Bevezetés a számításelméletbe II.
Megoldások
9. gyakorlat: Számelmélet bevezető

1. Az euklideszi algoritmussal számolva:

(a) $504 = 372 \cdot 1 + 132$
$372 = 132 \cdot 2 + 108$
$132 = 108 \cdot 1 + 24$
$108 = 24 \cdot 4 + \boxed{12}$
$24 = 12 \cdot 2$

(b) $844 = 612 \cdot 1 + 222$
$612 = 222 \cdot 2 + 168$
$222 = 168 \cdot 1 + 54$
$168 = 54 \cdot 3 + \boxed{6}$
$54 = 6 \cdot 9$

A legkisebb közös többszörösöket megkaphatjuk az $[a, b] = \frac{a \cdot b}{(a,b)}$ összefüggésből.

2. Polinomokon elvégzett euklideszi algoritmussal kapjuk, hogy

(a) $x^3 + 3x^2 + 5x + x = (x^2 + 2x + 2) \cdot (x + 1) + (x + 1)$
$x^2 + 2x + 2 = (x + 1) \cdot (x + 1) + \boxed{1}$
$x + 1 = (x + 1) \cdot 1$

(b) $x^4 + x^3 + x^2 = (x^4 + x^2 + 1) \cdot 1 + (x^3 - 1)$
$x^4 + x^2 + 1 = (x^3 - 1) \cdot x + \boxed{(x^2 + x + 1)}$
$x^3 - 1 = (x^2 + x + 1) \cdot (x - 1)$

3. $a = 50700 = 2^2 \cdot 3 \cdot 5^2 \cdot 13$ és $b = 111384 = 2^3 \cdot 3^2 \cdot 7 \cdot 13 \cdot 17$,
ebből $(a, b) = 2^2 \cdot 3 \cdot 13$ és $[a, b] = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 13 \cdot 17$.
Ahhoz, hogy megkapjuk azt, hogy hány olyan szám van, ami a-t vagy b-t osztja a és b osztóinak összegéből le kell vonnunk a közös osztók számát. Szerencsére tudjuk, hogy a közös osztók egyben osztói (a, b)-nek is. Így az eredmény:
$(2 + 1)(1 + 1)(2 + 1)(1 + 1) + (3 + 1)(2 + 1)(1 + 1)(1 + 1)(1 + 1) - (2 + 1)(1 + 1)(1 + 1) = 120$.

4. Egy páratlan szám négyzete $(2k + 1)^2 = 4k^2 + 4k + 1$, vagyis $4l + 1$ alakú. Két ilyen összege tehát $4k + 2$ alakú lesz, vagyis páros, de nem osztható 4-el.

5. Egy páratlan szám négyzete: $(2k + 1)^2 = 4k^2 + 4k + 1 = (2k)(2k + 2) + 1$ alakú, 8 pedig mindig osztja két egymást követő páros szám szorzatát (mert az egyik biztosan osztható 4-el is).

6. A maradékosztályokat sorra véve adódik, hogy mindegyik esetben csak egy megoldás van:

(a) $p = 3$ jó megoldás, de $p = 3k + 1$ illetve $p = 3k + 2$ esetekben vagy $p + 10$ vagy $p + 14$ oszható lesz 3-mal, vagyis nem lehet prím.

(b) $p = 3$ itt is jó, de a többi esetben 3 osztja $p^2 + 2$-t.

(c) Itt az 5 maradékosztályait kell vizsgálni. $p = 5$ jó megoldás, de a többi esetben vagy $p^2 + 4$ vagy $p^2 + 6$ biztosan 5-el osztható lesz.

7. A Fibonacci-számok a következők: $1, 1, 2, 3, 5, 8, 13, \ldots$. Tehát az n-edik Fibonacci számot az előtte lévő kettő összegeként kapjuk: $a_n = a_{n-1} + a_{n-2}$.
   Ha két szomszédos Fibonacci-szám nem volna relatív prím, ez azt jelentené, hogy létezik olyan $c \neq$ egész, hogy $c|a_n$ és $c|a_{n-1}$. De ekkor $c|a_{n-2}$ is igaz volna (hiszen két számnak egy közös osztója osztja a két szám különbségét is). Ez pedig azt jelentené, hogy visszamenőleg c osztaná az összes Fibonacci-számot, még az 1-et is.
   Másodszomszédos Fibonacci-számokra a helyzet hasonló. Ha $c|a_n$ és $c|a_{n-2}$, akkor $c|a_{n-1}$ is igaz. Ezután viszont az előzőekből következik, hogy c minden Fibonacci-számot oszt.

8. Ha a Péter születési évszáma b pedig a nagyapjáé, akkor tudjuk, hogy $a-b = 53$ és $1 \neq (a, b)$. Ha viszont létezik egy $1 < c|(a, b)$, akkor $c|(a-b) = 53$ is igaz, amiből $c = 53$ adódik. Mivel $53|a$ és $53|b$, és $1950 < a < 2000$, ezért $a = 37 \cdot 53 = 1961$ lesz Péter születési évszáma.

9. Öt egymást követő szám közül mindig lesz egy 5-el osztható, legalább egy 3-al osztható, legalább egy $4k$ és egy másik $4k+2$ alakú. E miatt a számok szorzata is oszható lesz $2 \cdot 3 \cdot 4 \cdot 5 = 120$-al.

10. Egy szám akkor és csakis akkor négyzetszám, ha a prímtényzős felbontásában minden kitevő páros. Egy tetszőleges n egész szám $n = k^2 q$ alakra való felbontása ebből adódik: ha ebben p_i prím kitevője, $\alpha_i = 2k_i+1$ alakú volt, akkor k-ban p_i kitevője k_i legyen q-ban pedig 1. Ha $\alpha_i = 2k_i$ alakú, akkor k-ban p_i kitevője ismét k_i és q prímtényezős felbontásában ne szerepeljen a p_i prím.

11. Ha n-nek 15 osztója van, vagyis $d(n) = 15$, akkor az osztók számára vonatkozó tételből következően vagy $(\alpha_1 + 1) = 15$ vagy $(\alpha_1 + 1 = 5)$ és $(\alpha_2 + 1 = 3)$ adódik a prímtényzős felbontásában szereplő két kitevőre. Ezek közül a legkisebb felbontás amiben 3 nem szerepelhet: $2^4 \cdot 5^2$.

12. Az előző feladathoz hasonlóan itt is $d(n)$ képletéből adódik, hogy kell legyen n felbontásában egy α_i kitevő, melyre $11|(\alpha_i + 1)$. A legkisebb ilyen szám 2^{10} lenne, ami viszont már nagyobb 1000-nél, tehát megfelelő 3-jegyű számot nem találhatunk.