Bsc Algebra és számelmélet gyakorlat

A 28. előadás-diához tartozó feladatsor feladatainak megoldásai

1. Határozzuk meg az alábbi elemrendeket: $o_7(2)$, $o_7(3)$, $o_{17}(3)$, $o_{128}(5)$, $o_{25}(2)$, $o_{100}(3)$. □

Használni fogjuk, hogy az elemrend minden „jó" kitevőnek osztója, speciálisan $\varphi(n)$-nek is. Ezért $o_7(a) \mid \varphi(7) = 6$. A 2 hatványai 2, 4, $2^3 = 8$, utóbbi az első, ami 1-et ad maradékul 7-tel osztva, ezért $o_7(2) = 3$. A három hatványai 3, 9, $3^3 = 27$, ezek egyike sem kongruens 1-gyel mod 7. Ezért $o_7(3) > 3$, de osztója 6-nak, és így csak 6, lehet, azaz a 3 *primitív gyök* mod 7. Hasonlóan $o_{17}(3) \mid \varphi(17) = 16$, azaz 2-hatvány. Ezért elég kiszámolni a 2-hatványadik hatványait, ami ismételt négyzetre emeléssel lehetséges: $3^2 = 9$, $3^4 = 9^2 = 81 \equiv -4$ (17), végül $3^8 \equiv (-4)^2 \equiv -1$ (17). Ezért 16 a legkisebb jó kitevő, azaz $o_{17}(3) = 16$, ez is primitív gyök. Mivel $\varphi(128) = 64$ is 2-hatvány, itt is ismételt négyzetre emeléssel számolhatunk, az eredmény $o_{128}(5) = 32$. A 25 esetében $\varphi(25) = 20$ már nem 2-hatvány. Itt azt kell észrevenni, hogy a 20 szám valódi osztói mind osztói vagy $20/2 = 10$-nek, vagy $20/5 = 4$-nek, ezek az úgynevezett *maximális osztók*. Ezért ha $o_{25}(2)$ kisebb lenne 20-nál, akkor osztója lenne 10-nek vagy 4-nek, és akkor 2^4 vagy 2^{10} kongruens lenne 1-gyel mod 25. De sem $2^4 = 16$, sem $2^{10} = 1024$ nem ilyen, és ezért $o_{25}(2) = 20$, ez is primitív gyök. Végül $\varphi(100) = 40$, aminek a maximális osztói 8 és 20. Modulo 100 számolva ismételt négyzetre emeléssel $3^8 \equiv 61$ (100), $3^{10} \equiv 61 \cdot 9 \equiv 49$ (100), és ismét négyzetre emelve $3^{20} \equiv 1$ (100). Vagyis $o_{100}(3)$ nem osztója sem 8-nak, sem 10-nek, de 20-nak igen, és ezért csakis 20 lehet, ez nem primitív gyök.

2. Adjunk meg olyan számot, ami egyszerre primitív gyök modulo 11 és modulo 14 is. □

Az előző feladat módszerével 2 primitív gyök mod 11 és 5 primitív gyök mod 14 (rendjük 10, illetve 6). Tehát az az x szám jó lesz, amire $x \equiv 2$ (11) és $x \equiv 5$ (14). A kínai maradéktétel alapján egyértelmű megoldás van modulo $11 \cdot 14$. Végigszámolva $x = 101$ megfelelő.

3. Keressünk primitív gyököt mod 23, készítsünk logaritmus-táblázatot, majd oldjuk meg a $11x^{17} \equiv 3$ (23) és a $4 \cdot 9^x \equiv 16$ (23) kongruenciákat. □

Némi próbálgatással kiderül, hogy az 5 primitív gyök lesz mod 23, a táblázat:

5	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
5^n	1	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14

(ha alulról fölfelé olvassuk, akkor ez az 5 alapú diszkrét logaritmus táblázata mod 23.) Először „leosztunk" 11-gyel, azaz megoldjuk a $11z \equiv 3$ (23) kongruenciát. A tanult módszerrel azt kapjuk, hogy $z \equiv 17$ (23). Utána vesszük az $x^{17} \equiv 17$ (23) kongruencia 5 alapú logaritmusát, az eredmény $17y \equiv 7$ (22), ahol $y = \log_{5,23}(x)$, hiszen a táblázat alapján $\log_{5,23}(17) = 7$. Ezt a lineáris kongruenciát ismét a hagyományos módszerrel megoldjuk, az eredmény $y \equiv 3$ (22). Innen a táblázatból $x \equiv 5^3 \equiv 10$ (23).

