Nekonečno a dôkazové techniky

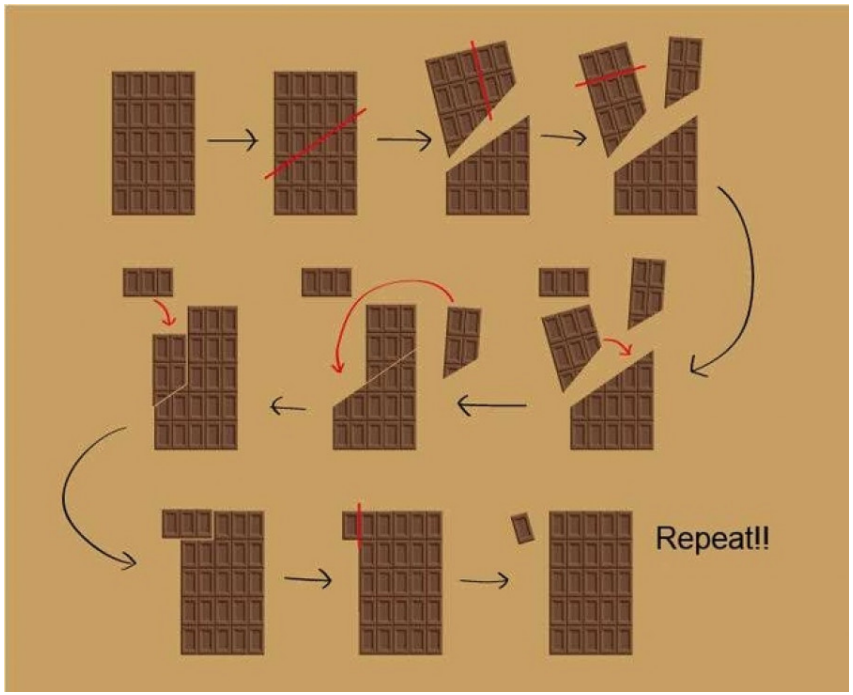
- Nekonečno-trochu histórie
- Rôzne metódy riešenia úloh

Druhy paradoxov

- Vyzerá, že to platí, ale neplatí
- Vyzerá, že neplatí, ale platí

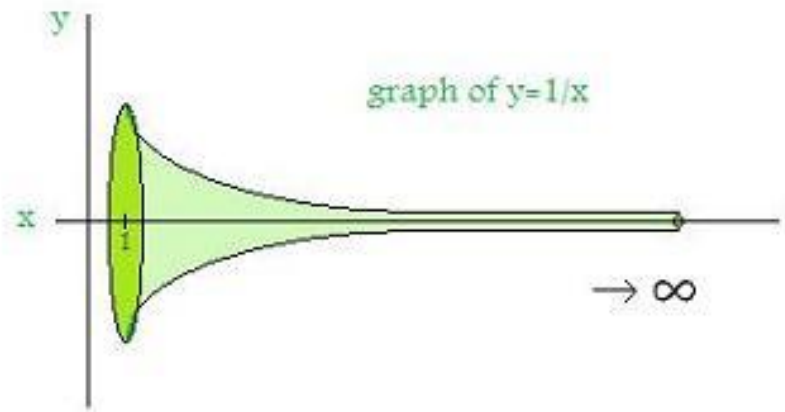
Paradoxy

- Vyzerá, že to platí, ale neplatí:



Paradoxy

- Vyzerá, že neplatí, ale platí:

