Дељивост и канонска факторизација

верзија 2.0: 19.11.2014.

Душан Ђукић

1° Основне чињенице

Теорема 1. Нека су a, b, c цели и n природан број.
(а) Ако су a и b узајамно прости и $ab = c^n$, тада су a и b потпуни n-ти степени.
(б) Ако је $(a, b) = d$ и $ab = c^2$, тада су a/d и b/d потпуни квадрати.

Доказ. (а) Нека су $a = p_1^{i_1} \cdots p_k^{i_k}$ и $b = q_1^{j_1} \cdots q_l^{j_l}$ канонске факторизације a и b. Сви p_i и q_j су међусобно различити и $ab = p_1^{i_1} \cdots p_k^{i_k} q_1^{j_1} \cdots q_l^{j_l}$ је n-ти степен, одакле n дели $i_1, \dots, i_k$ и $j_1, \dots, j_l$, тј. a и b су n-ти степени.

(б) Бројеви $\frac{a}{d}$ и $\frac{b}{d}$ су узајамно прости и њихов производ је квадрат, дакле оба су квадрати.

Теорема 2. Ако природни бројеви a, b, c, d задовољавају $ab = cd$, тада постоје природни бројеви x, y, z, t такви да је $a = xy$, $b = zu$, $c = xz$ и $d = yu$.

Доказ. Пошто x дели a и c, ставимо $x = (a, c)$ и даље $y = \frac{a}{x}$, $z = \frac{c}{x}$ и $u = \frac{b}{z}$. Ови бројеви очигледно задовољавају $a = xy$, $b = zu$, $c = xz$ и $d = yu$.

Бројеви x, y, z су цели. Осим тога, знамо да $c = xz \mid ab$, тј. $z \mid \frac{ab}{x} = by$. Како је $(z, y) = 1$, следи да $z \mid b$, дакле и u је цео број.

Теорема 3. Експонент простог броја p у $n!$ је једнак $[\frac{n}{p}] + [\frac{n}{p^2}] + [\frac{n}{p^3}] + \cdots$.

Доказ. Међу бројевима $1, 2, \dots, n$, број оних који су дељиви са p^i а нису са p^{i+1} је $[\frac{n}{p^i}] - [\frac{n}{p^{i+1}}]$. Зато је укупан експонент p у $n!$ једнак $\sum i([\frac{n}{p^i}] - [\frac{n}{p^{i+1}}]) = [\frac{n}{p}] + [\frac{n}{p^2}] + \cdots$.

Теорема 4. За прост број p, кажемо да p^α *тачно дели* n и пишемо $p^\alpha \parallel n$ ако $p^\alpha \mid n$ и $p^{\alpha+1} \nmid n$. Ако $p^\alpha \parallel a$ и $p^\beta \parallel b$, где је $\alpha > \beta$, онда $p^\beta \parallel a \pm b$.

Доказ. Ако означимо $a = p^\alpha a_1$ и $b = p^\beta b_1$ $(p \nmid a_1, b_1)$, имамо $a \pm b = p^\beta (a_1 \pm p^{\alpha-\beta} b_1)$, при чему $a_1 \pm p^{\alpha-\beta} b_1$ није дељиво са p.

Теорема 5. Ако је $x^a = y^b$ за неке природне бројеве x, y, a, b, тада постоји природан број z такви да је $x = z^m$ и $y = z^n$ за $m = \frac{b}{(a,b)}$ и $n = \frac{a}{(a,b)}$.

Доказ. Имамо $\frac{a}{b} = \frac{n}{m}$ и $(m, n) = 1$, па је $x^n = y^m$. Нека су $p_i^{\alpha_i}$ и $p_i^{\beta_i}$ степени простог броја p_i у x и y редом. Из $x^n = y^m$ следи $n\alpha_i = m\beta_i$, дакле $\frac{\alpha_i}{m} = \frac{\beta_i}{n} = r_i$ за све i, дакле $x = z^m$ и $y = z^n$ за $z = \prod p_i^{r_i}$.

