1. Számelmélet gyakorlat (2009/2010)
Néhány megoldás

Ha összeadás vagy szorzás után egy adott n számmal vett maradékra vagyunk kíváncsiak, akkor mindig elég a maradékokkal dolgozni. Prcízen: Ha k_1 maradéka m_1 és k_2 maradéke m_2 az n-nel osztva, akkor $k_1 + k_2$ (hasonlóan $k_1 k_2$) maradéka n-nel osztva ugyanaz, mint $m_1 + m_2$ (hasonlóan $m_1 m_2$) maradéka n-nel osztva.

1. (a): Vizsgáljuk meg 2^{3n+1} maradékát 7-tel osztva: $n = 0$-ra 2 és $n = 1$-re is 2. Valójában minden n-re 2, mert teljes indukcióval, ha 2^{3n+1} maradéka 2, akkor $2^{3(n+1)+1} = 8 \cdot 2^{3n+1}$ maradéka $1 \cdot 2 = 2$.

(b): $360 = 2^3 3^2 5$ és $n^6 + 85n^4 + 994n^2 = n^2(n^4 + 85n^2 + 994) = n^2(n^2 + 14)(n^2 + 71)$. Vizsgáljuk meg például a kifejezés 3^2-tel való oszthatóságát: Ha $3 \mid n$, akkor készen vagyunk az n^2 miatt. Ha n maradéka 3-mal osztva 1 vagy 2, akkor n^2 maradéka 1, így $n^2 + 14$ és $n^2 + 71$ is osztható 3-mal, tehát a kifejezés osztható 3^2-tel. A 2^3-nal illetve 5-tel való oszthatóság teljesen hasonlóan látható be.

2. Észrevétel: ha $d \mid a$ és $d \mid b$, akkor minden $x, y \in \mathbb{Z}$-re $d \mid ax + by$.

(b): Ha $d = (5^n - 1, 5^{n+2} - 20)$, akkor $d \mid 25(5^n - 1) - (5^{n+2} - 20) = -5$, amiből $d = 1$ vagy $d = 5$. Azonban $d = 5$ nem lehet, mert $5 \nmid 5^n - 1$ kivéve $n = 0$ esetén, de azt kizártuk.

(c): Ha $d = (n^3 + 2n, n^4 + 3n^2 + 1)$, akkor $d \mid -n(n^3 + 2n) + 1(n^4 + 3n^2 + 1) = n^2 + 1$, amiből $d \mid 1(n^3 + 2n) - n(n^2 + 1) = n$, amiből $d \mid 1(n^2 + 1) - n(n) = 1$, vagyis $d = 1$.

3. **1.**(a)-hoz hasonló teljes indukcióval kapjuk a következő felhasználásával: $147^{n+1} + 7^{3(n+1)-1} = 147(147^n + 7^{3n-1}) + 196 \cdot 7^{3n-1}$.

4. (a): n-re teljes indukcióval bizonyítunk. $n = 0$-ra igaz az állítás. Tegyük fel hogy igaz n-re (és a nála kisebb természetes számokra). $n + 1$-re felírva a bal oldalt: $\sum_{k=0}^{n+1} F_k = \sum_{k=0}^{n} F_k + F_{n+1}$, ami az indukciós feltevés szerint tovább egyenlő $F_{n+2} - 1 + F_{n+1} = F_{n+3} - 1 = F_{(n+1)+2} - 1$.

(d): $F_{n+k} = F_k F_{n+1} + F_{k-1} F_n$-t fix n mellett $1 \leq k$-ra teljes indukcióval bizonyítjuk.

$k = 1$ esetén $F_{n+1} = F_1 F_{n+1} + F_0 F_n$ igaz, hiszen $F_1 = 1$ és $F_0 = 0$.

$k = 2$ esetén $F_{n+2} = F_2 F_{n+1} + F_1 F_n$ igaz, hiszen $F_2 = F_1 = 1$.

