Bevezetés a számításelméletbe II.

10. gyakorlat, 2014. április 15.

Lineáris kongruenciák, kis Fermat tétel, Euler-Fermat tétel

Tudnivalók

Ha $a, b, k \in Z$ és $b = k \cdot a$, akkor a *osztója* b-nek (b *többszöröse* a-nak), jelölése $a \mid b$.

A $p \in Z$, $|p| > 1$ szám *felbonthatatlan*, ha csak $1 \cdot p, p \cdot 1, (-1) \cdot (-p)$ és $(-p) \cdot (-1)$ alakban áll elő egészek szorzataként. (Azaz, ha $a \mid p$ és $1 < |a|$, akkor $|a| = |p|$.) A $z \in Z$ *összetett*, ha $|z| > 1$ és z nem felbonthatatlan. A $p \in Z$, $|p| > 1$ szám *prím*, ha $p \mid ab, \quad a, b \in N \Rightarrow p \mid a$ vagy $p \mid b$. (Egészek szorzatát csak úgy oszthatja, ha vmik tényezőt osztja.)

Állítás: Tetszőleges 1-nél nagyobb egész szám előáll felbonthatatlan számok szorzataként.

Tétel: A p szám pontosan akkor felbonthatatlan, ha prím.

Következmény: (A számelmélet alaptétele) Tetszőleges n egész (melyre $2 \leq |n|$) a tényezők sorrendjétől és esetleges (-1) tényezőktől eltekintve egyértelműen áll elő felbonthatatlan számok szorzataként.

Az n *kanonikus alakja* $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, ahol a p_i-k prímek, és $1 \leq \alpha_i \in N \ \forall i$.

Állítás: Egy $d > 0$ egész pontosan akkor osztója n-nek, ha d kanonikus alakjában csak n prímosztói szerepelnek, legfeljebb az n kan. alakjában szereplő kitevőn. ($n = \prod_{i=1}^{k} p_i^{\alpha_i} \Rightarrow d = \prod_{i=1}^{k} p_i^{\beta_i}, 0 \leq \beta_i \leq \alpha_i$.)

Következmény: Ha $1 < n$ kanonikus alakja $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, akkor n poz. osztóinak száma $d(n) = \prod_{i=1}^{k}(\alpha_i + 1)$ill. az n pozitív osztóinak összege $\sigma(n) = \prod_{i=1}^{k} \sum_{j=0}^{\alpha_i} p_i^j = \prod_{i=1}^{k} \frac{p_i^{1+\alpha_i}-1}{p_i-1}$.

Az a és b egészek *legnagyobb közös osztója* $(a, b) := \max\{d : d \mid a, d \mid b\}$, *legkisebb közös többszörösük* pedig $[a, b] := \min\{0 < d : a \mid d, b \mid d\}$. Az a és b egészek *relatív prímek*, ha $(a, b) = 1$.

Állítás: Ha $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ és $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$ ($\alpha_i = 0$ és $\beta_i = 0$ is lehet), akkor $(a, b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \ldots \cdot p_k^{\min(\alpha_k,\beta_k)}$, $[a, b] = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \ldots \cdot p_k^{\max(\alpha_k,\beta_k)}$, valamint $ab = (a, b) \cdot [a, b]$. Továbbá, ha $d \mid a$ és $d \mid b$ az a és b közös osztója, akkor $d \mid (a, b)$.

Állítás: Ha a, b egészek, akkor $(a, b) = (a - b, b) = (a - kb, b)$ tetszőleges egész k esetén.

Euklideszi algoritmus Input: $a, b \in Z$. Output: (a, b).

Tfh $a \geq b$. Legyen $a_0 := a, a_1 := b$ és $a_0 = a_1 h_1 + a_2$, ahol $0 \leq a_2 < a_1$ (maradékos osztás). Általában $a_{i-1} = a_i h_i + a_{i+1}$, ahol $0 \leq a_{i+1} < a_i$. Ha $a_{k+1} = 0$, akkor $(a_0, a_1) = (a_1, a_2) = (a_2, a_3) = \ldots = (a_k, 0) = a_k$ a keresett lnko.

