p-valuace

Matěj Doležálek

Abstrakt. V teorii čísel se občas vyplatí vědět nejen to, zda jedno číslo dělí druhé, ale i jak moc ho dělí. To vystihují p-valuace. Postupně se naučíme počítat je v rozmanitých situacích a používat je k dokazování dělitelností a řešení rovnic.

Definice. Pro celá čísla a, b říkáme, že a *dělí* b (značíme $a \mid b$), pokud existuje celé číslo c splňující $b = ac$.

Definice. Pro prvočíslo p definujeme p-valuaci celého čísla $a \neq 0$ jako největší nezáporné celé k takové, že $p^k \mid a$. Značíme $v_p(a) = k$. Pro $a = 0$ budeme brát $v_p(a) = \infty$ pro každé p.

Tedy neformálně: $v_p(a)$ je exponent u p v prvočíselném rozkladu čísla a. Jak uvidíme, p-valuace dávají způsob, jak se na situaci podívat z pohledu jednoho prvočísla. Jedná se přitom o trochu jemnější informaci než pouhý zbytek modulo p.

Základní vlastnosti

Tvrzení. *Platí $a \mid b$, právě pokud $v_p(a) \leq v_p(b)$ pro každé prvočíslo p.*

Tvrzení. *Pro $a, b > 0$ platí $a = b$, právě když $v_p(a) = v_p(b)$ pro každé prvočíslo p.*

Tvrzení. *Platí $v_p(ab) = v_p(a) + v_p(b)$.*

Tvrzení. *Platí $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$. Pokud navíc $v_p(a) \neq v_p(b)$, potom v předchozí nerovnosti nutně nastane rovnost. Obdobně platí totéž pro rozdíl $a - b$.*

Cvičení. Rozmyslete si, že p-valuace se dají rozumně dodefinovat i pro racionální čísla a že i po tomto rozšíření většina z předchozího stále platí.

Cvičení. Nahlédněte, že pro přirozené n je $v_p(n) \leq \log_p n \leq n - 1$.

Obecnější podoba předchozího cvičení:

Lemma. *Pro každé přirozené n platí odhad $n - v_p(n) \geq n - \log_p(n)$, přičemž výraz napravo je pro $n \geq 2$ rostoucí vzhledem k n.*

Tvrzení. *Přirozené číslo a je k-tou mocninou přirozeného čísla právě tehdy, když $k \mid v_p(a)$ pro každé prvočíslo p.*

Tvrzení. *Nechť* gcd *značí největšího společného dělitele a* lcm *nejmenší společný násobek. Potom platí*

$$v_p(\gcd(a,b)) = \min\{v_p(a), v_p(b)\}, \qquad v_p(\operatorname{lcm}(a,b)) = \max\{v_p(a), v_p(b)\}.$$

Úloha 1. Dokažte, že pro libovolná přirozená čísla a, b, c platí

$$\frac{(\gcd(a,b,c))^2}{\gcd(a,b)\cdot\gcd(b,c)\cdot\gcd(c,a)} = \frac{(\operatorname{lcm}(a,b,c))^2}{\operatorname{lcm}(a,b)\cdot\operatorname{lcm}(b,c)\cdot\operatorname{lcm}(c,a)}.$$

Úloha 2. Jsou dána přirozená čísla a, b taková, že

$$a \mid b^2, \quad b^2 \mid a^3, \quad a^3 \mid b^4, \quad b^4 \mid a^5, \quad a^5 \mid b^6, \quad \ldots$$

Dokažte, že $a = b$.

Úloha 3. Dokažte, že pro přirozená a, b, c, d splňující $ab = cd$ platí

$$\gcd(a,c)\cdot\gcd(a,d) = a\cdot\gcd(a,b,c,d).$$

Úloha 4. Jsou dána přirozená a, b, c splňující $a^b \mid b^c$, $a^c \mid c^b$. Dokažte, že $a^2 \mid bc$.

Úloha 5. Řekneme, že kladné reálné číslo je *copaté*, pokud není celé a v jeho desetinném zápisu následuje za desetinnou čárkou jen konečně mnoho nenulových číslic. Rozhodněte, zda existují copatá čísla a, b, c taková, že všechna tři čísla ab, bc i ca jsou celá. (MO 64–C–II–4)

Faktoriály a kombinační čísla

V dělitelnostech a rovnostech obsahujících faktoriály se často hodí spočítat nebo alespoň odhadnout p-valuaci. Vznikávají tím relativně nevábné výrazy s dolními celými částmi – občas je stačí odhadnout, jindy je třeba preciznější přístup. Základní pomůckou je Legendreova formule, zbylé dvě větičky jsou jen trochu specializovaná tvrzení plynoucí z ní.

