

Számelmélet pótZH, megoldások

2005 december 16.

1. Keressük meg az

$$5x \equiv 561 \pmod{1968}$$

kongruencia összes megoldását.

Megoldás:

Először a kibővített euklideszi-algoritmussal számolva megadjuk 5 és 1968 legnagyobb közös osztójának előállítását 5 és 1968 lineáris kombinációjaként.

$$\begin{array}{rcl} 1968 & = & 5 \cdot 393 + 3 \\ 5 & = & 3 \cdot 1 + 2 \\ 3 & = & 2 \cdot 1 + 1 \\ 2 & = & 1 \cdot 2 + 0 \\ 1 & & \end{array} \quad \left| \begin{array}{rcl} 1968 \cdot x & + & 5 \cdot y \\ 1 & & 0 \\ 0 & & 1 \\ 1 & & -393 \\ -1 & & 394 \\ 2 & & -787 \end{array} \right|$$

Ezek szerint $2 \cdot 1968 - 787 \cdot 5 = 1$, tehát $5^{-1} \equiv -787 \equiv 1181 \pmod{1968}$.
Miután $1181 \cdot 561 = 662541 \equiv 1293 \pmod{1968}$, tehát $x \equiv 1293 \pmod{1968}$ az egyetlen megoldás.

2. Adjuk meg az

$$x^{11} + x + 1 \equiv 0 \pmod{121}$$

összes megoldását.

Megoldás:

Miután $121 = 11^2$, ezért oldjuk meg először modulo 11. Ha $11 \mid x$, akkor nem kapunk megoldást, tehát feltehető $(x, 11) = 1$, és így $x^{11} \equiv x \pmod{11}$ a kis Fermat-tétel szerint. Megoldandó tehát a $2x + 1 \equiv 0 \pmod{11}$ kongruencia, aminek egyetlen megoldása $x \equiv 5 \pmod{11}$.

Ezek után kereshetjük a modulo 11^2 megoldást $5 + 11y$ alakban. Legyen $f(x) = x^{11} + x + 1$, így azt kapjuk, hogy

$$\begin{aligned} 0 &\equiv f(5 + 11y) \equiv f(5) + 11yf'(5) \pmod{11^2}, \text{ azaz} \\ 0 &\equiv \frac{f(5)}{11} + yf'(5) \pmod{11}. \end{aligned}$$

$5^3 \equiv 4 \pmod{11^2}$, így $5^{11} = (5^3)^3 \cdot 25 \equiv 64 \cdot 25 \equiv 27 \pmod{11^2}$, tehát $f(5) \equiv 33 \pmod{11^2}$. Másrészt $f'(x) = 11x^{10} + 1 \equiv 1 \pmod{11}$, így az egyenletünk

$$0 \equiv 3 + y \pmod{11}.$$

Innen $y \equiv 8 \pmod{11}$, és ezért $x \equiv 5 + 11 \cdot 8 = 93 \pmod{11^2}$.

A Hensel-felemelésről szóló tétel miatt más megoldása nincs a kongruenciának.

3. Mutassuk meg, hogy tetszőleges p prím és n egész szám esetén $n^{p^p} - n$ osztható p -vel.

Megoldás:

Miután $p^p \equiv 1^p = 1 \pmod{p-1}$, így $n^{p^p} \equiv n^1 = n \pmod{p}$, ami igazolja az állítást.

4. Bizonyítsuk be, hogy 2^n nem osztója $n!$ -nak

Megoldás:

Legyen $t = \lfloor \log_2 n \rfloor$, azaz $2^t \leq n < 2^{t+1}$. A 2 kitevője $n!$ prímtényezősz felbontásában

$$\sum_{i=1}^t \left\lfloor \frac{n}{2^i} \right\rfloor \leq \sum_{i=1}^t \frac{n}{2^i} = \frac{n}{2} \sum_{i=0}^{t-1} 2^{-i} = \frac{n}{2} \cdot \frac{2^{-t} - 1}{2^{-1} - 1} = n(1 - 2^{-t}) < n.$$

5. Bizonyítsuk be, hogy 4 semmilyen $m > 1$ -re nem lehet primitív gyök modulo m . Melyik az a legkisebb szám, amellyel $o_m(4) = 4$?

Megoldás:

Ha $(4, m) \neq 1$, akkor természetesen nem lehet 4 primitív gyök. Egyébként $4^{\frac{\varphi(m)}{2}} \equiv 2^{\varphi(m)} \equiv 1 \pmod{m}$ igaz az Euler–Fermat-tétel szerint, tehát 4 rendje kisebb, mint $\varphi(m)$, azaz nem lehet primitív gyök.

Az $o_m(4)$ akkor értelmes, ha 4 relatív prím m -hez, olyan m -et keresünk tehát, amely páratlan. Ráadásul $4 = o_m(2^2) = \frac{o_m(2)}{(o_m(2), 2)}$ miatt $o_m(2) = 8$ és ezért olyan m jöhet csak szóba, amelyre 8 osztója $\varphi(m)$ -nek. Az első ilyen a 15, de $o_{15}(4) = 2$, a második a 17, ami viszont megfelelő.

6. Legyen p egy $4k+1$ alakú prím. Számítsuk ki az $\left(\frac{1}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-2}{p}\right)$ összeget.

Megoldás:

A $4k+1$ alakú prímekre -1 négyzetszám, tehát $\left(\frac{i}{p}\right) = \left(\frac{-i}{p}\right) = \left(\frac{p-i}{p}\right)$. Így $2 \left(\left(\frac{1}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-2}{p}\right) \right) = \left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \left(\frac{3}{p}\right) + \cdots + \left(\frac{p-1}{p}\right)$. Utóbbi összeg a négyzetelemek száma mínusz a nem négyzetek száma, ez összesen 0, hiszen mindkettőből $\frac{p-1}{2}$ van.