Дефиниција. Функција $f : \mathbb{N} \to \mathbb{R}$ је *мултипликативна* ако је $f(mn) = f(m)f(n)$ кад год је $(m, n) = 1$.

Теорема 6. Број делилаца $\tau(n)$ и збир делилаца $\sigma(n)$ природног броја n су мултипликативне функције по n.

Доказ. Сваки делилац $d \mid mn$ је облика $d = d_m d_n$, где је $d_m = (d, m)$ и $d_n = (d, n)$. Пошто се d_m и d_n могу изабрати на $\tau(m)$ и $\tau(n)$ начина, укупан број делилаца $d \mid mn$ је тачно $\tau(m)\tau(n)$.

Слично, збир делилаца броја mn је $\sum_{\substack{d_m \mid m \\ d_n \mid n}} d_m d_n = \sigma(m)\sigma(n)$.

Теорема 7. Важе формуле $\tau(n) = \prod_i (\alpha_i + 1)$ и $\sigma(n) = \prod_i \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$, где је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ канонска факторизација броја n.

Доказ. За степене простих бројева ово је тачно, а за остале следи из претходног тврђења.

2° **Задаци**

1. Ако су x, y, z природни бројеви, доказати да важи:
(а) $(x,y)[x,y] = xy$; (б) $[x,y][y,z][z,x] \geqslant [x,y,z]^2$.

2. Ако су $a,b,c,d \in \mathbb{N}$ и $ab = cd$, доказати да је број $a+b+c+d$ сложен.

3. Ако се природан број n може написати као збир два квадрата на два различита начина, доказати да је он сложен. (Пример: $65 = 8^2 + 1^2 = 7^2 + 4^2$.)
Напомена. Важи и ово: ако се n може написати као збир два квадрата на тачно један начин, он је или прост, или прост пута два.

4. Нека су a и b природни бројеви. Ако $a \mid b^2 \mid a^3 \mid b^4 \mid a^5 \mid \cdots$, доказати да је $a = b$.

5. Дат је природан број n. Нека су $a,b,c,m \in \mathbb{N}$ такви да $a \mid b^n$, $b \mid c^n$ и $c \mid a^n$, али $abc \nmid (a+b+c)^m$. Одредити највећу могућу вредност m.

6. Нека су a, b природни бројеви. Ако је $a^2 + b^2$ дељиво са ab, доказати да је $a = b$.

7. Претпоставимо да су a, b, c и $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ цели бројеви. Доказати да је abc потпун куб.

8. Ако су a, b, c, $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ и $\frac{a}{c} + \frac{c}{b} + \frac{b}{a}$ цели бројеви, доказати да је $|a| = |b| = |c|$.

9. Нека су $m, n \in \mathbb{N}$. Ако је $\frac{m^2+n^2-m}{mn}$ цео број, доказати да је m потпун квадрат.

10. Природни бројеви a, b, c, d су сви дељиви са $ad - bc$. Доказати да је $|ad - bc| = 1$.

11. Ако су $a, b, c \in \mathbb{N}$ такви да је $\frac{1}{a} + \frac{1}{b} = \frac{1}{c}$, доказати да је $abc(a,b,c)$ потпун квадрат.

12. Нека су $b, n > 1$ природни бројеви. Ако за свако $k > 1$ постоји цео број a_k такав да $k \mid b - a_k^n$, доказати да је $b = B^n$ за неки цео број B.

13. Нека су $1 = d_1 < d_2 < \cdots < d_k = n$ сви позитивни делиоци природног броја $n > 1$. Означимо $D = \sum_{i=1}^{k-1} d_i d_{i+1}$.
(а) Доказати да је $D < n^2$.
(б) Одредити све n за које је D делилац n^2.

