Tema 3

Valechi Emilia, M532

2 Demonstrați că

dacă $n = \prod_{i=1}^{k} p_i^{\alpha_i}$,

$\forall p_i,\ a^{p_i} \equiv a \pmod{p_i}$ $\Rightarrow$ $a^n \equiv a \pmod{n}$

Mica th. a lui Fermat:

$\forall a \in \mathbb{Z}$, p - prim, (a nedivizibil cu p)

$a^{p-1} \equiv 1 \pmod{p} \Rightarrow \boxed{a^p \equiv a \pmod{p}}$

Fie $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, a.î.

$a^{p_i} \equiv a \pmod{p_i} \Rightarrow a^n \equiv a \pmod{p_i^{\alpha_i}}$

Lema chineză a resturilor:

Fie $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, cu $\alpha_i \in \mathbb{Z}_+^*$ și p_i = prim, $p_i \neq p_j$, $i \neq j$

a.î. $\begin{cases} x \equiv a \pmod{p_1^{\alpha_1}} \\ x \equiv a \pmod{p_2^{\alpha_2}} \\ \vdots \\ x \equiv a \pmod{p_k^{\alpha_k}} \end{cases}$ are sol. unică.

~~P.p. ... a.î. ... $a \equiv a \pmod{p_i^{\alpha_i}}$~~

Dem. că $a^{p_i^{\alpha_i}} \equiv a \pmod{p_i}$

$P(k)$: $a^{p_i^k} \equiv a \pmod{p_i}$ (A), $\forall k \geq 1$

Dem că $P(k+1)$: $a^{p_i^{k+1}} \equiv a \pmod{p_i}$ (A)

$a^{p_i^{k+1}} = a^{p_i \cdot p_i^k} = \left(a^{p_i^k}\right)^{p_i}$

(ip.) $\Rightarrow p_i^k \equiv a \pmod{p_i} \Rightarrow (a^{p_i})^{p_i} \equiv a^{p_i} \pmod{p_i}$ } $\Rightarrow$

$a^{p_i} \equiv a \pmod{p_i}$ ~~////~~

$\Rightarrow a^{p_i^{k+1}} \equiv a \pmod{p_i}$ ✓

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

Aplicăm Lema chineză a rest:

$a^{p_i^{\alpha_i}} \equiv a \pmod{p_i^{\alpha_i}}, \forall i$

$\Rightarrow \boxed{a^n \equiv a \pmod{n}}$ ■

---

2) Folosind exercițiul anterior, arătați că următoarele numere sunt Carmichael:

// pp. n = prim, at. $\forall b \in \{1, 2, .., n-1\}$

$b^n \equiv b \pmod{n} \Rightarrow n$ = nr. Carmichael

⊙ pt. 1729 —//—

$1729 \div 7 = 247$

$247 : 13 = 19$

$\Rightarrow 1729 = 7 \cdot 13 \cdot 19$

$1729 - 1 = 1728$

$7 - 1 = 6 \Rightarrow 1728 \mid 6$

$13 - 1 = 12 \Rightarrow 1728 \mid 12$

$19 - 1 = 18 \Rightarrow 1728 \mid 18$

} $\Rightarrow$ 1729 este nr. Carmichael

(•) $10585 : 5 = 2117$

$2117 : 29 = 73$

$10585 = 5 \cdot 29 \cdot 73$

$10585 - 1 = 10584$

$5 - 1 = 4 \mid 10584$

$29 - 1 = 28 \mid 10584$

$73 - 1 = 72 \mid 10584$

$\Rightarrow$ 10585 este Carmichael

(•) $75361 : 11 = 6851$

$6851 : 13 = 527$

$527 : 17 = 31$

$\Rightarrow 75361 = 11 \cdot 13 \cdot 17 \cdot 31$

$75361 - 1 = 75360$

$11 - 1 = 10 \mid 75360$

$13 - 1 = 12 \mid 75360$

$17 - 1 = 16 \mid 75360$

$31 - 1 = 30 \mid 75360$

$\Rightarrow$ 75361 este Carmichael

---

(3) Arătați că dacă $2^n - 1$ este prim, atunci n este prim.

R.A.

Vom demonstra prin reducere la absurd

$2^n - 1 = \text{prim} \rightarrow n = \text{compus}$

$n = \text{compus} \Rightarrow n = a \cdot b, \quad a, b \in (1, n)$

$\Rightarrow 2^n - 1 = 2^{ab} - 1$

$$x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \dots + x + 1)$$

$x = 2^a, \quad m = b$

$$2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)\left((2^a)^{b-1} + (2^a)^{b-2} + \dots + 2^a + 1\right)$$

$a \geq 2 \Rightarrow 2^a - 1 > 1$

$(2^a)^{b-1} + \dots + 2^a + 1 > 1$ pt. $b \geq 2$

$\Rightarrow$ $2^n - 1$ este produs de 2 nr. > 1 $\Rightarrow$ nu este prim

Dar în ipoteză, $2^n - 1$ este prim

$\Rightarrow$ n nu poate fi compus

$\Rightarrow$ n = prim.

---

9 (14) Aplicați alg. lui Fermat pt. a determina primalitatea nr. 36791.

//

Fie n = prim. At. $\forall b \in \{1, \dots, n-1\}$

$b^{n-1} \equiv 1 \pmod n$ $(\star)$

Dacă găsim un b pt. care $(\star)$ nu este satisf.

et $b \neq$ prim.

calculele sunt pus anvoiase, de aceea am făcut implementarea în FermatPrimality.cs.