

## Tema 3

① Demonstrați că  $m = \prod_{i=1}^K p_i^{\alpha_i}$  și  $a^{p_i} \equiv a \pmod{m}$ ,  $\forall p_i$  atărtă  $a^m \equiv a \pmod{m}$ .

Pentru a demonstra că  $a^m \equiv a \pmod{m}$ , folosind proprietățile exponentelor și a convergențelor, vom cau că:

$$a^{p_i} \equiv a \pmod{p_i}, \forall p_i - prim$$

$$a^{p_i} \equiv a \pmod{p_i^{k_i}}, k_i > 0 \text{ (pozitiv)}$$

Vom demonstra  $a^m \equiv a \pmod{m}$

$$m = \prod_{i=1}^K p_i^{\alpha_i}$$

Fie  $m_i = \frac{m}{p_i^{\alpha_i}}$ ,  $m_i$  inversul modular al lui  $\frac{m}{p_i^{\alpha_i}} \pmod{p_i^{\alpha_i}}$ .

$$\Rightarrow m_i \cdot \frac{m}{p_i^{\alpha_i}} \equiv 1 \pmod{p_i^{\alpha_i}}$$

$$a^m = a \prod_{i=1}^K p_i^{\alpha_i} = \prod_{i=1}^K a^{p_i^{\alpha_i}} \equiv a \sum_{i=1}^K p_i^{\alpha_i} \pmod{p_i^{\alpha_i}}$$

$$\equiv a^m \pmod{p_i^{\alpha_i}}$$

Deoarece această congruență este adeuțată, pt fiecare  $p_i$  T. Chiaruză a resturilor  $a^m \equiv a \pmod{m}$

② Făcând exercițiul anterior, arătați că numerele 1729, 10585 și 75361 sunt numere Carmichael

! Un număr Carmichael este un nr compus pozitiv care are proprietatea că pt.  $\forall a \in \{1, m\}$  este prim cu  $m$  și verifică  $a^m \equiv a \pmod{m}$

Pentru a verifica dacă numerele sunt Car., vom verifica dacă  $\forall a$  prim cu  $m$  verifică  $a^m \equiv a \pmod{m}$

$$\text{i. } m = 1729 = 7 \cdot 13 \cdot 19$$

$$\text{verif: } a^{1729} \equiv a \pmod{1729}$$

7, 13, 19 - prime distincte  $\Rightarrow$  putem să ne folosim ex 1.

$$\text{ii. } m = 10585 = 5 \cdot 13 \cdot 17 \cdot 29$$

$$\text{verif: } a^{10585} \equiv a \pmod{10585}$$

5, 13, 17, 29 - prime distincte  $\Rightarrow$  fals ex 1.

$$\text{iii. } m = 75361 = 11 \cdot 13 \cdot 17 \cdot 31$$

$$a^{75361} \equiv a \pmod{75361}$$

11, 13, 17, 31 - prime distincte  $\Rightarrow$  fals de ex. 1.

$\Rightarrow$  Cele trei numere sunt Carmichael.

3)  $2^m - 1$  prim  $\Rightarrow m$  prim

P.p.  $2^m - 1$  - prim, dar  $m$  nu este prim

Dacă  $m$  nu este prim  $\Rightarrow \exists d_1, d_2 \in \mathbb{Z}_+, d_1 \neq d_2 \neq 1, m$

$$\text{a.i } m = d_1 \cdot d_2$$

$$2^m - 1 = 2^{d_1 \cdot d_2} - 1$$

$$2^{d_1 \cdot d_2} - 1 = (2^{d_1})^{d_2} - 1, d_2 = (2^{d_1})^{d_2} - 1$$

$$(2^{d_1})^{d_2} - 1 = (2^{d_1} - 1)((2^{d_1})^{d_2-1} + (2^{d_1})^{d_2-2} + \dots + 2^{d_1} + 1)$$

$2^{d_1} - 1$  - este un factor al lui  $2^m - 1$ , deoarece  $d_1$  - factor al lui  $m$ , dar al doilea factor este întreg  $> 1$ .

