Аритметичка својства биномних коефицијената

верзија 1.4: 17.5.2017.

Душан Ђукић

1. *(Кумерова теорема)* Доказати да је степен простог броја p у биномном коефицијенту $\binom{n}{m}$ $(0 \leqslant m \leqslant n)$ једнак броју преноса цифара у основи p при сабирању m и $n-m$.

2. Нека је p прост број и $0 \leqslant m \leqslant n$. Ако $p^k \mid \binom{n}{m}$, доказати да је $n \geqslant p^k$.

3. Доказати да је нзс$\{1, 2, \dots, n\}$ дељив са нзс$\{\binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n}\}$ за свако $n \in \mathbb{N}$.

4. Доказати да је степен двојке у $\binom{2n}{n}$ једнак броју јединица у бинарном запису n.

5. Доказати да $\binom{2n}{n}$ нема простих делилаца у интервалу $(\frac{2n}{3}, n)$.

6. Доказати да је $C_n = \frac{1}{n+1}\binom{2n}{n}$ цео број за свако $n \in \mathbb{N}_0$ (*Каталанов број*).

7. Дат је природан број k. Одредити најмањи природан број C такав да је $\frac{C}{n+k+1}\binom{2n}{n+k}$ цео број за сваки природан број $n \geqslant k$.

8. (а) Нека је n природан број и p прост делилац броја n. Ако $p^m \parallel n$ и $k \leqslant m$, доказати да онда $p^{m-k} \parallel \binom{n}{p^k}$. ($p^m \parallel n$ значи да $p^m \mid n$ и $p^{m+1} \nmid n$.)

   (б) Ако је $p^k \geqslant n$ и $p^m \parallel n$, доказати да $p^{k-m} \parallel \binom{p^k}{n}$.

9. Нека је $n > 1$ природан број. Ако је нзд$\{\binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n-1}\} = m > 1$, доказати да је m прост број и $n = m^k$ за неко $k \in \mathbb{N}$.

10. Ако су $k < m < n$ природни бројеви, доказати да $\binom{n}{k}$ и $\binom{n}{m}$ нису узајамно прости.

11. Нека су k и m дати природни бројеви.

    (а) Доказати да постоји n такво да су $\binom{n}{k}, \binom{n+1}{k}, \dots, \binom{n+k-1}{k}$ сви дељиви са m.

    (б) Доказати да су $\binom{n}{k}, \binom{n+1}{k}, \dots, \binom{n+k}{k}$ узајамно прости за свако $n \in \mathbb{N}$.

12. За дати природан број r, означимо са N_r најмањи природан број такав да су сви бројеви $\frac{N_r}{n+r}\binom{2n}{n}$ цели. Доказати да је $N_r = \frac{r}{2}\binom{2r}{r}$.

13. За природан број n, означимо са $n\sharp$ производ свих простих бројева не већих од n. Доказати да је $n\sharp < 4^n$.

14. Доказати *Бертранов постулат*: за свако $n > 1$ постоји прост број p са $n < p < 2n$.

15. Нека је p прост и i, j цели бројеви, $0 \leqslant i, j < p$.

    (а) Доказати да $p \mid \binom{p}{i}$ за $i > 0$.

    (б) Доказати да је $\binom{p-1}{i} \equiv (-1)^i \pmod{p}$.

    (в) Доказати да је $\frac{1}{p}\binom{p}{i} \equiv \frac{(-1)^{i-1}}{i} \pmod{p}$ за $i > 0$.

    (г) Доказати да је $\binom{i+j}{j} \equiv (-1)^j\binom{p-1-i}{j} \equiv (-1)^i\binom{p-1-j}{i}$.

16. Нека је n природан број. Ако је $\binom{n-1}{i} \equiv (-1)^i \pmod{n}$ за $i = 0, 1, \dots, n-1$, доказати да је n прост.

17. Доказати да за прост број p и $0 < n < p$ важи $\binom{2n}{n} \equiv (-4)^n\binom{\frac{p-1}{2}}{n} \pmod{p}$.

18. Доказати да је $\binom{0}{0} - 2\binom{2}{1} + 2^2\binom{4}{2} - \dots + (-2)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 1 \pmod{p}$ за сваки прост број $p > 3$.

19. Доказати да је $\sum_{k=1}^{n} C_k \equiv 1 \pmod 3$ ако и само ако број $n+1$ садржи цифру 2 у запису са основом 3.

20. *(Лукасова теорема)* Ако су $m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0$ и $n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$ записи природних бројева m, n у основи p, тада је
$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod p.$$

21. Ако је n природан и p прост број, доказати да је $\binom{n}{p} \equiv [\frac{n}{p}] \pmod p$.

