1} \pmod{15} = 13^{8-1} \pmod{15} = 13^7 \pmod{15} = ?$

Теорема за китайския остатък

Решаване на системата от уравнения, когато **x** е сходно на няколко цели числа:

$x \equiv a_1 \pmod{n_1}$
$x \equiv a_2 \pmod{n_2}$
……
$x \equiv a_k \pmod{n_k}$

Системата има единствено решение $\mathbf{x \in Zn}$ и $\mathbf{n = n_1.n_2 \ldots n_k}$

Алгоритъм на Гаус:

Нека $\mathbf{m_i = n/n_i}$, за i=1,2,… k

Ако $\mathbf{y_i = m_i^{-1} (mod\ n_i)}$, то решението на системата е

$x = \sum_{i=1}^{k} \mathbf{a_i . m_i . y_i\ (mod\ n)}$

Теорема за китайския остатък

Пример: Да се реши системата:

$x \equiv 1 \pmod{3}$
$x \equiv 2 \pmod{4}$
$x \equiv 3 \pmod{5}$

$\mathbf{a_1=1}$, $\mathbf{a_2=2}$, $\mathbf{a_3=3}$

$n_1=3$, $n_2=4$, $n_3=5$ => $n=60$

$\mathbf{m_1}=n/n_1=\mathbf{20}$, $\mathbf{m_2}=n/n_2=\mathbf{15}$, $\mathbf{m_3}=n/n_3=\mathbf{12}$

$\mathbf{y_1}=20^{-1}(\text{mod } 3) = \mathbf{2}$
$\mathbf{y_2}=15^{-1}(\text{mod } 4) = \mathbf{3}$
$\mathbf{y_3}=12^{-1}(\text{mod } 5) = \mathbf{3}$

=> $x = 1.20.2 + 2.15.3 + 3.12.3 \pmod{60} = 238 \pmod{60} = \mathbf{58}$

Изчисляване на обратен множител чрез теоремата за китайския остатък

Пример: Да се намери решението на уравнението 13.x ≡ 1 (mod 70).

70 = 2.5.7
13.x ≡ 1 (mod 2) => $x=13^{-1}(\text{mod } 2)$ => x=1 (mod 2)
13.x ≡ 1 (mod 5) => $x=13^{-1}(\text{mod } 5)$ => x=2 (mod 5)
13.x ≡ 1 (mod 7) => $x=13^{-1}(\text{mod } 7)$ => x=6 (mod 7)

a_1=1, **a_2=2**, **a_3=6**
n_1=2, n_2=5, n_3=7 => n=70
m_1=n/n_1=**35**, **m_2**=n/n_2=**14**, **m_3**=n/n_3=**10**

y_1=35^{-1}(mod 2) = **1**
y_2=14^{-1}(mod 5) = **4**
y_3=10^{-1}(mod 7) = **5**
=> x = 1.35.1 + 2.14.4 + 6.10.5 (mod 70) = 447 (mod 70) = **27**

Задачи

Задача5: Да се реши системата:
x ≡ 2 (mod 3)
x ≡ 3 (mod 4)
x ≡ 4 (mod 5)

Отговор: 59

Задача6: Да се намери **x**, ако 5.x (mod 7) = 2

Отговор: 6

Задача7: Да се намери **x**, ако 9.x (mod 14) = 6

Отговор: 10

Задача8: Ако секретният ключ е (7, 33), да се определи публичния ключ и да се криптира текста **john** с RSA.

Отговор: 10, 9, 17, 5

Задачи

Задача9: Да се криптира текста **phew** с RSA, ако p=11, q=3, e=17.

Отговор: 25, 2, 14, 23

Задача10: Криптограмата (25 60 24) е шифрирана с RSA с ключ [11, 65]. Да се намери открития текст.

Отговор: yes