Mat-tanári gyakorlat, első évfolyam, második félév
Nyolcadik alkalom

Legyen p prím és $(a, p) = 1$. Az a *kvadratikus maradék mod* p, ha belőle vonható négyzetgyök mod p, ellenkező esetben *a kvadratikus nemmaradék.* Az Euler-lemma szerint ha p páratlan, akkor $a^{(p-1)/2} \equiv 1\ (p)$ ha a kvadratikus maradék, és $\equiv -1$ ha nemmaradék.

1. *Határozzuk meg a $\mathbb{Z}_n^\times$ csoport összes elemének a rendjét, ha $n = 2, 3, 4, 5, 6, 8, 9, 12, 24$.*

2. *Legyenek a, n, m pozitív egészek, és $d = (a^n - 1, a^m - 1)$. Mutassuk meg, hogy $o_d(a) \mid n$, és hogy $(a^n - 1, a^m - 1) = a^{(n,m)} - 1$.*

3. *Keressünk primitív gyököt mod 19, majd oldjuk meg az $x^{300} \equiv 11\ (19)$ kongruenciát.*

4. *Legyen g primitív gyök mod p, ahol $p > 2$ prímszám. Igazoljuk az alábbi állításokat.*

a) *A -1 szám g alapú indexe $(p-1)/2$.*

b) *Legyen $(a, p) = 1$, és ℓ az a szám g alapú indexe. Az a pontosan akkor kvadratikus maradék mod p, ha ℓ páros, és pontosan akkor primitív gyök, ha ℓ relatív prím $p-1$-hez.*

c) *A modulo p primitív gyökök száma $\varphi(p-1)$, a kvadratikus maradékoké és nemmaradékoké egyaránt $(p-1)/2$.*

d) *Adjunk a fentiek felhasználásával közvetlen bizonyítást az Euler-lemmára.*

5. *Legyen p páratlan prím. Lehet-e egy primitív gyök kvadratikus maradék modulo p? Lehet-e két primitív gyök szorzata is primitív gyök modulo p?*

6. *Mutassuk meg, hogy a^4+1 minden páratlan prímosztója $8k+1$ alakú. Mit mondhatunk $a^4 - a^2 + 1$ prímosztóiról? A Dirichlet-tétel mely speciális esetét lehet ezekből megkapni?*

Feladatok az elméleti anyaghoz

Ha R gyűrű, akkor R^+ jelöli azt a csoportot, amit R elemei az összeadásra alkotnak (ez R *additív csoportja*). Ha R egységelemes, akkor $R^\times$ jelöli az R invertálható elemeinek a csoportját a szorzásra (ez R *multiplikatív csoportja*).

7. *Mutassuk meg, hogy $R^\times$ tényleg csoport.*

8. *Legyen G csoport, $g, h \in G$, $m, n \in \mathbb{Z}$. Igazoljuk az alábbiakat (az inverzet $^{-1}$ jelöli).*

a) *Ha $n > 0$, akkor $(g^n)^{-1} = (g^{-1})^n$ (definíció szerint ez g^{-n}).*

b) *$g^{n+m} = g^n g^m$ és $g^{nm} = (g^n)^m$.*

c) *Ha $gh = hg$, akkor $(gh)^n = g^n h^n$.*

d) *Ha a g* **egész** *kitevős hatványai között van két egyenlő, akkor g-nek csak véges sok különböző hatványa van. (Ezek száma $o(g)$, a g rendje, egyébként $o(g) = \infty$.)*

e) *Ha $o(g)$ véges, akkor $g^n = g^m \iff o(g) \mid n - m$, és $o(g^n) = o(g)/(o(g), n)$.*

9. *Vezessük le az Euler-lemmából az $x^2 \equiv -1$ kongruencia megoldhatóságáról szóló tételt.*

10. *Mutassuk meg, hogy ha p prím, akkor az $x^k \equiv a\ (p)$ akkor és csak akkor oldható meg, ha $(k, p-1)$ osztja az a szám indexét (bármelyik mod p primitív gyökre nézve).*

11. *Adjunk új bizonyítást a Wilson-tételre a primitív gyök létezésének felhasználásával.*

Fordíts!