22. Дат је природан број n. Доказати да је број непарних међу бројевима $\binom{n}{i}$ $(0 \leqslant i \leqslant n)$ једнак неком степену двојке.

23. Доказати да је за свако $m \in \mathbb{N}$, међу биномним коефицијентима $\binom{n}{k}$ $(0 \leqslant k \leqslant n < 2^m)$, број непарних једнак 3^m.

24. Дат је природан број n. Доказати да је број непарних међу бројевима $\binom{n-i}{i}$ $(0 \leqslant i \leqslant \frac{n}{2})$ паран ако и само ако је $n \equiv 2 \pmod 3$.

25. Нека је p прост и n природан број. Ако су $1 \leqslant j, k \leqslant p-1$ природни бројеви и $n \equiv k \pmod{p-1}$, доказати да је $\binom{n}{j} + \binom{n}{j+(p-1)} + \binom{n}{j+2(p-1)} + \cdots \equiv \binom{k}{j} \pmod p$.

26. Ако је $p \geqslant 5$ прост број, доказати:
(а) $p \mid 1 + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2}$;
(б) $p^2 \mid 1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$ *(Волстенхолмова теорема)*;
(в) $p \mid \sum_{1 \leqslant i < j < p} \frac{1}{ij}$.

27. Ако је $p > 3$ прост број, доказати да $p^3 \mid \binom{2p}{p} - 2$.

28. Доказати да за прост број $p > 3$ и природан број n важи $p^3 \mid \binom{np}{p} - n$.

29. Ако је n природан и $p \geqslant 5$ прост број, доказати да је $\binom{p^n}{p} \equiv p^{n-1} \pmod{p^{2n+1}}$.

30. Нека је $S_n = \left\{ \binom{n}{n}, \binom{2n}{n}, \binom{3n}{n}, \ldots, \binom{n^2}{n} \right\}$ за $n \in \mathbb{N}$. Доказати да постоји бесконачно много сложених природних бројева n таквих да S_n (а) *није*; (б) *јесте* потпун систем остатака по модулу n.

31. Ако је $p > 3$ прост број, доказати да је $\sum_{i=0}^{p} \binom{p}{i} \binom{p+i}{i} \equiv 2^p + 1 \pmod{p^2}$.

32. Нека је p непаран прост број. За свако a, дефинишимо $S_a = \frac{a}{1} + \frac{a^2}{2} + \cdots + \frac{a^{p-1}}{p-1}$. Ако је $S_3 + S_4 - 3S_2 = \frac{m}{n}$, $m, n \in \mathbb{N}$, доказати да је m дељиво са p.

33. Ако је $p > 2$ прост број, доказати да је $\frac{2^{p-1}-1}{p} \equiv 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2} \pmod p$.

34. За дати непаран број p, означимо $H_k = \sum \frac{1}{i_1 i_2 \cdots i_k}$, где се сумира по k-торкама непарних индекса $0 < i_1 < i_2 < \cdots < i_k < p$. (Нпр. $H_1 = 1 + \frac{1}{3} + \cdots + \frac{1}{p-2}$.) Доказати да је
$$2^{p-1} = 1 + pH_1 + p^2 H_2 + \cdots + p^{\frac{p-1}{2}} H_{\frac{p-1}{2}}.$$

35. За прост број $p \geqslant 5$, доказати да је $\binom{p-1}{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} 4^{p-1} \pmod{p^3}$.

36. Ако је n природан број, доказати да је збир $\sum_{k=0}^{3^n-1} \binom{2k}{k}$ (а) дељив са 3; (б) дељив са 3^n.

37. Нека је n природан број. Доказати да бројеви $\binom{2^n-1}{0}, \binom{2^n-1}{1}, \binom{2^n-1}{2}, \ldots, \binom{2^n-1}{2^{n-1}-1}$ при дељењу са 2^n дају остатке $1, 3, 5, \ldots, 2^n - 1$ неким редом.

38. За природан број $k \geqslant 2$, доказати да је $\binom{2^{k+1}}{2^k} - \binom{2^k}{2^{k-1}}$ дељиво са 2^{3k}, а није са 2^{3k+1}.

Решења

1. Степен p у $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ је $\sum_{i>0}([\frac{n}{p^i}] - [\frac{m}{p^i}] - [\frac{n-m}{p^i}])$. У овој суми, i-ти сабирак је једнак 1 ако се преноси цифра уз p^{i-1}, и 0 у супротном. Одавде следи тврђење.

2. Одмах следи из претходног задатка.

3. По задатку 2, за сваки прост број p, ако $p^i \mid \binom{n}{k}$ за неко k, онда је $p^i < n$, дакле $p^i \mid$ нзс$\{1, 2, \dots, n\}$. Према томе, $\binom{n}{k}$ дели нзс$\{1, 2, \dots, n\}$ за све k.

