Bsc Algebra és számelmélet gyakorlat

A 9. és 10. előadás-diákhoz tartozó feladatsor feladatainak megoldásai

1. Határozzuk meg az Euklideszi algoritmussal 112 és 301 legnagyobb közös osztóját. Írjuk föl a legnagyobb közös osztót $112x + 301y$ alakban, ahol x és y egész. $\square$

$301 = 2\cdot 112 + 77,\ 112 = 1\cdot 77 + 35,\ 77 = 2\cdot 35 + 7,\ 35 = 5\cdot 7 + 0$. Ezért $(301, 112)$ az utolsó nem nulla maradék, vagyis 7. A visszahelyettesítéseket hátulról előrefelé haladva végezzük: $7 = 77 - 2\cdot 35 = 77 - 2(112 - 77) = 3\cdot 77 - 2\cdot 112 = 3(301 - 2\cdot 112) - 2\cdot 112 = 3\cdot 301 - 8\cdot 112$.

2. Az $(a, b) = au + bv$ előállításban mi u és v legnagyobb közös osztója? $\square$

$(u, v) = 1$, mert $1 = u\cdot\big(a/(a, b)\big) + v\cdot\big(b/(a, b)\big)$, **az** $(ec, ed) = e(c, d)$ **azonosság miatt**.

3. Mely (a, b) természetes számokból álló párokra lesz $ab = 1452$ és $(a, b) = 11$? $\square$

Figyeljünk rá, hogy a feladatban (a, b) az első helyen rendezett párt, a másodikon legnagyobb közös osztót jelöl, ez mindig kontextusfüggő. Az $(ec, ed) = e(c, d)$ azonosság miatt $(a/11, b/11) = 1$, és $(a/11)(b/11) = 1452/(11^2) = 12$. A 12-t két relatív prím természetes szám szorzatára csak úgy lehet felbontani, hogy $3\cdot 4$ vagy $1\cdot 12$. Ezért (a, b) lehet $(33, 44)$, $(44, 33)$, $(11, 132)$, $(132, 11)$.

4. Mely pozitív egész n-ekre igaz, hogy $n - 1 \mid n^2 + 1$? $\square$

$n^2 + 1 = (n + 1)(n - 1) + 2$, ezért $n - 1 \mid 2$, azaz $n = 2$ vagy 3.

6. Határozzuk meg $(n - 1, n^2 + 1)$ és $(n! + 1, (n + 1)! + 1)$ értékét. $\square$

Ha $d \mid n - 1$ és $d \mid n^2 + 1$, akkor $d \mid (n + 1)(n - 1) - (n^2 + 1) = -2$. Ezért a keresett legnagyobb közös osztó csak 1 és 2 lehet. Akkor 1, ha n páros, mert akkor $n - 1$ páratlan. Ha viszont n páratlan, akkor $n - 1$ és $n^2 + 1$ is páros, ezért ebben az esetben az eredmény 2.

Hasonlóan, ha $d \mid n! + 1$ és $d \mid (n + 1)! + 1$, akkor $d \mid (n + 1)(n! + 1) - \big((n + 1)! + 1\big) = n$. Ezért $d \mid n! + 1$ és $d \mid n$ miatt $d = 1$. A második legnagyobb közös osztó tehát 1.

5. Melyik igaz az alábbi állítások közül:

(1) Ha $a \mid 8b + 5c$ és $a \mid 5b + 3c$ akkor $a \mid b$ és $a \mid c$.

(2) Ha $a \mid 2b + c$ és $a \mid b + 2c$ akkor $a \mid b$ és $a \mid c$.

$\square$

(1): $a \mid 3(8b + 5c) - 5(5b + 3c) = -b$. Hasonlóan $a \mid 5(8b + 5c) - 8(5b + 3c) = c$. Tehát (1) igaz. Ez a Gauss-eliminációra hasonlít, elimináltuk c-t, majd b-t.
(2): Most hasonló gondolatmenettel csak az jön ki, hogy $a \mid 3b$ és $a \mid 3c$. Érezhetjük, hogy $a = 3$ is egy lehetőség, és ennek alapján ellenpéldát találhatunk, pl. $b = c = 1$ és $a = 3$ jó, mert $3 \mid 2b + c = 3$ és $3 \mid b + 2c = 3$, de $3 \nmid b = 1$. Ezért (2) hamis.