14. (а) Нека су $a, b \in \mathbb{N}$. Ако је $[a, a+5] = [b, b+5]$, доказати да је $a = b$.
(б) Може ли да важи $[a, a+c] = [b, b+c]$ за неке $a, b, c \in \mathbb{N}$, $a \neq b$?

15. Постоје ли природни бројеви $a_1 < a_2 < \cdots < a_{100}$ такви да је (а) $(a_1, a_2) > (a_2, a_3) > \cdots > (a_{99}, a_{100})$; (б) $[a_1, a_2] > [a_2, a_3] > \cdots > [a_{99}, a_{100}]$; (ц) оба?

16. Нека су $a_1 < a_2 < \cdots < a_{100}$ природни бројеви. Доказати да је $\frac{1}{[a_1,a_2]} + \frac{1}{[a_2,a_3]} + \cdots + \frac{1}{[a_{99},a_{100}]} \leqslant 1$.

17. Наћи све парове природних бројева (x, y) за које је $x^y = y^{x-y}$.

18. (а) Одредити све парове a, b природних бројева за које је $a^b = b^a$.
(б) Исто питање ако су a и b позитивни *рационални* бројеви.

19. Одредити све парове природних бројева x, y за које је $x^{y^2} = y^x$.

20. Природни бројеви x, a, b задовољавају $x^{a+b} = a^b b$. Доказати да је $a = x$ и $b = x^x$.

21. Нека су $1 = d_1 < d_2 < \cdots < d_k = n$ сви делиоци броја n. Наћи све n за које је $n = d_1^2 + d_2^2 + d_3^2 + d_4^2$ ($k \geqslant 4$).

22. Наћи све природне бројеве n такве да је $n = d_6^2 + d_7^2 - 1$, где су $1 = d_1 < d_2 < \cdots < d_k = n$ сви природни делиоци броја n.

23. Ако за природан број n важи $2\sigma(n) = n\tau(n) + 2$, доказати да је n прост или $n = 4$.

24. За дати природан број n, посматрајмо низ дат са $a_0 = n$ и $a_{k+1} = \tau(a_k)$. Наћи све n за које низ (a_k) не садржи ниједан потпун квадрат.

25. Ако су $m < n$ природни бројеви и $m \mid n$, доказати да је $\frac{\sigma(m)}{m} < \frac{\sigma(n)}{n}$.

26. Природан број је *савршен* ако је једнак збиру свих својих правих делилаца, тј. $\sigma(n) = 2n$. Ако је $n > 28$ савршен број и $7 \mid n$, доказати да $49 \mid n$.

27. Ако је n паран савршен број, доказати да је $n = 2^{k-1}(2^k - 1)$ за неко $k \geqslant 2$.

28. За сваки природан број d, означимо са $f(d)$ најмањи природан број који има тачно d делилаца (на пример, $f(1) = 1$, $f(5) = 16$ и $f(6) = 12$). Доказати да за сваки цео број $k \geqslant 0$, $f(2^k)$ дели $f(2^{k+1})$.

3° Решења

1. Нека су експоненти простог броја p у x, y, z редом r, s, t, и нека је $r \leqslant s \leqslant t$.
(а) Експоненти p у $(x, y), [x, y]$ и xy су редом $\min(r, s) = r$, $\max(r, s) = s$ и $r + s$.
(б) Експонент p на левој страни је $\max(r, s) + \max(s, t) + \max(r, t) = s + 2t$, а на десној $2\max(r, s, t) = 2t$.

2. На основу претходног задатка постоје $x, y, z, u \in \mathbb{N}$ такви да је $a = xy$, $b = zu$, $c = xz$ и $d = yu$. Тада је $a + b + c + d = xy + zu + xz + yu = (x + u)(y + z)$.

