$a^n \pm b^n$

Hugo Trebše (hugo.trebse@gmail.com)

18. november 2025

Zapiski sledijo avtorjevem predavanju na pripravah za mednarodna matematična tekmovanja. Za vse napake ter netočnosti je odgovoren avtor sam. Če imate vprašanje ali popravek, se obrnite na e-poštni naslov zgoraj.

Zahvaljujem se Luku Horjaku za pomoč pri urejanju ter mnoge nasvete.

Lema o dvigu eksponenta je podobna
Svetemu rimskem cesarstvu; ni sveto,
ni rimsko in niti ni cesarstvo.

---

prirejeno po Voltairu

Kazalo

1 Uvod

Na matematičnih tekmovanjih se pogosto pojavijo razlike oziroma vsote istih potenc naravnih števil. Ta izroček je namenjen predstavljanju različnih metod, ki jih lahko uporabimo, ko se soočamo s takimi izrazi.

Brez dokaza navedemo naslednji trditvi, ki sta vam gotovo znani.

Trditev 1.1. *Za vse $a, b \in \mathbb{R}$ ter vse $n \in \mathbb{N}$ velja*

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right) = (a-b)\left(\sum_{i=0}^{n-1} a^i b^{n-1-i}\right).$$

Če je n lih, velja še

$$\begin{aligned} a^n + b^n &= (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 + \cdots + a^2b^{n-3} - ab^{n-2} + b^{n-1}) \\ &= (a+b)\left(\sum_{i=0}^{n-1} (-1)^i a^i b^{n-1-i}\right). \end{aligned}$$

Izrek 1.2 (Binomski izrek). *Naj bosta $a, b \in \mathbb{R}$ ter $n \in \mathbb{N}$. Tedaj velja*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

1.1 Naloge za vajo

Naloga 1.3. *Naj bodo a, m in n naravna števila. Pokaži, da je*

$$\gcd(a^n - 1, a^m - 1) = a^{\gcd(m,n)} - 1.$$

Definicija 1.4. Za naravni števili a, n imenujemo d *red a modulo n*, če je d najmanjše naravno število, za katerega velja $a^d = 1 \pmod{n}$. Če ima a red po modulu n označimo $d = \operatorname{ord}_n(a)$.

Naloga 1.5 (Red elementa).

- *Pokaži, da če je $\gcd(a, n) = 1$, potem obstaja $\operatorname{ord}_n(a)$.*
- *Pokaži, da če za $\ell \in \mathbb{N}$ velja $a^\ell = 1 \pmod{n}$, potem red obstaja in velja $\operatorname{ord}_n(a) \mid \ell$.*
- *Naj bo $n = p$ praštevilo in $a \in \mathbb{N}$ naravno število tuje p. Pokaži, da števila $\left\{1, a, \ldots, a^{d-1}\right\}$ puščajo različne ostanke po modulu p.*
- *Naj bo a naravno število, ki je tuje praštevilu p. Pokaži, da $\operatorname{ord}_p(a) \mid p - 1$.*

2 Pregled p-adične valuacije

Definicija 2.1: p-adična valuacija

Naj bo $p \in \mathbb{P}$ ter $n \in \mathbb{N}$. *p-adična valuacija* števila n je tako nenegativno celo število $\nu_p(n)$, da velja

$$p^{\nu_p(n)} \mid n \quad \text{in} \quad p^{\nu_p(n)+1} \nmid n.$$

Lema 2.2 (Alternativna karakterizacija p-adičnosti). *$\nu_p(n)$ je ravno potenca prafaktorja p, ki nastopa v praštevilskem razcepu n.* Osnovni izrek aritmetike *tako na alternativen način karakterizira p-adično valuacijo, namreč*

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}.$$

Naslednje lastnosti so po alternativni karakterizaciji p-adičnosti očitne.

