Számelmélet

2014. február 23.

Hatványok, prímek

Euler-Fermat-tétel $a^{\varphi(m)} \equiv 1 \pmod{m}$ pontosan akkor, ha $(a, m) = 1$.
($\varphi(m)$ az Euler-fv; az m-hez relatív prím maradékosztályok száma.)

Egy elem rendje $\pmod{n}$

Legyen $n \in \mathbb{Z}^+$, és a számra $(a, n) = 1$, azaz relatív prímek. A legkisebb $d \in \mathbb{Z}^+$, amire $a^d \equiv 1 \pmod{n}$ az a **elem rendje** $\pmod{n}$.

Lemma, elem rendje kapcsán

- Ha $(a, n) = 1$ és a rendje $d \pmod{n}$, akkor $1, a, a^2 \dots a^{d-1}$ különbözőek $\pmod{n}$.
- Ha $n = p$ prím, akkor ráadásul $1 + a + \dots a^{d-1} \equiv 0 \pmod{p}$ (feltéve $a \not\equiv 0, 1 \pmod{p}$)
- $d|p-1$, d a ciklus, utána ismétlődés a hatványok maradékain.
- Ha $n = p$ prím, akkor a p-hez rel prím maradékok hatványösszegei: $\sum_{x=0}^{p-1} x^k = 0$, ha $0 < k < p-1$. (Polinomoknál is jó tudni!!)

Sok (olimpiai) feladatban kérdéses: mekkora a legnagyobb k kitevő, amire p^k oszt egy kifejezést. Ennek kapcsán vezessük be a $p^k||n$ jelölést: $p^k|n$, de $p^{k+1} \nmid n$.

1. Legyen p páratlan prím, $n, a, b \in \mathbb{Z}^+$, $(a, p) = (b, p) = 1$. Ha $a \equiv b \pmod{p}$, akkor

$$p^k||(a-b),\ p^l||n \quad \Rightarrow \quad p^{k+l}||a^n - b^n$$

p helyett 2-vel hasonlóan:

2. $n, a, b \in \mathbb{Z}^+$, $(a, 2) = (b, 2) = 1$.

$$2^{k+1}||(a^2-b^2),\quad 2^l||n \quad \Rightarrow \quad 2^{k+l}||a^n - b^n.$$

3. Ha p páratlan prím, $a > 1$, akkor $a^p - 1$-nek van olyan prímosztója, ami nem osztja $a - 1$-et.

4. Ha p páratlan prím, $a > 2$, akkor $a^p + 1$-nek van olyan prímosztója, ami nem osztja $a + 1$-et.

5. Igazoljuk, hogy minden $k \in \mathbb{Z}^+$ számhoz létezik N, amely feléírható két t-edik hatvány összegeként minden $t \in \{1, 2, \dots k\}$-ra

6. $p|x^2 + y^2$ és $p \equiv 3 \pmod{4}$, akkor $p|x$ és $p|y$. (következmény: $n^2 + 1$-nek nincs $4k + 3$ alakú osztója!)

7. Legyen n pozitív egész, igazoljuk hogy $2^{2^n} + 1$ minden prímosztója nagyobb mint 2^{n+1}.

8. Adjuk meg a legkisebb pozitív k-t, melyre $2^{2014}|(17^k - 1)$.

9. Határozzuk meg azon n pozitív egészeket, melyre $\frac{2^n+1}{n^2}$ egész!

10. Határozzuk meg azon n számokat, melyre az n-nél kisebb n-hez relatív prím számok számtani sorozatot alkotnak!

11. Egy valós számokból álló véges sorozatban bármely 7 egymást követő tag összege negatív, míg bármely 11 egymást követő tagé pozitív. Állapítsuk meg a sorozat maximális tagszámát!