

Prvočíselné počítání

Matěj Doležálek



Abstrakt. Prvočísla jsou denním chlebem olympiádní teorie čísel. Pojďme s nimi počítat do šířky i do hloubky.

(plná verze s hinty)

<https://gimli.ms.mff.cuni.cz/~matej/olymp/23prosinec/full.pdf>

Rychloúvod do dělitelnosti a modulární aritmetiky

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

Fakt (alternativní definice prvočísla). Je-li p prvočíslu a a, b celá čísla taková, že $p \mid ab$, pak už $p \mid a$ nebo $p \mid b$.

Definice. Pro celá čísla a, b, m říkáme, že a je kongruentní b modulo m (značíme $a \equiv b \pmod{m}$), pokud $m \mid a - b$. Množinu všech navzájem kongruentních celých čísel nazýváme *zbytkovou třídou* (modulo m). Množinu všech zbytkových tříd mod m značíme $\mathbb{Z}_m$ a můžeme na ní zavést operace sčítání a násobení očekávatelným způsobem.

Úmluva. Množinu těch zbytkových tříd ze $\mathbb{Z}_m$, jež jsou s m nesoudělné, značíme $\mathbb{Z}_m^\times$.

Blažený svět modulo prvočíslu

Pozorování. Buď p prvočíslu a uvažme $a \in \mathbb{Z}_p^\times$. Pak je zobrazení

$$\begin{aligned}\mathbb{Z}_p &\rightarrow \mathbb{Z}_p, \\ x &\mapsto ax\end{aligned}$$

prosté (a tudíž rovnou bijektivní).

Důsledek (nenulovými zbytky lze dělit). Ke každému $b \in \mathbb{Z}_p^\times$ existuje nějaké $b' \in \mathbb{Z}_p^\times$ tak, že $bb' \equiv 1 \pmod{p}$. Toto b' budeme bez ostychu značit $\frac{1}{b}$.

Lze si rozmyslet, že z hlediska úpravy výrazů apod. má toto dělení zcela totožné vlastnosti s obvyklým dělením racionálních (reálných, komplexních, ...) čísel. Jediný zádrhel, na který je třeba si dávat pozor, je, že nesmíme dělit nulou, tedy jakýmkoliv násobkem p . Z toho také plyne:

Pozorování (úhel pohledu). Dosud jsme modulili celá čísla. Protože ale v $\mathbb{Z}_p$ smíme povětšinou dělit, je zcela validní a dobře definované se dívat modulo p i na zlomky, **dokud se však ve jmenovateli nevyskytne žádný násobek p .**

Úloha 1. Buď $p \geq 3$ prvočíslo. Dokažte, že je-li

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{m}{n},$$

pak m je násobkem p .

Věta (malý Fermat). Pro $a \in \mathbb{Z}_p^\times$ platí $a^{p-1} \equiv 1 \pmod{p}$.

Důsledek. Pro polynomy nad $\mathbb{Z}_p$ platí rovnost

$$x^p - x = \prod_{a \in \mathbb{Z}_p} (x - a).$$

Úloha 2. Určete všechna kladná celá čísla, která jsou nesoudělná s každým členem posloupnosti $a_n = 2^n + 3^n + 6^n - 1$ pro $n = 1, 2, \dots$ (IMO 2005)

Věta (Wilson). Pro prvočíslo p platí $(p-1)! \equiv -1 \pmod{p}$.

První setkání s p -valuací

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 další způsob, jak se na situaci podívat z pohledu jednoho prvočísla. Jedná se přitom o jemnější informaci než pouhý zbytek modulo p .

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

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

Úloha 3. Dokažte, že pro libovolná přirozená čísla a, b, c platí

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

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

Faktoriály a kombinační čísla

V dělitelnostech a rovnostech obsahujících faktoriály se často hodí spočítat nebo alespoň odhadnout p -valuaci. Vznikávají tím relativně nevábne 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.

Úloha 5. Pro libovolná celá nezáporná m, n je

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

celé číslo.