A második kongruenciát 4-gyel egyszerűsítjük, ezt szabad, mert $(4, 23) = 1$. A kapott $9^x \equiv 4$ (23) nem binom kongruencia, mert az ismeretlen x a kitevőben van. Logaritmust véve $10x \equiv 4$ (22), azaz $5x \equiv 2$ (11). A megoldás $x \equiv 7$ (11).

4. Hány megoldása van az $x^{18} \equiv 6$ (29) kongruenciának? □

A tanult tétel (lásd 28. előadás-dia, 3. oldal) szerint a kongruencia pontosan akkor oldható meg, ha $6^{28/(18,28)} = 6^{14} \equiv 1$ (29). Ez igaz (valójában $o_{29}(6) = 14$). A tétel szerint a megoldások száma $(18, 28) = 2$ modulo 29. A feladat nem kérdezte a megoldásokat, ha valaki gyakorolni akar, akkor a 2 primitív gyök mod 29, és a megoldások $x \equiv 3, 26$ (29).

5. Mely p prímszámokra és k és a természetes számokra teljesül, hogy az $x^k \equiv a\ (p)$ kongruenciának pontosan $p-2$ megoldása van? □

Ha $(a,p)=1$, akkor az iménti tétel szerint az $a^{(p-1)/(k,p-1)} \equiv 1\ (p)$ és a $(k,p-1)=p-2$ feltételeknek kell teljesülnie. De $p-2 \mid p-1$ csak $p=3$ esetén lehetséges. Ekkor $(k,p-1)=1$ akkor igaz azaz k páratlan. Teljesülnie kell még az $a^2 \equiv 1\ (2)$ kongruenciának is de ez mindig így van, mert $(\pm 1)^2 = 1$. Ha viszont $p \mid a$, akkor $x \equiv 0\ (p)$ az egyetlen megoldás, ezért $p-2=1$ és $p=3$. Ilyenkor k tetszőleges.

6. Számítsuk ki az alábbi Jacobi-szimbólumokat: $\left(\frac{-99}{207}\right)$, $\left(\frac{1234567}{225}\right)$, $\left(\frac{31}{95}\right)$, $\left(\frac{589}{1999}\right)$, $\left(\frac{1113}{11131}\right)$. □

Minta: 28. előadás-dia, 10. oldal. $\left(\frac{-99}{207}\right)=0$, mert $(-99,207)\neq 1$ (hiszen a 3 közös osztó).
$\left(\frac{1234567}{225}\right)=\left(\frac{-8}{225}\right)=\left(\frac{-1}{225}\right)\left(\frac{2}{225}\right)^3=(-1)^{(225-1)/2}\left((-1)^{(225^2-1)/8}\right)^3=1.$
$\left(\frac{31}{95}\right)=\left(\frac{95}{31}\right)(-1)^{15\cdot 47}=-\left(\frac{95}{31}\right)=-\left(\frac{2}{31}\right)=-(-1)^{120}=-1.$
$\left(\frac{589}{1999}\right)=\left(\frac{1999}{589}\right)=\left(\frac{232}{589}\right)=\left(\frac{2}{589}\right)^3\left(\frac{29}{589}\right)=(-1)^3\left(\frac{589}{29}\right)=-\left(\frac{3^2}{29}\right)=-1.$
$\left(\frac{1113}{11131}\right)=\left(\frac{11131}{1113}\right)=\left(\frac{1}{1113}\right)=1.$

