Prvočísla a ich číselní príbuzní

Miroslav Haviar

Katedra matematiky, FPV UMB
Banská Bystrica

CaKS, N. Smokovec
12.10. 2010

Európska únia
Európsky fond regionálneho rozvoja

Operačný program
VÝSKUM a VÝVOJ

Agentúra
Ministerstva školstva, vedy, výskumu a športu SR
pre štrukturálne fondy EÚ

Podporujeme výskumné aktivity na Slovensku/
Projekt je spolufinancovaný zo zdrojov EÚ

Primoriálne čísla - pojem

- Prvočíslo je prirodzené číslo $p \geq 2$, ktorého jedinými kladnými deliteľmi je p a 1.

Primoriálne čísla - pojem

- Prvočíslo je prirodzené číslo $p \geq 2$, ktorého jedinými kladnými deliteľmi je p a 1.

Primoriálne čísla - pojem

- Prvočíslo je prirodzené číslo $p \geq 2$, ktorého jedinými kladnými deliteľmi je p a 1.
- *Primoriálne číslo* $P_k = p_1 \cdot p_2 \cdot \dots \cdot p_k$ je súčin prvých k prvočísel.

Primoriálne čísla - pojem

- Prvočíslo je prirodzené číslo $p \geq 2$, ktorého jedinými kladnými deliteľmi je p a 1.
- *Primoriálne číslo* $P_k = p_1 \cdot p_2 \cdot \dots \cdot p_k$ je súčin prvých k prvočísel.

$$P_1 = 2$$
$$P_2 = 2 \cdot 3 = 6$$
$$P_3 = 2 \cdot 3 \cdot 5 = 30$$
$$P_4 = 2 \cdot 3 \cdot 5 \cdot 7 = 210$$
$$P_5 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$$

Primoriálne čísla - pojem

- Prvočíslo je prirodzené číslo $p \geq 2$, ktorého jedinými kladnými deliteľmi je p a 1.
- *Primoriálne číslo* $P_k = p_1 \cdot p_2 \cdot \dots \cdot p_k$ je súčin prvých k prvočísel.

$$
\begin{aligned}
P_1 &= 2 \\
P_2 &= 2 \cdot 3 = 6 \\
P_3 &= 2 \cdot 3 \cdot 5 = 30 \\
P_4 &= 2 \cdot 3 \cdot 5 \cdot 7 = 210 \\
P_5 &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310
\end{aligned}
$$

- Prvočísel je nekonečne veľa. *Euklides*: *Ak je ich zoznam konečný, $p_1, p_2, \dots, p_n$, tak číslo $P_n + 1$ je prvočíslo väčšie ako p_n, spor.*

Primoriálne prvočísla - problém

Pre žiaka či študenta predstavuje takýto dôkaz nekonečného počtu prvočísel niekoľko "intelektuálnych obtiaží":

Primoriálne prvočísla - problém

Pre žiaka či študenta predstavuje takýto dôkaz nekonečného počtu prvočísel niekoľko "intelektuálnych obtiaží":

- Pojem dôkazu a motivácia preň;

Primoriálne prvočísla - problém

Pre žiaka či študenta predstavuje takýto dôkaz nekonečného počtu prvočísel niekoľko “intelektuálnych obtiaží”:

- Pojem dôkazu a motivácia preň;
- Argument “dôkazu sporom”;

Primoriálne prvočísla - problém

Pre žiaka či študenta predstavuje takýto dôkaz nekonečného počtu prvočísel niekoľko "intelektuálnych obtiaží":

- Pojem dôkazu a motivácia preň;
- Argument "dôkazu sporom";
- Uvedomenie si, že dôkaz neukazuje, že čísla $P_n + 1$ sú prvočísla: Pre $n = 1, 2, 3, 4, 5$ je $P_n + 1$ prvočíslo, ale
$$P_6 + 1 = 30031 = 59 \times 509.$$

Primoriálne prvočísla - problém

Pre žiaka či študenta predstavuje takýto dôkaz nekonečného počtu prvočísel niekoľko "intelektuálnych obtiaží":

