1. *Legyen $x \in \mathbb{R}^+$ és $d \in \mathbb{N}^+$. Mutassuk meg, hogy az x-nél nem nagyobb, d-vel osztható pozitív egészek száma $\left\lfloor \frac{x}{d} \right\rfloor$.*

Megoldás: $\left|\{\, m \in \mathbb{N}^+ \mid m \le x,\ d \mid m, \}\right| = \left|\{\, m \in \mathbb{N}^+ \mid \frac{m}{d} \in \mathbb{Z},\ \frac{m}{d} \le \frac{x}{d} \,\}\right| = \left|\{\, k \in \mathbb{N}^+ \mid k \le \frac{x}{d} \,\}\right| = \left|\{\, k \in \mathbb{N}^+ \mid k \le \left\lfloor \frac{x}{d} \right\rfloor \,\}\right| = \left\lfloor \frac{x}{d} \right\rfloor$.

2. *Mutassuk meg, hogy $n!$ prímtényezős felbontásában p kitevője $\displaystyle\sum_{i \ge 1} \left\lfloor \frac{n}{p^i} \right\rfloor$*

Megoldás: Jelöljük $[m]_p$-vel az $m \in \mathbb{Z}$ kanonikus felírásában a p prím kitevőjét! Ekkor $[n!]_p = \displaystyle\sum_{k=1}^{n} [k]_p = \left|\{(k,i) \mid 1 \le k \le n,\ 1 \le i,\ p^i \mid k\}\right| = \sum_{i \ge 1} \left|\{\, k \mid 1 \le k \le n,\ p^i \mid k \,\}\right| = \sum_{i \ge 1} \left\lfloor \frac{n}{p^i} \right\rfloor$ az 1. feladat eredeménye alapján.

3. *Bizonyítsuk be, hogy n, a, b pozitív egészekre $\left\lfloor \frac{n}{ab} \right\rfloor = \left\lfloor \frac{\left\lfloor \frac{n}{a} \right\rfloor}{b} \right\rfloor$.*

Megoldás: Legyen az n maradékos osztása a-val $n = aq + r$, ahol $0 \le r \le a-1$, és q maradékos osztása b-vel $q = bq_1 + r_1$, ahol $0 \le r_1 \le b-1$. Ekkor $n = abq_1 + (ar_1 + r)$, és itt $0 \le ar_1 + r \le ab - a + a - 1 = ab - 1$, tehát ez n maradékos osztása ab-vel. Ebből következik, hogy $\left\lfloor \frac{n}{ab} \right\rfloor = q_1$, míg $\left\lfloor \frac{\left\lfloor \frac{n}{a} \right\rfloor}{b} \right\rfloor = \left\lfloor \frac{q}{b} \right\rfloor = q_1$, tehát igaz az állítás.

4. *Hány nullára végződik* $100!$*?*

Megoldás: Egy n szám pontosan k nullára végződik, ha 10^k osztója az adott számnak, de 10^{k+1} nem. Mivel $10^k = 2^k \cdot 5^k$ relatív prím prímhatványok szorzata, ehhez az kell, hogy $[n]_2$ és $[n]_5$ mindegyike legalább k, de az egyik pontosan k. Az $n = 100!$ esetben $[100!]_2 = \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{2^2} \right\rfloor + \ldots > 50$, míg $[100!]_5 = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor + 0 + 0 + \ldots = 24$, tehát $100!$ pontosan 24 darab 0-ra végződik.

5. *Bizonyítsuk be, hogy a szomszédos Fibonacci-számok relatív prímek.*

Megoldás: Teljes indukcióval bizonyítjuk az állítást. $(f_0, f_1) = (0,1) = 1$ igaz. Tegyük fel, hogy $(f_n, f_{n+1}) = 1$ valamely n-re. Ekkor $(f_{n+1}, f_{n+2}) = (f_{n+1}, f_n + f_{n+1}) = (f_{n+1}, f_n) = 1$ az indukciós feltevés szerint, tehát a következő két Fibonacci-szám is relatív prím egymáshoz.

6. *Mutassuk meg, hogy*

a) $4k+1$ alakú számok szorzata $4k+1$ alakú.

b) végtelen sok $4k+3$ alakú prímszám van (Útmutatás: tekintsük a $4p_1p_2 \ldots p_n - 1$ számot, ahol a p_i prímek mindegyike $4k+3$ alakú.)

Megoldás: a) Elég belátni, hogy két $4k+1$ alakú szám szorzata $4k+1$ alakú, abból már teljes indukcióval következik tetszőlegesen sok tényezős szorzatra is az állítás. $(4k+1)(4\ell+1) = 16k\ell + 4k + 4\ell + 1 = 4(4k\ell + k + \ell) + 1$.

b) Tegyük fel, hogy csak véges sok $4k+3$ alakú prím van, legyenek ezek $p_1, \ldots, p_n$. Ekkor $m = 4p_1 \cdots p_n - 1 > 1$ páratlan szám, amelynek semelyik p_i nem lehet osztója, mert akkor $m - 4p_1 \cdots p_n = -1$-nek is osztója lenne. Másrészt viszont m-nek csak páratlan,

tehát $4k+1$ és $4k+3$ alakú prímosztói lehetnek, de az a) rész miatt nem lehet mindegyik $4k+1$ alakú, így van $4k+3$ alakú prímosztója, ami szükségképpen különbözik $p_1, \ldots, p_n$ mindegyikétől. Ez ellentmond annak a feltevésnek, hogy $p_1, \ldots, p_n$ az összes $4k+3$ alakú prímszám.