7. Bizonyítsuk be, hogy ha a rendje 3 modulo p (prím), akkor $a+1$ rendje 6. □

Ha a rendje 3, akkor $p \mid a^3-1=(a-1)(a^2+a+1)$, de $p \nmid a-1$, és így $p \mid a^2+a+1$. Legyen $b=a+1$, ekkor $p \mid b^2-b+1=a^2+a+1$. Itt $p\neq 3$, mert mod 3 nincs harmadrendű elem. Ezért alkalmazhatnánk a 27. dia 9. oldalának alján lévő tételt, hiszen x^2-x+1 a hatodik körosztási polinom. Ehelyett direkt bizonyítást adunk: vegyük észre, hogy $b^2=a^2+2a+1\equiv a\ (p)$. A hatvány rendjének képlete miatt $3=o_p(a)=o_p(b^2)=o_p(b)/(o_p(b),2)$. Ezért $o_p(b)$ csak 3 vagy 6 lehet. Azonban ha $p \mid b^3-1=(b+1)(b^2-b+1)+2$, akkor $p \mid 2$, ami nem lehet, mert $p \mid b^2-b+1$, ami páratlan.

9. Igazoljuk az elemrend felhasználásával is, hogy $(a^n-1,a^m-1)=a^{(n,m)}-1$. □

Legyen $d=(a^n-1,a^m-1)$. Ekkor $d \mid a^n-1$ és ezért $a^n \equiv 1\ (d)$, azaz n jó kitevője a-nak mod d, és így $o_d(a) \mid n$. Hasonlóan $o_d(a) \mid m$. Ezért $o_d(a) \mid (n,m)$, azaz (n,m) is jó kitevő, és így $d \mid a^{(n,m)-1}$. A másik irányú oszthatóság nyilvánvaló, de itt is lehet használni az elemrendet: legyen $c=a^{(n,m)-1}$, ekkor $o_c(a) \mid (n,m) \mid n$, ezért $c \mid a^n-1$. Hasonlóan $c \mid a^m-1$, és ezért $c \mid (a^n-1,a^m-1)$.

10. Legyenek $1<a,n$ egészek. Igazoljuk, hogy $n \mid \varphi(a^n-1)$. □

Mivel $(a,a^n-1)=1$, elég belátni az Euler–Fermat-tétel miatt, hogy $o_{a^n-1}(a)=n$. Nyilván $a^n-1 \mid a^k-1$ ha $k=n$, de ha $k<n$, akkor nem, mert ilyenkor $a^n-1>a^k-1$.

11. Adjunk meg egy primitív gyököt modulo 625, és egy olyan számot is, ami modulo 5 primitív gyök, de modulo 625 nem. □

Mod 5 a primitív gyökök 2 és 3 (és minden más is, ami ezekkel kongruens mod 5). A 27. dia 12. és 13. oldalán szerepel, hogy ha g primitív gyök mod 5, akkor g vagy $g+5$ primitív gyök mod 25, és ha g primitív gyök mod 25, akkor primitív gyök minden nagyobb 5-hatványra is. A megfordítás nyilvánvaló: ha g hatványai kiadják a mod 625 redukált maradékosztályokat, akkor kiadják a mod 25 redukált maradékosztályokat is. Ezért mod 25 érdemes vizsgálódni. A 2 rendje 20, a $2+5=7$ rendje 4 mod 25. Ezért a 2 primitív gyök mod 25, a 7 pedig mod 5 igen, mod 625 nem.

13/1. $3x^2+5x+5\equiv 0\ (13)$. □

A $\mathbb{Z}_{13}$ testben használjuk a másodfokú egyenlet megoldóképletét. A négyzetgyök alatti kifejezés $5^2-4\cdot 3\cdot 5=-35\equiv 4\ (13)$. Ennek négyzetgyöke ± 2, a megoldások 1 és 5 mod 13.

13/2. $7x^2+8x\equiv 5\ (17)$; □

Szintén a megoldóképlettel a gyök alatt 0 áll, a kétszeres gyök $x\equiv 14\ (17)$.

13/3. $6x^{25}+x^5+5x\equiv 0\ (23)$; □

A kis-Fermat-tétel miatt $x^{23}\equiv x\ (23)$, ezért x^{25} helyébe x^3 írható. Az $x\equiv 0\ (23)$ megoldás. Egyszerűsítve $6x^2+x^4+5$ adódik, ami x^2-re másodfokú egyenletet ad $\mathbb{Z}_{23}$-ban. A gyökképlettel megoldva $x^2\equiv 18, 22\ (23)$. Mivel 23 egy $4k-1$ alakú prím, a $-1\equiv 22$ nem kvadratikus maradék. A 18 igen, a két négyzetgyöke ± 8, hiszen $64-18=2\cdot 23$. Így három megoldás van.