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. Určete 729. nejmenší přirozené číslo n takové, že kombinační číslo $\binom{2n}{n}$ není násobkem 5.

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

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

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

$$v_2(x^n - y^n) = v_2(x - y) + v_2(x + y) + v_2(n) - 1.$$

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

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

Tvrzení. Budiž p prvočíslo a necht' $p \nmid a, b$. 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 7. Dokažte, že pro každé přirozené n lze zvolit přirozené k tak, že

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

Úloha 8. Najděte všechna přirozená n splňující $2^n \mid 3^n - 1$.

Další úlohy

Úloha 9. 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 10. Bud' p prvočíslo a $0 < k < p$.

- (i) Ukažte, že kombinační číslo $\binom{p}{k}$ je násobkem p .
- (ii) Jaký zbytek dává $\binom{p}{k}$ po dělení číslem p^2 ?

Úloha 11. Platí $v_p(n!) \leq \left\lfloor \frac{n-1}{p-1} \right\rfloor$.

Úloha 12. Najděte všechna přirozená n , pro něž $v_2(n!) = n - 1$.

Úloha 13. Jsou dána přirozená čísla a, b taková, že

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

Dokažte, že $a = b$.

Úloha 14. 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)

Úloha 15. Najděte všechna prvočísla p , pro která je číslo

$$\binom{p}{1}^2 + \binom{p}{2}^2 + \dots + \binom{p}{p-1}^2$$

dělitelné číslem p^3 .

(CPS 2008)

Úloha 16. Pro prvočíslo p platí $p^n \nmid ((p-1)n)!$.

Úloha 17. Dokažte, že pro přirozená n platí

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

Úloha 18. 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 19. Je dáno prvočíslo p . Najděte všechna n , pro něž p nedělí

$$\binom{n}{0} \cdot \binom{n}{1} \cdots \binom{n}{n}.$$

Úloha 20. Jsou dána přirozená n, q taková, že všichni prvočíselní dělitelé q jsou větší než n . Dokažte, že pak platí

$$n! \mid (q-1) \cdot (q^2-1) \cdots (q^{n-1}-1).$$

Úloha 21. Najdi největší mocninu 1991, která dělí číslo

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

(ISL 1991)

Úloha 22. 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 23. Prvočíslo p a přirozená a, n splňují $2^p + 3^p = a^n$. Dokažte, že $n = 1$. (Irsko)

Úloha 24. Přirozená a, n, k splňují $n \mid (a-1)^k$. Dokažte $n \mid a^{n-1} + a^{n-2} + \cdots + a + 1$.

Úloha 25. Najděte všechny trojice (x, y, p) , kde x, y jsou přirozená čísla a p prvočíslo splňující $p^x - y^p = 1$.

Úloha 26. Je dáno bezčtvercové¹ přirozené n . Dokažte, že neexistují nesoudělná přirozená čísla x, y splňující $(x + y)^3 \mid x^n + y^n$.

Úloha 27. Mějme liché přirozené $n > 1$ a nesoudělná přirozená $a > b$. Dokažte, že $a^n - b^n$ má prvočíselného dělitele, který nedělí $a - b$.

Úloha 28. Najděte všechny dvojice přirozených čísel (a, b) , které splňují $b^a \mid a^b - 1$.

Úloha 29. Najděte všechna přirozená a , pro něž je $4(a^n + 1)$ třetí mocninou celého čísla pro každé přirozené n .

Úloha 30. 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 31. Budte 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 32 (Wolstenholmova věta). Bud' $p \geq 5$ prvočíslo. Dokažte, že je-li

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} = \frac{m}{n},$$

pak m je dokonce násobkem p^2 .