$\Rightarrow$  Preocuparea primă contradicție este falsă  
 $\Rightarrow m$  prim

4. Legea reciprocității statice al lui Gauss afirma că  $\nexists p, q$  prime impare distințe, simbolul lui Legendre  $\left(\frac{p}{q}\right)$  este dat de resturile pătratice  $(\text{mod } p)$  și  $(\text{mod } q)$

Enunțăm astfel:

$\forall p$ -prim impar,  $\forall a \in \mathbb{Z}$  avem:

$\left(\frac{a}{p}\right)\left(\frac{p}{a}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{a-1}{2}}$ , unde  $\left(\frac{a}{p}\right)$  - simbolul lui Legendre  
 = este rezidul pătratic al lui  $a$  (mod  $p$ ), iar  $\left(\frac{p}{a}\right)$  rezidul  
 pătratic al lui  $p$  (mod  $a$ )

Demonstratie

Caz I: Dacă  $p \neq 2$  eamnante modula 4 cu 3  $\Rightarrow$  simbolul  $\left(\frac{p}{2}\right) = -1$   
 deoarece  $p, 2$  prime impară eamnante modula 4 cu 3

Obs:  $-1$  nu este rezidu pătratic modula.

Caz II: Dacă  $p \neq 2$  este congruentă cu 1,  $\Rightarrow$  rezultatul  
 depinde de rezidurile pătratice  $\left(\frac{P}{2}\right)$  și  $\left(\frac{2}{p}\right)$ .

T. reciprocă a lui Euler:  $\forall a \in \mathbb{Z}, a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) (\text{mod } p)$

Caz III. Dacă  $p, 2$  eamnă modula 4 cu 1, atunci simbolul lui  
 Legendre  $\left(\frac{p}{2}\right) = \left(\frac{2}{p}\right)$  (fiecare dintre ele este rezidul  
 pătratic al celuilalt)

5. Funcție ptu calcularea simb. lui Jacobi

#include <iostream>

```
int jacobi (int a, int m) {
```

```
if (m <= 0 or m % 2 == 0) {
```

    throw std::invalid\_argument ("m trebuie

    să fie un număr întreg impar");

```

int symbol = 1;
while (a != 0) {
    while (a % 2 == 0) {
        a /= 2;
        if (m % 8 == 3 || m % 8 == -5) {
            symbol *= -1;
        }
    }
    if (a < 0) {
        a = -a;
        if (m % 4 == 3) {
            symbol *= -1;
        }
    }
    int temp = a;
    a = m;
    m = temp;
    if (a % 4 == m % 4 and a % 4 == 3) {
        symbol *= -1;
    }
    if (m == 1) return symbol;
}
return 0;

```

↓ Jacobi.cpp

6. pe github → Solavay Strassen.cpp

### 8) Simbolul lui Kronecker

Este o generalizare a simbolului lui Legendre și a lui Jacobi:  $a \in \mathbb{Z}$ ,  $m \in \mathbb{Z}_+$

Dacă  $m = m_1 m_2 \dots m_k$ , simb.  $K\left(\frac{a}{m}\right)$  este definit astfel:

- Dacă  $m$  împarte  $a$ , simbolul este 0
- Dacă  $m$  NU împarte  $a$ , simbolul este produsul simbolurilor lui L. corespunzătoare factorilor primi divizori ai lui  $m$ , ridicate la puterile lor corespunzătoare din factorizarea lui  $a$ .

Simbolul lui  $K$  are diverse aplicații în teoria numerelor și alte domenii ale matematicii, inclusiv criptografie și în teoria funcțiilor speciale.

### 9) Determinați utilizând algoritmul lui Fermat dacă numarul 86813 este prim sau compus.

Veifică dacă un nr.  $m$  este prim sau compus.

Pasul 1: alegem un nr. aleator  $a$  între 2 și  $m-1$

Pasul 2: Verifică dacă  $a^{m-1} \equiv 1 \pmod{m}$ , calculăm  $a^{m-1}$

Pasul 3: Dacă ptu toate valurile alese ptu.a

re verifică această

$$a=2 \Rightarrow 2^{86812} \pmod{86813}$$

Dacă = 1 avem probabil mare că nu să fie prim

$$2^{86812} \pmod{86813} = 33280 \pmod{86813}$$

!  $a^{p-1} \equiv 1 \pmod{p}$

$$p = 86813$$

$$\text{Verif: } 2^{86812} \equiv 1 \pmod{86813}$$

dar  $33280 \neq 1 \Rightarrow$  compus