7. Tudjuk, hogy a $\frac{8n+3}{7n+1}$ tört egyszerűsíthető. Melyik számmal? $\square$

Ha $d \mid 8n + 3$ és $d \mid 7n + 1$, akkor $d \mid 7(8n + 3) - 8(7n + 1) = 13$, ami prím. A számláló és a nevező nem relatív prímek, így legnagyobb közös osztójuk 13. Ez megvalósul pl., ha $n = 11$.

8. Lássuk be, hogy $\frac{a^3+2a}{a^4+3a^2+1}$ nem egyszerűsíthető. $\square$

Ha $d \mid a^3 + 2a$ és $d \mid a^4 + 3a^2 + 1$ közös osztó, akkor $d \mid a^4 + 3a^2 + 1 - a(a^3 + 2a) = a^2 + 1$. De $a^4 + 3a^2 + 1 = a^2(a^2 + 1) + a^2 + (a^2 + 1)$, így $d \mid a^2$, és akkor $d \mid a^4 + 3a^2 + 1$ miatt $d \mid 1$.

9. Igazoljuk, hogy $\sqrt[5]{24}$ és $\log_{12} 78$ irracionálisak. ☐

Tudjuk, hogy $\sqrt[k]{n}$ pontosan akkor racionális, ha egész, és ez pontosan akkor áll, ha n kanonikus alakjában minden prímszám kitevője k-val osztható. Mivel 24 kanonikus alakja $2^3 \cdot 3$, és $5 \nmid 3$, ezért $\sqrt[5]{24}$ irracionális. Tegyük fel, hogy $p/q = \log_{12} 78$, ahol p és q pozitív egészek. Ez azt jelenti, hogy $12^{p/q} = 78$, azaz $12^p = 78^q$. Ez nem lehet, mert $13 \mid 78^q$, de $13 \nmid 12^p$.

10. Adjuk meg egy-egy valódi osztóját a következő két számnak: $7^{21} + 4^{21}$, $2^{1111} - 1$. ☐

Az ismert azonosságok miatt $7 + 4 \mid 7^{21} + 4^{21}$ és $2^{11} - 1 \mid 2^{1111} - 1$ (hiszen $11 \mid 1111$).

11. Melyek oldhatók meg az alábbi egyenletek közül? $x^2 - 4y = 10$, $x^2 + y^2 = 99999999$, $x^2 + y^2 = 100000001$, $x^2 + y^2 = 1001$. ☐

A harmadik egyenletben $x = 10000$ és $y = 1$ megfelelő. Az első két egyenletet vizsgáljuk modulo 4. Páratlan szám négyzete 1-et, párosé nullát ad maradékul. Ezért az első egyenlet bal oldala 0 vagy 1 maradékot adhat, a jobb oldal 2-t. A második egyenlet bal oldala 0, 1, vagy 2 maradékot adhat, a jobb oldal pedig 3-at. Ezért ennek a két egyenletnek nincs megoldása. A negyedik egyenletben ilyen ellentmondást nem kapunk, még sincs megoldása. Ugyanis modulo 7 vizsgálódva négyzetszám 0, 1, 2, 4 maradékot adhat, a jobb oldal viszont 7-tel osztható. Az 1, 2, 4 számok közül semelyik kettő összege nem 7. Ezért csak az a lehetőség marad, hogy $7 \mid x$ és $7 \mid y$. De akkor $7^2 \mid x^2 + y^2 = 1001$, ami ellentmondás.

---

12. Oldjuk meg a pozitív egész számok körében az $x^3 - y^3 = 3^n$ egyenletet. ☐

Nincs ilyen x és y. A megoldás hasonlít a 8. feladatsor 32-es feladatához, csak most az $x^3 - y^3 = (x-y)\big((x-y)^2 + 3xy\big)$ azonosságot kell használni. Ha $n = 0$, akkor $x - y = 1$ és $(x-y)^2 + 3xy = 1$, azaz $xy = 0$, amit kizártunk. Így $3 \mid 3^n = x^3 - y^3$. Ezért ha $3 \mid x$, akkor $3 \mid y$, és megfordítva, tehát az egyenlet 3^3-nel egyszerűsíthető. Ha már $3 \nmid x$ és $3 \nmid y$, akkor $x - y$ nem lehet 1, mert akkor $(x-y)^2 + 3xy$ sem osztható 3-mal. Tehát $3 \mid x - y$, de akkor $9 \nmid (x-y)^2 + 3xy$, hiszen $9 \mid (x-y)^2$, de $9 \nmid 3xy$. Ezért $4 \le (x-y)^2 + 3xy = 3$, ellentmondás.