3. Нека је $n = a^2 + b^2 = c^2 + d^2$. Можемо да претпоставимо да су a и c исте парности, b и d такође, и да је $a > c$ и $d > b$. Имамо $a^2 - c^2 = d^2 - b^2$, тј. $\frac{a+c}{2} \cdot \frac{a-c}{2} = \frac{d+b}{2} \cdot \frac{d-b}{2}$. На основу задатка 3 постоје $m, n, p, q \in \mathbb{N}$ такви да је $\frac{a+c}{2} = mn$, $\frac{a-c}{2} = pq$, $\frac{d+b}{2} = mp$, $\frac{d-b}{2} = nq$. Тада је $a = mn + pq$ и $b = mp - nq$, па је $a^2 + b^2 = (mn + pq)^2 + (mp - nq)^2 = m^2n^2 + p^2q^2 + m^2p^2 + n^2q^2 = (m^2 + q^2)(n^2 + p^2)$, што је сложен број.

4. Нека је p прост број и нека $p^\alpha \parallel a$ и $p^\beta \parallel b$. Из $a^{2n-1} \mid b^{2n} \mid a^{2n+1}$ следи $(2n-1)\alpha \leqslant 2n\beta \leqslant (2n+1)\alpha$ за свако $n \in \mathbb{N}$, тј. $1 - \frac{1}{2n} \leqslant \frac{\beta}{\alpha} \leqslant 1 + \frac{1}{2n}$, одакле следи $\alpha = \beta$ за свако p, тј. $a = b$.

5. Посматрајмо неки прост број $p \mid a$. Нека $p^\alpha \parallel a$, $p^\beta \parallel b$ и $p^\gamma \parallel c$ и нека је без смањења општости $\gamma < \alpha, \beta$. По услову задатка је $\alpha < n\beta < n^2\gamma$, па је $\alpha + \beta + \gamma \leqslant (n^2 + n + 1)\gamma$. Како $p^\gamma \mid a + b + c$ и $p^{\alpha+\beta+\gamma} \parallel abc$ (што важи за свако p), следи да $abc \mid (a + b + c)^{n^2+n+1}$. Дакле, $m \leqslant n^2 + n$.

   С друге стране, за $a = c^{n^2}$ и $b = c^n$, $abc = c^{n^2+n+1}$ не дели $(a + b + c)^{n^2+n}$. Овај пример показује да је $\max m = n^2 + n$.

6. Нека је p произвољан прост број и нека $p^\alpha \parallel a$ и $p^\beta \parallel b$. Ако је $\alpha \neq \beta$, онда $p^{\alpha+\beta} \parallel ab$ и $p^{2\min\{\alpha,\beta\}} \parallel a^2 + b^2$, што је немогуће јер је $2\min\{\alpha, \beta\} < \alpha + \beta$. Следи да је $\alpha = \beta$ за свако p, тј. $a = b$.

7. Треба да покажемо да је експонент сваког простог броја у abc дељив са 3. Посматрајмо било који прост делилац $p \mid abc$; нека $p^\alpha \parallel a$, $p^\beta \parallel b$ и $p^\gamma \parallel c$, при чему је без смањења општости $\gamma \geqslant \alpha, \beta$. Тада $p^{\alpha-\beta} \parallel \frac{a}{b}$, $p^{\beta-\gamma} \parallel \frac{b}{c}$ и $p^{\gamma-\alpha} \parallel \frac{c}{a}$.
Ако је $\alpha - \beta \neq \beta - \gamma$, онда $p^k \parallel \frac{a}{b} + \frac{b}{c} + \frac{c}{a}$, где је $k = \min\{\alpha - \beta, \beta - \gamma\}$. Али $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ је цео број, дакле $k \geqslant 0$, одакле следи $\alpha = \beta = \gamma$ и $p^{3\alpha} \parallel abc$.
С друге стране, ако је $\alpha - \beta = \beta - \gamma$, онда је $\alpha + \beta + \gamma = 3\beta$ и $p^{3\beta} \parallel abc$.

