Nichita Bogdan Valentin

M531

TEMA 3

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

Fie $n = p_i^{\alpha_1} \cdot p_i^{\alpha_2} \cdot \dots \cdot p_i^{\alpha_k}$

$a^{p_i} \equiv a(mod\ p_i) => p_i|(a^{p_i} - a) => Pentru\ p_i^{\alpha_i}\ avem\ a^{{p_i}^m} \equiv a(mod\ p_i)$

Prin recurenta ajungem la $a^{{p_i}^{\alpha_i}} \equiv a\left(mod\ p_i^{\alpha_i}\right)$

Deci avem ca $a^{{p_i}^{\alpha_i}} \equiv a\left(mod\ p_i^{\alpha_i}\right)$ si cum ${p_i}^{\alpha_i}$ sunt coprime intre ele, din Th chineza a resturilor $=> a^n \equiv a\ (mod\ n)$

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

1729 = 13 · 7 · 19

6|1728 (A)

12|1728 (A)

18|1728 (A)

Deci 1729 este numar Carmichael

10585 = 5 · 29 · 73

4|10584 (A)

28|10584 (A)

72|10584 (A)

Deci 10585 este numar Carmichael

75361=11·13·17·19

10|75360 (A)

12|75360 (A)

16|75360 (A)

18|75360 (A)

Deci 75361 este numar Carmichael

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

Pp ca n = ab, a,b > 1

$$2^n - 1 = 2^{ab} - 1 = (2^a - 1) \cdot \sum_{k=0}^{b-1} 2^{ka}$$

Deci daca n nu este prim atunci si $2^n - 1$ nu este prim.

Pentru ca $2^n - 1$ sa fie prim, n nu trebuies sa fie compus, deci trebuie sa fie prim

4. Demonstrați legea reciprocității pătratice

Legea reciprocității pătratice: $\left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \left(\frac{n}{m}\right), m, n$ impare

8. Descrieți simbolul lui Kronecker

Simbolul lui Kronecker, este o generalizare a simbolului lui Legendre și a simbolului lui Jacobi, permițându-i să fie definit pentru orice număr întreg, nu doar pentru numere impare și prime.

9. Algoritmi de primalitate

23.Folosiți algoritmul Miller-Rabin pentru a verifica dacă numărul 881 este prim sau compus. (cel mult 3 martori).

$881 - 1 = 880 = 2^4 \cdot 55$

$2^{55} \pmod{881} \equiv 2048^5 \pmod{881} \equiv 286^5 \pmod{881} \equiv 286 \cdot 81796^2 \pmod{881} \equiv$

$286 \cdot 744^2 \pmod{881} \equiv 286 \cdot (-137)^2 \pmod{881} \equiv 286 \cdot 18769 \pmod{881} \equiv$

$286 \cdot 268 \pmod{881} \equiv 76648 \pmod{881} \equiv 1 \pmod{881}$

$2^{110} \pmod{881} \equiv 1^2 \pmod{881} \equiv 1 \pmod{881}$

$3^{55} \pmod{881} \equiv 3 \cdot 9^{27} \pmod{881} \equiv 27 \cdot 81^{13} \pmod{881} \equiv 2187 \cdot 6561^6 \pmod{881} \equiv$

$425 \cdot 394^6 \pmod{881} \equiv 425 \cdot 155236^3 \pmod{881} \equiv 425 \cdot 180^3 \pmod{881} \equiv$

$76500 \cdot 32400 \pmod{881} \equiv 734 \cdot 684 \pmod{881} \equiv (-147) \cdot (-197) \pmod{881} \equiv$

$767 \pmod{881}$

$3^{110} \pmod{881} \equiv 767^2 \pmod{881} \equiv 662 \pmod{881}$

$5^{55} \pmod{881} \equiv 5 \cdot 25^{27} \pmod{881} \equiv 125 \cdot 625^{13} \pmod{881} \equiv 78125 \cdot 625^{12} \pmod{881} \equiv$