13. Bizonyítsuk be, hogy n egész szám közül mindig kiválasztható néhány úgy, hogy az összegük osztható n-nel. Igaz-e ez az állítás $n - 1$ darab számra? ☐

Legyenek a számok $a_1, \ldots, a_n$. Ha $b_1 = a_1, b_2 = a_1 + a_2, \ldots, b_n = a_1 + \ldots + a_n$ valamelyike osztható n-nel, akkor készen vagyunk. Ha nem, akkor ezek legfeljebb $n - 1$-féle maradékot adhatnak n-nel osztva (hiszen nullát nem). A skatulyaelv miatt tehát van kettő, ami ugyanazt a maradékot adja, mondjuk b_i és b_j, ahol $i < j$. Ekkor $n \mid b_j - b_i = a_{i+1} + \ldots + a_j$.

Az állítás $n - 1$ számra nem igaz, például ha mindegyik 1 maradékot ad n-nel osztva, akkor akárhányat is adunk össze közülük, az összeg maradéka 1 és $n - 1$ között lesz.

14. Maximum hány szám választható ki az $\{1, 2, \ldots, 2n\}$ halmazból úgy, hogy egyik sem osztója a másiknak? ☐

Kiválasztható n darab, ha az $n + 1, n + 2, \ldots, 2n$ számokat vesszük, az megfelelő. Ennél több nem választható ki. Rendeljük ugyanis hozzá minden számhoz a legnagyobb páratlan osztóját (pl. a 60-hoz a 15-öt). Ha a c és d számokhoz ugyanazt a t páratlan számot rendeljük, akkor $c = 2^k t$ és $d = 2^\ell t$, és így c és d közül valamelyik osztója a másiknak. Ezért ha kiválasztunk számokat úgy, hogy egyik se ossza a másikat, akkor a hozzájuk rendelt páratlan osztók páronként különbözők lesznek. De 1-től $2n$-ig n darab páratlan szám van.

---

15. Mutassuk meg, hogy $n > 0$, $k > 0$, $a > 1$ egészek esetén $(a^n - 1, a^k - 1) = a^{(n,k)} - 1$. $\square$

Indukciót alkalmazunk $n + k$ szerint. Ha $n = k$, akkor az állítás nyilvánvaló, így feltehető, hogy $n > k$. Ekkor $(n, k) = (n - k, k)$, ezért az indukciós feltevés miatt elegendő belátni, hogy $(a^n - 1, a^k - 1) = (a^{n-k} - 1, a^k - 1)$. Nyilván $a^n - 1 = a^k(a^{n-k} - 1) + a^k - 1$. Ha d közös osztója $a^n - 1$-nek és $a^k - 1$-nek, akkor $d \mid a^k(a^{n-k} - 1)$. De d szükségképpen relatív prím a-hoz, hiszen $a^k - 1$-nek osztója, és ezért $d \mid a^{n-k} - 1$. A fordított oszthatóság nyilvánvaló.

20. Legyen f_n a Fibonacci sorozat n-edik tagja ($f_0 = 0$, $f_1 = 1$, és $f_{n+1} = f_n + f_{n-1}$ ha $n \geq 1$). Igazoljuk, hogy $f_{(n,k)} = (f_n, f_k)$. Vezessük le ebből, hogy $f_k \mid f_n$ akkor és csak akkor, ha $k \mid n$ vagy $k = 2$. $\square$

