/

Teorema lui Wilson

Dacă p prim, atunci $p \mid ((p-1)!+1)$

$p = 7$

$6!+1 = 720+1 = 721 \Rightarrow 7 \mid 721$

$p = 23$ $\mathbb{Z}_{23}$

$22! = (2 \cdot 12) \cdot (3 \cdot 8) \cdot (5 \cdot 14) \cdot (7 \cdot 10) \cdot (9 \cdot 18) \cdot$

$(15 \cdot 20) \, (16 \cdot 13) \cdot (21 \cdot 11) \, (17 \cdot 19) \, (1 \cdot 1)$

$\cancel{(22 \cdot 22)}$

$\overline{22} \cdot \overline{22} = 1$

Demonstrație $(G, \cdot)$ grup comutativ finit

$g_1 \cdot g_2 \cdots g_n = a_1 a_2 \dots a_j =$ unde $a_i^2 = e$

Dacă $g \neq g^{-1}$ ~~diferite~~ $\Rightarrow$

$g = g^{-1} \Leftrightarrow g^2 = e$

$= \prod_{\substack{g \in G \\ g^2 = e}}$

1/

$G = U(\mathbb{Z}_p)$

grup cu $\varphi(p) = p-1$

Câte elemente din G, $g^2 = e$?

$\Rightarrow p \mid (x^2-1) \Leftrightarrow p \mid (x+1)(x-1) \Rightarrow$

$\Rightarrow p \mid (x+1)$ sau $p \mid (x-1)$ $\Big| \Rightarrow x = p-1$ sau $x = 1$

$x = \overline{1, p-1}$

$\prod_{g \in G} g = (\overline{p-1}) \cdot \overline{1} = \overline{p-1}$

$2017 = 44^2 + 9^2$

$$\begin{array}{r|l} 2017 & 4 \\ \hline 16 & 504,1 \\ 417 & \end{array}$$

p prim, $p = 4k+1 \Rightarrow p = a^2 + b^2$

Criptează numerele

A B C D E F .... Z ..

1 2 3 26

X = produsul literelor

1. restul împărțirii

2. " la 2017

3. $X = a^2 + b^2$

Dacă ∃ soluții

Demonstrație

p prim $\quad p = 4k+1, \quad m = \left(\frac{p-1}{2}\right)! \Rightarrow \overline{m}^2 = -1$

$p = 13 \quad \overline{1} = \overline{1}$

$\overline{2} = \overline{2}$

$\vdots$

$\overline{6} = \overline{6}$

$\overline{7} = -\overline{6}$

$\vdots$

$\overline{12} = -\overline{1}$

$\overline{1} = \overline{1}$

$\overline{2} = \overline{2}$

$\vdots$

$\overline{\frac{p-1}{2}} = \overline{\frac{p-1}{2}}$

$\overline{\frac{p+1}{2}} = -\overline{\frac{p-1}{2}}$

$\vdots$

$\overline{p-1} = \overline{-1}$

$$\overline{(p-1)!} = \overline{(-1)^{\frac{p-1}{2}}} \cdot \left[\overline{\left(\frac{p-1}{2}\right)!}\right]^2$$

2) $\overline{m}^2 = -1$

3/

$p = 4k+1$, $k \in \mathbb{N}$, $m = \left(\frac{p-1}{2}\right)!$ Atunci $\hat{m}^2 = -\hat{1}$ în $\mathbb{Z}_p$

Demonstrație

~~$z \leq [x] \leq z+1$~~

$[\sqrt{p}] < a[\sqrt{p}] < [\sqrt{p}] + 1$

$\sqrt{p}$ $z^2 < p$

cel puțin $p+1$ nr

$\exists x, y$ care au același rest - principiul cutiei

STOP

Fie grup $(G, \cdot)$, $H \subseteq G$

$(H, \cdot)$ subgrup - parte stabilă

- $\forall x \in H$, atunci $x^{-1} \in H$

Th lui Lagrange pe cazul general

Dem. dir.: $\overline{1}=\overline{1}$

$\overline{2}=\overline{2}$

$\vdots$

$\overline{\frac{p-1}{2}}=\overline{\frac{p-1}{2}}$

$\overline{\frac{p+1}{2}}=-\left(\overline{\frac{p-1}{2}}\right)$

$\overline{\frac{p+3}{2}}=-\left(\overline{\frac{p-3}{2}}\right)$

$\vdots$

$\overline{p-1}=-\overline{1}$

$\Rightarrow \overline{(p-1)!}=(-1)^{\frac{p-1}{2}}\left[\overline{\left(\frac{p-1}{2}\right)!}\right]^2$

m^2

$(-1)^{2k}=1$

$\overline{m^2}=-\overline{1}$

$m=\frac{p-1}{2}!$

$\overline{m^2}=-\overline{1} \quad (\mathbb{Z}_p)$

$x+my \quad , x,y\in\{0,1,2,\dots,[\sqrt{p}]\}$

$([\sqrt{p}]+1)^2$ valori $>p$

$z-1<[z]\leq z$

$[z]+1>z \Rightarrow [\sqrt{p}]+1>\sqrt{p}$

$([\sqrt{p}]+1)^2>p$

$a_1, a_2, \dots, a_{p+1}$

Restul împ. la p: $0,1,2,\dots,p-1$ $\Big\}$ $\exists\, 1\leq i<j\leq p+1$ a.î. $\hat{a}_i=\hat{a}_j$ în $\mathbb{Z}_p$

$\Rightarrow \exists\,(x_1,y_1)\neq(x_2,y_2)$ a.î. $\overline{x_1+my_1}=\overline{x_2+my_2}$ în $\mathbb{Z}_p$

Scanned by CamScanner

Notăm $a = x_1 - x_2$
$b = y_1 - y_2$

$|a| \le [\sqrt{p}] < \sqrt{p}$ $\qquad \overline{x_1 - x_2 + m(y_1 - y_2)} = \overline{0}$

$|b| \le [\sqrt{p}] < \sqrt{p}$ $\qquad \overline{a + bm} = \overline{0}$

$\overline{(a+bm)} \cdot \overline{(a-bm)} = \overline{0}$

$\overline{a^2 - b^2 m^2} = \overline{0}$, $\overline{m^2} = \overline{-1}$

$\left.\begin{array}{l} \overline{a^2 + b^2} = \overline{0} \\ \mathbb{Z}_p \end{array}\right| \Rightarrow p \mid a^2 + b^2$

Dc. $a^2 + b^2 = 0 \Rightarrow a = b = 0 \Rightarrow x_1 = x_2 \wedge y_1 = y_2$ abs.

$\left.\begin{array}{l} 0 < a^2 + b^2 < 2p \\ p \mid a^2 + b^2 \end{array}\right| \Rightarrow a^2 + b^2 = p$

$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$

Definiție:

$(G, \cdot)$ grup

Fie $H \subseteq G$

H = subgrup dacă:

1) $\forall x, y \in H \Rightarrow x \cdot y \in H$

2) $\forall x \in H \Rightarrow x^{-1} \in H$

$(H, \cdot) \le (G, \cdot)$
$\hookrightarrow$ subgrup

E posibil să existe $(H, \cdot) \le (G, \cdot)$? NU
$|H| = 2$
$|G| = 9$