Algèbre modulaire

1. Introduction

- $3 + 4 + 5 \equiv 1 \pmod{11}$
- $3 + 4 + 5 \equiv 0 \pmod{12}$
- $6 \cdot 7 \equiv 9 \pmod{11}$
- $6 \cdot 7 \equiv 6 \pmod{12}$
- $6^{10} \equiv 1 \pmod{11}$
- $6^{10} = 6^2 \cdot 6^8 \equiv 0 \pmod{12}$
- $6^{11} = 6^2 \cdot 6^9 \equiv 0 \pmod{12}$
- $3 - 7 \equiv 7 \pmod{11}$
- $2 - 7 - 9 \equiv 10 \pmod{12}$
- $6(-9) \equiv 1 \pmod{11}$
- $7(-3) \equiv 3 \pmod{12}$

2. Petit théorème de Fermat

- $6^{1010} = (6^{10})^{101} = 1 \pmod{11}$
- $n^{p \cdot 10} = (n^{10})^p = 1 \pmod{11}$
- " " "
- " " "
- " " "
- " " "
- $6^{1011} = 6^{1011} \cdot 6 = 6 \pmod{11}$
- $6^{3024} = 6^{1010 \cdot 3 + 4} = 6^{1010} \cdot 6^2 \cdot 6^2 \equiv 9 \pmod{11}$

3. Modulo inverse

- $3^{-1} = 4 \pmod{11} \quad = \emptyset \pmod{12} \quad gcd(3, 12) \neq 1$
- $5^{-1} = 9 \pmod{11} \quad = 5 \pmod{12}$
- $7^{-1} = 8 \pmod{11} \quad = 7 \pmod{12}$
- $2^{-1} = 6 \pmod{11} \quad = \emptyset \pmod{12} \quad gcd(2, 12) \neq 1$
- $6^{-1} = 2 \pmod{11} \quad = \emptyset \pmod{12} \quad gcd(6, 12) \neq 1$
- $10^{-1} = 10 \pmod{11} \quad = \emptyset \pmod{12} \quad gcd(10, 12) \neq 1$

4. Divisions discrètes

- $4 \cdot 3^{-1} = 4 \cdot 4 = 5 \pmod{11}$
- $2 \cdot 3^{-1} = 2 \cdot 4 = 8 \pmod{11}$
- $10 \cdot 7^{-1} = 10 \cdot 8 = 3 \pmod{11}$
- $7 \cdot 2^{-1} = 7 \cdot 6 = 9 \pmod{11}$
- $3 \cdot 9^{-1} = 3 \cdot 5 = 4 \pmod{11}$
- $7 \cdot 10^{-1} = 7 \cdot 10 = 4 \pmod{11}$
- $7 \cdot 8^{-1} = 7 \cdot 7 = 5 \pmod{11}$
- $4 \cdot 3^{-1} = \emptyset \pmod{12}$
- $2 \cdot 5^{-1} = 2 \cdot 5 = 10 \pmod{12}$
- $8 \cdot 7^{-1} = 8 \cdot 7 = 8 \pmod{12}$
- $9 \cdot 2^{-1} = \emptyset \pmod{12}$
- $9 \cdot 10^{-1} = \emptyset \pmod{12}$
- $7 \cdot 8^{-1} = \emptyset \pmod{12}$
- $5 \cdot 9^{-1} = \emptyset \pmod{12}$

5. Racines carrées discrètes

- $\sqrt{5} = 4; 7 \pmod{11}$
- $\sqrt{3} = 5; 6 \pmod{11}$
- $\sqrt{9} = 8; 3 \pmod{11}$
- $\sqrt{4} = 9; 2 \pmod{11}$
- $\sqrt{1} = 10; 1 \pmod{11}$
- $\sqrt{6} = \emptyset \pmod{11}$

6. Logarithmes discrets

- $log_2(3) = 8 \pmod{11} \quad 2^8 = 3 \pmod{11}$
- $log_2(4) = 2 \pmod{11} \quad 2^2 = 4 \pmod{11}$
- $log_2(5) = 4 \pmod{11} \quad 2^4 = 5 \pmod{11}$
- $log_2(6) = 9 \pmod{11} \quad 2^9 = 6 \pmod{11}$
- $log_2(7) = 7 \pmod{11} \quad 2^7 = 7 \pmod{11}$
- $log_2(9) = 6 \pmod{11} \quad 2^6 = 9 \pmod{11}$
- $log_2(10) = 5 \pmod{11} \quad 2^5 = 10 \pmod{11}$
- $log_5(3) = 2 \pmod{11} \quad 5^2 = 3 \pmod{11}$
- $log_5(4) = 3 \pmod{11} \quad 5^3 = 4 \pmod{11}$
- $log_5(9) = 4 \pmod{11} \quad 5^4 = 9 \pmod{11}$
- $log_5(5) = 6 \pmod{11} \quad 5^6 = 5 \pmod{11}$
- $log_2(8) = 3 \pmod{11} \quad 5^3 = 8 \pmod{11}$

7. Exercise 7

Write a program (choose your language) that computes:

$z^{b^k} \; mod \; n$

Python

```python
lambda z, b, k, n: pow(z, b**k, n)
```