Számelméleti bevezető

Borbényi Marci

2026. október 22.

Fogalmak. Teljes és redukált maradékrendszer, kongruenciák

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 $\mod b_1 b_2 \dots b_n$.

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

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

3. 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 rácspontja sem látható.

4. Bizonyítsd be, hogy minden pozitív egész n-re léteznek $k_0, k_1, \dots, k_n$ különböző relatív prím pozitív egészek úgy, hogy $k_0 \cdot k_1 \cdot \ldots \cdot k_n$ két egymást követő egész szám szorzata.

---

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

6. Legyenek a, b, c olyan számok, amire $6a \equiv 5,\ 4b \equiv -2,\ 12c \equiv 4 \mod n,\ (6, n) = 1$. Mennyi

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

7. Bizonyítsd be, hogy $\sum_{k|n} \varphi(k) = n$.

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

9. * Bizonyítsd be, hogy ha $n = \prod p_i^{\alpha_i}$, akkor $\varphi(n) = \prod \varphi(p_i^{\alpha_i})$.

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

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

10. Határozd meg $2008^{2007^{2006^{\cdots^{2^1}}}}$ utolsó három számjegyét.

11. Bizonyítsd be, hogy ha $(a, 10) = 1$, akkor

$$a^{100} \equiv 1 \mod 1000.$$

Milyen kitevőt adna az Euler-Fermat?

12. Legyen $p = 2017$ prím. Határozd meg az

$$\lfloor \frac{1^p}{p} \rfloor + \lfloor \frac{2^p}{p} \rfloor + \lfloor \frac{3^p}{p} \rfloor + \cdots + \lfloor \frac{2015^p}{p} \rfloor$$

összeg p-vel vett osztási maradékját.

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

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

15. * Bizonyítsd be, hogy bármely n esetén a sorozat

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

egy idő után konstans.

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

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

16. A multiplikatív inverz létezésének segítségével bizonyítsuk be Wilson tételét.

17. 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.

18. Bizonyítsd be, hogy bármely $p = 4k + 1$ alakú prímszám esetén létezik x egész úgy, hogy $x^2 \equiv -1 \mod p$.

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

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

20. * Melyek azok a prímek, amelyekre a $(p-1)! + 1$ szám p-nek egész kitevős hatványa.

21. Mennyi lnko$(n! + 1, (n + 1)!)$ =?



Kiegészítő feladatok

22. a) Bizonyítsd be a kínai maradéktételeben a maradékosztály egyértelműséget.
b) Adott b_k sorozat esetén hány ilyen típusú egyenlet van? És mennyi lehetséges megoldás?
c) Bizonyítsuk be a megoldás létezését.

23. Legyen $p > 3$ prím, és legyen

$$N = (p-1)! \left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{p-1} \right).$$

a) Bizonyítsd be, hogy $p|N$. **b)** * Bizonyítsd be, hogy $p^2|N$.

24. Partícionáljuk fel az $\{1, 2, \ldots, 1998\}$ halmazt $x_1, \ldots, x_{999}$, $y_1, \ldots, y_{999}$ sorozatokra úgy, hogy az $|x_n - y_n|$ értéke 1 vagy 6 legyen minden $n \in \{1, \ldots, 999\}$ esetén. Bizonyítsd be, hogy az

$$|x_1 - y_1| + |x_2 - y_2| + \cdots + |x_{999} - y_{999}|$$

összeg 9-es számjegyre végződik.

25. Legyenek k, n pozitív egészek, és legyenek $a_1, a_2, a_3, \ldots, a_k$ $(k \geq 2)$ különbő számok az $\{1, 2, \ldots, n\}$ halmazból úgy, hogy $n|a_i(a_{i+1} - 1)$ minden $i = 1, 2, \ldots, k-1$ esetén. Bizonyítsd be, hogy n nem osztja $a_k(a_1 - 1)$-t.

26. Határozd meg azon $s \geq 4$ számokat, amikre léteznek a, b, c, d pozitív egészek úgy, hogy $s = a + b + c + d$ és s osztja az $abc + abd + acd + bcd$ összeget.