

Konštrukcie v teórii čísel

Dominik Rigasz

Úvod

Úlohy v teórii čísel (ale aj v iných oblastiach) od nás často chcú aby sme rozhodli/ukázali, že nejaký objekt existuje. To vieme urobiť dvoma spôsobmi: Buď daný objekt priamo nájdeme (skonštruujeme) a ukážeme, že má požadované vlastnosti, alebo existenciu dokážeme nepriamo (napríklad pravdepodobnostný dôkaz). V týchto prednáškach sa budeme venovať prvému spôsobu – takzvaným konštrukčným úlohám. Máme niekoľko typov konštrukčných úloh v teórii čísel:

1. Úlohy, kde sa nás priamo pýtajú na existenciu nejakého objektu, a my ho musíme skonštruovať. Nedávnym príkladom je napríklad:

Príklad 1 (MO-75 A-II-2). Ukážte, že pre nekonečne veľa prirodzených čísel d existujú nesúdeliteľné prirodzené čísla a, b také, že $d = \text{NSD}(5a^2 + b, 5b^2 + a)$.

2. Úlohy, kde máme nejakú podmienku, ktorá platí napríklad pre všetky prirodzené čísla n , a my na základe toho musíme niečo ukázať. Podstata "konštruovania" v takýchto úlohach je hľadať správne n na dosadenie, ktoré nám toho povedia o danej situácii čo najviac. Napríklad:

Príklad 2 (ISL 2005 N6). Nech a, b sú kladné celé čísla také, že $a^n + n \mid b^n + n$ pre všetky $n \in \mathbb{N}$. Ukážte, že potom $a = b$.

3. Úlohy, ktoré od nás chcú, aby sme našli najväčšiu/najmenšiu možnú hodnotu niečoho. V jednej časti riešenia totižto ukážeme, že naša hodnota nemôže byť viac ako tvrdené maximum M , a v druhej časti ukážeme, že M je dosiahnuteľné (konštrukciou). Tieto dve časti spolu súvisia, a konštrukcia je často motivovaná odhadmi z prvej časti. Napríklad:

Príklad 3 (MO-74 A-I-3). Na tabuli sú napísané navzájom rôzne prirodzené čísla so súčtom 2024. Každé z nich okrem najmenšieho je násobkom súčtu všetkých menších napísaných čísel. Koľko najviac čísel môže na tabuli byť?

Všeobecné tipy, stratégia

1. Hľadať nutné podmienky, ktoré konštrukcia musí spĺňať, konštruovať spätne.
2. "Wishful thinking": Opýtať sa čo by sme potrebovali/čo by nám stačilo na vyriešenie úlohy. Skúsiť to zariadiť.
3. Zabudnúť na niektoré podmienky a riešiť jednoduchšiu úlohu, potom podmienky pridávať.

4. Nájsť "voľnú premennú", ktorou vieme hýbať ako potrebujeme (ak už nie je priamo v zadaní).
5. Nebáť sa plýtvat' prvočíslami/číslami, je ich veľa...
6. Skladať modulárne podmienky pomocou Čínskej Zvyškovej Vety.
7. Občas mať na pamäti kladivá (Bertrand, Zsigmondy, Dirichlet).
8. Urobiť malú konštrukciu, snažiť sa pridávať prvky indukciou.
9. Ak od nás otázka chce aby sme rozhodli, či niečo platí, je dôležité veriť obom možnostiam.

Čínska zvyšková veta

Čínska zvyšková veta (CRT) nám hovorí o riešení lineárnych sústav kongruencií. Jej sila pri konštrukčných úlohách je tá, že si vieme navoliť veľa modulárnych podmienok na voľnú premennú n , a CRT nám garantuje (za istých podmienok), že také n existuje. Alternatívne, často nám úlohu stačí namiesto zložených čísel riešiť iba pre prvočíselné monciny (čo úlohu zjednoduší), a potom to spätne poskladať z CRT.

