19.03.24

Clasa TN 4_312

T1 (Euler) $\forall n \in \mathbb{N}\ (n \geq 2 \Rightarrow \forall a \in \mathbb{Z}\ ((a,n)=1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod n))$

Dem: $(a,n)=1 \Rightarrow \hat{a} \in U(\mathbb{Z}_n) \Rightarrow$

$\operatorname{ord}_{U(\mathbb{Z}_n)} \hat{a} \mid |U(\mathbb{Z}_n)| = \varphi(n)$.

Ca urmare, $\hat{a}^{\varphi(n)} = \hat{1}$, deci $a^{\varphi(n)} \equiv 1 \pmod n$

T2 (Fermat) Pentru orice număr natural prim p, $\forall$ pt. orice $a \in \mathbb{Z}$, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod p$

T3 (Wilson) Pentru orice număr natural prim p, $(p-1)! \equiv -1 \pmod p$ □

---

1. Pentru ce $p \in \mathbb{N}$ prime avem $\frac{2^p+1}{p} \in \mathbb{Z}$?
2. Pentru orice $n \in \mathbb{N}$ restul împărțirii lui $10^n - 1$ la 37 e pătrat perfect.
3. Determinați restul împărțirii lui 100! la 109.

Obs: ○ Orice pătrat de număr par e $\equiv 4$.

○ Orice pătrat de număr impar e $\equiv 1 \pmod 8$

T (GAUSS – LEGENDRE)

Un număr natural se scrie ca sumă de trei pătrate de numere întregi dacă și NUMAI dacă e de forma $4^k(8T+7)$ $(k, T \in \mathbb{N})$

Fie $x \in \mathbb{Z}$, $x = a^2+b^2+c^2$, $a, b, c \in \mathbb{N}$

Presupunem că $\exists k, T \in \mathbb{N}$ $x = 4^k(8T+7)$

Atunci $4^k(8T+7) = a^2+b^2+c^2$

Dacă $k > 0$, fie a, b, c sunt pare

deci $4^k(8T+7) = 4(a_1^2+b_1^2+c_1^2) \Rightarrow$

$4^{k-1}(8T+7) = a_1^2+b_1^2+c_1^2$

Dacă continuăm, raționând numai pe cazuri particulare, obținem

$\exists a_k, b_k, c_k \in \mathbb{Z}$ $8T+7 = a_k^2+b_k^2+c_k^2$

În MD nu putem avea decât:

- 1 nr. impar și 2 pare.

Atunci $MD \equiv \underbrace{1+\alpha+\beta}_{m}$, unde $\alpha, \beta \in \{0, 4\}$

$m \equiv r \pmod 8$, $r \neq 7$.

Sau

- Toate impare

Atunci $MD \equiv 3 \pmod 8$, $\not\equiv$

Dacă $x = 4^k(8T+7) = a^2+b^2+c^2$ și MD avem 1 nr par și 2 impare, $MD \equiv 2 \pmod 4$, $\not\equiv$.

Deci, AM DEMONSTRAT „$\Rightarrow$" !!

Sol 3: $100! \cdot (-8) \cdot (-7) \cdot (-6) \cdot (-5) \cdot (-4) \cdot (-3) \cdot (-2) \equiv -1 \pmod{109}$

Cum calculăm inversul (mod n) al unui element?

Ex: Care e inversul lui 83 (mod 601)?

1. „La înfrângere":

$$\left.\begin{aligned} 83 \cdot 7 &\equiv -20 \\ (-20)\cdot(-30) &\equiv -1 \end{aligned}\right\} \Rightarrow 83 \cdot 7 \cdot 30 \equiv 1$$

$$83 \cdot 210 \equiv 1$$

Deci inversul (mod 601) al lui 83 e 210

2. Folosind algoritmul lui Euclid:

De fapt, inversul lui 83 (mod 601) e un număr $x \in \mathbb{Z}$ cu proprietatea că $83 \cdot x \equiv 1 \pmod{601}$