8. Нека су α, β, γ експоненти простог броја p у a, b, c редом и нека је $\gamma \geqslant \alpha, \beta$. Из решења претходног задатка, из $\frac{a}{b} + \frac{b}{c} + \frac{c}{a} \in \mathbb{Z}$ следи да је $s = \alpha + \beta + \gamma = 3\beta$, а из $\frac{b}{a} + \frac{a}{c} + \frac{c}{b} \in \mathbb{Z}$ следи да је $s = 3\alpha$. Одавде је $\alpha = \beta = \gamma$. Ово важи за свако p, па је $|a| = |b| = |c|$.

9. Посматрајмо неки прост делилац $p \mid m$; нека $p^r \parallel m$ и $p^s \parallel n$. Тада $p^{r+s} \mid mn$, док $p^r \parallel m^2 - m = m(m-1)$ и $p^{2s} \parallel n^2$. Ако је $r \neq 2s$, онда је степен p у m^2+n^2-m једнак $p^{\min(r,2s)}$, што је мање од p^{r+s}, па mn не може да дели m^2+n^2-m. Према томе, мора бити $r = 2s$. То важи за свако p, дакле сви експоненти у канонској факторизацији m су парни, тј. m је квадрат.

10. Претпоставимо да је $|ad-bc| \neq 1$ и посматрајмо неки прост делилац p са $p^k \parallel ad-bc$. По услову задатка $p^k \mid a,b,c,d$, дакле $p^{2k} \mid ad-bc$, противно избору k.

11. Нека је $d = (a,b)$ и $a = dm$, $b = dn$. Тада је $dmn = (m+n)c$ и $(m+n, mn) = (m,n) = 1$, па $m+n \mid d$. Ставимо $d = k(m+n)$. Тада је $a = km(m+n)$, $b = kn(m+n)$, $c = kmn$ и $(a,b,c) = (k(m+n), kmn) = k$, дакле $abc(a,b,c) = (k^2mn(m+n))^2$.

12. Ставимо $k = b^2$; тада $b^2 \mid b - a_k^n$. Ако је p неки прост делилац b и $p^{r_p} \parallel b$, онда $p^{r_p} \parallel a_k^n$, дакле $n \mid r_p$, То важи за свако p, тј. b је n-ти степен.

13. (а) Пошто је $\frac{d_i}{n} = \frac{1}{d_{k+1-i}}$, имамо $\frac{D}{n^2} = \frac{1}{d_k d_{k-1}} + \cdots + \frac{1}{d_2 d_1}$. Одавде следи $\frac{1}{d_2 d_1} \leqslant \frac{D}{n^2} \leqslant \left(\frac{1}{d_{k-1}} - \frac{1}{d_k}\right) + \cdots + \left(\frac{1}{d_1} - \frac{1}{d_2}\right) = 1 - \frac{1}{d_k} < 1$, тј. $d_1 = 1 < \frac{n^2}{D} \leqslant d_2$. Дакле, $D < n^2$.

   (б) Ако D дели n^2, по претходном мора бити $\frac{n^2}{D} = d_2$ и $k = 2$, што значи да је n прост број.

14. (б) Не може. Индукција по c. За $c = 1$ је тривијално; нека је $c > 1$. Ако је $(a,c) > 1$, онда постоји прост број p који дели a и c; онда је $[a, a+c] = [b, b+c]$ дељиво са p, дакле $p \mid b$, па се a,b,c сви могу скратити са c тако да једнакост остане на снази, супротно индукцијској претпоставци. Остаје само случај $(a,c) = (b,c) = 1$, а тада је $a(a+c) = [a, a+c] = [b, b+c] = b(b+c)$ и одатле $a = b$.

15. (а) За $a_k = 2^{100} - 2^{100-k}$ је $(a_k, a_{k+1}) = 2^{99-k}$ и опада по k, док низ a_k расте.

   (б) За $a_k = 2^{99} + 2^{k-1}$ је $[a_k, a_{k+1}] = \frac{a_k a_{k+1}}{(a_k, a_{k+1})} = \frac{a_k a_{k+1}}{2^{k-1}}$ што опада по k, док a_k расте.