7. *Határozzuk meg* $2^{67} \bmod 71$ *értékét!*

Megoldás: A 67-et 2-es számrendszerben való felírásának segítségével állítsuk elő 67-et 2-hatványok összegeként: $67 = 64 + 2 + 1$. Így elég a hatványalap 2-hatványadik hatványait kiszámítani modulo 71 többszörös négyzetre emeléssel, és ezek (modulo 71) szorzatát kiszámítani.

$$2^1 \equiv 2 \pmod{71}$$
$$2^2 \equiv 4 \pmod{71}$$
$$2^4 \equiv 16 \pmod{71}$$
$$2^8 \equiv 256 \equiv 43 \pmod{71}$$
$$2^{16} \equiv 1849 \equiv 3 \pmod{71}$$
$$2^{32} \equiv 9 \pmod{71}$$
$$2^{64} \equiv 81 \equiv 10 \pmod{71}$$
$$2^{67} \equiv 2 \cdot 4 \cdot 10 \equiv 9 \pmod{71}$$

8. *A páros számok körében definiált oszthatóságra nézve mely számok írhatók fel lényegében egyértelműen felbonthatatlanok szorzataként?*

Megoldás: $2\mathbb{N}$-ben nincs egységelem, de még olyan szám sem, amit ilyen esetben egységnek hívhatnánk, azaz amelyik minden más számnak osztója, ugyanis semelyik $2\mathbb{N} \setminus \{0\}$-beli szám nem osztója (nem páros számszorosa) sajátmagának. Tehát a felbonthatatlan számok azok, amelyek semmilyen módon nem bonthatók fel két páros szám szorzatára, azaz amelyek 2-vel oszthatók, de 4-gyel nem. Ilyen számok szorzatára mindegyik $2\mathbb{N}$-beli szám felbontható, de nem feltétlenül egyértelműen. Legyen $n = 2^k m \in 2\mathbb{N}$, ahol $m \geq 1$ páratlan és $k \geq 1$. Ha $k = 1$, akkor n felbonthatatlan, ha $k \geq 2$, és $m = 1$ vagy m prím, akkor n csak $2m \cdot 2 \cdots 2$ alakban bontható fel felbonthatatlanok szorzatára. Viszont ha $k \geq 2$ és m összetett szám: $m = m_1 m_2$, ahol $m_1, m_2 > 1$, akkor $2m \cdot 2 \cdots 2$ és $2m_1 \cdot 2m_2 \cdots 2$ két lényegesen különböző felbontás. Tehát pontosan azoknak a számoknak van itt egyértelmű irreducibilisekre való felbontásuk, amelyek nem oszthatók néggyel (mert ezek maguk irreducibilisek), 2-hatványok vagy 2-hatványok páratlan prímszámszorosai.

9. *Mutassuk meg, hogy* $a|c$ *és* $b|c$ *pontosan akkor teljesül, ha* $[a,b]|c$*. Adjunk példát, hogy* $a|c$ *és* $b|c$*-ből nem következik* $ab|c$*.*

Megoldás: Ha a vagy b nulla, akkor igaz az állítás, mert ekkor a-nak és b-nek $[a,b] = 0$ az egyetlen közös többszöröse. Ha $a, b \neq 0$, akkor definíció szerint $[a,b]$ a legkisebb olyan pozitív egész, amely közös többszöröse a-nak és b-nek. Tehát ha c közös többszörös, és c maradékos osztása $[a,b]$-vel $c = [a,b]q + r$, akkor a és b is osztója c-nek és $[a,b]q$-nak is, így r közös többszörös. De $0 \leq r < [a,b]$, így $r = 0$, vagyis $[a,b] \mid c$.
Ha viszont $[a,b] \mid c$, akkor $a, b \mid [a,b]$ miatt $a, b \mid c$.
Ellenpélda a második állításra: $6 \mid 12$ és $4 \mid 12$, de $6 \cdot 4 = 24$ nem osztója 12-nek.

10. *Mutassuk meg, hogy ha $a, n \geq 2$, és $a^n - 1$ prím, akkor $a = 2$ és n prím.*

Megoldás: Ha $a > 2$, akkor $(a-1) \mid (a^n - 1)$, és $1 < a - 1 < a^n - 1$, tehát $a - 1$ valódi osztó lenne.
Ha $a = 2$ és $n = k\ell$, $k, \ell > 1$, akkor $(a^k - 1) \mid ((a^k)^\ell - 1) = a^n - 1$, és $1 < a^k - 1 < (a^k)^\ell - 1$, tehát megint csak lenne valódi felbontása $(a^n - 1)$-nek.
Tehát $a^n - 1$ legföljebb akkor lehet prím, ha $a = 2$ és n prím (ezek a Mersenne-számok).

11. *Mutassuk meg, hogy egy szám 9-cel való osztási maradéka a számjegyek összegének 9-cel való osztási maradéka. Fogalmazzunk meg hasonló szabályt 11-re.*

Megoldás: $10 \equiv 1 \pmod 9 \Rightarrow 10^k \equiv 1^k \equiv 1 \pmod 9$, tehát
$a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0 \equiv a_n + \cdots + a_1 + a_0 \pmod 9$.
Hasonlóan, $10 \equiv -1 \pmod{11} \Rightarrow 10^k \equiv (-1)^k \pmod{11}$, tehát
$a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0 \equiv (-1)^n a_n + (-1)^{n-1} a_{n-1} + \cdots - a_1 + a_0 \pmod{11}$, vagyis a 11-gyel való osztási maradék a számjegyek váltott előjeles összegének 11 szerinti maradéka.