Bevezetés a számításelméletbe II.

11. gyakorlat, 2014. április 22.

kis Fermat tétel, Euler-Fermat tétel, csoportelmélet

Tudnivalók

Az április 29-i gyakorlatokat Ács Bernadett, a május 6-i gyakorlatokat Sali Attila helyettesíti. A második ZH-kkal kapcsolatban reklamálni Fleiner Tamásnál (IB 136, fleiner@cs.bme.hu) lehet, vagy május 13-án nálam.

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.

Az $f : H^n \to H$ függvény a H halmazon értelmezett *n-változós művelet.*

0 változós művelet N-en az, hogy 42. Egyváltozós művelet az $f(x) = x^2+1$ a Z-n. Kétváltozós művelet R-en az összeadás, ahol $+(x, y)$ helyett $x+y$-t írunk. Nem művelet N-en a kivonás, mert pl a $0-1$ kivezet a halmazból. (R-en már művelet!) Nem művelet a vektor skalárral való szorzása, mert az összeművelt elemek nem ugyanabból a halmazból vannak. Nem művelet a vektorok skaláris szorzása sem, mert az eredmény nem vektor. Művelet viszont az $R \to R$ függvények kompozíciója, amire $(f \circ g)(x) := f(g(x))$ vagy a húsvéti nyulak halmazán az, ami két nyúlhoz a nehezebbiket rendeli.

A kétváltozós $\star$ művelet *kommutatív (felcserélhető)*, ha $a \star b = b \star a$ tetsz. a, b-re.

Kommutatív a szorzás és az összeadás R-n, nem kommutatív a kivonás és a fvkompozíció.

A $\star$ művelet *asszociatív (átzárójelezhető)*, ha $(a \star b) \star c = a \star (b \star c)$ tetsz. $a, b, c \in H$-ra.

Asszociatív az összeadás, szorzás, függvénykompozíció. Nem asszociatív a pozitív egészek hatványozása, vagy a számtani közép, mint kétváltozós művelet.

Az $\langle S, \star \rangle$ algebrai struktúra *félcsoport*, ha $\star$ asszociatív, *Abel-félcsoport*, ha kommutatív is.

Az $\langle R, + \rangle$ és $\langle R \backslash \{0\}, \cdot \rangle$ Abel-félcsoportok. A valós függvények is félcsoportot alkotnak a kompozícióra.

A H alaphalmaz e eleme a $\star$ művelet *egységeleme*, ha $e \star a = a \star e = a$ tetsz. $a \in H$ elemre.

A szokásos összeadás egységeleme a 0, a szorzásé az 1, a függvénykompozícióé az identikus $f(x) = x$ függvény.

a^{-1} az a *elem inverze*, ha $a \star a^{-1} = a^{-1} \star a = e$ tetsz. a elemre (ahol e az egységelem).

Összeadásnál az inverz az ellentett, szorzásnál a reciprok, kompozíciónál az inverz leképezés, ha van.

Az egységelem és az inverz (ha létezik) egyértelmű.

$\langle G, \cdot \rangle$ *csoport*, ha (1) G félcsoport, (2) létezik $e \in G$ egység, és (3) minden elemnek létezik inverze. A G csoport *Abel-csoport*, ha a $\cdot$ csoportművelet kommutatív. A $(G, \cdot)$ csoport *rendje* $|G|$.

Konvenció: A $\langle G, \cdot \rangle$ csoportot, ha világos, hogy a művelet a szorzás, akkor G-vel jelöljük.

Az R az összeadásra Abel-csoportot alkot. Hasonlóan, $Q \setminus \{0\}$ (vagy $R \setminus \{0\}$) is a szorzásra. A modulo n maradékosztályok Z_n halmaza Abel-csoport az összeadásra, az n-hez relatív prím modulo n maradékosztályok Z_n^* halmaza pedig a szorzásra.

Feladatok

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

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

3. 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)

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

5. 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?

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

7. Mennyi maradékot ad 2010-zel osztva 49^{1585}? (ZH '10)

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

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

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

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

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

13. Mennyi maradékot ad 3^{2011}-nel osztva $100^{3^{2011}}$? (ZH '11)

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

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

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

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

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

19. Pataki Ferenc fejszámolóművész egyszer a tévében a következő trükköt mutatta be: felkért a közönségből valakit, hogy gondoljon egy háromjegyű számra, szorozza meg 667-tel majd az eredmény utolsó három jegyét közölje. Ebből ő pillanatok alatt kitalálta a gondolt számot. Vajon hogyan csinálta?