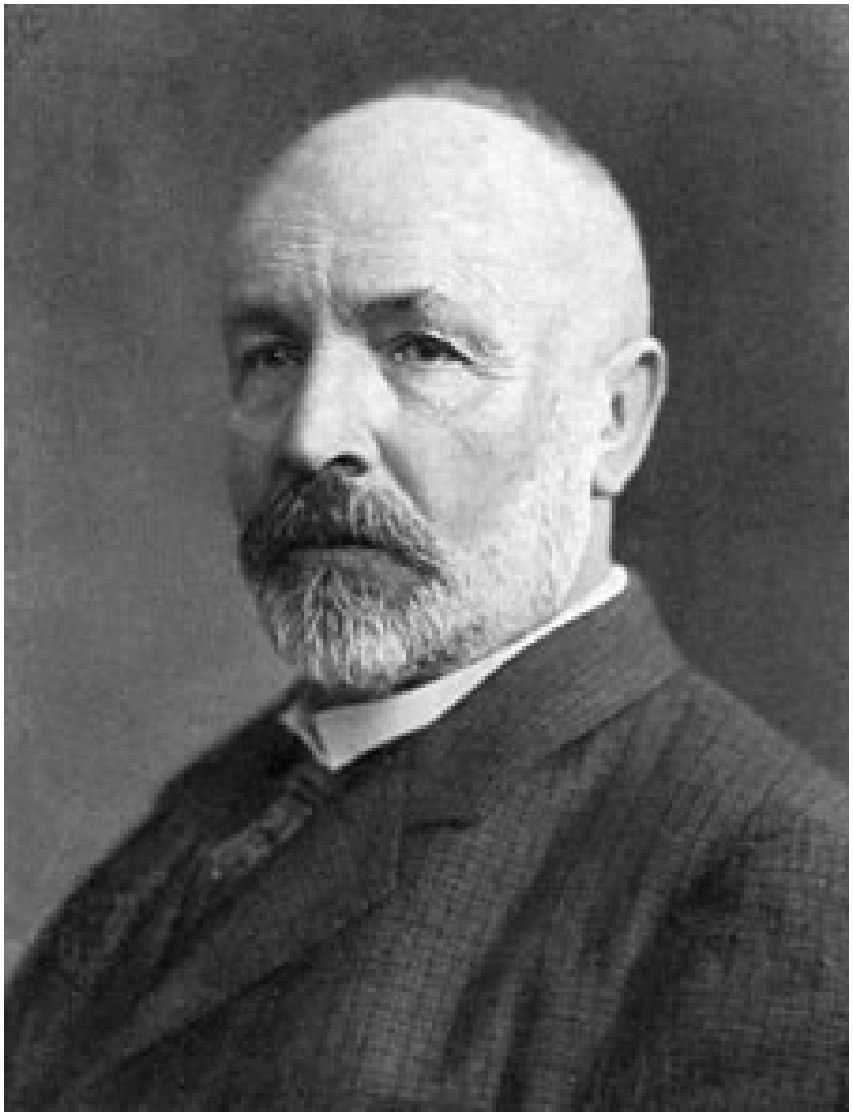


Paradoxy

Banach-Tarski:

Paradox?

Georg Ferdinand Ludwig Philipp Cantor



Nekonečno a čas

- 4. st. BC: Zenonove paradoxy (vieme sčítať nekonečné rady, zrejme aj on vedel, že sa mýli)
- 3. st. BC: Euklides-prvočísel je nekonečne mnoho
- 207 BC: Aristoteles: nekonečno je niečo ako čas, nie je to permanenná entita, skôr niečo, k čomu sa blížime
- 13. st. - Tomáš Akvinský: nekonečne veľký súbor nemôže existovať, súbory vecí vieme špecifikovať podľa počtu vecí v nich a žiadne číslo nie je nekonečné
- G. Cantor-kardinality množín (prevratné objavy prijala len časť matematickej obce, mnohí vplyvní matematici ho nepochopili)

Vlastnosti zobrazení

- **Definícia.** Ak existuje bijekcia množiny A na množinu B hovoríme, že množina A je ekvivalentná s množinou B a píšeme $A \sim B$.

Vlastnosti zobrazení

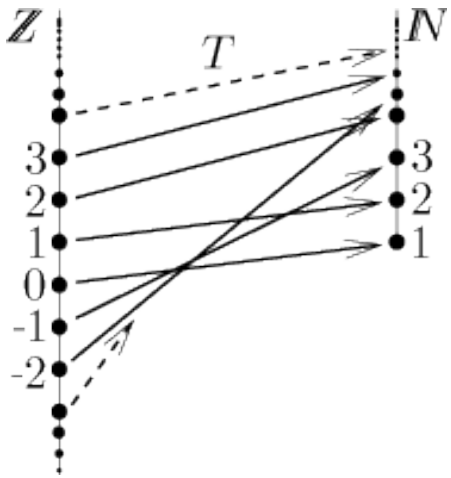
- **Definícia.** Ak existuje bijekcia množiny A na množinu B hovoríme, že množina A je ekvivalentná s množinou B a píšeme $A \sim B$.
- **Veta.** Pre ľubovoľné množiny A, B, C platí
  - $A \sim A$
  - $A \sim B \Rightarrow B \sim A$
  - $A \sim B \wedge B \sim C \Rightarrow A \sim C$

Mohutnosti (kardinality) množín

- konečné množiny
- nekonečné množiny
  - spočítateľné (existuje bijekcia s množinou prir. čísel)
  - nespočítateľné (neexistuje bijekcia s množinou prir. čísel)