   (ц) Ако постоје, онда је $a_1 a_2 = (a_1, a_2)[a_1, a_2] > (a_2, a_3)[a_2, a_3] = a_2 a_3$, контрадикција.

16. Довољно је доказати индукцијом по n да за све природне бројеве $c_1 < c_2 < \cdots < c_n$ важи $\frac{1}{[c_1,c_2]} + \frac{1}{[c_2,c_3]} + \cdots + \frac{1}{[c_{n-1},c_n]} \leqslant \frac{1}{c_1}$.

   Ово тврђење важи за $n = 1$. За $n > 1$ је $\sum_{i=1}^{n-1} \frac{1}{[c_i,c_{i+1}]} = \frac{1}{[c_1,c_2]} + \sum_{i=2}^{n-1} \frac{1}{[c_i,c_{i+1}]} \leqslant \frac{1}{[c_1,c_2]} + \frac{1}{c_2} \leqslant \frac{1}{c_1}$ по индуктивној претпоставци.

17. За $x = 1$ или $y = 1$ једино решење је $(1,1)$. Надаље сматрамо да су $x, y > 1$. Пошто је $y^{x-y} > 1$ цео број, важи $x > y$. Онда из једначине следи и $y < x - y$, тј. $x > 2y$. Како y^y дели $x^y = y^{x-y}$, следи да $y \mid x$; нека је $x = zy$. Једначина постаје $(zy)^y = y^{(z-1)y}$, што је еквивалентно са $z = y^{z-2}$.

   За $z \leqslant 4$ добијамо решења $(8,2)$ и $(9,3)$. За $z \geqslant 5$ је $y^{z-2} \geqslant 2^{z-2} > z$, па тада нема решења.

18. Означимо $\frac{b}{a} = q$. Једначина $a^b = b^a$ постаје $a^{qa} = (qa)^a$, тј. $a^q = qa$ и одатле $a = q^{\frac{1}{q-1}}$. Покажимо да је a рационално ако и само ако је $n = \frac{1}{q-1}$ цео број.

   Нека је $\frac{1}{q-1} = \frac{r}{s}$, где су $r, s \neq 0$ узајамно прости цели бројеви. Тада је $q = \frac{r+s}{r}$ и $a = (\frac{r+s}{r})^{r/s}$, па су сви експоненти простих делилаца у $\frac{r+s}{r}$ дељиви са s, тј. $r+s$ и r (будући узајамно прости) су s-ти степени, рецимо $r+s = u^s$ и $r = v^s$ $(u, v \in \mathbb{N})$. Али тада је $u^s - v^s = s$, што је немогуће за $s > 1$ јер је $u^s - v^s \geqslant (v+1)^s - v^s = sv^{s-1} + \cdots + 1 > s$. Према томе, $s = 1$, тј. $n \in \mathbb{Z}$. Сада је $q = 1 + \frac{1}{n}$ и $a = (1+\frac{1}{n})^n$, $b = (1+\frac{1}{n})^{n+1}$.

19. Постоје природни бројеви z, m, n такви да је $(m,n) = 1$, $x = z^m$ и $y = z^n$. Тада је $z^{mz^{2n}} = x^{y^2} = y^x = z^{nz^m}$, дакле $z^{m-2n} = \frac{m}{n}$. Разликујемо два случаја.

   (i) $m < 2n$. Тада је $\frac{m}{n} = \frac{1}{z^{2n-m}}$, одакле је $m = 1$ и $n = z^{2n-m} = z^{2n-1}$. Како је $z^{2n-1} > 2n - 1 \geqslant n$ за $z > 1$, мора бити $z = n = 1$, па имамо решење $(x,y) = (1,1)$.

(ii) $m \geqslant 2n$. Тада је $n = 1$ и $m = z^{m-2n} = z^{m-2}$. За $z > 4$ је $z^{m-2} > m$. За $z = 3$ једино решење је $m = 3$, што даје решење $(x, y) = (27, 3)$. За $z = 2$ једино решење је $m = 4$, што даје $(x, y) = (16, 2)$.

