OLIMPIAI ISKOLA

SZAKKÖR

Számelméleti beveztő

Borbényi Marci szakköre

Elmélet

- Kongruenciák
- Teljes és redukált maradékrendszer
- A p szám mindig prímet jelöl

Feladatok

F/1. **a)** Mi történik a $\mod n$ redukált maradékrendszerrel, ha megszorozzuk egy a, n-hez relatív prím számmal?
b) Bizonyítsuk be **a)**-ból, hogy létezik egy b egész, amire $ab \equiv 1 \mod n$. Sőt, ez a b valamilyen értelemben egyértelmű. Ezt nevezzük multiplikatív inverznek.
c) Bizonyítsuk be **a)**-ból, hogy $a^{\varphi(n)} \equiv 1 \mod n$. Itt $\varphi(n)$ a redukált maradékrendszer mérete.

F/2. Bizonyítsd be, hogy $\varphi(p^n) = (p-1)p^{n-1}$.

F/3. Legyenek a, b, c olyan számok, amire $6a \equiv 5,\ 4b \equiv 2,\ 12c \equiv 4 \mod n$. Mennyi

$$a + b - c \equiv ? \mod n$$

F/4. * Bizonyítsd be (φ explicit képletét nem használva), hogy $\sum_{k|n} \varphi(k) = n$.

F/5. (Euklideszi algoritmus) Bizonyítsuk be, hogy $a < b$ esetén $(a, b) = (a, b-a)$. Mi történik, ha ezt tovább folytatjuk?

F/6. Bizonyítsd be, hogy $(a^n - 1, a^k - 1) = a^{(n,k)} - 1$.

F/7. (Bézout-lemma) Bármely a, b egész számok esetén léteznek x, y egészek úgy, hogy $ax + by = (a, b)$.

F/8. Gabinak van egy 5, illetve egy 7 literes kancsója. Hogyan tudna ezek segítségével 1 litert kimérni?

2023. október 28.
Szakkörvezető: Borbényi Marci (marton.borbenyi@gmail.com)
Az Olimpiai Iskola email címe: olimpiai.iskola@gmail.com

Tétel (Kínai maradéktétel). Amennyiben a $b_1, b_2, \dots b_n$ számok páronként relatív prímek, az

$$\begin{cases} x \equiv a_1 \mod b_1, \\ x \equiv a_2 \mod b_2, \\ \vdots \\ x \equiv a_n \mod b_n, \end{cases}$$

egyenletrendszernek van megoldása. Ez a megoldás egyértelmű $\mod b_1 b_2 \dots b_n$.

F/9. Oldjuk meg az alábbi egyenletrendszert: $\begin{cases} x \equiv 3 \mod 5, \\ x \equiv 4 \mod 11. \end{cases}$

F/10. **a)** Bizonyítsd be a tételt $n = 2$ esetén.
b) Bizonyítsd be általános n-re.

F/11. Mutassuk meg bármely k-ra, hogy létezik k darab egymást követő szám, amik egyike sem hatványszám.

F/12. Bizonyítsuk be, hogy

$$\varphi(n) = n \prod_{p|n \text{ prím}} \left(1 - \frac{1}{p}\right).$$

F/13. * Egy rácspontot a síkon *látható*-nak hívunk, ha a koordinátáinak legnagyobb közös osztója 1. Bizonyítsuk be, hogy van egy 100×100 négyzet a síkon, aminek semelyik pontja sem látható.

Tétel (Euler-Fermat-tétel). Legyen $(a, n) = 1$. Ekkor

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Speciálisan, ha $n = p$ prímszám, $p \nmid a$, akkor

$$a^{p-1} \equiv 1 \mod p.$$

F/14. Határozd meg $2008^{2007^{2006^{\dots^{2^1}}}}$ utolsó három számjegyét.

F/15. Bizonyítsd be, hogy minden $c \in \mathbb{Z}$ és p prímszám esetén az $x^x \equiv c \mod p$ egyenletnek van megoldása.

F/16. * Határozzuk meg az összes pozitív egész k-t, amivel az $a_n = 2^n + 3^n + 6^n - 1$ sorozat minden eleme relatív prím.

F/17. * Bizonyítsd be, hogy bármely n esetén a

$$2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \dots \mod n$$

sorozat egy idő után konstans.