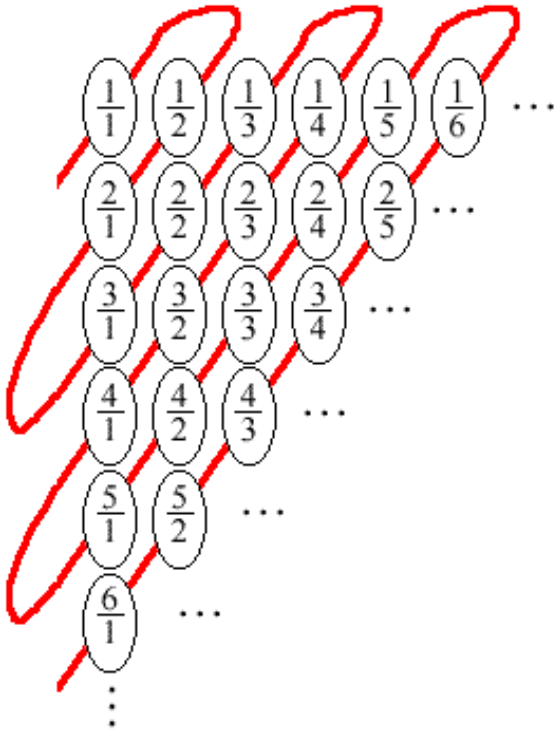
Mohutnosti množín

- Množina celých čísel

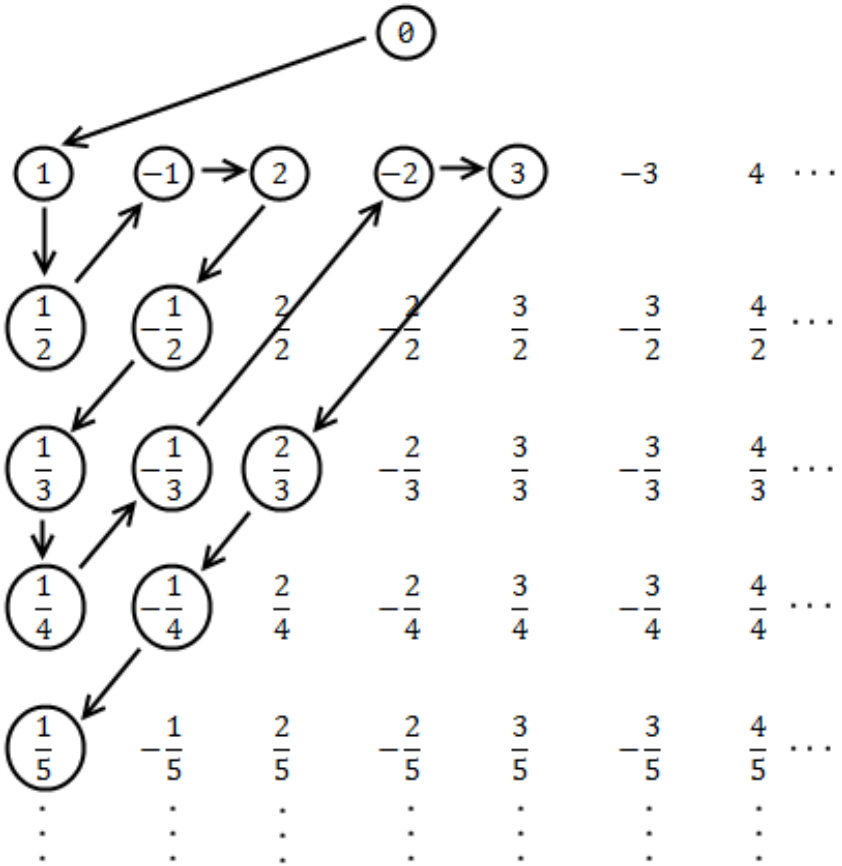


Mohutnosti množín

- Množina racionálnych čísel

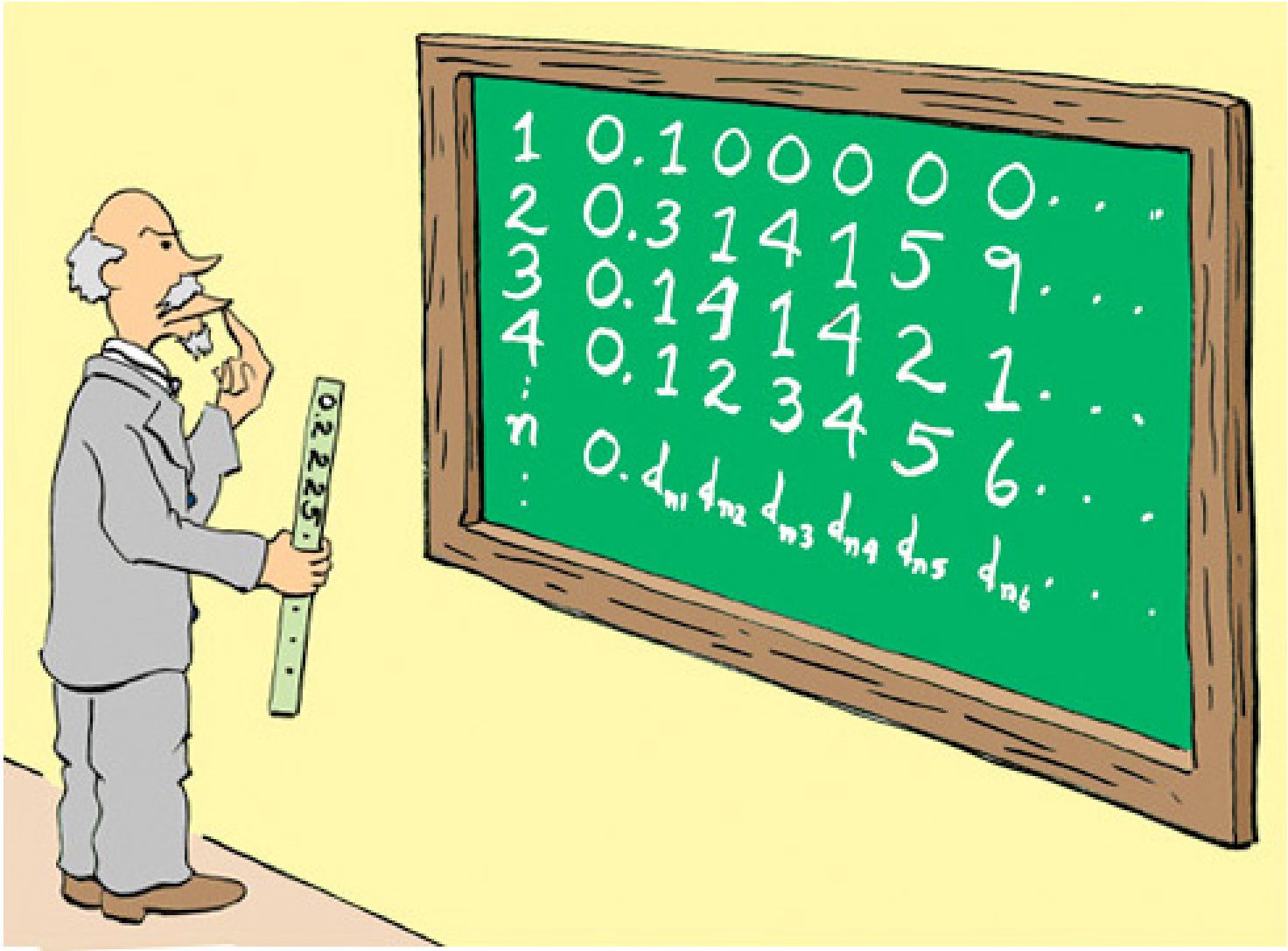


Mohutnosti množín



Mohutnosti množín

- Množina reálnych čísel



Riešenie problémov

- Hľadanie zákonitostí
- Kreslenie obrázkov
- Formulovanie ekvivalentných problémov
- Modifikácia problému
- Výber efektívneho označenia
- Využitie symetrie
- Rozdelenie problému na špeciálne prípady
- Spätný postup
- Nepriamy postup
- Sledovanie parity
- Skúmanie extrémnych prípadov
- Zovšeobecnenie