20. Ако је $x = 1$, онда је и $a = b = 1$. Претпоставимо да је $x > 1$ и p неки његов прост делилац, и нека су p^α, p^β и p^γ редом степени p у a, b и x. По услову задатка је

$$(a + b)\gamma = b\alpha + \beta. \qquad (*)$$

Ако је $\beta = 0$, тј. $p \nmid b$, онда је $a\gamma = b(\alpha - \gamma)$, одакле је $0 < \alpha - \gamma < p^\alpha$ и $p^\alpha \mid \alpha - \gamma$, што је немогуће. Дакле, $\beta > 0$. Даље, из $(*)$ следи да $p^\beta \nmid a$ за свако p, дакле $a \mid b$, а одатле и $a \mid \beta$ због $(*)$. То значи да је $b = c^a$ за неко $c \in \mathbb{N}$.

Нека је $\frac{x}{a} = \frac{m}{n}$, $(m, n) = 1$. Тада је $x^a m^b = bn^b$, а одавде $m^b \mid b$, па мора бити $m = 1$, тј. $x \mid a$ и $\alpha \geqslant \gamma$. Ако је $x = a$, онда је $b = x^x$. Претпоставимо да је $\alpha \geqslant \gamma + 1$. Тада је по $(*)$ $\gamma(a + b) > (\gamma + 1)b$, дакле $c^a = b < a\gamma < ap^\gamma \leqslant a^2$, тј. $a^2 \geqslant c^a + 2$. Како је $a^2 < 2^a + 2$ за све a, мора бити $c = 1$, а тада је $a = b = x = 1$.

21. Ако је n непарно, сви d_i су непарни па је $d_1^2 + \cdots + d_4^2$ парно, контрадикција. Значи, n је парно и $d_2 = 2$, а одатле је тачно један од d_3, d_4 паран.

(i) Ако је $d_3 = 2a$, онда $a \mid n$, па мора бити $a = 2$ и $d_3 = 4$. Сада је $n = d_4^2 + 21$, али то није дељиво са 4.

(ii) Нека је $d_4 = 2a$. Ако је $a = 2$, онда је $d_4 = 4$, $d_3 = 3$ и $n = 30$, али $4 \nmid 30$. Следи да је $a > 2$. Сада је $d_3 = a$ и $n = 5a^2$, дакле $a_4 > 5 \mid n$, одакле је $d_3 = 5$, $d_4 = 10$ и $n = 130$, што јесте решење.

22. Из услова следи да $d_7 \mid d_6^2 - 1$, $d_6 \mid d_7^2 - 1$ и $(d_6, d_7) = 1$.

Ако је $d_6 = ab$, $d_7 = cd$ са $1 < a < b$, $1 < c < d$, онда n има 7 делилаца мањих од d_7 (то су $1, a, b, c, d, ab, ac$), што је немогуће. Према томе, d_6 или d_7 је облика p или p^2, где је $p > 2$ прост број. Нека је то d_i, $\{i, j\} = \{6, 7\}$; онда $d_i \mid (d_j - 1)(d_j + 1)$ повлачи да $d_j \equiv \pm 1 \pmod{d_i}$ и отуда $(d_i^2 - 1)/d_j \equiv \pm 1$. Број d_j или $(d_i^2 - 1)/d_j$ је мањи од d_i, па је једнак $d_i - 1$ или 1. Једине нетривијалне могућности су $(d_i^2 - 1)/d_j = 1$ и $d_j = d_i \pm 1$. У првом случају је $d_i < d_j$, па је $d_7 = d_6^2 - 1 = (d_6 - 1)(d_6 + 1)$ и зато је $d_6 + 1$ делилац n између d_6 и d_7, контрадикција. Зато мора бити $d_7 = d_6 + 1$. Ако ставимо $d_6 = x$ и $d_7 = x + 1$, добијамо да је $n = x^2 + (x + 1)^2 - 1 = 2x(x + 1)$ парно.