Veta 1 (CRT). *Nech $a_1, a_2, \dots, a_n$ sú celé čísla, $m_1, m_2, \dots, m_n$ sú kladné celé čísla, ktoré sú po dvoch nesúdeliteľné, a nech $M = m_1 m_2 \dots m_n$. Potom existuje celé číslo x také, že*

$$\begin{aligned}x &\equiv a_1 \pmod{m_1}, \\x &\equiv a_2 \pmod{m_2}, \\&\vdots \\x &\equiv a_n \pmod{m_n},\end{aligned}$$

a navyše toto x je unikátne modulo M .

Dôkaz. (Unikátnosť) Ak x_1, x_2 sú dve riešenia danej sústavy kongruencií, potom $m_i \mid x_1 - a_i$ a aj $m_i \mid x_2 - a_i$, a teda $m_i \mid x_1 - x_2$. Nakoľko $\gcd(m_i, m_j) = 1$ pre $i \neq j$, tak dostávame $M \mid x_1 - x_2$.

(Existencia) Uvažujme mapovanie f , ktoré nám ku každému zvyšku $x \pmod{M}$ priradí n -ticu zvyškov $(x \pmod{m_1}, x \pmod{m_2}, \dots, x \pmod{m_n})$. Mapovanie f je prosté (z unikátnosti). Navyše, definičný obor aj obor hodnôt f majú rovnako veľa prvkov (M), teda f je bijekcia. Preto existuje x také, že $x \pmod{M}$ mapuje na $(a_1 \pmod{m_1}, a_2 \pmod{m_2}, \dots, a_n \pmod{m_n})$. $\square$

Všimnime si, že tento dôkaz je nekonštruktívny. Postup ako také x vypočítať súvisí z Bezoutovými koeficientami a Euklidovým algoritmom.

Niekedy by sa nám pri volení modulárnych podmienok na našu voľnú premennú hodilo, aby bola prvočíslom. O tom nám hovorí Dirichletova veta. Poznamenajme, že jej dôkaz je neelementárny.

Veta 2 (Dirichlet). *Nech a, m sú nesúdeliteľné kladné celé čísla. Potom existuje nekonečne veľa prvočísel p takých, že $p \equiv a \pmod{m}$.*

Pri koštruovaní (obzvlášť vhodných exponentov) sa nám získa aj Fermatova malá veta. Je veľmi užitočná pri zbavovaní sa otravných exponentov (napríklad keď sa modulo p pozeráme na a^n , tak keď si zvolíme $n \equiv 1 \pmod{p-1}$, tak nám z toho vznikne iba a).

Veta 3 (malý Fermat). *Nech p je prvočíslo a $p \nmid a$ je celé číslo. Potom $a^{p-1} \equiv 1 \pmod{p}$.*

Príklady 1 (CRT)

Cvičenie 1. Ukážte, že pre každé $c \in \mathbb{Z}$ a prvočíslo p má rovnica $x^x \equiv c \pmod{p}$ riešenie.

Hinty: 1

Cvičenie 2 (ťažšie, USAMO 2008/1). Ukážte, že pre každé n existujú po dvoch nesúdeliteľné čísla $k_1, k_2, \dots, k_n > 1$ také, že $k_1 k_2 \cdots k_n - 1$ je súčinom dvoch po sebe idúcich prirodzených čísel. **Hinty:** 2

Cvičenie 3 (ťažšie, ISL 2005). Nech a, b sú celé čísla také, že $a^n + n \mid b^n + n$ pre všetky $n \in \mathbb{N}$. Ukážte, že $a = b$. **Hinty:** 3

Cvičenie 4. Dokážte, že pre každé $n \in \mathbb{N}$ existuje n -tica po sebe idúcich čísel, z ktorých každé je deliteľné štvorcom nejakého prirodzeného čísla väčšieho než 1. **Hinty:** 4

Cvičenie 5. Dokážte, že pre každé prirodzené n existuje n po sebe idúcich prirodzených čísel, z ktorých žiadne nie je prvočíselná mocnina. **Hinty:** 5

Cvičenie 6. Uvažujme v rovine mriežkové body (a, b) s celočíselnými súradnicami. Bod (a, b) je viditeľný, pokiaľ sú a, b nesúdeliteľné celé čísla. Dokážte, že pre ľubovoľné $n \in \mathbb{N}$ existuje štvorec $n \times n$ mriežkových bodov, z ktorých žiadny nie je viditeľný. **Hinty:** 6

