2. Házi feladat (határidő: 2015-09-25)

A feladatokra teljes megoldást kérünk részletszámításokkal, indoklással, az eredmény leírása nem elegendő. Más megoldását lemásolni nem szabad!

1. Mutassuk meg, hogy $n!+1$-nek mindig van n-nél nagyobb prímosztója! Vezessük le ebből, hogy végtelen sok prímszám van!
2. Bizonyítsuk be, hogy a szomszédos Fibonacci-számok relatív prímek.
3. Bizonyítsuk be, hogy hat egymást követő természetes szám közül mindig kiválasztható egy, amelyik relatív prím az összes többihez.
4. Mutassuk meg, hogy *(a)* $4k+1$ alakú számok szorzata $4k+1$ alakú. *(b)* végtelen sok $4k+3$ alakú prímszám van (Útmutatás: tekintsük a $4p_1p_2\dots p_n - 1$ számot, ahol a p_i prímek mindegyike $4k+3$ alakú.)
5. Határozzuk meg az alábbi számok legnagyobb közös osztóját és legkisebb közös többszörösét! *(a)* $2^{23}3^{10}7^{13}$, $2^{15}7^{10}13^5$; *(b)* $2^{23}3^{10}7^{13}$, $2^{15}7^{10}13^5$, $3^{15}7^{20}11^2$.
6. Számítsuk ki $25^{101} \bmod 11$ értékét!
7. Oldjuk meg a következő lineáris kongruenciákat!
   (a) $4x \equiv 6 \pmod{14}$,
   (b) $4x \equiv 6 \pmod{16}$,
   (c) $4x \equiv 8 \pmod{16}$.
8. Számítsuk ki $3^{-1} \bmod 13$, $3^{-1} \bmod 26$ és $3^{-1} \bmod 52$ értékét!
9. Készítsük el a modulo 12 összeadás és szorzás művelettábláját! Készítsük el a 12-höz relatív prímek és a 8-hoz relatív prímek szorzástábláját!
10. Oldjuk meg az
$$\begin{aligned} x &\equiv 1 \pmod 3\\ x &\equiv 1 \pmod 4\\ x &\equiv 3 \pmod 5\end{aligned}$$
kongruenciarendszert!

Gyakorló feladatok

1. Mutassuk meg, hogy a 2-t kivéve nincs n^3+1 alakú prím ($2 = 1^3+1$)!
2. Igazoljuk, hogy $a \mid c,\ b \mid c \iff [a,b] \mid c$ (mutassunk példát, hogy $a \mid c,\ b \mid c \not\Rightarrow ab \mid c$).
3. Legyen n olyan természetes szám, hogy ha $p \mid n$, akkor $p^2 \mid n$ is igaz. Mutassuk meg, hogy n felírható egy négyzetszám és egy köbszám szorzataként!
4. Legyenek a és k egynél nagyobb egészek. Mutassuk meg, hogy ha $a^n - 1$ prím, akkor $a = 2$ és n prím!
5. Legyenek a és k egynél nagyobb egészek. Mutassuk meg, hogy ha $a^n + 1$ prím, akkor n kettőhatvány!
6. Melyik az a legkisebb n természetes szám, melyre $n^2 - n + 41$ nem prím?
7. Mutassuk meg, hogy bármely pozitív a és b egészhez van olyan m és n egész, hogy $m \mid a$, $n \mid b$, $(m,n) = 1$ és $mn = ab$.
8. Mutassuk meg, hogy $n!$ prímtényezős felbontásában a p prím kitevője
$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots.$$
9. Állítsuk elő $(4864, 3458)$ értékét $4864m + 3458n$ alakban, ahol $m, n \in \mathbb{N}^+$.
10. Oldjuk meg fejben a következő három kongruenciarendszert!
    (a) $x \equiv 1 \pmod 3$
    $x \equiv 1 \pmod 5$
    $x \equiv 1 \pmod 7$
    (b) $x \equiv 2 \pmod 3$
    $x \equiv 4 \pmod 5$
    $x \equiv 6 \pmod 7$
    (c) $x \equiv 1 \pmod 3$.
    $x \equiv 2 \pmod 4$
    $x \equiv 3 \pmod 5$

11. Igazoljuk, hogy egy pozitív egész 9-cel való osztási maradéka megegyezik számjegyei összegének 9-cel való osztási maradékával! Fogalmazzunk meg és igazoljunk egy hasonló állítást a 11-gyel való osztás maradékára! Hogyan általánosíthatóak e szabályok b alapú számrendszer esetén?

12. Igazoljuk, hogy egy pozitív egész pontosan akkor osztható 7-tel (11-gyel, illetve 13-mal), ha a belőle hátulról képzett 3-jegyű számok váltakozó előjelű összege osztható 7-tel (11-gyel, illetve 13-mal). Például 4124729063 osztható 7-tel és 13-mal, de nem osztható 11-gyel, mert $4 - 124 + 729 - 63 = 546$, és $546 = 2 \cdot 3 \cdot 7 \cdot 13$, ami 7-tel és 13-mal osztható, de 11-gyel nem.

13. Mutassuk meg, hogy ha két egymáshoz relatív prím szám szorzata k-adik hatvány, akkor különkülön is k-adik hatványok.

Szorgalmi feladatok

*1 Igazoljuk, hogy ha $a, b \in \mathbb{N}^+$ és $a \bmod b = r$, akkor

(a) $(2^a - 1) \bmod (2^b - 1) = 2^r - 1$,

(b) $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$.

*2 Mutassuk meg, hogy az

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

kongruenciarendszer pontosan akkor oldható meg, ha $(m, n) \mid (a - b)$. Ha a rendszer megoldható, a megoldás egyértelmű modulo $[m, n]$.