(i) Нека је један од $x, x+1$ једнак простом p. Други од њих има највише 6 делилаца, па може бити само облика $2^3, 2^4, 2^5, 2q, 2q^2, 4q$, где је q прост. За 2^5 добијамо решење $x = 31$ и $n = 1984$. Остали случајеви не дају решење.

(ii) Један од $x, x + 1$ је p^2; други има највише 5 делилаца (искључујући p), па је облика $2^3, 2^4, 2q$ за просто $q > 2$. За 2^3 добијамо решење $x = 8$ и $n = 144$. Остале могућности не дају решење.

23. Претпоставимо да је $n > 4$ сложен и нека су $1 = d_1 < d_2 < \cdots < d_{\tau(n)} = n$ сви делиоци броја n. Сабирањем једнакости $2(d_1 + d_{\tau(n)}) = 2n + 2$ и неједнакости $d_i + d_{\tau(n)+1-i} < n$ за $1 < i < \tau(n)$ добијамо $2\sigma(n) < n\tau(n) + 2$.

24. За $a_k > 2$ је $a_{k+1} < a_k$, па мора бити $a_m = 2$ за неко m. Претпоставимо да је $m \geqslant 2$. Тада је a_{m-1} прост број јер је $\tau(a_m) = 2$, дакле $\tau(a_{m-2}) = a_{m-1}$ је непаран, одакле следи да је a_{m-2} потпун квадрат.

Следи да је $m \leqslant 2$, дакле $a_1 = \tau(n) = 2$, одакле следи да је n прост број.

25. Нека су $d_1, d_2, \ldots, d_r$ сви делиоци броја m и нека је $n = km$. Бројеви $kd_1, kd_2, \ldots, kd_r$ су делиоци броја n, али не сви (нпр. 1 није међу њима), па је зато $\sigma(n) > kd_1 + \cdots + kd_r = k\sigma(m)$.

26. Претпоставимо да је $n = 7m$, $7 \nmid m$. Тада је $2n = \sigma(n) = \sigma(7)\sigma(m) = 8\sigma(m)$, одакле $4 \mid n$. Ако $2^k \parallel n = 7 \cdot 2^k r$ за $k \geqslant 2$, онда је $\sigma(n) = \sigma(7)\sigma(2^k)\sigma(r) > 8(2^{k+1} - 1)r \geqslant 8 \cdot \frac{7}{4} \cdot 2^k n = 2n$, контрадикција. Следи да $7 \mid m$, тј. $49 \mid n$.

27. Нека је $n = 2^{k-1}n_1$, где $2 \nmid n_1$. Из $2^k n_1 = \sigma(n) = \sigma(2^{k-1})\sigma(n_1) = (2^k-1)\sigma(n_1)$ добијамо $\sigma(n_1) = \frac{2^k}{2^k-1}n_1$, па n_1 мора бити дељиво са $2^k - 1$. Али тада је $\frac{\sigma(n_1)}{n_1} \geqslant \frac{\sigma(2^k-1)}{2^k-1}$, уз једнакост само за $n_1 = 2^k - 1$.

28. Нека је $\tau(n) = 2^k$ и $n = p_1^{r_1}p_2^{r_2}\cdots p_m^{r_m}$, где су p_i различити прости и r_i природни бројеви. Како је $(r_1+1)\cdots(r_m+1) = 2^k$, сви r_i су облика $r_i = 2^{s_i}-1$ за $s_i \in \mathbb{N}$ и $s_1+\cdots+s_m = k$. Како је тада $p_i^{r_i} = \prod_{j=0}^{s_i-1} p_i^{2^j}$, закључујемо да је n производ тачно k бројева облика p^{2^j}. Због минималности, $f(2^k)$ је производ k *најмањих* бројева тог облика, па тврђење одмах следи.

Београд, 2012-2014