2023. október 28.
Szakkörvezető: Borbényi Marci (marton.borbenyi@gmail.com)
Az Olimpiai Iskola email címe: olimpiai.iskola@gmail.com

Tétel (Wilson-tétel). Legyen p prímszám. Ekkor

$$(p-1)! \equiv -1 \mod p.$$

F/18. A multiplikatív inverz létezésének segítségével bizonyítsuk be a Wilson-tételt.

F/19. Bizonyítsd be, hogy bármely $p = 4k+1$ alakú prímszám esetén $\left(\frac{p-1}{2}!\right)^2 \equiv -1 \mod p$.

F/20. Legyen $a_1, a_2, ..., a_{11}$ és $b_1, b_2, ..., b_{11}$ az $\{1, 2, ..., 11\}$ számok felsorolásai valamilyen sorrendben. Bizonyítsd be, hogy ekkor $a_1b_1, a_2b_2, ..., a_{11}b_{11}$ számok 11-gyel való osztási maradékai között van 2 azonos.

F/21. Legyen $a_1, a_2, \ldots a_{30}$ redukált maradékrendszer modulo 31. Bizonyítsd be, hogy

$$31 \mid (a_1a_2a_3)^3 + (a_4a_5 \ldots a_{30})^{27}.$$

F/22. * Legyen p prím és $n > 1$ egész. Mik a $p^n = (p-1)! + 1$ egyenlet megoldásai?

Definíció — Adott n és k relatív prímek esetén legyen k rendje modulo n, $\mathrm{ord}_n(k)$ az a legkisebb pozitív egész m, amire $k^m \equiv 1 \mod n$.

F/23. Bizonyítsd be, hogy létezik $\mathrm{ord}_n(k)$ és $\mathrm{ord}_n(k) | \varphi(n)$.

F/24. Bizonyítsd be, hogy amennyiben az $x^2 \equiv -1 \mod p$ megoldható, akkor $p = 4k+1$ alakú.

F/25. Legyenek $a \geq 2$ és $n \geq 1$ egészek. Bizonyítsd be, hogy n osztja $\varphi(a^n - 1)$-t.

F/26. Bizonyítsd be, hogy $2^p - 1$ minden prímosztója p-nél nagyobb.

F/27. * Bizonyítsd be, hogy nincs olyan $n \geq 2$ egész, amire $2^n - 1$ osztható n-nel.

F/28. * Határozzuk meg azokat az (n, k) pozitív egészekből álló számpárokat, amelyekre

$$\frac{(2^{2^n}+1)(2^{2^k}+1)}{nk} \in \mathbb{Z}.$$

OLIMPIAI ISKOLA

SZAKKÖR

Számelméleti beveztő

Borbényi Marci szakköre

Házi feladatok

Beadási határidő: 2023. november 5. (vasárnap)

HF/1. Bizonyítsuk be a Bézout-lemmát több tagra is (használva az $n = 2$ esetet), azaz bármely $a_1, a_2, ..., a_n$ egész számok esetén léteznek $x_1, x_2, ..., x_n$ egész számok, amikre

$$\text{lnko}\,(a_1, a_2, ..., a_n) = a_1x_1 + a_2x_2 + ... + a_nx_n.$$

HF/2. Bizonyítsd be, hogy bármely $2 < a, b$ egész számok esetén $2^a - 1 \nmid 2^b + 1$.

HF/3. Bizonyítsuk be, hogy létezik olyan $A \subset \{2^n - 1 \mid n = 2, 3, \dots\}$, ami végtelen, és elemei páronként relatív prímek.

HF/4. Mennyi $\text{lnko}(n! + 1, (n + 1)!) =$?

HF/5. * **a)** Bizonyítsuk be, hogy rögzített a, b relatív prím esetén minden $c \geq (a - 1)(b - 1)$ egész előáll $c = xa + yb$ alakban, ahol x, y természetes számok.
b) Bizonyítsuk be, hogy $(a - 1)(b - 1) - 1$ nem áll elő ilyen alakban.
c) Hány természetes szám nem áll elő ilyen alaban?

2023. október 28.
Szakkörvezető: Borbényi Marci (marton.borbenyi@gmail.com)
Az Olimpiai Iskola email címe: olimpiai.iskola@gmail.com