4. Степен броја 2 у $\binom{2n}{n}$ је $\sum_{i>0}([\frac{2n}{2^i}] - 2[\frac{n}{2^i}])$. Сабирак $[\frac{2n}{2^i}] - 2[\frac{n}{2^i}]$ је једнак i-тој бинарној цифри отпозади у n.

5. За прост број $p \in (\frac{2n}{3}, n)$, експонент уз p у $\binom{2n}{n}$ је $[\frac{2n}{p}] - 2[\frac{n}{p}] = 2 - 2 \cdot 1 = 0$.

6. Довољно је показати да је $[\frac{2n}{p^i}] - [\frac{n}{p^i}] - [\frac{n+1}{p^i}] \geqslant 0$ за свако $i \in \mathbb{N}$ и просто p. Ово, међутим, одмах следи из једнакости $[2x] = [x] + [x + \frac{1}{2}]$ за $x = \frac{n}{p^i}$.

   Решење 2. $C_n = \binom{2n}{n} - \binom{2n}{n+1}$.

7. Одговор је $C = 2k + 1$. За $n = k$, број $\frac{C}{2k+1}$ је цео, дакле $2k + 1 \mid C$. С друге стране, број $\frac{2k+1}{n+k+1}\binom{2n}{n+k} = 2\binom{2n}{n+k} - \frac{2n+1}{n+k+1}\binom{2n}{n+k} = 2\binom{2n}{n+k} - \binom{2n+1}{n+k+1}$ је цео.

8. (а) Степен p у $\binom{n}{m}$ је $v_p = \sum_{i>0}([\frac{n}{p^i}] - [\frac{m}{p^i}] - [\frac{n-m}{p^i}])$. Сабирак $[\frac{n}{p^i}] - [\frac{p^k}{p^i}] - [\frac{n-p^k}{p^i}]$ је једнак 0 за $1 \leqslant i \leqslant k$ и $i > m$, и 1 за $k < i \leqslant m$, одакле следи $v_p = m - k$.

   (б) Степен p у $\binom{p^k}{n}$ је $\sum_{i>0}([\frac{p^k}{p^i}] - [\frac{n}{p^i}] - [\frac{p^k-n}{p^i}]$, при чему је i-ти сабирак једнак 1 за $m < i \leqslant k$, и 0 у супротном.

9. Из услова следи да $m \mid n$. Посматрајмо неки прост делилац p броја m; нека $p^k \parallel n$. По претходном задатку, $p \nmid \binom{n}{p^k}$, дакле $m \nmid \binom{n}{p}$, па по услову задатка мора бити $n = p^k$; уједно је и m степен броја p. Такође, из $p^1 \parallel \binom{n}{p^{k-1}}$ следи $m = p$.

10. Број парова A, B подскупова датог n-елементног скупа са $|A| = k$, $|B| = m$ и $A \subset B$ једнак је $\frac{n!}{k!(m-k)!(n-m)!} = \binom{n}{k}\binom{n-k}{m-k} = \binom{n}{m}\binom{m}{k}$. Одавде је $\frac{\binom{n}{k}}{\binom{n}{m}} = \frac{\binom{m}{k}}{\binom{n-k}{m-k}}$, дакле леви разломак је скратив јер је $\binom{m}{k} < \binom{n}{k}$, и тврђење одмах следи.

11. (а) На пример, $n = mk!$ задовољава услове.

    (б) Тврђење је тривијално за $k = 1$. Претпоставимо да је $k \geqslant 2$ најмањи природан број за који постоје n и d такви да су $\binom{n}{k}, \binom{n+1}{k}, \dots, \binom{n+k}{k}$ дељиви са d. Тада су и све разлике $\binom{n+i+1}{k} - \binom{n+i}{k} = \binom{n+i}{k-1}$ за $i = 0, 1, \dots, k-1$ дељиве са d, што је у супротности са минималношћу броја k.

12. Покажимо прво да $N_r \mid \frac{r}{2}\binom{2r}{r}$. Потребно је да докажемо да $n+r$ дели $A_{n,r} = \frac{r}{2}\binom{2r}{r}\binom{2n}{n} = \frac{(2r-1)!(2n)!}{(r-1)!^2 n!^2}$ за свако n.