- Pojem dôkazu a motivácia preň;
- Argument "dôkazu sporom";
- Uvedomenie si, že dôkaz neukazuje, že čísla $P_n + 1$ sú prvočísla: Pre $n = 1, 2, 3, 4, 5$ je $P_n + 1$ prvočíslo, ale

$$P_6 + 1 = 30031 = 59 \times 509.$$

Prvočísla v tvare $P_n + 1$ alebo $P_n - 1$ sa nazývajú *primoriálne prvočísla.*

Primoriálne prvočísla - problém

Pre žiaka či študenta predstavuje takýto dôkaz nekonečného počtu prvočísel niekoľko "intelektuálnych obtiaží":

- Pojem dôkazu a motivácia preň;
- Argument "dôkazu sporom";
- Uvedomenie si, že dôkaz neukazuje, že čísla $P_n + 1$ sú prvočísla: Pre $n = 1, 2, 3, 4, 5$ je $P_n + 1$ prvočíslo, ale
$$P_6 + 1 = 30031 = 59 \times 509.$$
Prvočísla v tvare $P_n + 1$ alebo $P_n - 1$ sa nazývajú *primoriálne prvočísla.*
- **Problém:** ***Je primoriálnych prvočísel nekonečne veľa?***

Prvočísla majú “častý výskyt”

Nielenže existuje nekonečne veľa prvočísel, ale existuje nekonečne veľa prvočísel mnohých rozličných druhov:

Prvočísla majú “častý výskyt”

Nielenže existuje nekonečne veľa prvočísel, ale existuje nekonečne veľa prvočísel mnohých rozličných druhov:

- Dirichletova veta (1837): *Ak* $a, b \in \mathbb{N}$ *sú nesúdeliteľné, tak existuje nekonečne veľa prvočísel v rámci aritmetickej postupnosti*

$$a, a+b, a+2b, a+3b, \ldots .$$

Prvočísla majú “častý výskyt”

Nielenže existuje nekonečne veľa prvočísel, ale existuje nekonečne veľa prvočísel mnohých rozličných druhov:

- *Dirichletova veta (1837)*: *Ak $a, b \in \mathbb{N}$ sú nesúdeliteľné, tak existuje nekonečne veľa prvočísel v rámci aritmetickej postupnosti*
$$a, a+b, a+2b, a+3b, \ldots.$$
- *Hypotéza prvočíselných dvojčiat*: *Existuje nekonečne veľa prvočíselných dvojčiat.*

Prvočísla majú “častý výskyt”

Nielenže existuje nekonečne veľa prvočísel, ale existuje nekonečne veľa prvočísel mnohých rozličných druhov:

- *Dirichletova veta (1837)*: *Ak* $a, b \in \mathbb{N}$ *sú nesúdeliteľné, tak existuje nekonečne veľa prvočísel v rámci aritmetickej postupnosti*
$$a, a+b, a+2b, a+3b, \ldots .$$
- *Hypotéza prvočíselných dvojčiat*: *Existuje nekonečne veľa prvočíselných dvojčiat. (Prvočíselné dvojčatá sú dvojice prvočísel tvaru* $(p, p+2)$ *ako* $(3,5), (11,13), (17,19)$*).*

Prvočísla majú “častý výskyt”

Nielenže existuje nekonečne veľa prvočísel, ale existuje nekonečne veľa prvočísel mnohých rozličných druhov:

- *Dirichletova veta (1837)*: *Ak* $a, b \in \mathbb{N}$ *sú nesúdeliteľné, tak existuje nekonečne veľa prvočísel v rámci aritmetickej postupnosti*
$$a, a+b, a+2b, a+3b, \dots .$$
- *Hypotéza prvočíselných dvojčiat*: *Existuje nekonečne veľa prvočíselných dvojčiat. (Prvočíselné dvojčatá sú dvojice prvočísel tvaru* $(p, p+2)$ *ako* $(3,5), (11,13), (17,19)$*).*
- *Goldbachova hypotéza (1742)*: *Každé párne prirodzené číslo* $n \geq 4$ *je súčtom dvoch prvočísel.*

Prvočísla majú “zriedkavý výskyt”

Medzi členmi rodiny prvočísel možno nájsť medzery ľubovoľne veľkej dĺžky.

