TEMA 3

1. Dacă $n = \prod_{i=1}^{k} p_i^{a_i}$ și $a^{p_i} \equiv a \pmod{p_i}$, $\forall p_i$ <u>at. $a^n \equiv a \pmod{n}$</u>

$a^{p_i} \equiv a \pmod{p_i^{a_i}} \Big/ {}^{n/p_i}$

~~$(a^{p_i} = a \cdot p_i^{a_i})$~~

$a^n = a^{n/p_i} \cdot a \equiv a \pmod{p_i^{a_i}}$ T.C.R.

$p_i^{a_i}$ coprime $\Rightarrow a^n \equiv a \pmod{p_i^{a_i}}, \forall i \Rightarrow a^n \equiv a \pmod{n}$ □

2. 1729, 10585, 75361 <u>numere Carmichael</u>

1729	7
247	13
19	19
1	

$1729 = 7 \cdot 13 \cdot 19$ (toți la puterea 1)

$p_i - 1 \mid n - 1$

1728	2
864	2
432	2
216	2
108	2
54	2
27	3
1	

$1728 = 2^6 \cdot 3^3 \Rightarrow 6 \mid 1728$

$12 \mid 1728$

$18 \mid 1728$

$\Rightarrow a^{1729} \equiv a \pmod{1729}$

$\Rightarrow$ 1729 <u>este nr. Carmichael.</u>

10585	5
2117	29
73	73
1	

$10585 = 5 \cdot 29 \cdot 73$ (toți la puterea 1)

$p_i - 1 \mid n - 1.$

10584	2
5292	2
2646	2
1323	7
189	3
63	3
21	3
7	7
1	

$10584 = 2^3 \cdot 7^2 \cdot 3^3 \Rightarrow 4 \mid 10584$

$28 \mid 10584$

$72 \mid 10584$

$\Rightarrow a^{10585} \equiv a \pmod{10585}$

$\Rightarrow$ 10585 <u>este nr. Carmichael.</u>

75361	17
6851	13
527	17
31	31
1.	

$75361 = 11 \cdot 13 \cdot 17 \cdot 31$ (forma patrata)

$\rho = 1 \,//\, m4$

75360	10
7536	12
628	2
314	2
157	

$75360 = 10 \cdot \underbrace{12}_{2^2 \cdot 3} \cdot 2^2 \cdot 157$

$\Rightarrow$ $10 \mid 75360$
$12 \mid 75360$
$16 = 2^4 \mid 75360$
$30 = 3 \cdot 10 \mid 75360$

$\Big\}$ odata $\Rightarrow a^{75361} \equiv a \pmod{75361} \Rightarrow$ 75361 este nr. Carmichael.

3. Daca $2^n - 1$ prim at. n prim //

Pp n nu este prim $\Rightarrow n = a \cdot b$, $a, b > 1$.

$2^n - 1 = 2^{a \cdot b} - 1 \Rightarrow 2^n - 1 = 2^{a \cdot b} - 1 \;\vdots\; 2^a - 1$

$a < n$, $a > 1$ $\Big| \Rightarrow 2^a - 1 < 2^n - 1 \Rightarrow$

$\Rightarrow 2^n - 1$ nu poate fi prim (are un divizor diferit de 1 si el insusi)

$\Rightarrow$ contradictie cu $2^n - 1$ prim $\Rightarrow$ n este prim $\square$.

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

$\left(\frac{a}{p}\right) = \begin{cases} 1, & p \nmid a \wedge \exists x : b \equiv x^2 \text{ - rest patratic} \\ 1, & \forall x : b \not\equiv x^2 \pmod p \text{ - rest nepatratic} \\ 0, & p \mid a \end{cases}$

Folosim criteriul lui Gauss

$\left(\frac{m}{n}\right) = (-1)^{N_m}$, N_m = nr. de inversiuni de resturi din multimea:

$$\left\{-\frac{1}{2}n,\ 2n,\ 3n,\ \dots,\ \frac{n-1}{2}n\right\} \bmod n$$

$$\left(\frac{n}{m}\right) = (-1)^{N_n}.$$

$$N_m + N_n = \frac{(m-1)(n-1)}{4} \Rightarrow \left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \left(\frac{n}{m}\right) \quad \square$$

8. Simbolul Kronecker : $\left(\frac{a}{n}\right)$ este o generalizare a simbolului Jacobi, $\forall n \in \mathbb{Z}$.

Fie $n \neq 0$, $n = u \cdot p_1^{\ell_1} \cdots p_k^{\ell_k}$, unde $u = \pm 1$, p_i prime.