$597 \cdot (-256)^{12} \pmod{881} \equiv 597 \cdot 65536^6 \pmod{881} \equiv 597 \cdot 342^6 \pmod{881} \equiv$

$597 \cdot 116964^3 \pmod{881} \equiv 597 \cdot 672^3 \pmod{881} \equiv (-284) \cdot (-209)^3 \pmod{881} \equiv$

$59356 \cdot 43681 \pmod{881} \equiv 329 \cdot 512 \pmod{881} \equiv 177 \pmod{881}$

$5^{55} \pmod{881} \equiv 177^2 \pmod{881} \equiv 31329 \pmod{881} \equiv 494 \pmod{881}$

10. Algoritmi de factorizare

Folosind QS sau Fermat, factorizați următoarele numere:

23. 10191

$\sqrt{10191} \approx 100.9$

t = 101 => 101^2 – 10191 = 10201 – 10191 = 10

t = 102 => 102^2 – 10191 = 10404 – 10191 = 213

t = 103 => 103^2 −10191=10609−10191= 418

t = 104 => 104^2 −10191=10816−10191= 625 = 25^2

10191 = 104^2 – 25^2 = (104−25)(104+25)

11. Realizați o comparație între algoritmii de primalitate studiați la seminar.

i) Împărțiri successive: Algoritm determinist, necondiționat, exponential
ii) Algoritmul lui Fermat: Algoritm probabilist, necondiționat, polinomial
iii) Algoritmul Miller – Rabin: Algoritm probabilist, necondiționat, polinomial
iv) Algoritmul Solovay – Strassen: Algoritm probabilist, conditionat, polynomial

12. Studiați algoritmul de factorizare rho al lui Pollard și aplicați-l pentru 10909.

f(x) = (x^2 + 1) (mod 10909)

Fie x_0 =2

x_1 = f(x_0) =2^2 + 1= 5 (mod 10909) (|2-5|,10909)= 1

x_2 = f(x_1) =5^2 + 1= 26 (mod 10909) (|5-26|,10909)= 1

x_3 = f(x_2) =26^2 + 1= 677 (mod 10909) (|26-677|,10909)= 1

x_4 = f(x_3) =677^2 + 1= 152 (mod 10909) (|677-152|,10909)= 1

x_5 = f(x_4) =152^2 + 1= 1287 (mod 10909) (|152-1287|,10909)= 1

x_6 = f(x_5) =1287^2 + 1= 9111 (mod 10909)

x_7 = f(x_6) =9111^2 + 1= 3741 (mod 10909)

$x_8 = f(x_7) = 3741^2 + 1 = 9744 \pmod{10909}$

$x_9 = f(x_8) = 9744^2 + 1 = 4510 \pmod{10909}$

$x_{10} = f(x_9) = 4510^2 + 1 = 5725 \pmod{10909}$

$x_{11} = f(x_{10}) = 5725^2 + 1 = 4990 \pmod{10909}$

$x_{12} = f(x_{11}) = 4990^2 + 1 = 5763 \pmod{10909}$

$x_{13} = f(x_{12}) = 5763^2 + 1 = 5174 \pmod{10909}$

$x_{14} = f(x_{13}) = 5174^2 + 1 = 10500 \pmod{10909}$

$x_{15} = f(x_{14}) = 10500^2 + 1 = 3647 \pmod{10909}$

$x_{16} = f(x_{15}) = 3647^2 + 1 = 2539 \pmod{10909}$

$x_{17} = f(x_{16}) = 2539^2 + 1 = 10212 \pmod{10909}$

$x_{18} = f(x_{17}) = 10212^2 + 1 = 5814 \pmod{10909}$

$x_{19} = f(x_{18}) = 5814^2 + 1 = 6515 \pmod{10909}$

$x_{20} = f(x_{19}) = 6515^2 + 1 = 9216 \pmod{10909}$