.

FEJEZETEK A SZÁMELMÉLETBŐL ELŐADÁS

Waldhauser Tamás

SZTE Bolyai Intézet

2021. február 9.

Bemelegítő feladat: $101^{658} \equiv ?$ (mod 99)

$101^{658} \equiv 2^{658}$ (mod 99) $\quad 2 \perp 99$

$\varphi(99) = \varphi(9) \cdot \varphi(11) = (9-3) \cdot (11-1) = 60$

$2^{658} \equiv (2^{60})^{10} \cdot 2^{58} \equiv 2^{58} \equiv 2^{-2} \equiv 4^{-1} \equiv x$ (mod 99)

$2^{60} \equiv 1$

$4x \equiv 1$ (mod 99)

$4x \equiv 100$ (mod 99) $/:4 \quad 4 \perp 99$

$x \equiv 25$ (mod 99)

$2^1 \equiv 2$

$2^2 \equiv 4$

$2^4 \equiv 16$

$2^8 \equiv 256 \equiv 2 \cdot \overbrace{100}^{1} + 56 \equiv 58 \equiv -41 \pmod{99}$

$2^{16} \equiv 41^2 = (40+1)^2 \equiv 1600 + 80 + 1 \equiv 97 \equiv -2$

$2^{32} \equiv 4$

$58 = \overset{32}{1}\ \overset{16}{1}\ \overset{8}{1}\ \overset{4}{0}\ \overset{2}{1}\ \overset{1}{0}_{(2)} = 32 + 16 + 8 + 2$

$2^{58} = 2^{32} \cdot 2^{16} \cdot 2^8 \cdot 2^2 \equiv 4 \cdot (-2) \cdot (-41) \cdot 4 = 16 \cdot (-17) \equiv$

$\equiv 4 \cdot (-68) \equiv 4 \cdot 31 \equiv 124 \equiv \underline{\underline{25}} \pmod{99}$

NÉGYZETES MARADÉKOK

$\underbrace{11\ldots1}_{2021} \equiv 2021 \equiv 5 \equiv 2 \pmod 3$ $\Rightarrow$ nem lehet □

$p=2 \quad a \equiv 0,1 \pmod 2$ ✓

DEF LEGENDRE-szimbólum p pr. pár., $a \perp p$

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{ha } \exists x \in \mathbb{Z}: x^2 \equiv a \pmod p \\ -1, & \text{ha } \nexists x \in \mathbb{Z}: x^2 \equiv a \pmod p \end{cases}$$

Pl. $\left(\frac{2}{3}\right) = -1 \quad \left(\frac{1}{3}\right) = 1 \quad \left(\frac{0}{3}\right)$

WILSON TÉTELE Ha p prím, akkor $(p-1)! \equiv -1 \pmod p$.

EULER-KRITÉRIUM $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

Biz.: $A = \{1, \dots, p-1\}$

u is v ergyes párja, ha $u \cdot v \equiv a \pmod p$

Mikor lehet u párja saját maga?

$$u \cdot u \equiv u^2 \equiv a \pmod p$$

$$(p-u)(p-u) \equiv (p-u)^2 \equiv (-u)^2 \equiv u^2 \equiv a \pmod p$$

$u \neq p-u$

$x^2 \equiv a \pmod p \iff p \mid x^2 - a \iff p \mid x^2 - u^2 = (x-u)(x+u)$

$\Rightarrow p \mid x-u \vee p \mid x+u$

$x \equiv u \qquad x \equiv -u$

1) $\left(\frac{a}{p}\right)=-1$ $\quad -1\equiv(p-1)!\equiv(\underset{\text{II}}{\underset{a}{\_\_}})\cdot(\underset{\text{III}}{\underset{a}{\_\_}})\cdot\ldots\cdot(\underset{\text{III}}{\underset{a}{\_\_}})\equiv a^{\frac{p-1}{2}}\ (\text{mod } p)$

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

2) $\left(\frac{a}{p}\right)=1$ $\quad -1\equiv(p-1)!\equiv(\underset{\text{III}}{\underset{a}{\_\_}})\cdot\ldots\cdot(\underset{\text{III}}{\underset{a}{\_\_}})\cdot\underbrace{u\cdot(p-u)}_{\text{III}}\equiv -a^{\frac{p-1}{2}}\ (\text{mod } p)$

$-u^2\equiv -a$

$a=1$

□

PÉLDA

$\left(\frac{10}{13}\right)\equiv 10^6\equiv 100^3\equiv 9^3\equiv 27^2\equiv 1^2\equiv 1\ (\text{mod } 13)$

$\Rightarrow \exists x\in\mathbb{Z}: x^2\equiv 10\ (\text{mod } 13)$ $\quad x=6$

Kör. $\forall p$ pk $p>1$: $\forall a,b \in \mathbb{Z}$, $a,b \perp p$

(1) $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$

(3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4} \\ -1, & \text{ha } p \equiv 3 \pmod{4} \end{cases}$

Biz.

(1) ✓

(2) $\left(\frac{ab}{p}\right) \overset{\text{E.K.}}{=} (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \overset{\text{E.K.}}{=} \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) \pmod{p}$

$\left(\frac{ab}{p}\right) = \pm 1$, $\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) = \pm 1$

$+1 \equiv -1 \pmod{p} \Leftrightarrow p \mid 2 \nleq p$ pk.

(3) ✓

□

NF: $p \equiv 1 \pmod 4 \Rightarrow \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$

(1)

PÉLDA $\left(\frac{10}{13}\right) \overset{(1)}{=} \left(\frac{36}{13}\right) = 1$

$\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{5}{13}\right)$

$\| \qquad \| ? \qquad \| ?$

$1 \qquad -1 \qquad -1$

KVADRATIKUS RECIPROCITÁS Ha $p \neq q$ ész. pth. prímek, akk

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} +1, \text{ ha } p \equiv 1 \vee q \equiv 1 \pmod 4 \\ -1, \text{ ha } p \equiv 3 \equiv q \pmod 4 \end{cases}$$

$x^2 \equiv p \pmod q \qquad x^2 \equiv q \pmod p$