    Посматрајмо неки прост делилац $p \mid n+r$; нека $p^k \parallel n+r$. Степен p у $A_{n,r}$ је $v_p = \sum_{i>0} c_i$, где је $c_i = ([\frac{2r-1}{p^i}] - 2[\frac{r-1}{p^i}]) + ([\frac{2n}{p^i}] - 2[\frac{n}{p^i}]) \geqslant 0$. Претпоставимо да је $c_i = 0$: тада је $[\frac{2r-1}{p^i}] = 2[\frac{r-1}{p^i}]$ и $[\frac{2n}{p^i}] = 2[\frac{n}{p^i}]$, одакле следи да r и n дају остатке не веће од $\frac{p^i-1}{2}$ при дељењу са p^i, при чему $p^i \nmid r$, одакле одмах добијамо $p^i \nmid n + r$. Следи да је $c_i \geqslant 1$ за $i = 1, \dots, k$, и према томе $v_p \geqslant k$. Како ово важи за свако p, закључујемо да $n+r \mid A_{n,r}$.

    Претпоставимо сада да је $N_r < \frac{r}{2}\binom{2r}{r}$. То би значило да $\frac{\frac{r}{2}\binom{2r}{r}}{N_r}$ дели $\frac{A_{n,r}}{n+r}$ за све n, тј. постоји прост број p који дели $\frac{A_{n,r}}{n+r}$ за све n. Ставимо $n + r = p^k$. За $1 \leqslant i \leqslant k$ имамо $[\frac{2r-1}{p^i}] + [\frac{2n}{p^i}] = 2p^{k-i} - 1$ и $[\frac{r-1}{p^i}] + [\frac{n}{p^i}] = p^{k-i} - 1$, одакле је $c_i = 1$ за $1 \leqslant i \leqslant k$ и $c_i = 0$ за $i > k$. Дакле, $v_p = k$, тј. $p^k \parallel A_{n,r}$, па $p \nmid \frac{A_{n,r}}{n+r}$, контрадикција.

13. Број $\binom{2n+1}{n} = \frac{(2n+1)!}{n!(n+1)!}$ је дељив сваким простим бројем у интервалу $(n+2, 2n+1]$, одакле следи $\frac{(2n+1)\sharp}{(n+1)\sharp} \leqslant \binom{2n+1}{n} < 2^{2n}$.

Сада тврђење задатка доказујемо индукцијом по n: ако је оно тачно за n, онда је по претходном $(2n+1)\sharp \leqslant 2^{2n}(n+1)\sharp < 2^{2n}4^{n+1} = 4^{2n+1}$, тј. тачно је и за $2n+1$ и $2n+2$.

Напомена. Познато је из аналитичке теорије бројева да је $\lim_{n\to\infty} \sqrt[n]{n\sharp} = e$.

14. Претпоставимо да у интервалу $(n, 2n)$ нема простих бројева. По задатку 5, сви прости делиоци броја $\binom{2n}{n}$ су не већи од $\frac{2n}{3}$. Нека је $\binom{2n}{n} = p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$ канонска факторизација броја $\binom{2n}{n}$. По задатку 2, за свако p_i је $p_i^{r_i} < 2n$. Тако за $\sqrt{2n} < p_i \leqslant \frac{2n}{3}$ важи $r_i \leqslant 1$. Следи да је по задатку 13

$$\frac{4^n}{2n} < \binom{2n}{n} = \prod_{p_i \leqslant \sqrt{2n}} p_i^{r_i} \prod_{\sqrt{2n} < p_i \leqslant \frac{2n}{3}} p_i < \prod_{p_i \leqslant \sqrt{2n}} (2n) \cdot \left(\left[\frac{2n}{3}\right]\right)\sharp < (2n)^{\sqrt{2n}} 4^{\frac{2n}{3}}.$$

Следи да је $4^{\frac{n}{3}} < (2n)^{\sqrt{2n}+1}$ што није тачно за $n \geqslant 500$, чиме је за ове n доказ завршен. За $n < 500$ тврђење такође важи јер интервал $(n, 2n)$ садржи бар један од следећих простих бројева: $3, 5, 7, 13, 23, 43, 83, 163, 317, 631$.

15. (а) Ово је тривијално: $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, где $p \mid p!$ и $p \nmid i!(p-i)!$.
(б) $\binom{p-1}{i} = \frac{(p-1)(p-2)\cdots(p-i)}{i!} \equiv \frac{(-1)(-2)\cdots(-i)}{i!} = (-1)^i \pmod{p}$;
(в) $\frac{1}{p}\binom{p}{i} = \frac{1}{i}\frac{(p-1)!}{(i-1)!(p-i)!} = \frac{1}{i}\binom{p-1}{i-1} \equiv \frac{1}{i}(-1)^{i-1}$ по делу (б).
(г) $\binom{p-1-i}{j} = \frac{(p-i-1)(p-i-2)\cdots(p-i-j)}{j!} \equiv (-1)^j \frac{(i+j)\cdots(i+2)(i+1)}{j!} = (-1)^j\binom{i+j}{j} \pmod{p}$.