Következmény: Ha $a, b \in Z$ (nem mind nullák), akkor létezik $k, l \in Z$, melyre $(a, b) = ka + lb$.

Tétel: Végtelen sok prímszám van. Bármely $n \in N$-re létezik n egymást követő összetett szám.

Sejtés: Végtelen sok ikerprím van. (olyan (p, p') prím-pár, amelyre $p' - p = 2$).

Tétel: Végtelen sok olyan (p, p') prím-pár van, amelyre $|p' - p| < 600$).

Csebisev tétel: Minden $0 < n \in N$-re létezik p prím, melyre $n \leq p \leq 2n$.

Dirichlet tétel: Ha $(a, d) = 1$, akkor az $a, a + d, a + 2d, \ldots$ számtani sorban végtelen sok prím van.

Euler tétel: $\sum_{p \text{ prim}} \frac{1}{p} = \infty$.

$a, b, m \in Z$ esetén $a \equiv b (\text{mod } m)$ (a *kongruens* b *modulo* m, röviden $a \equiv b(m)$), ha $m \mid a - b$.

A Z halmaz m db diszjunkt halmaz diszjunkt uniója azzal a tulajdonsággal, hogy két egész pontosan akkor kongruens modulo m, ha ugyanabba a részhalmazba esnek. (Az i-dik ilyen részhalmazba a $\{i+km : k \in Z\}$ számok tartoznak.) E részhalmazok az m *szerinti maradékosztályok*.

Állítás: Ha $a \equiv b(m)$ (a és b ugyanabból a mod m maradékosztályból valók) akkor $(a, m) = (b, m)$.

Következmény: Ha $(a, m) = 1$, akkor az a maradékosztályának bármely eleme relatív prím a modulushoz.

Kongruenciák tulajdonságai: Tetsz $a, b, c, d, m \in Z$-re (1) $a \equiv a(m)$, (2) $a \equiv b(m) \Rightarrow b \equiv a(m)$
(3) $a \equiv b(m), b \equiv c(m) \Rightarrow a \equiv c(m)$ (4) $a \equiv b(m)$, $c \equiv d(m) \Rightarrow a + c \equiv b + d(m)$, $ac \equiv bd(m)$
(5) $a \equiv b(m) \iff ac \equiv bc(mc)$ (6) $ad \equiv bd(m) \Rightarrow a \equiv b\left(\frac{m}{(m,d)}\right)$

Az $\{a_1, a_2, \ldots, a_m\} \subset Z$ halmaz *teljes maradékrendszer modulo* m (röviden *tmr mod* m), ha minden mod m maradékosztályból pontosan egy elemet tartalmaz, azaz $a_i \equiv a_j(m) \Rightarrow i = j$. (Pl. $\{1, 2, \ldots, m\}$)

Az $\{a_1, a_2, \ldots, a_n\} \subset Z$ halmaz *redukált maradékrendszer modulo* m (röviden *rmr mod* m), ha minden m-hez relatív prím mod m maradékosztályból pontosan egy elemet tartalmaz. (Pl. az m-nél kisebb, m-hez relatív prím természetes számok.) Az m szerinti rmr mérete $\varphi(m)$. (*Euler-féle* φ *függvény.*)

Tétel: Ha $\{a_1, a_2, \ldots, a_m\}$ rmr mod m, és $(b, m) = 1$, akkor $\{ba_1, ba_2, \ldots, ba_m\}$ is rmr mod m.
Euler-Fermat tétel: $(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1(m)$. **Kis Fermat tétel:** p prím, $a \in Z \Rightarrow a^p \equiv a(p)$.
Tétel: Ha p prím, akkor (1) $\varphi(p) = p - 1$, (2) $\varphi(n) = (p-1)p^{\alpha-1}$.
(3) $(a, b) = 1 \Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$. (4) Ha $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, akkor $\varphi(n) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$.
Wilson tétel: $(p-1)! \equiv -1(p)$, ha p prím; $(n-1)! \equiv 0(n)$, ha $n > 4$, összetett.
Tétel (lineáris kongruenciák megoldása): Az $ax \equiv b(m)$ kongruencia megoldható $\iff (a, m) \mid b$. Ekkor (a, m) db maradékosztály modulo m a megoldás. Ha $(a, m) = 1$, akkor a fenti kongruencia megoldása $x \equiv a^{\varphi(m)-1}b(m)$.