Tegyük fel, hogy k-ig (k-ra is) igaz az állítást. $(k + 1)$-re:

$$F_{n+(k+1)} \stackrel{\text{def.}}{=} F_{n+(k-1)} + F_{n+k} \stackrel{\text{ind.felt.}}{=} F_{k-1}F_{n+1} + F_{k-2}F_n + F_k F_{n+1} + F_{k-1}F_n.$$

Az első tagnál k helyére $k - 1$-et helyettesítettünk a képletbe. Ezt azért tehettük meg, mert $k + 1 > 2$, így k-ra és $k - 1$-re is alkalmazható az indukciós feltevés.

F_{n+1}-et és F_n-et kiemelve:

$$F_{n+(k+1)} = (F_{k-1} + F_k)F_{n+1} + (F_{k-2} + F_{k-1})F_n = F_{k+1}F_{n+1} + F_k F_n,$$

ami pont a várt képlet $(k + 1)$-re.

(e): Fix n esetén k-ra teljes indukcióval bizonyítunk. $k = 1$-re triviális. Tegyük fel, hogy k-ra igaz az állítás. Ekkor $F_{n(k+1)} = F_{nk+n}$, ami a (d) rész felhasználásával tovább egyenlő $F_n F_{nk+1} + F_{n-1} F_{nk}$, melyben mindkét tényező osztható F_n-nel (az első triviálisan, a második az indukciós feltevés miatt).

5.* Az $F_{n+1} = \sum\left\{\binom{\ell}{k} : \ell \geq k \geq 0 \text{ és } \ell + k = n\right\}$ képletet teljes indukcióval kapjuk $n \geq 1$-re. $n = 1$-re $F_2 = \binom{1}{0} = 1$ és $n = 2$-re $F_3 = \binom{2}{0} + \binom{1}{1} = 2$ igazak.

Tegyük fel, hogy n-ig (n-re is) igaz a képlet. $(n+1)$-re: $F_{(n+1)+1} = F_{n+1} + F_n = \sum\left\{\binom{\ell_1}{k_1} : \ell_1 \geq k_1 \geq 0 \text{ és } \ell_1 + k_1 = n\right\} + \sum\left\{\binom{\ell_0}{k_0} : \ell_0 \geq k_0 \geq 0 \text{ és } \ell_0 + k_0 = n-1\right\}$. (Ismét kettővel korábbi értékre is felhasználtuk az indukciós feltevést.)

I. eset: $n = 2d$ páros. Ekkor $F_{2d+2} = \left(\binom{2d}{0} + \binom{2d-1}{1} + \binom{2d-2}{2} + \cdots + \binom{d}{d}\right) + \left(\binom{2d-1}{0} + \binom{2d-2}{1} + \cdots + \binom{d}{d-1}\right) = \binom{2d}{0} + \left(\binom{2d-1}{1} + \binom{2d-1}{0}\right) + \left(\binom{2d-2}{2} + \binom{2d-2}{1}\right) + \cdots + \left(\binom{d}{d} + \binom{d}{d-1}\right) = \binom{2d+1}{0} + \binom{2d}{1} + \binom{2d-1}{2} + \cdots + \binom{d+1}{d} = \sum\left\{\binom{\ell_2}{k_2} : \ell_2 \geq k_2 \geq 0 \text{ és } \ell_2 + k_2 = 2d+1\right\}$.

II. eset: $n = 2d+1$ páratlan. Teljesen hasonlóan.

6. (a): Tegyük fel, hogy $a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$ prím. A második tényező biztosan nagyobb mint 1, így az első 1, amiből $a = 2$. Ha k összetett lenne, $k = nm$, ahol $n, m > 1$, akkor $a^{nm} - 1 = (a^n)^m - 1^m = (a^n - 1)((a^n)^{m-1} + (a^n)^{m-2} + \cdots + a^n + 1)$, ahol mindkét tényező nagyobb mint 1, ellentmondás.

(b): Tegyük fel, hogy $a^k + 1$ prím. Indirekt, ha $p \mid k$ és $p > 1$ páratlan, akkor $k = np$, amiből $a^{np} + 1 = (a^n)^p + 1^p = (a^n + 1)((a^n)^{p-1} - (a^n)^{p-2} + \cdots - a^n + 1)$, ahol mindkét tényező nagyobb mint 1, ellentmondás. Tehát k-nak nem lehet páratlan osztója, így k kettőhatvány.