16. Из услова је $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1} \equiv (-1)^i + (-1)^{i-1} = 0$, тј. $n \mid \binom{n}{i}$ за $i = 1, 2, \ldots, n-1$. Из задатка 9 следи да је n прост број.

Решење 2. Нека је n сложен и p његов најмањи прост делилац. Тада је $(-1)^p \equiv \binom{n-1}{p} = \frac{n-1}{1}\cdots\frac{n-p+1}{p-1}\cdot\frac{n-p}{p} \equiv (-1)^{p-1}(\frac{n}{p}-1)$, дакле $\frac{n}{p} - 1 \equiv -1 \pmod{n}$, тј. $n \mid \frac{n}{p}$, контрадикција.

17. $\binom{2n}{n} = \frac{(2n)!}{n!^2} = \frac{2^n(2n-1)!!}{n!} \equiv \frac{(-2)^n(p-1)(p-3)\cdots(p-2n+1)}{n!} \equiv \frac{(-4)^n\frac{p-1}{2}\frac{p-3}{2}\cdots\frac{p-2n+1}{2}}{n!} = (-4)^n\binom{\frac{p-1}{2}}{n} \pmod{p}$.

18. Сума из задатка је $\sum_{n=0}^{\frac{p-1}{2}}(-2)^n\binom{2n}{n} \equiv \sum_{n=0}^{\frac{p-1}{2}} 8^n\binom{\frac{p-1}{2}}{n} = (1+8)^{\frac{p-1}{2}} = 3^{p-1} \equiv 1 \pmod{p}$.

19. Како је $2C_n = 4\binom{2n}{n} - \binom{2n+2}{n+1} \equiv \binom{2n}{n} - \binom{2n+2}{n+1} \pmod{3}$, сума из задатка се крати до $\frac{1}{2}(\binom{2}{1} - \binom{2n+2}{n+1})$. Ово је конгруентно са $1 \pmod{3}$ ако и само ако $3 \mid \binom{2n+2}{n+1}$. Тврђење следи из Кумерове теореме.

20. Довољно је доказати да важи $\binom{m}{n} = \binom{m'}{n'}\binom{m_0}{n_0} \pmod{p}$ ако је $m = pm' + m_0$ и $n = pn' + n_0$, $0 \leqslant m_0, n_0 < p$ - одатле ће Лукасова теорема следити индукцијом.

Број $\binom{m}{n}$ је коефицијент уз x^n у полиному $(1+x)^m$. На основу задатка 15 је $(1+x)^p \equiv 1 + x^p \pmod{p}$, па је $(1+x)^m \equiv (1+x)^{m'p}(1+x)^{m_0} \equiv (1+x^p)^{m'}(1+x)^{m_0} \pmod{p}$. Коефицијент уз $x^n = x^{n'p+n_0}$ у полиному $(1+x^p)^{m'}(1+x)^{m_0}$ је једнак $\binom{m'}{n'}\binom{m_0}{n_0}$, чиме је доказ завршен.

21. По Лукасовој теореми је $\binom{n}{p} \equiv \binom{n'}{1}\binom{n_0}{0} = n' \pmod{p}$, где је $n = pn' + n_0$ и $0 \leqslant n_0 < p$.

22. Нека су $n = n_k2^k + \cdots + n_0$ и $i = i_k2^k + \cdots + i_0$ бинарни записи бројева n и i. По Лукасовој теореми, $\binom{n}{i} \equiv \prod_j \binom{n_j}{i_j} \pmod{2}$ је непарно ако и само ако су сви $\binom{n_j}{i_j}$ непарни, ако и само ако $n_j = 0 \Rightarrow i_j = 0$ за све j. За дате бинарне цифре n_j, цифре i_j се могу одабрати на тачно 2^r начина тако да ово буде задовољено, где је r број јединица међу цифрама n_j. Дакле, међу $\binom{n}{i}$ има 2^r непарних бројева.

23. Нека су у биномном запису $n = \overline{n_{m-1}\cdots n_1n_0}$ и $k = \overline{k_{m-1}\cdots k_1k_0}$. Број $\binom{n}{k}$ је непаран ако и само ако је $k_i \leqslant n_i$ за свако i. Тако за сваку позицију i пар (n_i, k_i) можемо одабрати на 3 начина, па је укупан број могућности за пар (n, k) једнак 3^m.

24. Следи из познате једнакости о Фибоначијевим бројевима: $\sum_i \binom{n-i}{i} = F_{n+1}$, што је парно ако и само ако $3 \mid n+1$.

