

Семінар 6. Конгруентність (порівняння за модулем)

19 травня 2023

Означення

Натуральні числа a і b називають конгруентними по модулю n ($a \equiv b \pmod{n}$), якщо

- $n \mid (b - a)$
- b і a дають однаковий (невід'ємний) залишок при діленні на n
- $a = b + kn$

Доведіть еквівалентність цих означень. Доведіть, що конгруентність це відношення еквівалентності на цілих числах

Властивості модуля

$a \equiv b \pmod{n}; c \equiv d \pmod{n}$

- $a + b \equiv c + d \pmod{n}$
- $a - b \equiv c - d \pmod{n}$
- $ab \equiv cd \pmod{n}$
- $a^k \equiv c^k \pmod{n}$

Наслідок: $ab \pmod{n} \equiv (a \pmod{n})(b \pmod{n}) \pmod{n}; a^m \equiv (a \pmod{n})^m \pmod{n}$

Задача 1

Обчисліть

- $7549 + 8131 + 954321 \pmod{10}$
- $7549 * 8131 * 954321 \pmod{10}$
- $7549 + 8131 + 954321 \pmod{17}$
- $7549 * 8131 * 954321 \pmod{17}$

Приклад

$$12^{43} \bmod 37$$

$$43 = 32 + 8 + 2 + 1$$

$$12^{32+8+2+1} = 12^{32} * 12^8 * 12^2 * 12$$

$$12^2 = 144 \bmod 37 = 6$$

$$12^4 = 6^2 \bmod 37 = 36 = -1$$

$$12^8 = (-1)^2 \bmod 37 = 1$$

$$12^{16} = 12^{32} = 1^2 = 1^4 = 1 \bmod 37$$

$$12^{43} = 12 * 6 * 1 * 1 = 72 = 35 = -2 \pmod{37}$$

Задача 2

Обчисліть

- $14^2 \bmod 55, 14^4 \bmod 55, 14^8 \bmod 55, \text{ and } 14^{16} \bmod 55$
- $14^{27} \bmod 55$
- $675^{23} \bmod 31$