Cvičenie 7. Dané je $n \in \mathbb{N}$. Koľko riešení má $x^2 \equiv x \pmod{n}$ v množine $\{1, 2, \dots, n\}$? **Hinty:** 7

Cvičenie 8. Dokážte, že pre každé prirodzené číslo k možno zvoliť $2k$ navzájom rôznych prirodzených čísel $a_1, \dots, a_k, b_1, \dots, b_k$ takých, že zlomky

$$\frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots, \frac{a_k}{b_k}$$

sú všetky v základnom tvare a tvoria aritmetickú postupnosť. **Hinty:** 8

Cvičenie 9. Rozhodnite, či možno prirodzené čísla zoradiť do postupnosti $a_1, a_2, \dots$ (pričom každé prirodzené číslo sa vyskytne práve raz) tak, aby pre každé prirodzené n platilo $n \mid a_1 + \dots + a_n$. **Hinty:** 9

Cvičenie 10. Nájdite všetky trojice prirodzených čísel (a, b, c) také, že pre každé prirodzené n , ktoré nemá žiadneho prvočíselného deliteľa menšieho než 2014, platí $n + c \mid a^n + b^n + n$. **Hinty:** 10

Cvičenie 11 (ELMO SL 2014). Nech $f : \mathbb{N} \rightarrow \mathbb{N}$ je funkcia spĺňajúca pre každé $a, b \in \mathbb{N}$:

(i) $f(a), f(b)$ sú nesúdeliteľné práve vtedy, keď a, b sú nesúdeliteľné.

(ii) $a \leq f(a) \leq a + 2012$.

Dokážte, že ak prvočíslo p delí $f(n)$, potom už aj $p \mid n$. **Hinty:** 11

Cvičenie 12 (USA TSTST 2012). Tabuľka 2018×2018 je vydláždená dominami 2×1 . Dokážte, že možno do políčok vpísať prirodzené čísla tak, že:

(i) Súčet dvoch čísel na každom domine je vždy rovnaký.

(ii) Ľubovoľné dve čísla, ktorých políčka susedia stranou, sú nesúdeliteľné práve vtedy, ak ležia na rovnakom domine.

Hinty: 12

Cvičenie 13. Dokážte, že $4a^2 + 9b^2 \equiv 1 \pmod{n}$ má pre ľubovoľné prirodzené n riešenie.

Hinty: 13

Cvičenie 14. Rozhodnite, či existuje prirodzené n také, že pre ľubovoľné celé číslo x nemá $x^2 + x + n$ žiadneho prvočíselného deliteľa menšieho než 2021. **Hinty:** 14

Cvičenie 15. Sú dané prirodzené čísla $a > b > c \geq 3$ spĺňajúce

$$a \mid bc + b + c, \quad b \mid ca + c + a, \quad c \mid ab + a + b.$$

Dokážte, že aspoň jedno z a, b, c je zložené číslo. **Hinty:** 15

Cvičenie 16 (IMO 2009/1). Sú dané prirodzené čísla $n, k \geq 2$ a k -tica po dvoch rôznych čísel $a_1, \dots, a_k$ z množiny $\{1, 2, \dots, n\}$ taká, že $n \mid a_i(a_{i+1} - 1)$ pre $i = 1, \dots, k - 1$. Dokážte, že $n \nmid a_k(a_1 - 1)$. **Hinty:** 16

Ručné hľadanie explicitných konštrukcií

CRT alebo Dirichletova veta nám garantujú existenciu nejakého objektu (čísla), avšak nevieme presne aké je to číslo. V tejto sekcii budeme objekty hľadať explicitne. Typické riešenie pri takýchto úlohách vyzerá: "Zvoľme $P(x) = 483x^3 - 29x + 3$. To funguje, takže sme hotoví." Za takým riešením sú často hodiny výpočtov, experimentov, skúšaní rôznych vecí... až kým niečo nezafunguje. Pri riešení je fajn začať sa hrať s nejakými konkrétnymi príkladmi na malých číslach, a postupne zovšeobecňovať. Využívať čísla, ktoré majú veľa deliteľov (napríklad faktoriály), a aj čísla, ktoré majú málo deliteľov (prvočísla).