Dôkazové techniky

Matematické tvrdenia:

- všeobecné
- existenčné

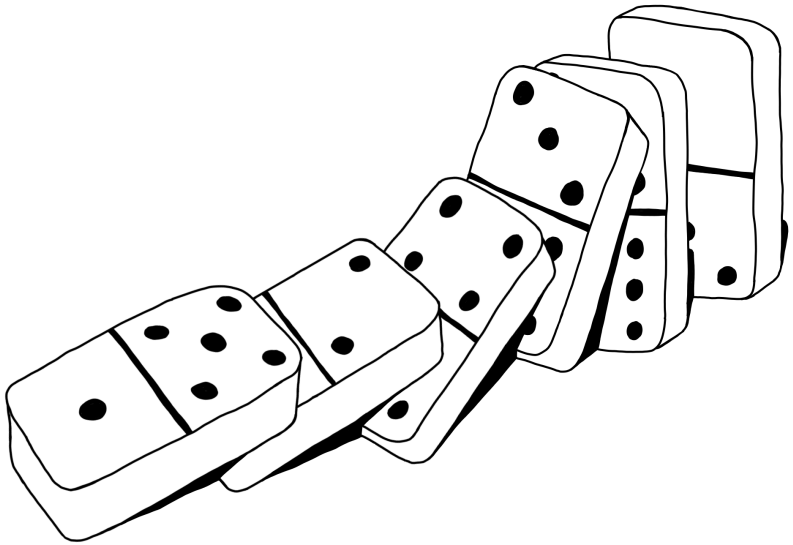
Dôležité dôkazové techniky

- priame odvodenie
- kontrapozícia (nepriamy dôkaz)
- dôkaz sporom
- Matematická indukcia

Užitočné "pomôcky"

- Dirichletov princíp
- Princíp inklúzie a exklúzie

Matematická indukcia



Matematická indukcia

Nech $a \in Z$ a nech $P(n)$ je tvrdenie o n pre každé celé $n \geq a$.
Princíp mat. indukcie stanovuje, že:
Ak

- $P(a)$ je pravdivé
- pre každé celé číslo k z pravdivosti $P(k)$ vyplýva pravdivosť $P(k+1)$, tak $P(n)$ je pravdivé pre všetky celé čísla $n \geq a$.

Matematická indukcia-trochu inak

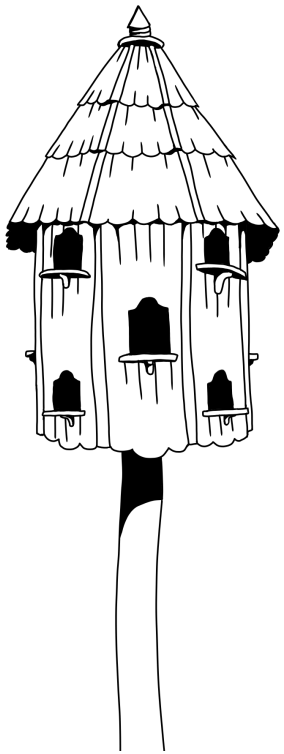
Nech $a \in Z$ a nech $P(n)$ je tvrdenie o n pre každé celé $n \geq a$.
Druhý princíp mat. indukcie stanovuje, že:
Ak

- $P(a)$ je pravdivé
- pre každé celé číslo $k \geq a$ z pravdivosti $P(a), P(a+1), \ldots, P(k)$ vyplýva pravdivosť $P(k+1)$, tak $P(n)$ je pravdivé pre všetky celé čísla $n \geq a$.

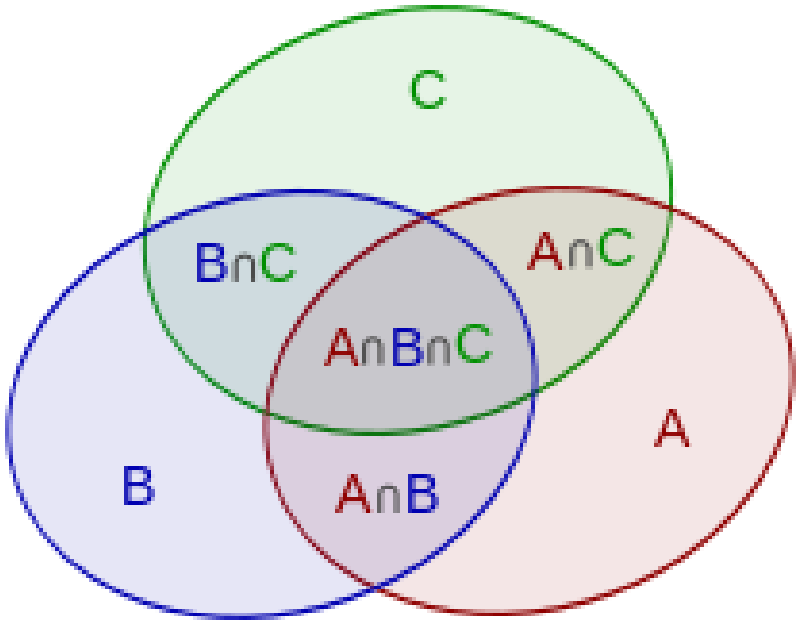
Johann Peter Gustav Lejeune Dirichlet

Dirichletov princíp

Ak je $kn + 1$ objektov $(k \geq 1)$ rozdelených do n škatúľ, tak jedna zo škatúľ obsahuje aspoň $k + 1$ objektov.