Prvočísla majú “zriedkavý výskyt”

Medzi členmi rodiny prvočísel možno nájsť medzery ľubovoľne veľkej dĺžky. Vieme, že pre primoriál P_k číslo $P_k + 1$ môže byť prvočíslo alebo zložené číslo,

Prvočísla majú “zriedkavý výskyt”

Medzi členmi rodiny prvočísel možno nájsť medzery ľubovoľne veľkej dĺžky. Vieme, že pre primoriál P_k číslo $P_k + 1$ môže byť prvočíslo alebo zložené číslo, ale nasledujúcich $p_{k+1} - 2$ čísel

$$P_k + 2,\; P_k + 3,\; \dots,\; P_k + i,\; \dots,\; P_k + p_{k+1} - 1$$

je zložených.

Prvočísla majú “zriedkavý výskyt”

Medzi členmi rodiny prvočísel možno nájsť medzery ľubovoľne veľkej dĺžky. Vieme, že pre primoriál P_k číslo $P_k + 1$ môže byť prvočíslo alebo zložené číslo, ale nasledujúcich $p_{k+1} - 2$ čísel

$$P_k + 2,\ P_k + 3,\ \dots,\ P_k + i,\ \dots,\ P_k + p_{k+1} - 1$$

je zložených.

Prvočísla majú “zriedkavý výskyt”

Medzi členmi rodiny prvočísel možno nájsť medzery ľubovoľne veľkej dĺžky. Vieme, že pre primoriál P_k číslo $P_k + 1$ môže byť prvočíslo alebo zložené číslo, ale nasledujúcich $p_{k+1} - 2$ čísel

$$P_k + 2,\ P_k + 3,\ \dots,\ P_k + i,\ \dots,\ P_k + p_{k+1} - 1$$

je zložených.

- Pre prvočíslo p_k sa medzera po nasledujúce prvočíslo nazýva *medzera prvočísel*:
$$g(p_k) = p_{k+1} - p_k.$$

Prvočísla majú “zriedkavý výskyt”

Medzi členmi rodiny prvočísel možno nájsť medzery ľubovoľne veľkej dĺžky. Vieme, že pre primoriál P_k číslo $P_k + 1$ môže byť prvočíslo alebo zložené číslo, ale nasledujúcich $p_{k+1} - 2$ čísel

$$P_k + 2,\ P_k + 3,\ \dots,\ P_k + i,\ \dots,\ P_k + p_{k+1} - 1$$

je zložených.

- Pre prvočíslo p_k sa medzera po nasledujúce prvočíslo nazýva *medzera prvočísel*:
$$g(p_k) = p_{k+1} - p_k.$$
(B. Nyman a T. Nicely v r. 2009 uvádzajú 1184 zložených čísel za prvočíslom 43 841 547 845 541 059.)

Prvočísla majú “zriedkavý výskyt”

Medzi členmi rodiny prvočísel možno nájsť medzery ľubovoľne veľkej dĺžky. Vieme, že pre primoriál P_k číslo $P_k + 1$ môže byť prvočíslo alebo zložené číslo, ale nasledujúcich $p_{k+1} - 2$ čísel

$$P_k + 2,\ P_k + 3,\ \dots,\ P_k + i,\ \dots,\ P_k + p_{k+1} - 1$$

je zložených.

- Pre prvočíslo p_k sa medzera po nasledujúce prvočíslo nazýva *medzera prvočísel*:
$$g(p_k) = p_{k+1} - p_k.$$
(B. Nyman a T. Nicely v r. 2009 uvádzajú 1184 zložených čísel za prvočíslom 43 841 547 845 541 059.)
- Množstvo štúdií pojednáva o tom ako $g(p)$ rastie s p, ktoré čísla vznikajú ako medzery prvočísel a ako často sa vyskytujú.

Jumping champions

- Pre malé hodnoty sú najčastejšie medzery prvočísel 2, potom 2 a 4, od 563 to “skočí” na 6, ktorá zatiaľ vedie ako “jumping champion”.

Jumping champions

- Pre malé hodnoty sú najčastejšie medzery prvočísel 2, potom 2 a 4, od 563 to “skočí” na 6, ktorá zatiaľ vedie ako “jumping champion”.
- Tvrdí sa, že okolo 10^{35} bude najčastejšia medzera 30, okolo 10^{425} bude 210 a že s výnimkou čísla 4 budú “jumping champions” **primoriálne čísla** $2, 6, 30, 210, 2310, \ldots$!