Príklady 2 (explicitné konštrukcie)

Cvičenie 17. Existuje n po sebe idúcich kladných celých čísel, z ktorých sú všetky zložené? **Hinty:** 17

Cvičenie 18. Existuje n po sebe idúcich kladných celých čísel takých, že každé sa dá zapísať ako $a^b + b$ pre nejaké celé čísla $a, b > 1$? **Hinty:** 18

Cvičenie 19. Existuje rastúca postupnosť prirodzených čísel $a_1 < a_2 < \dots$ taká, že pre každé $k \in \mathbb{N}$ je iba konečne veľa z čísel $a_1 + k, a_2 + k, \dots$ prvočíslami? **Hinty:** 19

Cvičenie 20. Existuje nekonečná množina S kladných celých čísel taká, že keď z nej vyberieme ľubovoľnú konečnú (neprázdnu) podmnožinu, tak jej súčet nie je perfektnou mocninou? **Hinty:** 20

Cvičenie 21. Nech a, b sú celé čísla také, že $2^n a + b$ je štvorec pre všetky $n \in \mathbb{N}$. Ukážte, že $a = 0$. **Hinty:** 21

Cvičenie 22. Nájdite nekonečne veľa dvojíc celých čísel $1 < a < b$ takých, že $ab \mid a^2 + b^2 - 1$. Aké všetky hodnoty môže pre takéto a, b nadobúdať zlomok $\frac{a^2 + b^2 - 1}{ab}$? **Hinty:** 22

Cvičenie 23 (MO-75 A-II-1). Nech x, y sú reálne čísla také, že $x + y$ aj $x^2 + y^2$ sú celé. Musí aj $x^3 + y^3$ byť celé? **Hinty:** 23

Cvičenie 24 (MO-75 A-II-2). Ukážte, že pre nekonečne veľa prirodzených čísel d existujú nesúdeliteľné prirodzené čísla a, b také, že $d = \text{NSD}(5a^2 + b, 5b^2 + a)$. **Hinty:** 24

Cvičenie 25 (MO-73 A-II-2). Určte všetky dvojice (k, n) kladných celých čísel, pre ktoré existujú kladné celé čísla a, b také, že platí $\text{NSD}(a + k, b) = n \cdot \text{NSD}(a, b)$. **Hinty:25**

Cvičenie 26 (MO-74 A-I-3). Na tabuli sú napísané navzájom rôzne prirodzené čísla so súčtom 2024. Každé z nich okrem najmenšieho je násobkom súčtu všetkých menších napísaných čísel. Koľko najviac čísel môže na tabuli byť? **Hinty:26**

Cvičenie 27 (USA 1998). Ukážte, že existuje ľubovoľne veľká množina S kladných celých čísel taká, že $(a - b)^2 \mid ab$ pre všetky rôzne $a, b \in S$. **Hinty:27**

Cvičenie 28 (RMM 2015/1). Existuje postupnosť kladných celých čísel $a_1, a_2, \dots$ taká, že a_m a a_n sú nesúdeliteľné práve vtedy ak $|m - n| = 1$? **Hinty:28**

Cvičenie 29. Ukážte, že rovnica $a^2 + b^2 = c^2 + 3$ má nekonečne veľa celočíselných riešení. **Hinty:29**

Cvičenie 30 (USAMTS 2017/18). Kladné celé číslo nazveme rastúce ak jeho cifry zľava doprava tvoria neklesajúcu postupnosť. Napríklad 114 aj 679 sú rastúce čísla. Nech $P(x)$ je polynóm s racionálnymi koeficientami taký, že pre každé rastúce číslo x je $P(x)$ celé číslo. Musí potom nutne byť $P(x)$ celé číslo pre všetky $x \in \mathbb{Z}$? **Hinty:30**

Kladivá (Dirichlet, Bertrand, Zsigmondy)

Na záver spomeňme pár zabitých viet, ktoré nám garantujú existenciu nejakých objektov, konkrétne prvočísel spĺňajúcich niečo.