Princíp inklúzie a exklúzie



Princíp inklúzie a exklúzie

- Dve množiny

$$|A \cup B| = |A| + |B| - |A \cap B|$$

- Tri množiny

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

- $n-$ množín

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{i,j;i<j} |A_i \cap A_j| + \sum_{i,j,k;i<j<k} |A_i \cap A_j \cap A_k| -$$

$$+ \cdots (-1)^{n+1} |A_1 \cap A_2 \cap \cdots A_n|$$

Teória čísel

Deliteľnosť (NSD, NSN)

- Ako zistím $NSD(a, b)$?
- Ako zistím $NSN(a, b)$?
- $NSD(a, b) \cdot NSN(a, b) = ?$

Deliteľnosť (NSD, NSN)

- Nech $b_1, b_2 \in N, b_1 > b_2$. Potom existujú $q, b_3 \in Z, 0 \leq b_3 < b_2$ také, že

$$b_1 = qb_2 + b_3.$$

Deliteľnosť (NSD, NSN)

- Nech $b_1, b_2 \in N, b_1 > b_2$. Potom existujú $q, b_3 \in Z, 0 \leq b_3 < b_2$ také, že

$$b_1 = qb_2 + b_3.$$

- Aké je $NSD(b_1, b_2)$ a $NSD(b_2, b_3)$?

Deliteľnosť (NSD, NSN)

- Nech $b_1, b_2 \in N, b_1 > b_2$. Potom existujú $q, b_3 \in Z, 0 \leq b_3 < b_2$ také, že

$$b_1 = qb_2 + b_3.$$

- Aké je $NSD(b_1, b_2)$ a $NSD(b_2, b_3)$?
- $b_2 = q'.b_3 + b_4$
- $\ldots$
- $b_1 > b_2 > b_3 > \cdots >$

Deliteľnosť (NSD, NSN)

- Nech $b_1, b_2 \in N, b_1 > b_2$. Potom existujú $q, b_3 \in Z, 0 \leq b_3 < b_2$ také, že

$$b_1 = qb_2 + b_3.$$

- Aké je $NSD(b_1, b_2)$ a $NSD(b_2, b_3)$?
- $b_2 = q'.b_3 + b_4$
- $\ldots$
- $b_1 > b_2 > b_3 > \cdots >$
- **Bezoutova veta.** Nech $a, b \in N$. Potom existujú $s, t \in Z$ také, že

$$sa + tb = NSD(a, b).$$

Deliteľnosť (NSD, NSN)

- Nech $b_1, b_2 \in N, b_1 > b_2$. Potom existujú $q, b_3 \in Z, 0 \leq b_3 < b_2$ také, že

$$b_1 = qb_2 + b_3.$$

- Aké je $NSD(b_1, b_2)$ a $NSD(b_2, b_3)$?
- $b_2 = q'.b_3 + b_4$
- $\ldots$
- $b_1 > b_2 > b_3 > \cdots >$
- **Bezoutova veta.** Nech $a, b \in N$. Potom existujú $s, t \in Z$ také, že

$$sa + tb = NSD(a, b).$$

- Euklidov algoritmus

Euklides

Étienne Bézout

Rovnica

$$ax + by = c,$$

kde a, b, c sú celé čísla, ma **celočíselné riešenie** *x, y práve vtedy, keď nsd(a, b) delí c.*
Ak navyše (x_0, y_0) je nejaké celočíselné riešenie, tak pre každé celé číslo k aj čísla

$$x^* = x_0 - \frac{bk}{d}, y^* = y_0 + \frac{ak}{d},$$

kde $d =$ nsd(a, b), sú riešením a všetky celočíselné riešenia majú tento tvar.

Prvočísla

- Prvočísel je nekonečne veľa
- **Fundamentálna veta aritmetiky.** Každé prirodzené číslo väčšie ako 1 sa dá jednoznačne rozložiť na súčin prvočísel.

Kongruencie

Relácia kongruencie alebo kongruencia je ekvivalencia na algebre (napr. grupe), ktorá je zlúčiteľná so všetkými operáciami na tejto algebre (teda napríklad, ak sú tri páry prvkov ekvivalentné a výsledky nejakej operácie na týchto pároch sú tiež ekvivalentné, potom existuje pre tieto páry zhodnosť). Teda ak sú operandy na rovnakom mieste po dvoch ekvivalentné, potom musia aj výsledky operácie byť ekvivalentné.

- Nech $(X, \circ)$ je algebra, R je ekvivalencia na X. Potom R je **kongruencia** na X ak platí:
  $[a, b] \in R \wedge [c, d] \in R \Rightarrow [a \circ c, b \circ d] \in R.$
- Hovoríme, že dve čísla $a, b \in \mathbb{Z}$ sú kongruentné, ak ich rozdiel je deliteľný číslom m, ktoré nazývame **modul** $(m|(a - b))$. Formálne

$$a \equiv b \pmod{m}.$$

Príklady kongruencií

- Zrejme

$$\left.\begin{array}{ll} a \equiv b & (\mathrm{mod}\ m) \\ c \equiv d & (\mathrm{mod}\ m) \end{array}\right\} \Rightarrow \quad a + c \equiv b + d \quad (\mathrm{mod}\ m).$$

  teda $\equiv$ je kongruencia na $(Z, +)$.