Tvrzení. (Legendreova formule) *Pro každé přirozené číslo n platí*

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

Poznámka. Součet v předchozí větě je sice formálně nekonečný, ale pro libovolné p a n budou od nějaké chvíle všechny členy nulové.

Věta. *Nechť $s_p(n)$ značí ciferný součet přirozeného čísla n v soustavě o základu p. Potom platí $v_p(n!) = \frac{n - s_p(n)}{p-1}$.*

Věta. (Kummer) *Kombinační číslo $\binom{n}{k}$ má p-valuaci rovnou počtu „přenosů jedničky do vyššího řádu“ při sčítání k a $n-k$ pod sebou v soustavě o základu p.*

Úloha 6. Pro prvočíslo p platí $p^n \nmid ((p-1)n)!$.

Úloha 7. Platí $v_p(n!) \leq \left\lfloor \frac{n-1}{p-1} \right\rfloor$.

Úloha 8. Najděte všechna přirozená n, pro něž $v_2(n!) = n-1$.

Úloha 9. Pro libovolná celá nezáporná m, n je

$$\frac{(2m)!(2n)!}{m!n!(n+m)!}$$

celé číslo.

Úloha 10. Dokažte, že pro přirozená n platí

$$(n+1) \cdot \operatorname{lcm}\left(\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}\right) = \operatorname{lcm}(1, 2, \ldots, n+1).$$

Úloha 11. Dokažte, že existuje konstanta c taková, že pro libovolná přirozená a, b, n splňující $a! \cdot b! \mid n!$ nutně platí $a + b < n + c \log n$. (Erdős)

Úloha 12. Pro přirozené $n \geq 3$ definujme posloupnost přirozených čísel $\alpha_1, \ldots, \alpha_k$ pomocí rozkladu

$$n! = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

kde $p_1 < p_2 < \cdots < p_k$ jsou prvočísla. Najděte všechna n, pro něž je posloupnost $\alpha_1, \ldots, \alpha_k$ geometrická. (MEMO 2017 T8)

Lifting the exponent (LTE)

Podkapitolou samou pro sebe jsou valuace na rozdílech mocnin. Z velké části je vystihuje lifting the exponent lemma (zkráceně LTE), při jeho aplikování je však třeba dávat pozor na podmínky. Hodí se také tušit něco o řádech prvků modulo p.

Lemma. *Nechť je p libovolné prvočíslo, m přirozené číslo a x, y celá čísla taková, že $p \nmid m, x, y$, ale $p \mid x - y$. Potom $v_p(x^m - y^m) = v_p(x - y)$.*

Lemma. *Nechť je $p > 2$ prvočíslo a x, y celá čísla splňující $p \nmid x, y$, ale $p \mid x - y$. Potom $v_p(x^p - y^p) = v_p(x - y) + 1$.*

Cvičení. Co se na důkazu předchozího lemmatu rozbije pro $p = 2$?

Věta. (lifting the exponent lemma) *Nechť je p liché prvočíslo, n přirozené číslo a x, y celá čísla splňující $p \nmid x, y$, ale $p \mid x - y$. Potom*

$$v_p\left(x^n - y^n\right) = v_p(x - y) + v_p(n).$$

Poznámka. Pokud je n liché, pak nahrazením y za $-y$ získáme obdobné tvrzení i pro součet namísto rozdílu.

Cvičení. Najděte příklady dosvědčující, že při vynechání jednoho z předpokladů (lichosti p, dělitelnosti $p \mid x-y$ či nedělitelnosti $p \nmid x, y$) už závěr LTE nemusí platit.

Věta. (LTE pro dvojku) *Nechť je n sudé přirozené číslo a x, y lichá celá čísla. Potom*

$$v_2\left(x^n - y^n\right) = v_2(x-y) + v_2(x+y) + v_p(n) - 1.$$

Cvičení. Rozmyslete si, že v LTE pro dvojku bude vždy právě jedno z $v_2(x \pm y)$ rovno 1, takže se pravá strana zjednoduší na

$$v_2(x-y) + v_2(n) \qquad \text{nebo} \qquad v_2(x+y) + v_2(n).$$

Tvrzení. *Budiž p prvočíslo a nechť $p \nmid a, b$. Pokud je k nejmenší přirozené číslo splňující $p \mid a^k - b^k$, pak pro přirozené n platí $p \mid a^n - b^n$ právě tehdy, když $k \mid n$.*

Úloha 13. Je dáno přirozené k. Najděte všechna přirozená n splňující $3^k \mid 2^n - 1$.