Jumping champions

- Pre malé hodnoty sú najčastejšie medzery prvočísel 2, potom 2 a 4, od 563 to “skočí” na 6, ktorá zatiaľ vedie ako “jumping champion”.
- Tvrdí sa, že okolo 10^{35} bude najčastejšia medzera 30, okolo 10^{425} bude 210 a že s výnimkou čísla 4 budú “jumping champions” **primoriálne čísla** $2, 6, 30, 210, 2310, \ldots$!
- Otvoreným problémom je, či každé párne číslo je rozdielom dvoch (nie nutne po sebe idúcich) prvočísel:

Jumping champions

- Pre malé hodnoty sú najčastejšie medzery prvočísel 2, potom 2 a 4, od 563 to “skočí” na 6, ktorá zatiaľ vedie ako “jumping champion”.
- Tvrdí sa, že okolo 10^{35} bude najčastejšia medzera 30, okolo 10^{425} bude 210 a že s výnimkou čísla 4 budú “jumping champions” **primoriálne čísla** $2, 6, 30, 210, 2310, \ldots$!
- Otvoreným problémom je, či každé párne číslo je rozdielom dvoch (nie nutne po sebe idúcich) prvočísel: *Polignacova hypotéza*:
  (P1) *Každé párne prirodzené číslo $2n$ je rozdielom dvoch prvočísel.*

Jumping champions

- Pre malé hodnoty sú najčastejšie medzery prvočísel 2, potom 2 a 4, od 563 to “skočí” na 6, ktorá zatiaľ vedie ako “jumping champion”.
- Tvrdí sa, že okolo 10^{35} bude najčastejšia medzera 30, okolo 10^{425} bude 210 a že s výnimkou čísla 4 budú “jumping champions” **primoriálne čísla** $2, 6, 30, 210, 2310, \ldots$!
- Otvoreným problémom je, či každé párne číslo je rozdielom dvoch (nie nutne po sebe idúcich) prvočísel: *Polignacova hypotéza*: (P1) *Každé párne prirodzené číslo $2n$ je rozdielom dvoch prvočísel.* (P2) *Dvojíc prvočísel s rozdielom $2n$ je nekonečne veľa.*

Jumping champions

- Pre malé hodnoty sú najčastejšie medzery prvočísel 2, potom 2 a 4, od 563 to "skočí" na 6, ktorá zatiaľ vedie ako "jumping champion".
- Tvrdí sa, že okolo 10^{35} bude najčastejšia medzera 30, okolo 10^{425} bude 210 a že s výnimkou čísla 4 budú "jumping champions" **primoriálne čísla** $2, 6, 30, 210, 2310, \ldots$!
- Otvoreným problémom je, či každé párne číslo je rozdielom dvoch (nie nutne po sebe idúcich) prvočísel: *Polignacova hypotéza*: (P1) *Každé párne prirodzené číslo* $2n$ *je rozdielom dvoch prvočísel.* (P2) *Dvojíc prvočísel s rozdielom* $2n$ *je nekonečne veľa.*
- **Hypotéza prvočíselných dvojčiat je vlastne Polignacova hypotéza (P2) pre** $2n = 2$.

Nevieme “nič”

Nevieme "nič"

- Nevieme, či je nekonečne veľa prvočíselných dvojčiat $(p, p + 2)$.

Nevieme “nič”

- Nevieme, či je nekonečne veľa prvočíselných dvojčiat $(p, p+2)$.
- Ale nevieme ani, či je nekonečne veľa prvočíselných trojčiat $(p, p+2, p+6)$

Nevieme “nič”

- Nevieme, či je nekonečne veľa prvočíselných dvojčiat $(p, p+2)$.
- Ale nevieme ani, či je nekonečne veľa prvočíselných trojčiat $(p, p+2, p+6)$ a nekonečne veľa prvočíselných trojčiat $(p, p+4, p+6)$.

Nevieme “nič”

- Nevieme, či je nekonečne veľa prvočíselných dvojčiat $(p, p+2)$.
- Ale nevieme ani, či je nekonečne veľa prvočíselných trojčiat $(p, p+2, p+6)$ a nekonečne veľa prvočíselných trojčiat $(p, p+4, p+6)$.
- Nevieme, či je nekonečne veľa prvočíselných štvorčiat $(p, p+2, p+6, p+8)$, atď.