- Ale aj

$$\left.\begin{array}{ll} a \equiv b & (\mathrm{mod}\ m) \\ c \equiv d & (\mathrm{mod}\ m) \end{array}\right\} \Rightarrow \quad a \cdot c \equiv b \cdot d \quad (\mathrm{mod}\ m).$$

  teda $\equiv$ je kongruencia aj na $(Z, \cdot)$.

Pierre de Fermat

Malá Fermatova veta

- **Veta.**Nech p je prvočíslo a $a \in Z, NSD(a,p) = 1$ potom

$$a^{p-1} \equiv 1 \pmod{p}.$$

Malá Fermatova veta

- **Veta.**Nech p je prvočíslo a $a \in Z, NSD(a,p) = 1$ potom

$$a^{p-1} \equiv 1 \pmod{p}.$$

- **Dôkaz.** Všimnime si čísla $1.a, 2.a, 3.a, \cdots, (p-1).a$, zrejme sú nesúdeliteľné s prvočíslom p a žiadne dve nie sú kongruentné $\pmod{p}$. Podobne sú na tom čísla $1, 2, \cdots, p-1$ a preto

$$(p-1)! \equiv 1.a.2.a.3.a.\cdots(p-1)a \pmod{p}.$$

Po vykrátení dostaneme

$$1 \equiv a^{p-1} \pmod{p}.$$

Čínska veta o zvyškoch

Veta. Nech $NSD(m,n) = 1$, $a, b \in Z$, potom existuje $x \in Z$ také, že

$$x = a \pmod{m},$$

$$x = b \pmod{n}.$$

Leonhard Euler

Eulerova funkcia

- **Definícia:**
  $\varphi(n)$ – počet prir. čísel, pre ktoré platí:
  - sú menšie ako n,
  - sú nesúdeliteľné s n.

Eulerova funkcia

- **Definícia:**
  $\varphi(n)$ – počet prir. čísel, pre ktoré platí:
  - sú menšie ako n,
  - sú nesúdeliteľné s n.
- **Vlastnosti:**
  - Ak p je prvočíslo, tak
    - $\varphi(p) = p - 1$,
    - $\varphi(p^k) = p^k - p^{k-1}$.
  - Ak $NSD(m, n) = 1$, tak $\varphi(m.n) = \varphi(m).\varphi(n)$.
  - Ak $n = p_1^{k_1}.p_2^{k_2} \cdots .p_s^{k_s}$, tak

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right).\left(1 - \frac{1}{p_2}\right).\cdots.\left(1 - \frac{1}{p_s}\right).$$

Eulerova veta

Eulerova veta. Nech $NSD(a, n) = 1$, potom

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dôkaz. *Inšpirujte sa dôkazom Fermatovej vety.*

Tri dôležité tvrdenia

- **Bertrandov postulát.** Pre každé $n \geq 1$ existuje aspoň jedno prvočíslo p také, že $n < p \leq 2n$.
- **Veta o hustote prvočísel.** Nech $\pi(x)$ je počet prvočísel od 1 do x, potom $\pi(x) = \Theta(x/\log x)$.
- **Prvočíselný harmonický rad.** Pre ľubovolné n platí

$$\sum_{1 \leq p \leq n} \frac{1}{p} = \mathcal{O}(\log \log n).$$

Dôkazy pre odvážnych

Prvočíselný harmonický rad

Prvočíselný harmonický rad. Pre ľubovolné n platí

$$\sum_{1 \leq p \leq n} \frac{1}{p} = \mathcal{O}(\log \log n).$$

Na dôkaz využijeme nasledujúce pomocné tvrdenia 1–5.

1. pomocné tvrdenie

- **1.** $\frac{4^n}{2n+1} \leq \binom{2n}{n} \leq 4^n$.
- Z binomickej vety máme:

$$4^n = 2^{2n} = (1+1)^{2n} = \binom{2n}{0} + \binom{2n}{1} + \cdots + \binom{\mathbf{2n}}{\mathbf{n}} + \cdots + \binom{2n}{2n}.$$

- Všetky sčítance sú kladné, preto $\binom{2n}{n} \leq 4^n$.
- Zrejme $\binom{2n}{n}$ je zo všetkých sčítancov najväčší, tak je aspoň taký ako ich aritmetický priemer, preto $\binom{2n}{n} \geq \frac{4^n}{2n+1}$.

2. pomocné tvrdenie

- **2.** $\binom{2n+1}{n} \leq 4^n$.
- Z binomickej vety máme:

$$2^{2n+1} = (1+1)^{2n+1} = \binom{2n+1}{0} + \binom{2n+1}{1} + \cdots + \binom{\mathbf{2n+1}}{\mathbf{n}} + \binom{\mathbf{2n+1}}{\mathbf{n+1}} + \cdots + \binom{2n+1}{2n+1}$$

Zrejme

$$\binom{2n+1}{n} = \binom{2n+1}{n+1},$$

preto $\binom{2n+1}{n}$ neprekročí polovicu celého súčtu (tieto dva sčítance sú uprostred riadku v Pascalovom trojuholníku, sú teda najväčšie), preto

$$\binom{2n+1}{n} \leq \frac{2.4^n}{2} = 4^n.$$

3. pomocné tvrdenie

- **3.** Nech $n+1 \leq p \leq 2n$, tak $p|\binom{2n}{n}$.
- Zrejme
$$\binom{2n}{n} = \frac{2n.(2n-1).\ldots.(n+1)}{n.(n-1).\ldots.1}.$$
- Každé $p \in \{n+1, n+2, \ldots, 2n\}$ je v čitateli zlomku, ale nie je v menovateli, preto $p|\binom{2n}{n}$. Treba si uvedomiť, že tie prvočísla sú "nevykrátiteľné".