Veta 4 (Dirichlet). *Nech a, m sú nesúdeliteľné kladné celé čísla. Potom existuje nekonečne veľa prvočísel p takých, že $p \equiv a \pmod{m}$.*

Veta 5 (Bertrand). *Nech $n > 1$ je celé číslo. Potom existuje prvočíslo p také, že $n < p < 2n$.*

Veta 6 (Zsigmondy). *Nech $a > b$ sú nesúdeliteľné kladné celé čísla, $a > 1$. Potom existuje prvočíslo $p \mid a^n - b^n$ také, že $p \nmid a^i - b^i$ pre všetky $1 \leq i < n$. Výnimkami sú prípady*

1. $(a, b, n) = (2, 1, 6)$,
2. $(a, b, n) = (a, 2^k - a, 2)$.

Vo vyšších súťažiach sa občas môže objaviť použitie jednej z týchto viet ako nejaký medzikrok, avšak väčšinou sa tieto vety až tak nepoužívajú (obzvlášť Zsigmondy). Oveľa dôležitejšie je vedieť v úlohách vidieť jednoduché veci, a nie všade hľadať kladivá.

Príklady 3 (kladivá)

Cvičenie 31. Odvodte variantu Zsigmondyho vety pre sčítanie (čiže hľadáme $p \mid a^n + b^n$ a $p \nmid a^i + b^i$). **Hinty:31**

Cvičenie 32. Ukážte, že existuje párovanie čísel $1, 2, \dots, 2n$ do n dvojíc také, že súčet čísel v každej dvojici je prvočíslo. **Hinty:32**

Cvičenie 33. Existuje n také, že medzi n a n^2 leží aspoň 2026 prvočísel? **Hinty:33**

Cvičenie 34. Ukážte, že existuje nekonečne veľa prirodzených čísel, ktoré nevieme zapísať ako $3ab + a + b$ pre $a, b \in \mathbb{N}$. **Hinty:34**

Cvičenie 35 (EMC 2024). Dvojicu rôznych prirodzených čísel (a, b) nazveme *binárnou*, ak $ab + 1$ je mocnina čísla 2. Nech S je množina n prirodzených čísel. Koľko najviac binárnych dvojíc môže byť v S ? **Hinty:35**

Cvičenie 36 (Peterburg 1996). Existujú prirodzené čísla a a b také, že kedykoľvek sú p a q rôzne prvočísla väčšie než 1000, potom aj $ap + bq$ je prvočíslo? **Hinty:**36

Cvičenie 37. Dokážte, že ak s, a, b sú prirodzené čísla a $\text{NSD}(a, b) = 1$, potom existuje nekonečne mnoho n takých, že $an + b$ je súčinom s rôznych prvočísel. **Hinty:**37

Cvičenie 38 (Mongolsko 2008). Nech m je kladné nepárne číslo. Ukážte, že existuje nekonečne veľa kladných n takých, že $mn + 1 \mid 2n - 1$. **Hinty:**38

Cvičenie 39. Pre každé prirodzené n ukážte, že existuje prirodzené k také, že

$$p_{k-1} < p_k - n < p_k + n < p_{k+1}.$$

Hinty:39

Cvičenie 40 (IMO 2008). Ukážte, že existuje nekonečne veľa prirodzených čísel n takých, že číslo $n^2 + 1$ má prvočíselného deliteľa väčšieho než $2n + \sqrt{2n}$. **Hinty:**40

Cvičenie 41 (IMO 2000). Existuje kladné celé číslo n s práve 2000 prvočíselnými deliteľmi také, že $n \mid 2^n + 1$? **Hinty:**41