25. По малој Фермаовој теореми важи $(1+x)^n \equiv (1+x)^k \pmod p$ за све $x \in \mathbb{Z}$. С друге стране, ако леву страну тражене релације означимо са L_j, онда је $(1+x)^n \equiv P(x) = \sum_{i=1}^{p-1} L_i x^i$ за $x \in \mathbb{Z}$. Следи да полином $(1+x)^k - P(x)$, који је степена највише $p-1$, има p нула у $\mathbb{Z}_p$, па сви његови коефицијенти дељиви са p - укључујући и коефицијент уз x^j, који је једнак $L_j - \binom{k}{j}$.

26. (а) Инверзи бројева $1^2, 2^2 \dots, (p-1)^2$ по модулу p су ови исти бројеви у неком редоследу. Зато је $1 + \frac{1}{2^2} + \dots + \frac{1}{(p-1)^2} \equiv 1^2 + 2^2 + \dots + (p-1)^2 = \frac{p(p+1)(2p+1)}{3} \equiv 0 \pmod p$;
(б) $2(1 + \frac{1}{2} + \dots + \frac{1}{p-1}) = \sum_i (\frac{1}{i} + \frac{1}{p-i}) = p \sum_i \frac{1}{i(p-i)} \equiv -p \sum_i \frac{1}{i^2} \equiv 0 \pmod{p^2}$;
(в) $2\sum_{i<j} \frac{1}{ij} = (\sum_i \frac{1}{i})^2 - \sum_i \frac{1}{i^2} \equiv 0 \pmod p$.

27. Подсетимо се да је $\binom{2p}{p} - 2 = \sum_{i=1}^{p-1} \binom{p}{i}^2$. При том $p^2 \mid \binom{p}{i}^2$ и $\frac{1}{p^2}\binom{p}{i}^2 \equiv \frac{1}{i^2}$ по задатку 15. Одавде је $\frac{1}{p^2}(\binom{2p}{p} - 2) \equiv \sum_{i=1}^{p-1} \frac{1}{i^2} \equiv 0 \pmod p$ по задатку 26.

28. Имамо $\binom{np}{p} = n \prod_{i=1}^{p-1} \frac{(n-1)p+i}{i} \equiv n \prod_{i=1}^{p-1} (1 + \frac{n-1}{i} p) \pmod{p^3}$, што након развијања даје $\binom{np}{p} \equiv n(1 + p(n-1)\sum_i \frac{1}{i} + p^2(n-1)^2 \sum_{i \neq j} \frac{1}{ij}) \equiv n \pmod{p^3}$ по задатку 26.

29. За $n \geqslant 2$ имамо $\binom{p^n}{p} = p^{n-1}\binom{p^n-1}{p-1}$, при чему је $\binom{p^n-1}{p-1} = \prod_{i=1}^{p-1} \frac{p^n-i}{i} = \prod_{i=1}^{p-1} \left(\frac{p^n}{i} - 1\right) \equiv (-1)^{p-1} + p^n \sum_{i=1}^{p-1} \frac{1}{i} \equiv 1 \pmod{p^{n+2}}$ по задатку 25. За $n = 1$ је тривијално.

30. (а) За прост број $p > 2$ и $n = 2p$ имамо $\binom{kn}{n} = k \prod_{i=1}^{p-1} \frac{2kp-i}{2p-i} \cdot (2k-1) \prod_{i=1}^{p-1} \frac{2kp-p-i}{p-i} \equiv k(2k-1) \pmod p$. Конкретно, одавде је $\binom{kn}{n}$ дељиво са p за $k \in \{\frac{p+1}{2}, p, 2p\}$, тј. S_n има три елемента дељива са p, па није потпун систем остатака.
(б) За прост број $p > 2$ и $n = p^2$ имамо $\binom{kn}{n} = \prod_{i=0}^{p^2-1} \frac{kp^2-i}{p^2-i} = k \prod_{j=1}^{p-1} \frac{kp^2-jp}{jp} \cdot \prod_{p \nmid j} \frac{kp^2-i}{p^2-i}$, одакле је $\binom{kn}{n} \equiv k \prod_{j=1}^{p-1} \frac{kp-j}{j} = k \prod_{j=1}^{p-1} \left(1 - \frac{kp}{j}\right) \equiv k - k^2 p \sum_{j=1}^{p-1} \frac{1}{j} \equiv k \pmod{p^2}$, дакле n задовољава услов задатка.

31. Како је $\binom{p+i}{i} = \frac{p+i}{i} \cdots \frac{p+1}{1} \equiv 1 \pmod p$ и $p \mid \binom{p}{i}$, за $i = 0, 1, \dots, p-1$ важи $\binom{p}{i}\binom{p+i}{i} \equiv \binom{p}{i} \pmod{p^2}$. Сабирањем ових једнакости и додавањем $\binom{2p}{p} \equiv 2 \pmod{p^2}$ следи тврђење.