4. pomocné tvrdenie

- **4.** Nech $\pi(a, b)$ je počet prvočísel $p \in \{a, a+1, \ldots, b\}$, potom

$$\pi(n+1, 2n) \leq \frac{2n}{\log_2 n}.$$

- Keďže každé prvočíslo $n+1 \leq p \leq 2n$ je deliteľom čísla $\binom{2n}{n}$, tak aj súčin týchto prvočísel je deliteľom čísla $\binom{2n}{n}$.
- Každé takéto prvočíslo je väčšie ako n, preto

$$n^{\pi(n+1,2n)} \leq \binom{2n}{n}.$$

- Potom

$$\pi(n+1, 2n) \leq \log_n \binom{2n}{n} = \frac{\log_2 \binom{2n}{n}}{\log_2 n}.$$

Už vieme, že $\binom{2n}{n} \leq 4^n$, tak aj $\log_2 \binom{2n}{n} \leq 2n$ a tým je dôkaz skončený.

5. pomocné tvrdenie

Označme: $H(n) = \sum_{i=1}^{n} \frac{1}{i}, \quad H(a,b) = \sum_{i=a}^{b} \frac{1}{i}.$

- **5.** Nech $n = 2^k$. Potom

$$H(n) = H(1,2) + \sum_{i=2}^{\log_2 n} H(2^{i-1}+1, 2^i).$$

Zrejme

$$\frac{3}{2} + \frac{1}{2}\log_2 n \leq H(n) \leq \frac{3}{2} + \log_2 n,$$

preto

$$H(n) = \Theta(\log_2 n).$$

Ak n nie je mocninou čísla 2, tak sa $H(n)$ dá zhora, aj zdola ohraničiť najbližšou nižšou a vyššou mocninou čísla 2.

Prvočíselný harmonický rad (dôkaz)

- Nech $P(n) = \sum_{1 \leq p \leq n} \frac{1}{p}$ a nech $n = 2^k$.

  Potom

$$P(n) = P(1,2) + \sum_{i=2}^{\log_2 n} P(2^{i-1}+1, 2^i), \text{ kde } P(a,b) = \sum_{a \leq p \leq b} \frac{1}{p}.$$

  Využijeme odhad pre harmonický rad a to, že $\pi(n+1, 2n) \leq \frac{2n}{\log_2 n}$. Potom pre jeden úsek máme:

$$\frac{2^i}{i-1} \cdot \frac{1}{2^i} \leq u \leq \frac{2^i}{i-1} \cdot \frac{1}{2^{i-1}},$$

$$\frac{1}{i} \leq \frac{1}{i-1} \leq u \leq \frac{2}{i-1} \leq \frac{4}{i}.$$

  Potom

$$P(n) = \sum_{i=1}^{\log_2 n} \mathcal{O}(\frac{1}{i}) = \mathcal{O}(H(\log_2 n)) = \mathcal{O}(\log_2 \log_2 n).$$

Bertrandov postulát

- **Bertrandov postulát.** Pre každé $n \geq 1$ existuje aspoň jedno prvočíslo p také, že $n < p \leq 2n$.

Na dôkaz využijeme nasledujúce pomocné tvrdenia 6–7.

Pomocné pojmy

Označme: $o_p(n)$ je exponent prvočísla p v prvoč. rozklade čísla n. Potom

- $o_p(x.y) = o_p(x) + o_p(y)$,
- $o_p(\frac{x}{y}) = o_p(x) - o_p(y)$,
- $o_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots + \lfloor \frac{n}{p^i} \rfloor + \cdots$.

6. pomocné tvrdenie

- **6.** Dokážeme, že
$$p^{o_p\left(\binom{2n}{n}\right)} \leq 2n.$$

- Zrejme
$$o_p\left(\binom{2n}{n}\right) = o_p\left(\frac{(2n)!}{(n)!^2}\right) = o_p\left((2n)!\right) - 2o_p(n!).$$

Preto
$$o_p\left(\binom{2n}{n}\right) = \left(\sum_{i\geq 1}\lfloor\frac{2n}{p^i}\rfloor\right) - 2\left(\sum_{i\geq 1}\lfloor\frac{n}{p^i}\rfloor\right) = \sum_{i\geq 1}\left(\lfloor\frac{2n}{p^i}\rfloor - 2\lfloor\frac{n}{p^i}\rfloor\right).$$

Zrejme $\lfloor 2x\rfloor - 2\lfloor x\rfloor \leq 1$ a pre $i > \log_p 2n$ budeme sčitovať už len nuly.

Potom
$$o_p\left(\binom{2n}{n}\right) \leq \log_p 2n,$$

a preto
$$p^{o_p\left(\binom{2n}{n}\right)} \leq p^{\log_p 2n} = 2n.$$

7. pomocné tvrdenie

- **7.** Dokážeme, že
$$\prod_{p \leq n} p \leq 4^n.$$
- Dôkaz urobíme mat. indukciou.
  - pre malé n tvrdenie evidentne platí (vyskúšajte si).
  - ak n je párne a $n > 2$, tak indukčný krok je triviálny, lebo n nie je prvočíslo
$$\prod_{p \leq n} p = \prod_{p \leq n-1} p \leq 4^{n-1} \leq 4^n.$$
  - ak n je nepárne, potom $n = 2m + 1$ a
$$\prod_{p \leq 2m+1} p = \left(\prod_{p \leq m+1} p \right) \cdot \left(\prod_{m+2 \leq p \leq 2m+1} p \right).$$