Izrek 2.3

Za $x, y \in \mathbb{N}$ velja:

- $\nu_p(xy) = \nu_p(x) + \nu_p(y)$
- $\nu_p(x^y) = y \cdot \nu_p(x)$
- $\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}$. Če velja $\nu_p(x) \neq \nu_p(y)$, potem sledi enakost.

p-adična valuacija je daleč najuporabnejša pri multiplikativnih problemih – tistih, ki pretežno sestojijo iz množenja ter potenciranja, kar zrcali tudi razlika med prvima dvema ter tretjo točko zgornjega izreka. Šibkost p-adične valuacije leži v seštevanju; pri slednjem je v splošnem najuporabnejši *Evklidov algoritem*.

Spomnimo se še naslednjih dveh konceptov iz teorije števil, katera se zelo lepo izrazita s p-adičnostmi.

Trditev 2.4. *Naj bodo $a_1, a_2, \cdots, a_n$ naravna števila. Z oznakama* gcd *in* lcm *označujemo funkciji največji skupni delitelj in najmanjši skupni večkratnik. Velja:*

$$\gcd(a_1, \ldots, a_n) = \prod_{p \in \mathbb{P}} p^{\min\{\nu_p(a_1), \nu_p(a_2), \cdots, \nu_p(a_n)\}}$$

ter

$$\operatorname{lcm}(a_1, a_2, \ldots, a_n) = \prod_{p \in \mathbb{P}} p^{\max\{\nu_p(a_1), \nu_p(a_2), \cdots, \nu_p(a_n)\}}.$$

Naslednji izrek ponovno prikaže moč p-adične valuacije pri mulitplikativnih problemih.

Definicija 2.5. Funkcija celi del je funkcija $\lfloor \cdot \rfloor : \mathbb{R} \mapsto \mathbb{Z}$, ki realnemu številu dodeli največje celo število, ki ne presega tega realnega števila. Se pravi, funkcija celi del realnemu številu x pripiše tako celo število $n = \lfloor x \rfloor$, da velja

$$n \leq x < n + 1.$$

Velja na primer $\lfloor \pi \rfloor = 3$, $\lfloor -e \rfloor = -3$ ter $\lfloor 2 \rfloor = 2$.

Pogosto je uporabno definirati funkcijo neceli del s predpisom $\{x\} = x - \lfloor x \rfloor$, saj po definiciji sledi $0 \leq \{x\} < 1$, kar omogoča bolj intuitivno omejevanje vrednosti.

Izrek 2.6: Legendrova formula

Naj bo $n \in \mathbb{N}$ ter $p \in \mathbb{P}$. Potem velja

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Dokaz. Opazimo, da za vse dovolj velike $j \in \mathbb{N}$ velja $p^j > n$, kar pomeni, da so vsi členi vsote z indeksi večjimi od j enaki 0. Sledi, da je vsota na desni končna. Sedaj pokažimo enakost. Obstaja natanko $\left\lfloor \frac{n}{p} \right\rfloor$ števil med 1 in n, ki so deljiva s p. Izmed teh jih je $\left\lfloor \frac{n}{p^2} \right\rfloor$ s p deljivo vsaj dvakrat, $\left\lfloor \frac{n}{p^3} \right\rfloor$ s p deljivo vsaj trikrat in podobno naprej.

Naj množica A_j vsebuje vsa števila med 1 in n, ki imajo p-adičnost vsaj j – sledi torej $|A_j| = \left\lfloor \frac{n}{p^j} \right\rfloor$. Očitno je

$$A_0 \supsetneq A_1 \supsetneq A_2 \supsetneq A_3 \supsetneq \cdots$$

Za vsako število, ki ima p-adičnost natanko j, velja, da je v množici števil s p-adičnostjo vsaj j ter ni v množici števil p-adičnosti vsaj $j+1$. Sledi, da je števil med 1 in n s p-adičnostjo natanko j enako $\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n}{p^{j+1}} \right\rfloor$. Števila med 1 in n s p-adičnostjo natanko j tako p-adičnosti fakultete doprinesejo