13/4. $2x^{17}+5x+1\equiv 0\ (19)$. □

Az $x\equiv 0$ nem megoldás, de ha x nem nulla, akkor $x^{18}\equiv 1\ (19)$. Ezért x-szel szorozva az $5x^2+x+2\in\mathbb{Z}_{19}[x]$ polinomot kapjuk. Nincs megoldás, $1^2-4\cdot 5\cdot 2$ nemmaradék mod 19.

---

8. Legyen $p>2$ prím és $(a,p)=1$. Igazoljuk, hogy $o_p(a)$ pontosan akkor páros, ha létezik olyan s, amelyre $a^s\equiv -1\ (p)$. □

Ha $a\equiv g^n\ (p)$, ahol g egy primitív gyök, akkor $o_p(a)=(p-1)/(n,p-1)$ a hatvány rendjének képlete miatt. Mivel $g^{(p-1)/2}\equiv -1\ (p)$, ezért az $a^s\equiv -1\ (p)$ kongruencia g alapú logaritmusát véve $sn\equiv (p-1)/2 \mod (p-1)$ adódik. Ez pontosan akkor oldható meg s-re, ha $(n,p-1)\mid (p-1)/2$, azaz ha $2\mid (p-1)/(n,p-1)$. *Második megoldás:* Ha $o_p(a)=2k$, akkor $(a^k)^2\equiv 1\ (p)$, de $a^k\not\equiv 1\ (p)$. Mivel p prím, az 1-nek csak ± 1 lesz négyzetgyöke, tehát $a^k\equiv -1\ (p)$. Megfordítva, ha $a^s\equiv -1\ (p)$, akkor $a^{2s}\equiv 1\ (p)$, ezért $o_p(a)\mid 2s$, de $o_p(a)\nmid s$. De ha $o_p(a)$ páratlan lenne, akkor $o_p(a)\mid 2s$-ből következne, hogy $o_p(a)\mid s$.

12. Legyen $\alpha\geq 3$. Igazoljuk, hogy $o_{2^\alpha}(5)=2^{\alpha-2}$, illetve hogy a $\{\pm 5^k\mid 0\leq k<2^{\alpha-2}\}$ számok redukált maradékrendszert alkotnak modulo 2^α. □

Ez a Freud–Gyarmati-könyvben a 3.3.12-es feladat, megoldással.

14. Ha p páratlan prím, akkor számítsuk ki az $\left(\frac{1}{p}\right)$, $\left(\frac{2}{p}\right),\dots,\left(\frac{p-1}{p}\right)$ Legendre-szimbólumok összegét és szorzatát. □

Az összeg 0 lesz, hiszen ugyanannyi kvadratikus maradék és nemmaradék van, nevezetesen $(p-1)/2$. A szorzat Wilson tétele miatt $\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$.

15. Bizonyítsuk be, hogy ha $1999\mid a^2+2b^2$, akkor $1999\mid a$ és $1999\mid b$. □

Ha $1999\mid b$, akkor $1999\mid a$. Ha nem, akkor megoldható c-re a $cb\equiv 1\ (1999)$ kongruencia. Ezért $(ac)^2\equiv -2(bc)^2\equiv -2\ (1999)$. De $\left(\frac{-2}{1999}\right)=-1$, ellentmondás.

17. Igazoljuk, hogy egy pitagoraszi számhármas tagjainak a szorzata osztható 60-nal. □

Mivel $3,4,5$ páronként relatív prímek, az általános megoldást felírva elég belátni, hogy ha m és n egyike páros, akkor $3,4,5\mid (m^2-n^2)2mn(m^2+n^2)=2mn(m^4-n^4)$. Nyilván 4-gyel osztható. Osztható 5-tel is, mert ha m és n valamelyike osztható 5-tel, akkor igaz, ha nem, akkor $m^4-n^4\equiv 1-1\equiv 0\ (5)$. Ugyanez működik 3-ra is, mert ha $3\nmid k$, akkor $k^4\equiv 1\ (3)$.