Úloha 14. Pro liché prvočíslo p, přirozené a a $n \geq 2$ platí $p^n \mid a^p - 1$ právě tehdy, když $p^{n-1} \mid a - 1$.

Poznámka. (makroskopická) Předchozí úloha ilustruje, že LTE říká „zhruba totéž“ jako cykličnost multiplikativních grup $\mathbb{Z}_{p^k}^*$ pro $k \geq 2$. V obojím se přidání p do exponentu projeví posunem přesně o 1 „úroveň“ výš, obojí řeší jen prvky nesoudělné s p a v obojím je dvojka trochu „rozbitá“ (ale ne zas tak moc).

Úloha 15. Dokažte, že pro každé přirozené n lze zvolit přirozené k tak, že

$$7^n \mid 2^k + 3^k + 4^k - 1.$$

Úloha 16. Prvočíslo p a přirozená a, n splňují $2^p + 3^p = a^n$. Dokažte, že $n = 1$. (Irsko)

Úloha 17. Přirozená a, n, k splňují $n \mid (a-1)^k$. Dokažte $n \mid a^{n-1} + a^{n-2} + \cdots + a + 1$.

Úloha 18. Najděte všechny trojice (x, y, p), kde x, y jsou přirozená čísla a p prvočíslo splňující $p^x - y^p = 1$.

Úloha 19. Je dáno bezčtvercové[1] přirozené n. Dokažte, že neexistují nesoudělná přirozená čísla x, y splňující $(x+y)^3 \mid x^n + y^n$.

Úloha 20. Mějme liché přirozené $n > 1$ a nesoudělná přirozená $a > b$. Dokažte, že $a^n - b^n$ má prvočíselného dělitele, který nedělí $a - b$.

Úloha 21. Najděte všechna přirozená n splňující $2^n \mid 3^n - 1$.

Úloha 22. Najděte všechny dvojice přirozených čísel (a, b), které splňují $b^a \mid a^b - 1$.

[1] Přirozené číslo nazýváme *bezčtvercovým*, pokud není násobkem žádného a^2 pro $a > 1$.

Úloha 23. Najděte všechna přirozená a, pro něž je $4(a^n+1)$ třetí mocninou celého čísla pro každé přirozené n.

Úloha 24. Pokud pro přirozená a, b, c platí $c \mid a^c - b^c$, pak už i $c \mid \frac{a^c-b^c}{a-b}$.

Úloha 25. Buďte a, b racionální čísla. Pokud je $a^n - b^n$ celé číslo pro nekonečně mnoho různých přirozených n, pak už jsou obě a, b celá.

Úloha 26. Budiž $k > 1$ přirozené číslo. Dokažte, že existuje nekonečně mnoho přirozených n splňujících

$$n \mid 1^n + 2^n + \cdots + k^n.$$

Úloha 27. Najděte všechna přirozená n, pro která je $2^{n+2}(2^n - 1) - 8 \cdot 3^n + 1$ čtverec. (Vietnam)

IMO úlohy

Úloha 28. Najdi největší mocninu 1991, která dělí číslo

$$1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

(ISL 1991)

Úloha 29. Najděte všechny dvojice přirozených čísel (n, k), které splňují

$$(2^k - 1)(2^k - 2)(2^k - 4) \cdots (2^k - 2^{k-1}) = n!.$$

(IMO 2019)

Úloha 30. Je dána nekonečná posloupnost $a_1, a_2, a_3, \ldots$ přirozených čísel taková, že

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1}$$

je přirozené číslo pro všechna $n \geq k$, kde k je nějaké pevné přirozené číslo. Dokažte, že $a_n = a_{n+1}$ pro všechna $n \geq m$, kde m je nějaké pevné přirozené číslo.

(IMO 2018)

Úloha 31. Najděte všechny trojice (p, x, y), kde p je prvočíslo a x, y jsou přirozená čísla taková, že $x^{p-1} + y$ i $x + y^{p-1}$ jsou mocniny p. (ISL 2014)

Návody

1. BÚNO si seřaď valuace, potom přímočaře počítej.

2. $a^n \mid b^{n+1}$ znamená $\frac{v_p(a)}{v_p(b)} \leq \frac{n+1}{n}$. V podstatě totéž jde říct s logaritmem místo valuací.