$$j \cdot \left(\left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n}{p^{j+1}} \right\rfloor \right)$$

faktorjev p. Sledi, da je

$$\begin{aligned}
\nu_p(n!) &= \sum_{i=1}^{\infty} i \cdot \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+i}} \right\rfloor \right) \\
&= \sum_{i=1}^{\infty} i \cdot \left\lfloor \frac{n}{p^i} \right\rfloor - \sum_{i=1}^{\infty} (i-1) \cdot \left\lfloor \frac{n}{p^i} \right\rfloor \\
&= \sum_{i=1}^{\infty} (i-(i-1)) \cdot \left\lfloor \frac{n}{p^i} \right\rfloor \\
&= \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.
\end{aligned}$$

□

Trditev 2.7. *Naj bo $n \in \mathbb{N}$ ter $p \in \mathbb{P}$. Potem velja*

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1},$$

kjer $s_p(n)$ označuje vsoto števk števila n zapisanega v bazi p.

Dokaz zgornje oblike Legendrove formule je razmeroma preprost, če poznamo Legendrovo formulo, ki vsebuje funkcijo celi del. Število n zapišemo v bazi p, nato pa se spomnimo na vsoto geometrijske vrste ter kaj $\left\lfloor \frac{n}{p^i} \right\rfloor$ predstavlja v zapisu n v bazi p.

Komentar 2.8: Neenakost p-adičnosti fakultete

Izpostavljeni dejstvi o p-adični valuaciji fakultete sta elegantni, a pogosto posebej uporabni, če ju povežemo z naslednjima ocenama, ki veljata za $n > 0$.

$$
\begin{aligned}
\sum_{i=1}^{K} \left(\frac{n}{p^i} - 1 \right) \leq \nu_p(n!) &= \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \leq \sum_{i=1}^{K} \frac{n}{p^i} \\
-K + \sum_{i=1}^{K} \frac{n}{p^i} &\leq \nu_p(n!) \leq \sum_{i=1}^{K} \frac{n}{p^i} \\
-K + n \cdot \frac{\frac{1}{p} - \frac{1}{p^{K+1}}}{1 - \frac{1}{p}} &\leq \nu_p(n!) \leq n \cdot \frac{\frac{1}{p} - \frac{1}{p^{K+1}}}{1 - \frac{1}{p}} \\
\frac{n - \frac{n}{p^K}}{p-1} - K < n \cdot \frac{1 - \frac{1}{p^K}}{p-1} - K &\leq \nu_p(n!) \leq n \cdot \frac{1 - \frac{1}{p^K}}{p-1} < \frac{n}{p-1},
\end{aligned}
$$

kjer je $K = \max \{x \in \mathbb{N} \mid p^x \leq n\} = \left\lfloor \log_p(n) \right\rfloor$, saj so sumandi vsote v Legendrovi formuli enaki 0 za $i \geq K$.
Lahko dobimo boljšo zgornjo mejo upoštevajoč trditev 2.7, saj je $s_p(n) \geq 1$. Tako je naša najboljša meja

$$
n \cdot \frac{1 - \frac{1}{p^K}}{p-1} - \left\lfloor \log_p(n) \right\rfloor \leq \nu_p(n!) \leq \frac{n-1}{p-1},
$$

oziroma upoštevajoč $n < p^{K+1}$ rahlo poenostavljeno

$$
\frac{n-p}{p-1} - \left\lfloor \log_p(n) \right\rfloor \leq \nu_p(n!) \leq \frac{n-1}{p-1} < \frac{n}{p-1}.
$$

Uporabnost teh neenakosti postane očitna pri reševanju Diofantskih enačb.

Na ne preveč zapletenem problemu prikažimo metodo p-adičnosti.

Naloga 2.9. *Naj bosta a in b celi števili, za kateri velja*

$$
a \mid b^2 \mid a^3 \mid b^4 \mid \cdots
$$

Pokaži, da je $a = b$.

