DOSOFTEI GEORGIANA-PARASCHEVA

TEMA 3

1. Demonstrați că dacă $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ și $a^{p_i} \equiv a \pmod{p_i}$, $\forall p_i$, atunci $a^n \equiv a \pmod{n}$.

Fie $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ unde p_i sunt numere prime distincte și α_i sunt puteri naturale. Dacă $a^{p_i} \equiv a \pmod{p_i}$, $\forall p_i$. Trebuie să demonstrăm că $a^n \equiv a \pmod{n}$.

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

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

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

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

Teorema Chineză a Resturilor

$\Bigg\} \Rightarrow \exists!\, x$ a.î. $x \equiv a^n \pmod{n}$ $\Rightarrow$

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

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

$b^{n-1} \equiv 1 \pmod{n}$ $\forall b$ a.î. $(b,n)=1$

a) 1729

$1729 = 7 \cdot 13 \cdot 19$

$\rightarrow$ n este un produs de numere prime distincte

$\rightarrow$ $p_i - 1$ trebuie să dividă $n-1$ pentru fiecare p_i

$\rightarrow$ Factori primi: 7, 13, 19

$\rightarrow$ $n-1$: $1729 - 1 = 1728$

$7 - 1 = 6 \mid 1728$

$13 - 1 = 12 \mid 1728$

$19 - 1 = 18 \mid 1728$

b) 10585

$10585 = 5 \cdot 29 \cdot 73$

$\Rightarrow$ Factori primi: 5, 29, 73

$\Rightarrow n-1: 10585-1 = 10584$

$5-1 = 4 / 10584$

$29-1 = 28 / 10584$

$73-1 = 72 / 10584$

c) 75361

$75361 = 11 \cdot 13 \cdot 17 \cdot 19$

$\Rightarrow$ Factori primi: 11, 13, 17, 19

$\Rightarrow n-1: 75361-1 = 75360$

$11-1 = 10 / 75360$

$13-1 = 12 / 75360$

$17-1 = 16 / 75360$

$19-1 = 18 / 75360$

$\Rightarrow$ 1729 și 10585 sunt numere Carmichael.

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

Pp. că n nu este prim $\Rightarrow$ n are divizori diferiți de n și 1.

Fie $n = a \cdot b$, $a, b \in \mathbb{Z}$

$a, b > 1$

$a, b < n$

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

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

$a, b > 1$ $\Big| \Rightarrow$

$\Rightarrow 2^a-1 > 1$

$(2^{a(b-1)} + \dots + 2^a + 1) > 1$ $\Big| \Rightarrow 2^{ab}-1$ produs de nr. $\Rightarrow$ nu este prim

$\downarrow$

$\Rightarrow$ n este prim.