3. Označ si p-valuace jednotlivých proměnných a rozebírej jejich možné pořadí.

4. AG nerovnost.

5. Chceš nezáporné 2-valuace a 5-valuace. Dirichlet pomůže.

6. V Legendreově formuli zahoď celé části.

7. Ukonči součet u indexu $j = k$ takového, že $1 \leq \frac{n}{p^k} < p$ a využij $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$.

8. V nerovnostech z důkazu předchozí úlohy musela všude nastat rovnost.

9. Odhadni zvlášť každý člen

$$\left\lfloor \frac{2m}{p^j} \right\rfloor + \left\lfloor \frac{2n}{p^j} \right\rfloor - \left\lfloor \frac{m}{p^j} \right\rfloor - \left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n+m}{p^j} \right\rfloor$$

z Legendreovy formule.

10. Využij Kummerovu větu. Pokud $\alpha = v_p(n+1)$, pak $n+1$ zapsané v soustavě o základu p končí α nulami.

11. Dělitelnost dává nerovnost (třeba) 2-valuací. Vhodně odhadni celé části v nenulových členech, těch je asymptoticky $\log n$.

12. Hodí se Bertrandův postulát: pro každé přirozené číslo $n \geq 2$ existuje prvočíslo p splňující $n < p < 2n$.

13. Přímočaře použij LTE. Pozor na předpoklady!

14. Nezapomeň na předpoklady LTE. Hodí se malá Fermatova věta: $a^p \equiv a \pmod{p}$ pro každé a.

15. Vol k tak, aby vznikly dvě LTEčkové dvojice.

16. LTE něco poví o 5-valuaci. Dej pozor na případ $p = 2$.

17. LTE na $a^n - 1$. Nezapomeňte pečlivě ověřit předpoklady.

18. Převeď y^p na pravou stranu a podívej se na p-valuaci.

19. Chceš aplikovat LTE a využít $v_p(n) \leq 1$, dej však pozor na degenerované případy související s dvojkou.

20. Má-li $a^n - b^n$ pouze prvočíselné dělitele, kteří dělí $a - b$, pak dovedeš odhadnout všechny p-valuace.

21. Rozkládej $3^n - 1 = (3^{n/2} + 1)(3^{n/2} - 1)$, dokud to jde.

22. Nejtěžší část: dokaž, že nejmenší prvočíslo $p \mid b$ také dělí $a - 1$. Potom rozliš paritu p, použij LTE a pečlivě odhadni $n - v_p(n)$.

23. Pokud má $4(a^n+1)$ lichého prvočíselného dělitele p, podívej se na $4(a^{pn}+1)$.

24. Pro každé prvočíslo $p \mid c$ rozliš případy dle toho, zda $p \mid a-b$ a zda $p \mid a, b$.

25. Předpokládej, že společný jmenovatel má prvočíselného dělitele, a najdi spor. Hodí se tušit něco o řádech prvků modulo p.

26. Zkus $n = p^m$, trik je ve správné volbě lichého prvočísla p. Zkus použít LTE na „zrcadlové“ členy.

27. Pojmenuj si čtverec a^2 a uprav na součin. Potom zkoumej 3-valuaci, zbav se a a omez n.

28. Prostě si vyrob LTEčkový tvar a moc se s tím nepárej.

29. Pomocí 2-valuace a 3-valuace omez k, zbytek dorozeber.

30. Stačí ukázat, že nepřibývají nová prvočísla a všechny p-valuace jsou od nějaké chvíle nerostoucí. Rozliš případy podle toho, zda někdy (za indexem k) nastane $v_p(a_n) \geq v_p(a_1)$.

31. Připrav se na spoustu rozebírání rozbitých případů. Hlavní myšlenka je hledat velké valuace p v rozdílech $y-x$ potažmo $y^p - x^p$.

Literatura a zdroje

[1] Anh Dung „Tonda“ Le: *Lifting The Exponent lemma*, Sklené, 2015.
[2] Ákos Záhorský: *P-adické hodnoty a Lifting The Exponent Lemma*, Kunžak, 2019.
[3] Amir Hossein Parvardi: *Lifting The Exponent Lemma (LTE)*.
[4] Yang P. Liu: v_p, MOP, 2018.