Rešitev. Prevedimo problem deljivosti na problem p-adičnosti. Iz osnovnega izreka aritmetike opazimo, da če $x \mid y$, potem za vsa praštevila p velja $\nu_p(x) \leq \nu_p(y)$. Pogoj naloge se tako prevede na: za vse $p \in \mathbb{P}$ in za vse $i \in \mathbb{N}$ velja

$$
\nu_p(a^{2i-1}) \leq \nu_p(b^{2i}) \quad \text{in} \quad \nu_p(b^{2i}) \leq \nu_p(a^{2i+1}),
$$

kar je ekvivalentno

$$(2i-1)\cdot\nu_p(a) \le (2i)\cdot\nu_p(b) \quad \text{in} \quad (2i)\cdot\nu_p(b) \le (2i+1)\cdot\nu_p(a).$$

Tako sledi

$$\frac{2i-1}{2i} = 1 - \frac{1}{2i} \le \frac{\nu_p(b)}{\nu_p(a)} \le \frac{2i+1}{2i} = 1 + \frac{1}{2i}$$

Če je kvocient $\frac{\nu_p(a)}{\nu_p(b)}$ različen od 1, lahko seveda najdemo tak indeks i, da je kvocient bodisi manjši od $1-\frac{1}{2i}$, bodisi večji od $1+\frac{1}{2i}$, zaradi česar sledi, da je $\frac{\nu_p(a)}{\nu_p(b)} = 1$ za vse $p \in \mathbb{P}$.

Po trditvi 2.2 sledi $a = b$. $\square$

2.1 Naloge za vajo

Naloga 2.10. *Pokaži, da* $\sum_{i=1}^{n} \frac{1}{i}$ *ni naravno število za* $n > 1$.

Naloga 2.11. *Pokaži, da* $\sum_{i=1}^{n} \frac{1}{2i+1}$ *ni naravno število za* $n \in \mathbb{N}$

Naloga 2.12. *Dokaži, da za vse* $n \in \mathbb{N}$ *velja*

$$n! \;\Big|\; \prod_{k=0}^{n-1} \left(2^n - 2^k\right).$$

3 Dvig eksponenta

Preden nadaljujemo z lemo o dvigu eksponenta, je obvezno rešiti naslednjo nalogo, da trditev leme ponotranjimo.

Naloga 3.1. *Naj bo k nenegativno celo število. Pokaži, da je $\nu_3(2^{3^k}+1)=k+1$.*

Rešitev. Trditev naloge pokažemo z indukcijo na k. V primeru $k\in\{0,1\}$ je trditev očitna. Denimo, da je $k\geq 2$ ter $\nu_3(2^{3^{k-1}}+1)=k$. V jeziku indukcije naša naloga trdi, da v prehodu $k\to k+1$ izraz $2^{3^{k-1}}+1$ pridobi natanko en faktor števila 3. Tako je zadosti pokazati, da je

$$\frac{2^{3^k}+1}{2^{3^{k-1}}+1}$$

deljivo s 3, ni pa deljivo z 9. Sedaj lahko razvijemo

$$\frac{2^{3^k}+1}{2^{3^{k-1}}+1}=\left(2^{3^{k-1}}\right)^2-2^{3^{k-1}}+1=2^{2\cdot 3^{k-1}}-2^{3^{k-1}}+1=(-1)^2-(-1)+1=3 \pmod{3^k}.$$

Ker je $k\geq 2$ (zato smo tudi preverili dva bazna primera), je $3\not\equiv 0 \pmod{3^k}$. $\square$

Lema 3.2: Dvig eksponenta za $p\neq 2$

Naj bo p liho praštevilo ter x,y celi števili tuji p.