$\Leftrightarrow \exists n \in \mathbb{Z} \quad 83x - 1 = 601n \Leftrightarrow$

$\exists n \in \mathbb{Z} \quad 83x - 601n = 1$

$601 = 7 \cdot 83 + 20$

$83 = 4 \cdot 20 + 3$

$20 = 6 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

	-1	0	1	2	3
q	0	7	4	6	1
α	0	1	-4	25	-29
β	1	-7	29	-181	210

$a = bq_0 + r_0 \Leftrightarrow r_0 = a - q_0 b$

$b = r_0 q_1 + r_1$ $\quad (\alpha_0 = 1, \beta_0 = -q_0)$

$r_0 = r_1 q_2 + r_2$

$\alpha_j = \alpha_{j-2} - q_j \alpha_{j-1}$

$\beta_j = \beta_{j-2} - q_j \beta_{j-1}$

Deci,

$1 = r_3 = -29 \cdot 601 + 210 \cdot 83$,

deci $83 \cdot 210 \equiv 1 \pmod{601}$,

deci inversul lui 83 (mod 601) e 210.

$b = 0 \cdot a + b$

$q_{-1} \quad r_{-1}$

$(0)\,a + (1)\,b = r_{-1}$

$\alpha_{-1} \quad \beta_{-1}$

3. Cu FRACȚII CONTINUE

$$\frac{601}{83} = 7 + \frac{20}{83} = 7 + \frac{1}{\frac{83}{20}} = 7 + \frac{1}{4 + \frac{3}{20}} =$$

$$= 7 + \frac{1}{4 + \frac{1}{\frac{20}{3}}} = 7 + \frac{1}{4 + \frac{1}{6 + \frac{2}{3}}} \overset{\text{not}}{=} \mathcal{F}$$

$$= 7 + \frac{1}{4 + \frac{1}{6 + \frac{1}{1 + \frac{1}{2}}}}$$

FRACȚIA CONTINUĂ ASOCIATĂ LUI $\frac{601}{83}$.

Fracțiile continue $R_0 = 7$; $R_1 = 7 + \frac{1}{4}$; $R_2 = 7 + \frac{1}{4 + \frac{1}{6}}$;

$R_3 \overset{\text{not}}{=} 7 + \frac{1}{4 + \frac{1}{6 + \frac{1}{1}}}$ $\quad$ $R_4 \overset{\text{not}}{=} 7 + \frac{1}{4 + \frac{1}{6 + \frac{1}{1 + \frac{1}{2}}}}$ $\quad$ s.a.

REDUSELE lui $\mathcal{F}$

$R_3 = 7 + \frac{7}{29} = \frac{210}{29}$

Obs: $210 \cdot 83 - 29 \cdot 601 = 1$,

deci $210 \cdot 83 \equiv 1 \pmod{601}$,

deci inversul lui 83 (mod 601) e 210.

4. Folosind T. Fermat

Cf T. Fermat (p : 601 e prim!!)

$83^{600} \equiv 1 \pmod{601}$,

deci inversul lui 83 (mod 601)

este 83^{599}

$599 = 512 + 64 + 16 + 4 + 2 + 1$,

deci $83^{599} = 83 \cdot 83^2 \cdot 83^4 \cdot 83^{16} \cdot 83^{64} \cdot 83^{512} = (1)$

Dar: $83^2 \equiv 278$

$83^4 \equiv 278^2 \equiv 356$

$83^8 \equiv 356^2 \equiv 526$ (toate $\pmod{601}$)

$83^{16} \equiv 526^2 \equiv 216$

$83^{32} \equiv 216^2 \equiv 379$

$83^{64} \equiv 379^2 \equiv 2$

$83^{128} \equiv 4$

$83^{256} \equiv 4^2 \equiv 16$

$83^{512} \equiv 256$,

Deci,

$(1) \equiv 83 \cdot 278 \cdot 356 \cdot 216 \cdot 2 \cdot 256 \equiv 210$

Ca urmare, inversul lui 83 (mod 601) e 210.