Fie $a \in \mathbb{Z}$, $\boxed{\left(\frac{a}{n}\right) := \left(\frac{a}{u}\right) \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\ell_i}}$

Pt p_i impare, $\left(\frac{a}{p_i}\right)$ = simbolul Legendre

Dacă $p_i = 2$, $\left(\frac{a}{2}\right) := \begin{cases} 0, & a \text{ par} \\ 1, & a \equiv \pm 1 \pmod 8 \\ -1, & a \equiv \pm 3 \pmod 8. \end{cases}$

$\left(\frac{a}{u}\right) = 1$, dacă $u = 1$.

$\left(\frac{a}{-1}\right) := \begin{cases} -1, & \text{dacă } a < 0 \\ 1, & \text{dacă } a \geq 0 \end{cases}$

$\left(\frac{a}{0}\right) := \begin{cases} 1, & \text{dacă } a = \pm 1 \\ 0, & \text{altfel.} \end{cases}$

Proprietăți:

- $\left(\frac{a}{n}\right) \begin{cases} \pm 1, & \text{dacă } \gcd(a, n) = 1. \\ 0, & \text{altfel.} \end{cases}$
- $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ în afară de at. când $n = -1$, a scrie $b = 0$ și calculat este negativ.

· $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$ dacă $a = -1$, $m = 0$ sau $n = 0$, ia calculat ca
pana impar conform cu 3 mod 4

· Pt $m > 0$, $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$ cand $a \equiv b \bmod \begin{cases} 4m, m \equiv 2 \pmod 4 \\ m, \text{altfel.} \end{cases}$

· Pt $a \not\equiv 3 \pmod 4$, $a \neq 0$, $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$ cand $m \equiv n \bmod \begin{cases} 4|a|, a \equiv 2 \pmod 4 \\ |a|, \text{altfel.} \end{cases}$

· Legea reciprocității pătratice: $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \pm(-1)^{\frac{m'-1}{2}\cdot\frac{n'-1}{2}}$.

9.21. 809 prim sau compus ? – Solovay-Strassen

$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod n$ | $\frac{809-1}{2} = \frac{808}{2} = 404$

$b^{404} \equiv \left(\frac{b}{809}\right) \pmod{809}$

$b = 2$

$2^{404} = \left(2^2\right)^{202} = 4^{202} = \left(4^2\right)^{101} = 16^{101} = 16 \cdot \left(16^4\right)^{50} =$

$= 16 \cdot 256^{50} = 16 \cdot \underbrace{\left(256^2\right)^{25}}_{7 \pmod{809}} = 16 \cdot 7^{25} = 16 \cdot \left(7^2\right)^{12} \cdot 7 =$

$= 112 \cdot 49^{12} = 112 \cdot \underbrace{\left(49^2\right)^6}_{-26} = 112 \cdot (-26)^6 =$

$= 112 \cdot \left(26^2\right)^3 =$

$= 112 \cdot 676 \cdot 676^2$

$= 112 \cdot (-133) \cdot (-133)^2$

$= -14896 \cdot 133^2$

$= 334 \cdot \underbrace{133^2}_{-109}$

$= -334 \cdot 109$

256 · 256 = 65536

49 · 49 = 2401 $= 2 \cdot 809 + 783$

809 − 676 = 133

809 − 783 = 26

$= -36406 = -1$

$36406 = 45 \cdot 809 + 1.$

$b = 3$

$3^{404} = (3^2)^{202} = 9^{202} = (9^2)^{101} = 81 \cdot 81^{100} =$

$= 81 \cdot (81^2)^{50} = 81 \cdot \underbrace{6561}_{89}{}^{50} = 81 \cdot (89^2)^{25} =$

$= 81 \cdot \underbrace{(7921)}_{640}{}^{25} = 81 \cdot (-169) \cdot (-169^2)^{12} =$

$\underbrace{-169}$

$= -\underbrace{13689}_{745} \cdot (\underbrace{169^2}_{246})^{12} = 64 \cdot 246^{12} = 64 \cdot (\underbrace{246^2}_{-159})^6 =$

$\underbrace{-64}$

$= 64 \cdot (\underbrace{159^2}_{202})^3 = 64 \cdot 202 \cdot 202^2 =$

$= \underbrace{12928}_{783} \cdot \underbrace{40804}_{354} = -16 \cdot 354 = -5664 = -1$

$\underbrace{-16}$

$5644 = 7 \cdot 809 + 1.$

$b = 5$

$5^{404} = (5^2)^{202} = (25^2)^{101} = 625^{101} = (-184)^{101} =$

$= -184 \cdot (184^2)^{50} = -184 \cdot (184^2)^{50} =$

$= -184 \cdot \underbrace{(33856)}_{607}{}^{50} = -184 \cdot (122^2)^{25} = -184 \cdot (122^2)^{25} =$

$\underbrace{-122}$

$= -184 \cdot \underbrace{14884}_{322}{}^{25} = -184 \cdot 322 \cdot (322^2)^{12} =$