Az előző megoldáshoz hasonlóan járunk el, elég megmutatni, hogy $(f_n, f_k) = (f_{n-k}, f_k)$. Teljes indukcióval igazolható, hogy $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$. Mivel mátrixszorzás asszociatív, $M^{u+v} = M^u M^v$ tetszőleges u, v pozitív egészekre, ahonnan $f_{u+1}f_v + f_u f_{v-1} = f_{u+v}$. Így $f_{n-k+1}f_k + f_{n-k}f_{k-1} = f_n$. Ezért $(f_{n-k}, f_k) \mid f_n$. Megfordítva, ha $d \mid f_k$ és $d \mid f_n$, akkor $d \mid f_{n-k}f_{k-1}$. De k szerinti indukcióval könnyen igazolható, hogy f_{k-1} és f_k relatív prímek, ezért $d \mid f_{n-k}$. Tehát $(f_n, f_k) = (f_{n-k}, f_k)$, és ezzel beláttuk a feladat első állítását.

Így $f_k \mid f_n$ pontosan akkor teljesül, ha $f_{(n,k)} = f_k$. Ezért azt kell belátni, hogy $f_u = f_v$ pontosan akkor teljesül, ha $u = v$, vagy ha u és v egyike 1, a másik 2. Ez nyilvánvaló, mert a Fibonacci-sorozat monoton nő, és ha $f_k = f_{k+1}$, akkor $f_{k-1} = 0$, azaz $k - 1 = 0$.

16. Bizonyítsuk be, hogy ha n természetes szám, akkor $\left(5 + \sqrt{26}\right)^n$ tizedestört alakjában a tizedesvesszőt követő első n jegy egyenlő. $\square$

Belátjuk, hogy $a_n = \left(5 + \sqrt{26}\right)^n + \left(5 - \sqrt{26}\right)^n$ egész szám. Valóban, $a_0 = 2$, $a_1 = 10$, és azonos átalakításokkal könnyen igazolható, hogy $a_{n+1} = 10a_{n+1} + a_n$ minden $n \geq 0$ egészre. De könnyen következik az állítás a *binomiális tételből* is. Viszont $0 < \sqrt{26} - 5 < 1/10$. Ezért ha n páratlan, akkor $\left(5 + \sqrt{26}\right)^n$ tizedestört alakjában a tizedesvesszőt követő első n jegy 0, ha meg n páros, akkor 9-es.

A **17**. Feladat kapcsán *Freud Róbert és Gyarmati Edit: Számelmélet* című könyvének **7.5.1**. Tétele szerint egy pozitív egész pontosan akkor áll elő két négyzetszám összegeként, ha a kanonikus alakjában minden $4k - 1$ alakú prím páros kitevőn szerepel.

18. Mely páratlan p prímekre lesz $\frac{2^{p-1}-1}{p}$ négyzetszám? $\square$

Csak $p = 3$ és $p = 7$ esetén, ekkor a tört értéke 1, illetve 9. Legyen $q = (p-1)/2 \geq 1$. Ekkor $2^{p-1} - 1 = (2^q - 1)(2^q + 1)$. A két tényező relatív prím, mert szomszédos páratlan számok. Ezért az egyik négyzetszám, a másik egy négyzetszám p-szerese. Ha $2^q - 1$ négyzetszám, akkor $4k + 1$ alakú, ezért $4 \nmid 2^q$, azaz $q \leq 1$, így $p = 3$. Ha $2^q + 1 = m^2$, akkor $(m-1)(m+1) = 2^q$, azaz mindkét tényező 2-hatvány. De egyikük nem osztható 4-gyel, hiszen a különbségük 2. Ezért ez a tényező 1 vagy 2. A négy esetet végignézve $m = 3$, ekkor $2^q = 8$, így $p = 7$.

19. Igazoljuk, hogy minden k pozitív egészhez van olyan n, amelyre $\varphi(n) = \varphi(n + k)$. $\square$

Az Euler-függvény képletéből látjuk, hogy ha m minden prímosztója osztója n-nek, akkor $\varphi(mn) = m\varphi(n)$. Legyen p a legkisebb prímszám, ami nem osztója k-nak. Ekkor az előző észrevétel miatt $\varphi\big((p-1)k\big) = (p-1)\varphi(k)$, és ugyanennyi $\varphi(pk) = \varphi(p)\varphi(k) = (p-1)\varphi(k)$ is. A feladat kapcsán érdemes utánakeresni a *Carmichael-sejtésnek* az interneten.