12. *A mod p primitív gyök létezésének bizonyítását módosítva igazoljuk, hogy minden T véges testnek van olyan eleme, melynek hatványaként T minden nem nulla eleme előáll.*

Gyakorló feladatok

13. *Határozzuk meg a g elem rendjét a G csoportban, ha (g, G) rendre $(-1, \mathbb{R}^+)$, $(-1, \mathbb{R}^\times)$, $(17, \mathbb{Z}_{19}^+)$, $(17, \mathbb{Z}_{19}^\times)$, $(17, \mathbb{Z}_{32}^+)$, $(17, \mathbb{Z}_{32}^\times)$, $(x+1, \mathbb{Z}_{11}[x]^+)$, $(5, \mathbb{Z}_{11}[x]^\times)$.*

14. *Keressünk primitív gyököt mod p, készítsük el a logaritmus (index) táblázatot, majd oldjuk meg az $x^n \equiv b\ (p)$ kongruenciát, ha (n, b, p) rendre $(4, 2, 11)$, $(7, 42, 43)$, $(10, 5, 37)$, $(10, 7, 17)$, $(14, 8, 17)$ (vö. Sárközy-Surányi 15/1, 16/29).*

15. *Mely p prímekre lesz $o_p(2) = 6$?*

16. *Tudjuk, hogy $c^{54} \equiv -1\ (109)$, és $c^{36} \not\equiv 1\ (109)$. Mennyi $o_{109}(c)$?*

17. *Gondoltam egy számot 200 és 2000 között. Ha a szám 501-edik és 201-edik hatványának összegéhez még a számot is hozáadjuk, az eredmény 998-ra végződik. Mire gondoltam?*

18. *Igazoljuk, hogy minden n egészre $930930 \mid n^{61} - n$.*

19. *Igazoljuk, hogy ha p prím és $o_p(a) = 3$, akkor $o_p(1 + a) = 6$.*

20. *Mely páratlan prímekre van olyan primitív gyök, melynek ellentettje is az?*

21. *Melyek azok a prímek, melyekre a kvadratikus nemmaradékok épp a primitív gyökök?*

22. *Igazoljuk, hogy ha p prím és g primitív gyök mod p^n, akkor g primitív gyök mod p.*

23. *Mi $49^{49^{50}}$ utolsó két jegye a tizes számrendszerben?*

43. *Határozzuk meg $43^{43^{\cdot^{\cdot^{43}}}}$ illetve $(\dots((43^{43})^{43})\dots)^{43}$ utolsó számjegyét a 49 alapú számrendszerben. Mindkét kifejezésben 43 darab 43 szerepel.*

24. *Adjuk meg azt a két polinomot $\mathbb{Z}_p$ felett, melynek gyökei a kvadratikus maradékok, illetve nemmaradékok. Határozzuk meg ennek alapján a kvadratikus maradékok illetve nemmaradékok összegét és szorzatát.*

25. *Mennyi egy véges test elemeinek összege? És a nem nulla elemek szorzata?*

Vegyes feladatok ínyenceknek

26. *A tizes számrendszerben $n > 1$ darab 1-esből álló szám lehet-e négyzetszám?*

27. *Igazoljuk, hogy ha $n > 1$ egész, akkor $2^n - 1$ nem lehet teljes hatvány.*

28. *Mely páros tökéletes számok állnak elő két relatív prím n-edik hatvány összegeként?*

29. *Határozzuk meg a primitív n-edik egységgyökök szorzatát és összegét, majd a primitív gyökök szorzatát és összegét modulo p.*

30. *Mutassuk meg, hogy ha $a, n > 1$ egészek, akkor $n \mid \varphi(a^n - 1)$. Ezt és a φ képletét felhasználva lássuk be a Dirichlet-tételt a $pk + 1$ esetre, ha p prím.*

31. *Mely n pozitív egészekre igaz, hogy $n \mid 2^n - 1$?*

32. *Legyen p prím. Igazoljuk, hogy $x^4 + 1$ és $x^4 - 10x^2 + 1$ nem irreducibilis $\mathbb{Z}_p$ felett. (Használjuk fel, hogy két kvadratikus nemmaradék szorzata kvadratikus maradék.)*