Nevieme “nič”

- Nevieme, či je nekonečne veľa prvočíselných dvojčiat $(p, p+2)$.
- Ale nevieme ani, či je nekonečne veľa prvočíselných trojčiat $(p, p+2, p+6)$ a nekonečne veľa prvočíselných trojčiat $(p, p+4, p+6)$.
- Nevieme, či je nekonečne veľa prvočíselných štvorčiat $(p, p+2, p+6, p+8)$, atď.
- Nevedeli sme dlho, či pre každé n existuje n po sebe idúcich prvočísel v aritmetickej postupnosti. (Potvrdené pre n do 22.) Terence Tao: riešenie a Fields medal (2006).

Nevieme "nič"

- Nevieme, či je nekonečne veľa prvočíselných dvojčiat $(p, p+2)$.
- Ale nevieme ani, či je nekonečne veľa prvočíselných trojčiat $(p, p+2, p+6)$ a nekonečne veľa prvočíselných trojčiat $(p, p+4, p+6)$.
- Nevieme, či je nekonečne veľa prvočíselných štvorčiat $(p, p+2, p+6, p+8)$, atď.
- Nevedeli sme dlho, či pre každé n existuje n po sebe idúcich prvočísel v aritmetickej postupnosti. (Potvrdené pre n do 22.) Terence Tao: riešenie a Fields medal (2006).

Nevieme “nič”

- Nevieme, či je nekonečne veľa prvočíselných dvojčiat $(p, p+2)$.
- Ale nevieme ani, či je nekonečne veľa prvočíselných trojčiat $(p, p+2, p+6)$ a nekonečne veľa prvočíselných trojčiat $(p, p+4, p+6)$.
- Nevieme, či je nekonečne veľa prvočíselných štvorčiat $(p, p+2, p+6, p+8)$, atď.
- Nevedeli sme dlho, či pre každé n existuje n po sebe idúcich prvočísel v aritmetickej postupnosti. (Potvrdené pre n do 22.) Terence Tao: riešenie a Fields medal (2006).
- Keď nie sú čísla $P_k + 1$ prvočísla, uvažujme najmenšie prirodzené d_k tak, že $P_k + d_k$ je prvočíslo.

Nevieme “nič”

- Nevieme, či je nekonečne veľa prvočíselných dvojčiat $(p, p+2)$.
- Ale nevieme ani, či je nekonečne veľa prvočíselných trojčiat $(p, p+2, p+6)$ a nekonečne veľa prvočíselných trojčiat $(p, p+4, p+6)$.
- Nevieme, či je nekonečne veľa prvočíselných štvorčiat $(p, p+2, p+6, p+8)$, atď.
- Nevedeli sme dlho, či pre každé n existuje n po sebe idúcich prvočísel v aritmetickej postupnosti. (Potvrdené pre n do 22.) Terence Tao: riešenie a Fields medal (2006).
- Keď nie sú čísla $P_k + 1$ prvočísla, uvažujme najmenšie prirodzené d_k tak, že $P_k + d_k$ je prvočíslo. Reo Fortune vyslovil hypotézu, že čísla d_k (nazývajú sa *fortunate numbers*) sú tiež prvočísla!

Vieme “všetko”

Vieme “všetko”

- Často sa tvrdí (aj v matematickej komunite), že neexistuje vzorec pre n-té prvočíslo ani žiadna rekurzívna formula, ktorá by určila $(n+1)$-vé prvočíslo z prvých n prvočísel.

Vieme “všetko”

- Často sa tvrdí (aj v matematickej komunite), že neexistuje vzorec pre n-té prvočíslo ani žiadna rekurzívna formula, ktorá by určila $(n+1)$-vé prvočíslo z prvých n prvočísel.
- Preto iste na mnohých zapôsobí šokujúco, že v r. 1971 J.M. Gandhi publikoval explicitný *vzorec (rekurzívnu formulu) pre n-té prvočíslo*!