Hinty

1. CRT + Fermat.
2. Vlastne sa iba chce aby $x^2 + x + 1$ malo dosť veľa prvočíselných deliteľov.
3. Vytvor pre $a - b$ veľa prvočíselných deliteľov. Modulá p a $p - 1$ sú nesúdeliteľné!
4. Predpíš každému číslu štvorcového deliteľa.
5. Predpíš každému číslu dva prvočíselné delitele.
6. Poruť si pre každý bod hľadaného štvorca prvočíslo, ktorým majú byť súradnice súdeliteľné.
7. Rieš pre prvočíselné mocniny.
8. Vezmi skrátenú postupnosť $\frac{x+1}{N}, \dots, \frac{x+k}{N}$ pre vhodné x, N . Jednotlivé b_i odliš skrátenými prvočíslami, a_i potom už odlišíš ľahko.
9. Pridávaj členy po dvoch – jeden zvol ľubovoľne a jeden určí.
10. S pomocou kanónu (Dirichlet) ukáž, že $a + b - c$ má veľa prvočíselných deliteľov. Navoľ si zvyšky v rôznych moduloch podľa ľubovôle najprv pre p , potom pre n .
11. Skús najskôr zabudnúť na n, p a pomocou zvyškovej vety skonštruovať také x , že $f(x) = x$. Potom do výrobného procesu pridaj $x \equiv 0 \pmod{p}$, $x \equiv 1 \pmod{n}$.
12. Vyplňuj na jednotlivé dominá dvojice čísel $S \pm x_i$ podľa šachovnicového ofarbenia. Kdekoľvek má byť dvojica čísel súdeliteľná, zvol si na to zvláštne prvočíslo.
13. Vyrieš modulo prvočíselné mocniny. Mocniny 2 a 3 sú trochu výnimočné, ostatné sú ľahké.
14. Polynóm $x^2 + x$ nevie modulo p nadobúdať všetky možné hodnoty – podľa toho navoľ $n \pmod{p}$ pre $p < 2021$.
15. Zlož do modula abc .
16. Z predpokladu sporu dokáž, že buď $a_i \equiv 0 \pmod{p^k}$ pre všetky i , alebo $\equiv 1$ pre všetky i .
17. Chceme aby $x + 1, x + 2, \dots, x + n$ boli zložené. Čo ak by x malo veľa deliteľov?
18. Chceme aby $x + 2, x + 3, \dots, x + (n + 1)$ boli daného tvaru. Vedeli by sme zariadiť aby x bola zároveň druhá, tretia, ..., $(n + 1)$ -vá mocnina?

19. Cvičenie 17. Čo ak $k = 1$?
20. Zaruč aspoň dvoch prvočíselných deliteľov s rôznou valuáciou.
21. Ako rastú štvorce? Aké operácie zachovávajú štvorce?
22. Skúšaj.
23. Aj $2xy$ je celé číslo. Čo ak je párne?
24. Eliminuj jednu premennú. Potom si tú druhú zvoľ v závislosti na tej eliminovanej.
25. Vieme, že $\text{NSD}(a, b) \mid k$. Čo je nejaký pekný deliteľ čísla k ?
26. Čo vieme povedať o $s_k = a_1 + \dots + a_k$.
27. Akú operáciu by si mohol aplikovať na prvky S aby sa správali pekne?
28. Pozeraj sa na čísla ako množiny ich prvočíselných deliteľov. Striedavo pridávaj prvky.
29. Skúšaj.
30. Ako vieme reprezentovať rastúce čísla?
31. Uvážte $a^{2n} - b^{2n}$.
32. Indukcia + Bertrand.
33. Použi Bertranda veľakrát za sebou.
34. Rozlož $3n + 1$ a Dirichlet.
35. Uvžuj graf na S , kde dve čísla su spojené ak tvoria binárny pár. Môže tento graf obsahovať cyklus?
36. Hľadaj prvočísla s rozdielom, ktorý je násobok $a + b$.
37. Indukcia + Dirichlet.
38. Zvoľte dostatočne vysoké prvočíslo $p = \varphi(m)k + 1$ a potom $n = \frac{2^p - 2}{m}$.
39. Zvoľte prvočíslo $p \equiv (q - 1)! - 1 \pmod{q!}$, kde q je dosť veľké prvočíslo.
40. Zvoľte $p = 20k + 1$, vezmite najmenšie n , ktoré spĺňa $n^2 \equiv -1 \pmod{p}$ a uvážte jeho vzdialenosť od $(p - 1)/2$.
41. Začni s $n = 9$ a postupne pridávaj prvočísla. Zsigmondy.

Literatúra a zdroje

1. Modern Olympiad Number Theory (MONT), Aditya Khurmi, 2020.
2. Čínská zbytková veta, Matej Doležálek, Zdobnice 2024.
3. Number Theory Constructions, Evan Chen, 2023.
4. <https://skmo.sk/dokumenty.php>.