Feladatok

1. Tudjuk, hogy ha az 10794 és 14890 számokat elosztjuk ugyanazzal a háromjegyű számmal, akkor ugyanazt a maradékot kapjuk. Mi ez a maradék?

2. Melyik az a legkisebb n pozitív egész szám, amire $3 \nmid n$ és n pozitív osztóinak száma $d(n) = 12$?

3. Legyen $k \geq 2$ és jelölje $(a_1, a_2, \ldots, a_k)$ az $a_1, a_2, \ldots, a_k$ számok legnagyobb közös osztóját, $[a_1, a_2, \ldots, a_k]$ pedig az $a_1, a_2, \ldots, a_k$ számok legkisebb közös többszörösét. Mutassuk meg, hogy $(a_1, a_2, \ldots, a_k) \cdot [a_1, a_2, \ldots, a_k] = a_1 \cdot a_2 \cdot \ldots \cdot a_k$ akkor és csak akkor áll fönn minden pozitív egészekbol álló szám k-asra, ha $k = 2$. (ZH '02)

4. Legyen n olyan páratlan egész szám, amelyik egyetlen prím négyzetével sem osztható. Bizonyítsuk be, hogy n pozitív osztóinak átlaga egész. (ZH '03)

5. A Fibonacci sorozat elemei $F_1 = 0, F_2 = 1$ és $i \geq 2$-re $F_i = F_{i-1} + F_{i-2}$. Bizonyítsuk be, hogy $i \geq 1$ esetén F_i és F_{i+1} relatív prímek. Határozzuk meg az F_i és F_{i+2} legnagyobb közös osztóját is!

6. Határozzuk meg az $n! + k$ és az $(n+1)! + k$ számok legnagyobb közös osztóját.

7. Legyen az n pozitív egész szám prímtényezős felbontása $n = \Pi_{i=1}^{k} p_i^{\alpha_i}$. Mennyi a $\sum_{d|n} \frac{1}{d}$ érték, vagyis hogyan számítható ki az n szám osztói reciprokának az összege? (V '99)

8. Határozzuk meg a $3, 8, 17, -17, 120, 54, -40, 236, 227$ számok legkisebb nemnegatív maradékait, legkisebb abszolút értékű maradékait ill. az egymással kongruenseket modolo 11.

9. Oldogassunk lineáris kongruenciákat. Pl: (a) $27x \equiv 15(60)$, (b) $19x \equiv 15(60)$
(g) $49^{49}x \equiv 3(15)$ (h) $3^{80}x \equiv 23(100)$

10. Oldjunk meg szimultán kongruenciákat is:
$x \equiv 3(5), x \equiv 4(7)$, avagy $y \equiv 6(8), y \equiv 2(4)$ ill. $3z \equiv 2(4), 2z \equiv 4(5)$.

11. Most bánjunk el néhány diofantikus egyenlettel: $15x + 13y = 19$; $17x + 11y = 22$; $12x + 30y = 26$.

12. Zebulonnak számos külföldi pénzérméje van, de a kedvencei az NDK márka és a szovjet rubel. Még azt is kiszámította, hogy a hivatalos 17 Ft= 1 rubel ill. 7 Ft = 1 márka árfolyamon a két valutában tartott vagyona pontosan 179 Ft-ot ér. Mekkora vásárlóerővel bír Zebulon külön-külön e két valutanemben, ha tudjuk, hogy se kopejkája, se pfennigje sincs apróban?