32. На основу задатка 15 је $S_a \equiv \sum_{i=1}^{p-1} \frac{(-1)^{i-1}}{p}\binom{p}{i} a^i = \frac{a^p - 1 - (a-1)^p}{p} \pmod p$. Одавде добијамо $S_3 + S_4 - 3S_2 = \frac{4^p - 4\cdot 2^p + 4}{p} = \frac{(2^p-2)^2}{p}$, што је дељиво са p.

33. По задатку 15 имамо $1 + \frac{1}{3} + \dots + \frac{1}{p-2} \equiv \frac{1}{p}\binom{p}{1} + \frac{1}{p}\binom{p}{3} + \dots + \frac{1}{p}\binom{p}{p-2} = \frac{2^{p-1}-1}{p} \pmod p$.

34. Имамо $2^{p-1} = \frac{(2p-2)!!}{(p-1)!} = \prod_{i=1}^{\frac{p-1}{2}} \frac{p+2i-1}{2i-1} = \prod_{i=1}^{\frac{p-1}{2}} (1 + \frac{p}{2i-1})$. Последњи израз је након развијања управо једнак десној страни тражене једнакости.

35. Уз ознаке из 34. задатка, имамо $(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} = \prod_{i=1}^{\frac{p-1}{2}} (1 - \frac{p}{i}) = 1 - pA + p^2 B \pmod{p^3}$, где је $A = \sum_i \frac{1}{i}$ и $B = \sum_{i<j} \frac{1}{ij}$ (обе суме су са индексима из $\{1, \dots, \frac{p-1}{2}\}$). При том је $\frac{1}{2}A + H_1 = 1 + \frac{1}{2} + \dots + \frac{1}{p-1} \equiv 0 \pmod{p^2}$ и $\frac{1}{4}B \equiv H_2 \pmod p$, дакле $(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 1 + 2pH_1 + 4p^2 H_2 \pmod{p^3}$.

С друге стране, важи $2^{p-1} \equiv 1 + pH_1 + p^2 H_2 \pmod{p^3}$ и $H_1^2 = \sum_i \frac{1}{i^2} + 2H_2 \equiv 2H_2 \pmod p$ (сума по непарним $1 \leqslant i < p$), дакле $2^{p-1} \equiv 1 + pH_1 + \frac{1}{2}p^2 H_1^2 \pmod{p^3}$. Квадрирање даје $4^{p-1} \equiv 1 + 2pH_1 + 2p^2 H_1^2 \pmod{p^3}$, што смо и желели да покажемо.

36. (а) По Кумеровој теореми, ако је $k = \overline{k_{n-1} \dots k_1 k_0}_3$ запис броја k у основи 3, $\binom{2k}{k}$ није дељив са 3 ако и само ако ниједна од цифара k_i није двојка, и тада је $\binom{2k}{k} \equiv$

$\binom{2k_{n-1}}{k_{n-1}}\cdots\binom{2k_0}{k_0} \pmod 3$. Према томе, збир $\sum_{k=0}^{3^n-1}\binom{2k}{k}$ је по модулу 3 конгруентан збиру $\sum_{k_i\in\{0,1\}}\binom{2k_{n-1}}{k_{n-1}}\cdots\binom{2k_0}{k_0} = \left(\binom{0}{0}+\binom{2}{1}\right)^n \equiv 0 \pmod 3$.

(б) Посматрани збир је једнак коефицијенту уз x^{3^n-1} у полиному

$$x^{3^n-1}\sum_{i=0}^{3^n-1}\frac{(x+1)^{2i}}{x^i} = \frac{(x+1)^{2\cdot 3^n}-x^{3^n}}{x^2+x+1} = (1-x)\cdot\frac{\sum_{i=0}^{2\cdot 3^n}\binom{2\cdot 3^n}{i}x^i - x^{3^n}}{1-x^3} = f(x).$$

Подсетимо се да је $\frac{1}{1-x^3}$ једнако степеном реду $\sum_{j=0}^{\infty}x^{3j}$. Како је по Кумеровој теореми $\binom{2\cdot 3^n}{i}$ дељиво са 3^n кад год $3\nmid i$, следи да је $f(x)\equiv(1-x)\left(\sum_{i=0}^{2\cdot 3^{n-1}}\binom{2\cdot 3^n}{3i}x^{3i}-x^{3^n}\right)\times\left(\sum_{j=0}^{\infty}x^{3j}\right) \pmod{3^n}$, па се у развоју $\frac{1}{1-x}f(x) \pmod{3^n}$ појављују само експоненти дељиви са 3. Према томе, након множења са $1-x$, у развоју $f(x) \pmod{3^n}$ неће бити експонената облика $3i-1$, па је коефицијент уз x^{3^n-1} једнак $0 \pmod{3^n}$.