- Če $p\mid x-y$, velja
$$\nu_p(x^n-y^n)=\nu_p(x-y)+\nu_p(n).$$
- Če $p\mid x+y$ in je n **lih**, velja
$$\nu_p(x^n+y^n)=\nu_p(x+y)+\nu_p(n).$$

Lema 3.3: Dvig eksponenta za $p=2$

Naj bosta x,y lihi celi števili.

- Če $4\mid x-y$, velja
$$\nu_2(x^n-y^n)=\nu_2(x-y)+\nu_2(n).$$
- Če $2\mid x-y$ in n **sod**, velja
$$\nu_2(x^n-y^n)=\nu_2(x^2-y^2)+\nu_2\left(\frac{n}{2}\right)=\nu_2(x+y)+\nu_2(x-y)+\nu_2(n)-1.$$

Obe lemi lahko dokažemo z indukcijo na $v_p(n)$. Dokaza nista zelo originalna, sta pa nekoliko bolj tehnično zahtevna, kot bi si želeli. Posledično dokazov ne navedemo tu, zainteresirani bralec pa ju lahko najde v [1] ali [3].

Na mestu je naslednji opomnik Evana Chena. Če se na katerikoli točki uporabi leme o dvigu eksponenta znajdete v situaciji, ko je $\nu_p(x\pm y)=0$, ste gotovo pozabili preveriti enega izmed pogojev za veljavnost leme.

Komentar 3.4

K lemi o dvigu eksponenta pripada še naslednja standardna metoda. Lema nam magično poda neko enakost, ki na eni strani morda vsebuje naše naravne spremenljivke, na drugi strani pa je vsota nekih p-adičnosti. Zelo ohlapna ocena

$$\nu_p(n) \leq \log_p(n),$$

ki sledi iz deljivosti, ter omenjene meje glede p-adičnosti fakultete so pogosto uporabne za dokazovanje protislovnosti po velikosti. Opozorimo, da spodnje meje na $\nu_p(n)$ zares nimamo, pogosto pa lahko vse faktorje p iz n izpostavimo brez kakšne izgube splošnosti.

3.1 Naloge

Naloga 3.5. *Naj bodo $a, b, c \in \mathbb{N}$, za katera velja $c \mid a^c - b^c$. Pokaži, da*

$$c \,\Big|\, \frac{a^c - b^c}{a - b}\,.$$

Naloga 3.6. *Določi vse $n \in \mathbb{N}$, za katere obstajata tuji števili $x, y \in \mathbb{N}$ ter $k > 1$, da*

$$3^n = x^k + y^k.$$

Naloga 3.7. *Najdi vse pare naravnih števil (n, m), ki rešijo enačbo*

$$(n-1)! + 1 = n^m.$$

Naloga 3.8 (AIME 2018). *Najdi najmanjše naravno število n, za katero se zapis števila 3^n v bazi 143 konča s števkama 01.*

Naloga 3.9 (ZDA 2008). *Pokaži, da $n^7 + 7$ ni popolni kvadrat za nobeno $n \in \mathbb{N}$.*

Naloga 3.10 (MMO 1999, posplošitev naloge 4). *Naj bosta x, p celi števili, za kateri velja*

$$x^{p-1} \mid (p-1)^x + 1.$$

- *Določi vse pare (x, p), če je p praštevilo in $x \leq 2p$.*
- *Določi vse pare (x, p), če je p praštevilo.*

4 Zsigmondyjeva izreka

Zsigmondyjev izrek je zelo uporaben pri izrazih oblike $a^n \pm b^n$. Med drugim nam pokaže, da izrazi te oblike skoraj nikoli niso trivialne potence. Pove nam, da ko eksponent n višamo generiramo nova praštevila.