Úloha 33. Budiž $k > 1$ přirozené číslo. Dokažte, že existuje nekonečně mnoho přirozených n splňujících

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

Úloha 34. Dokažte, že jsou-li p, q přirozená čísla taková, že

$$\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \dots - \frac{1}{1318} + \frac{1}{1319},$$

pak p je dělitelné číslem 1979. (IMO 1979)

Úloha 35. Pro liché prvočíslo p dokažte

$$1^{p-2} + 2^{p-2} + \dots + \left(\frac{p-1}{2}\right)^{p-2} \equiv \frac{2-2^p}{p} \pmod{p}.$$

(iKS 2012, N3)

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

Úloha 36. Najděte všechna přirozená n , pro která je $2^{n+2}(2^n - 1) - 8 \cdot 3^n + 1$ čtverec. (Vietnam)

Pořádné výzvy

Úloha 37. Na tabuli jsou napsána racionální čísla $\frac{m}{n}$ a $\frac{n}{m}$, kde m, n jsou nesoudělná kladná celá čísla. Evan může v každém kroku vybrat dvě čísla x, y na tabuli a napsat také jejich aritmetický průměr $\frac{x+y}{2}$ či jejich harmonický průměr $\frac{2xy}{x+y}$. Určete všechny dvojice (m, n) , pro něž dovede Evan po konečně mnoha krocích zapsat na tabuli 1. (USAJMO 2019)

Úloha 38. 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 39. Uvažujme neprázdnou množinu kladných celých čísel S takovou, že kdykoliv jsou a, b dva (ne nutně různé) prvky S , pak i $ab + 1 \in S$. Dokažte, že jen konečně mnoho prvočísel nedělí žádný prvek S . (ELMO 2019)

Úloha 40. Pro přirozené $n \geq 3$ definujme posloupnost přirozených čísel $\alpha_1, \dots, \alpha_k$ 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 $\alpha_1, \dots, \alpha_k$ geometrická. (MEMO 2017 T8)

Úloha 41. Je dána nekonečná posloupnost $a_1, a_2, a_3, \dots$ 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 42. Najděte všechny trojice (p, x, y) , kde p je prvočíslu a x, y jsou přirozená čísla taková, že $x^{p-1} + y$ i $x + y^{p-1}$ jsou mocniny p . (ISL 2014)

Literatura a zdroje

Tato přednáška vznikla vesměs tak, že jsem vzal svůj p -valuační příspěvek z letního PraSečího soustředění 2021 a představil před něj příspěvek o počítání mod p od *Pepy Tkadlece*, jemuž tímto děkuji. Některé úlohy jsem doplnil též z *iKSkového* příspěvku *Kuby Svobody*, jemuž rovněž patří mé díky.

[1] Pepa Tkadlec: *Počítání modulo p* , Mentaurov, 2013.

[2] Matěj Doležálek: *p -value*, Lysečiny, 2021.

[3] Kuba Svoboda: *p -value*, sborník *iKS*, 2015.

Hinty

Hint 1. $x \mapsto \frac{1}{x}$ je jen bijekce $\mathbb{Z}_p^\times$.

Hint 2. $1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}$.

Hint 3. BÚNO si seřaď valuační, potom přímočaře počítej.

Hint 4. AG nerovnost.

Hint 5. 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.

Hint 6. Kummer překládá mezi pětkovou a trojkovou soustavou.

Hint 7. Vol k tak, aby vznikly dvě LTEčkové dvojice.

Hint 8. Rozkládej $3^n - 1 = (3^{n/2} + 1)(3^{n/2} - 1)$, dokud to jde.

Hint 9. Označ si p -valuační jednotlivých proměnných a rozebírej jejich možné pořadí.

Hint 10. p v čitateli se nemá, chudáček, s čím zkrátit. No a jakmile už jsme v násobcích p , informace „který z nich mod p^2 “ už je jen informace o nějakém zbytku mod p .

Hint 11. Ciferný součet přirozeného čísla je ≥ 1 .

Hint 12. V nerovnostech z důkazu předchází úlohy musela všude nastat rovnost.

Hint 13. $a^n \mid b^{n+1}$ znamená $\frac{v_p(a)}{v_p(b)} \leq \frac{n+1}{n}$. V podstatě totéž jde říct s logaritmem místo valuačí.

Hint 14. Chceš nezáporné 2-valuační a 5-valuační. Dirichlet pomůže.