37. Бројеви $\binom{2^n-1}{i}$ ($i=0,1,\dots,2^{n-1}-1$) су непарни на основу Лукасове теореме. Довољно је показати да су они различити по модулу 2^n. Приметимо да је

$$\begin{aligned}&\binom{2^{n+1}-1}{2i}=\binom{2^{n+1}}{2i+1}-\binom{2^{n+1}-1}{2i+1}=\tfrac{2^{n+1}}{2i+1}\binom{2^{n+1}-1}{2i}-\binom{2^{n+1}-1}{2i+1}\equiv-\binom{2^{n+1}-1}{2i+1} \pmod{2^{n+1}} \quad \text{и}\\ &\binom{2^{n+1}-1}{2i}=\prod_{k=1}^{i}\tfrac{2^{n+1}-(2k-1)}{2k-1}\cdot\prod_{k=1}^{i}\tfrac{2^n-k}{k}\equiv(-1)^i\binom{2^n-1}{i} \pmod{2^{n+1}}.\end{aligned} \tag{$*$}$$

Тврђење задатка ћемо показати индукцијом по n. За $n=1$ је тривијално; претпоставимо да важи за неко $n\geqslant 1$. За $0\leqslant k\leqslant l<2^{n-1}$, из $(*)$ следи да $2^n \mid \binom{2^n-1}{k}-\binom{2^n-1}{l}$ ако и само ако $k=l$, и $2^n \mid \binom{2^n-1}{k}+\binom{2^n-1}{l}$ само за $l=k+1$. При том, у другом случају $2^{n+1}\nmid\binom{2^n-1}{k}+\binom{2^n-1}{l}=\binom{2^n}{l}$.

Нека су сада $0\leqslant i\leqslant j\leqslant 2^n-1$ цели бројеви за које је $\binom{2^{n+1}-1}{i}\equiv\binom{2^{n+1}-1}{j} \pmod{2^{n+1}}$. Из $(*)$ добијамо $\binom{2^n-1}{[i/2]}\equiv\pm\binom{2^n-1}{[j/2]} \pmod{2^{n+1}}$. Као што смо показали, ово је могуће само за $[\frac{j}{2}]=[\frac{i}{2}]$, тј. $j\in\{i,i+1\}$, а по $(*)$ је могуће једино $i=j$. Овим је тврђење задатка доказано и за $n+1$, и индукција је готова.

38. Како је $\binom{2^{k+1}}{2^k}=\frac{(2^{k+1})!}{(2^k)!^2}=\frac{2^{2^k}}{(2^k)!}(2^{k+1}-1)!!$ и слично $\binom{2^k}{2^{k-1}}=\frac{2^{2^{k-1}}}{(2^{k-1})!}(2^k-1)!!=\frac{2^{2^k}}{(2^k)!}((2^k-1)!!)^2$, разлика $D=\binom{2^{k+1}}{2^k}-\binom{2^k}{2^{k-1}}$ се може записати као

$$D=\frac{2^{2^k}(2^k-1)!!P(2^k)}{(2^k)!},\quad \text{за } P(x)=(x+1)(x+3)\cdots(x+2^k-1)-(x-1)(x-3)\cdots(x-2^k+1).$$

Будући непаран, полином $P(x)$ је облика $c_1x+c_3x^3+c^5x^5+\cdots$. Коефицијент c_1 је једнак $2(2^k-1)!!\sum_{i=1}^{2^{k-2}}\left(\frac{1}{2i-1}+\frac{1}{2^k-2i+1}\right)=2^{k+1}(2^k-1)!!\sum_{i=1}^{2^{k-2}}\frac{1}{(2i-1)(2^k-2i+1)}$ и $\sum_{i=1}^{2^{k-2}}\frac{1}{(2i-1)(2^k-2i+1)}$ $\equiv-\sum_{i=1}^{2^{k-2}}(2i-1)^2\equiv 2^{k-2} \pmod{2^k}$ по формули за збир квадрата, дакле $2^{2k-2}\parallel c_1$. Следи да је у развоју $P(2^k)=2^kc_1+2^{3k}c_3+\cdots$ први сабирак дељив тачно са 2^{3k-1}, дакле $2^{3k-1}\parallel P(2^k)$. Осим тога, $2^1\parallel\frac{2^{2^k}(2^k-1)!!}{(2^k)!}$, одакле следи тврђење.

Београд, 2013-2017.