Izrek 4.1: Zsigmondyjev izrek za razlike potenc

Naj bosta $a, b \in \mathbb{N}$ tuji si števili ter naj bo $n > 1$ naravno število. Tedaj obstaja praštevilski delitelj $a^n - b^n$, ki ni praštevilski delitelj nobenega izmed števil $a^k - b^k$ za $k \in \{1, 2, \ldots, n-1\}$, z naslednjimi izjemami:

- $2^6 - 1^6 = 3^2 \cdot 7$, kjer je $3 = 2^2 - 1$ ter $7 = 2^3 - 1$.
- $n = 2$ ter $a + b = 2^\ell$ za nek $\ell \geq 1$, saj je $a^2 - b^2 = (a-b)(a+b)$, edini praštevilski delitelj $a + b$ je 2, ki je tudi praštevilski delitelj $a - b$.

Tak praštevilski delitelj imenujemo *primitivni praštevilski delitelj.*

Dokaz. Dokaz tega izreka presega nivo priprav na matematične olimpijade. Dokaz med drugim uporabi lemo o dvigu eksponenta ter nekatere lastnosti ciklotomičnih polinomov. □

Izrek 4.2: Zsigmondyjev izrek za vsote potenc

Naj bosta $a, b \in \mathbb{N}$ tuji si števili ter $n > 1$ naravno število. Tedaj obstaja praštevilski delitelj $a^n + b^n$, ki ne deli nobenega izmed števil $a^k + b^k$ za $k \in \{1, 2, \ldots, n-1\}$ z izjemo primera $2^3 + 1^3 = 3^2 = (2^1 + 1^1)^2$. Tak praštevilski delitelj imenujemo *primitivni praštevilski delitelj.*

Dokaz. To obliko Zsigmondyjevega izreka lahko dokažemo z uporabo Zsigmondyjevega izreka za razlike potenc upoštevajoč $a^{2n} - a^{2n} = (a^n - b^n)(a^n + b^n)$. Primitivni praštevilski delitelj $a^{2n} - b^{2n}$ mora tako biti vsebovan v $a^n + b^n$. Obenem ta delitelj ne more biti vsebovan v $a^k + b^k$ za $k \in \{1, 2, \ldots, n-1\}$, saj bi tedaj ta isti praštevilski delitelj delil $a^{2k} - b^{2k} = (a^k + b^k)(a^k - b^k)$. □

Ta izreka sta mišljena bolj kot zanimivost kot dejansko uporabna izreka pri reševanju nalog iz teorije števil. Te čase so člani komisij za izbiro nalog bolj teoretično podkovani ter so seznanjeni s tem izrekom. Posledično je zelo neverjetno, da bi Zsigmondyjev izrek trivializiral katerokoli nalogo na tekmovanju.

Še zmeraj pa sta izreka lahko uporabna; nekatere podprimere, ki bi jih v preteklosti morali dejansko obravnavati, lahko morda samo »odpišemo« z uporabo Zsigmondyjevega izreka. Prav tako lahko izreka ovržeta morebitne domneve, ki jih postavimo, kar nam lahko prihrani dosti časa.

Naloga 4.3. *Najdi čim več nalog v tem izročku, ki jih Zsigmondyjev izrek trivializira.*

Naloga 4.4. *Naj bo $p \in \mathbb{P}$ ter $m > 1$ naravno število. Pokaži, da ima enačba*

$$\frac{x^p + y^p}{2} = (\frac{x+y}{2})^m$$

rešitev različno od $(x, y) = (1, 1)$ natanko tedaj, ko je $m = p$.

Literatura

[1] Aditya Khurmi. *Modern Olympiad Number Theory*. 2020. URL: https://math.univ-lyon1.fr/~ducatez/content/Modern_Olympiad_TN.pdf.

[2] Bart Michels. *Zsigmondy's theorem*. 2014. URL: https://pommetatin.be/files/zsigmondy_en.pdf.

[3] Amir Hossein Parvardi. *Lifting The Exponent Lemma (LTE)*. 2016. URL: https://pregatirematematicaolimpiadejuniori.wordpress.com/wp-content/uploads/2016/07/lte.pdf.

[4] Justin Stevens. *Olympiad Number Theory Through Challenging Problems*. URL: https://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/olympiad-number-theory.pdf.