20. Legyen $p > 2$ olyan prímszám, amelyre $2p+1$ is prím. Bizonyítsuk be, hogy ekkor fennáll az alábbi kongruencia: $(p-1)^{(p-2)^{p-1}} \equiv p - 1(2p + 1)$. (ZH '12)

21. Művelet-e egy H alaphalmaz részhalmazain az unió? Ha igen, akkor kommutatív ill. asszociatív-e? Van-e egységelem és inverz? Ugyanez a kérdés a szimmetrikus különbségre, aholis $A \nabla B := (A \setminus B) \cup (B \setminus A)$.

22. Ha G csoport és $a, b \in G$, akkor hogyan lehet az $(ab)^{-1}$ inverzelemet meghatározni a^{-1} és b^{-1} segítségével?

23. Állapítsuk meg, csoportot alkot-e a $H := \{0, 1, 2, \ldots, n-1\}$ halmaz a modulo n összeadásra ill. a modulo n szorzásra. Van-e a H halmaznak olyan nemtriviális részhalmaza, amin az említett műveletek csoportot alkotnak?

24. Legyen $n \geq 4$, H az n hosszú 0/1 sorozatok halmaza, H_2 a páros sok 1-est tartalmazó, H_3 a hárommal osztható számú egyest tartalmazó H-beli elemek halmaza. Legyen H-n a művelet az elemenkénti mod 2 összeadás. Csoport-e H_2 ill. H_3 erre a műveletre? (ZH '01)

25. Legyen $a * b := ab + a + b$. Bizonyítsuk be, hogy $Q \setminus \{-1\}$ csoport a $*$ műveletre nézve!

26. Legyen H az $x \mapsto ax + b$ alakú függvények halmaza, ahol $a \neq 0$. Csoport-e H a kompozícióra? (ZH '99)

27. Értelmezzük a térvektorok R^3 halmazán a $*$ műveletet a következoképpen: $(a, b, c) * (d, e, f) = (a + d, b + e, ae + c + f)$ Döntsük el, hogy R^3 csoportot alkot-e $*$-ra nézve! (ZH '11)

28. Legyen $H = \{(a, b, c) : a, b, c \in R, a \neq 0, b \neq 0\}$, vagyis H a térnek azokból a vektoraiból áll, amelyeknek az első két koordinátája nem 0. Értelmezzük H-n a $*$ műveletet a következőképpen: $(a, b, c) * (d, e, f) = (ad, be, af + ce)$ (így tehát például $(1, 2, 3) * (4, 5, 6) = (4, 10, 21)$.) Döntsük el, hogy H csoportot alkot-e $*$-ra nézve! (ZH '12)

29. Legyen H Abel-csoport a szorzásra. Mi lesz $\prod_{h \in H} h^2$?

30. Legyen G csoport, $g \in G$ és $H := \{h \in G : g \cdot h = h \cdot g\}$. Mutassuk meg, hogy $H \leq G$.

31. Legyen G Abel-csoport, $0 < k$ és $U := \{g^k : g \in G\}$. Bizonyítsuk be, hogy ekkor $U \leq G$! (V '99)

32. Írjuk fel D_{2n} szorzótábláját!

33. Hány olyan g eleme van a C_n ciklikus csoportnak, amire $\langle g \rangle = C_n$? (V '99)

34. A C_n csoport összes elemének négyzetét összeszorozzuk. Mit kapunk? (V '99)

35. Állapítsuk meg, hogy izomorf-e a mod 4 maradékosztályok additív csoportja (azaz $\langle Z_4, + \rangle$) a mod 8 redukált maradékosztályok multiplikatív csoportjával (azaz a $\langle Z_8^*, \cdot \rangle$ csoporttal). (ZH '02)

36. Hány különböző részcsoportja van a C_{2002} ciklikus csoportnak? (V '00)

37. Igaz-e, hogy ha egy legalább 2 rendű G csoportnak nincs valódi részcsoportja, akkor $G \cong C_p$, ahol p prím? (ZH '02)

38. Legyen $G = \{1, 5, 7, 11\}$, a művelet pedig a mod 12 szorzás. Csoport-e G? Ciklikus-e G? (V '01)