13. Szörnyű baleset történt: Zebulon kishúga megkaparintotta a Nokiás Dobozt, amiben Zebulon a legkedvesebb 555 pénzérméjét tartotta. Sajnos nézegetés közben a legnagyobb odafigyelés ellenére is szétszóródott a doboz tartalma. Az ordítás és hajcibálás elültével sikerült az ágy mögül, szekrény alól és egyéb ritkán takarított helyekről összeszedni a kollekció egy részét, de Zebulon már nem volt megfelelő idegállapotban ahhoz, hogy meg is számolja a zsákmányt. E helyett csak arra volt képes, hogy 10-esével, 12-esével és 7-esével csoportosítsa a gyűjtemény megtalált részét. Az első esetben egy, a másodikban 3, míg a harmadik próbálkozásra 5 érme maradt ki. Hány érme rejtőzik még a szobában Zebulon kedvencei közül?

14. Pataki Ferenc fejszámolóművész egyszer a tévében a következő trükköt mutatta be: felkért a közönségből valakit, hogy gondoljon egy háromjegyű számra, szorozza meg 563-mal, majd az eredmény utolsó három jegyét közölje. Ebből ő pillanatok alatt kitalálta a gondolt számot. Vajon hogyan csinálta?

15. Számítsuk ki a $\varphi(533)$, $\varphi(2007)$ és $\varphi(540)$ értékeket.

16. Bizonyítsuk be, hogy $11 \mid n^{11} + 10n$ és $42 \mid n^7 - n$ teljesül tetszőleges $n \in N$ esetén.

17. Bizonyítsuk be, hogy tetszőleges $h_1, h_2, \ldots, h_k$ pozitív egészekre és p prímszámra fennáll, hogy $(h_1 + h_2 + \ldots + h_k)^p \equiv h_1^p + h_2^p + \ldots + h_k^p (\text{mod } p)$. (ZH '02)

18. Milyen maradékot ad a 31-gyel osztva, ha $a^{100} \equiv 5 (\text{mod } 31)$ és $a^{101} \equiv 19 (\text{mod } 31)$? (V '00)

19. Mi a 403^{402} utolsó három, a $29^{39^{49}}$ utolsó két és a $7^{6^{5^{4^{3^2}}}}$ szám utolsó jegye tízes számrendszerben?

20. Milyen maradékot ad 59^{99} 101-gyel osztva? (ZH '03)

21. Mi az utolsó három jegye a $999^{777^{8888}}$ számnak? Mi az utolsó két jegye az $1997^{2001^{2005}}$ számnak?

22. Bb: ha $p > 5$ prím, akkor az $1, 11, 111, \ldots$ számok között végtelen sok többszöröse van! (ZH '01)

23. Bb: $17 | 2002^{2002} + 1$ (ZH '02)

24. Legyenek m és n pozitív egészek, továbbá $m \mid n$. Bizonyítsuk be, hogy $\varphi(m) \mid \varphi(n)$. (ZH '00)

25. Mely $m \in N$-re és p prímre lesz $\varphi(m) = \varphi(p)$? (ZH '01)

26. Mely n számokra lesz $\varphi(n)$ prímszám? Hát aztán mikor lesz $\varphi(n)$ páratlan? (ZH '99)

27. Mely n természetes számokra igaz, hogy $\varphi(5n) + \varphi(3n) = 7\varphi(n)$? (ZH '03)

28. Bb: ha $d \mid n$, akkor $d - \varphi(d) \leq n - \varphi(n)$. (V '00)

29. Bb: $\sum_{0<i<n,\ (i,n)=1} i = \frac{n \cdot \varphi(n)}{2}$, ha $n > 1$, egész. (V '99)

30. Ha $r_1, r_2, \ldots, r_{\varphi(n)}$ redukált maradékrendszer modulo n, akkor $\sum_{i=1}^{\varphi(n)} r_i \equiv 0 (\text{mod } n)$. (V '00)