7. pomocné tvrdenie-pokračovanie

Zrejme $m+1 < 2m+1$, preto

$$\prod_{p \leq m+1} p \leq 4^{m+1}.$$

Ďalej (3. pom. tvrdenie)

$$\left(\prod_{m+2 \leq p \leq 2m+1} p \right) \mid \binom{2m+1}{m},$$

podľa 2. pom. tvrdenia je toto kombinačné číslo zhora ohraničené číslom 4^m. Preto

$$\prod_{p \leq 2m+1} p = \left(\prod_{p \leq m+1} p \right) \cdot \left(\prod_{m+2 \leq p \leq 2m+1} p \right) \leq 4^{m+1}.4^m = 4^{2m+1}.$$

Bertrandov postulát (dôkaz)

- $\binom{2n}{n} = A.B.C.D \geq \frac{4^n}{2n+1}$ (1. pomoc. tvrdenie)
  - A zahŕňa prvočísla $p \leq \sqrt{2n}$
  - B zahŕňa prvočísla $\sqrt{2n} < p \leq \frac{2n}{3}$
  - C zahŕňa prvočísla $\frac{2n}{3} < p \leq n$
  - D zahŕňa prvočísla $n < p \leq 2n$
- Do časti A prispeje max. $\sqrt{2n}$ prvočísel a každé prispeje max. $2n$, preto $A \leq (2n)^{\sqrt{2n}}$.
- Prvočísla z časti B musia mať v komb. čísle exponent max. 1 a podľa 7. pomoc. tvrdenia je teda $B \leq 4^{\frac{2n}{3}}$.
- Pre p z časti C je $o_p(n!) = 1$ a $o_p((2n)!) = 2$, preto $o_p(\binom{2n}{n}) = o_p((2n)!) - 2.o_p(n!) = 2 - 2 = 0$, teda $C = 1$.

Bertrandov postulát (dôkaz)

- Ak by $D = 1$, tak

$$\frac{4^n}{2n+1} \leq \binom{2n}{n} \leq (2n)^{\sqrt{2n}}.4^{\frac{2n}{3}},$$

$$2^{2n-\log_2(2n+1)} \leq 2^{(\log_2 2n)\sqrt{2n}+\frac{4n}{3}},$$

$$2n - \log_2(2n+1) \leq (\log_2 2n)\sqrt{2n} + \frac{4n}{3},$$

$$\frac{2}{3}n \leq (\log_2 2n)\sqrt{2n} + \log_2(2n+1).$$

Ľavá strana rastie rýchlejšie ako pravá a pre $n = 1024$ už musí byť $D > 1$, pre zvyšných konečne mnoho n stačí uvažovať postupnosť:

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259.$$

Veta o hustote prvočísel

Veta o hustote prvočísel. Nech $\pi(x)$ je počet prvočísel od 1 do x, potom $\pi(x) = \Theta(x/\log x)$.

Veta o hustote prvočísel (dôkaz)

- Dolný odhad:

$$\log_2 \binom{2n}{n} = \log_2 \left(\prod_{p \leq 2n} p^{o_p\left(\binom{2n}{n}\right)} \right) = \sum_{p \leq 2n} \log_2 p^{o_p\left(\binom{2n}{n}\right)} =$$

$$= \sum_{p \leq 2n} o_p \left(\binom{2n}{n} \right) . \log_2 p.$$

Podľa 6. pomocného tvrdenia prispeje prvočíslo p najviac $2n$, potom jeho exponent $o_p\left(\binom{2n}{n}\right) \leq \log_p 2n = \frac{\log_2 2n}{\log_2 p}$, preto

$$\log_2 \binom{2n}{n} \leq \sum_{p \leq 2n} \frac{\log_2 2n}{\log_2 p} . \log_2 p \leq \sum_{p \leq 2n} \log_2 2n \leq \pi(2n) . \log_2 2n.$$

Veta o hustote prvočísel (dôkaz)

Z 1. pomoc. tvrdenia vieme, že

$$\binom{2n}{n} \geq \frac{4^n}{2n+1},$$

teda pre dosť veľké n bude $\log_2 \binom{2n}{n} \geq n$ a teda

$$\pi(2n) \geq \frac{n}{\log_2 2n}.$$

Pre párne x je $\pi(x) = \Omega(\frac{x}{\log_2 x})$ a vzhľadom k tomu, že π je neklesajúca funkcia, platí tento odhad aj pre nepárne čísla.

Veta o hustote prvočísel (dôkaz)

- Horný odhad:
  Nech $2^{k-1} \leq x \leq 2^k$ a budeme odhadovať počet prvočísel medzi 1 a 2^k. Znovu rozdelíme rad na vhodné úseky a využijeme 4. pomocné tvrdenie.

$$\pi(x) \leq \pi(2^k) \leq \pi(1,2) + \sum_{i=2}^{k} \pi(2^{i-1}+1, 2^i) \leq 1 + \sum_{i=2}^{k} \frac{2.2^{i-1}}{i-1}.$$

  Posledný sčítanec $(i = k)$ nám dáva odhad $\frac{x}{\log_2 x}$, ešte musíme zistiť, či zvyšné členy klesajú dosť rýchlo, aby nám nepokazili radosť.

Veta o hustote prvočísel (dôkaz)

Zrejme

$$\frac{\frac{2^i}{i-1}}{\frac{2^{i+1}}{i}} = \frac{i}{2(i-1)} \leq \frac{3}{4}, \qquad \forall k \in N; k \geq 3.$$

Preto:

$$\pi(x) \leq \pi(2) + \pi(2^{k-1}+1, 2^k).\sum_{i=0}^{\infty}\left(\frac{3}{4}\right)^i \leq 1 + \frac{2^k}{k-1}.4 =$$

$$= \mathcal{O}\left(\frac{2^k}{k}\right) = \mathcal{O}\left(\frac{x}{\log_2 x}\right).$$