Hint 15. Pamatuješ si vzoreček pro $1^2 + 2^2 + \dots + n^2$? Nebo aspoň znáš někoho, kdo si ho pamatuje?

Hint 16. V Legendreově formuli zahod' celé části.

Hint 17. Využij Kummerovu větu. Pokud $\alpha = v_p(n+1)$, pak $n+1$ zapsané v soustavě o základu p končí α nulami.

Hint 18. Dělitelnost dává nerovnost (třeba) 2-valuačí. Vhodně odhadni celé části v nenulových členech, těch je asymptoticky $\log n$.

Hint 19. Formuluj pomocí ciferného zápisu v p -soustavě.

Hint 20. Legendre vlevo, Fermat vpravo.

Hint 21. Prostě si vyrob LTEčkový tvar a moc se s tím nepárej.

Hint 22. Nezapomeň na předpoklady LTE. Hodí se malá Fermatova věta: $a^p \equiv a \pmod{p}$ pro každé a .

Hint 23. LTE něco poví o 5-valuační. Dej pozor na případ $p = 2$.

Hint 24. LTE na $a^n - 1$. Nezapomeňte pečlivě ověřit předpoklady.

Hint 25. Převeď y^p na pravou stranu a podívej se na p -valuační.

Hint 26. Chceš aplikovat LTE a využít $v_p(n) \leq 1$, dej však pozor na degenerované případy související s dvojkou.

Hint 27. Má-li $a^n - b^n$ pouze prvočíselné dělitele, kteří dělí $a - b$, pak dovedeš odhadnout všechny p -valuační.

Hint 28. Nejtěžší část: dokaž, že nejmenší prvočíslo $p \mid b$ také dělí $a - 1$. Potom rozliš paritu p , použij LTE a pečlivě odhadni $n - v_p(n)$.

Hint 29. Pokud má $4(a^n + 1)$ lichého prvočíselného dělitele p , podívej se na $4(a^{pn} + 1)$.

- Hint 30.** Pro každé prvočíslo $p \mid c$ rozliš případy dle toho, zda $p \mid a - b$ a zda $p \mid a, b$.
- Hint 31.** Předpokládej, že společný jmenovatel má prvočíselného dělitele, a najdi spor. Hodí se tušit něco o řádech prvků modulo p .
- Hint 32.** Posbírej k sobě $\frac{1}{a} + \frac{1}{p-a}$, tím získáš jedno p . Druhé vzejde prozkoumáním toho, co zbývá.
- Hint 33.** Zkus $n = p^m$, trik je ve správné volbě lichého prvočísla p . Zkus použít LTE na „zrcadlové“ členy.
- Hint 34.** Poupřavuj výraz tak, aby ses zbavil(a) mínusů – jakmile uvidíš nějakou „souvislou“ sumu převrácených hodnot, jsi $\pm$ správně.
- Hint 35.** Nalevo se sčítají převrácené hodnoty. Napravo může pomoci rozepsat $2^p \equiv (1+1)^2$ z binomické věty.
- Hint 36.** Pojmenuj si čtverec a^2 a uprav na součin. Potom zkoumej 3-valuaci, zbav se a a omez n .
- Hint 37.** Má-li $m + n$ lichého prvočíselného dělitele p , dívej se na celý proces mod p .
- Hint 38.** Pomocí 2-valuace a 3-valuace omez k , zbytek dorozeber.
- Hint 39.** Dívej se na $S \bmod p$. Při předpokladu sporu pak je každé $b \mapsto ab + 1$ jen permutace.
- Hint 40.** Hodí se Bertrandův postulát: pro každé přirozené číslo $n \geq 2$ existuje prvočíslo p splňující $n < p < 2n$.
- Hint 41.** 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 $v_p(a_n) \geq v_p(a_1)$.
- Hint 42.** Připrav se na spoustu rozebírání rozbitých případů. Hlavní myšlenka je hledat velké valuace p v rozdílech $y - x$ potažmo $y^p - x^p$.