Vieme “všetko”

- Často sa tvrdí (aj v matematickej komunite), že neexistuje vzorec pre n-té prvočíslo ani žiadna rekurzívna formula, ktorá by určila $(n+1)$-vé prvočíslo z prvých n prvočísel.
- Preto iste na mnohých zapôsobí šokujúco, že v r. 1971 J.M. Gandhi publikoval explicitný *vzorec (rekurzívnu formulu) pre n-té prvočíslo*! Jeho riešenie teraz uvedieme.

Vieme "všetko"

- Často sa tvrdí (aj v matematickej komunite), že neexistuje vzorec pre n-té prvočíslo ani žiadna rekurzívna formula, ktorá by určila $(n+1)$-vé prvočíslo z prvých n prvočísel.
- Preto iste na mnohých zapôsobí šokujúco, že v r. 1971 J.M. Gandhi publikoval explicitný *vzorec (rekurzívnu formulu) pre n-té prvočíslo*! Jeho riešenie teraz uvedieme.
- Primoriálne číslo $P_k = p_1 \cdot p_2 \cdot \dots \cdot p_k$ má 2^k deliteľov (keďže množina $\{p_1, p_2, \dots, p_k\}$ má 2^k podmnožín).

Vieme "všetko"

- Často sa tvrdí (aj v matematickej komunite), že neexistuje vzorec pre n-té prvočíslo ani žiadna rekurzívna formula, ktorá by určila $(n+1)$-vé prvočíslo z prvých n prvočísel.
- Preto iste na mnohých zapôsobí šokujúco, že v r. 1971 J.M. Gandhi publikoval explicitný *vzorec (rekurzívnu formulu) pre n-té prvočíslo*! Jeho riešenie teraz uvedieme.
- Primoriálne číslo $P_k = p_1 \cdot p_2 \cdot \dots \cdot p_k$ má 2^k deliteľov (keďže množina $\{p_1, p_2, \dots, p_k\}$ má 2^k podmnožín).
- Pre každý deliteľ $d|P_k$ položíme $\mu(d) = 1$, ak d je súčin párneho počtu prvočísel a $\mu(d) = -1$, ak d je súčin nepárneho počtu prvočísel.

Vieme "všetko"

- Často sa tvrdí (aj v matematickej komunite), že neexistuje vzorec pre n-té prvočíslo ani žiadna rekurzívna formula, ktorá by určila $(n+1)$-vé prvočíslo z prvých n prvočísel.
- Preto iste na mnohých zapôsobí šokujúco, že v r. 1971 J.M. Gandhi publikoval explicitný *vzorec (rekurzívnu formulu) pre n-té prvočíslo*! Jeho riešenie teraz uvedieme.
- Primoriálne číslo $P_k = p_1 \cdot p_2 \cdot \dots \cdot p_k$ má 2^k deliteľov (keďže množina $\{p_1, p_2, \dots, p_k\}$ má 2^k podmnožín).
- Pre každý deliteľ $d|P_k$ položíme $\mu(d) = 1$, ak d je súčin párneho počtu prvočísel a $\mu(d) = -1$, ak d je súčin nepárneho počtu prvočísel.
- μ sa volá *Möbiusova funkcia*.

Gandhiho algoritmus

Gandhiho algoritmus

- Uvažujme cez všetky delitele $d | P_k$ sumu

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1}.$$

Gandhiho algoritmus

- Uvažujme cez všetky delitele $d|P_k$ sumu

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1}.$$

- Napríklad, pre $k = 2$ je $P_k = 2 \cdot 3$ a suma je

Gandhiho algoritmus

- Uvažujme cez všetky delitele $d|P_k$ sumu

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1}.$$

- Napríklad, pre $k = 2$ je $P_k = 2 \cdot 3$ a suma je

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2^1 - 1} + \frac{-1}{2^2 - 1} + \frac{-1}{2^3 - 1} + \frac{1}{2^{2 \cdot 3} - 1}$$

$$= \frac{1}{1} - (\frac{1}{3} + \frac{1}{7}) + \frac{1}{63} = 1 - \frac{29}{63}.$$

Gandhiho algoritmus

- Uvažujme cez všetky delitele $d|P_k$ sumu
$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1}.$$

- Napríklad, pre $k = 2$ je $P_k = 2 \cdot 3$ a suma je
$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2^1 - 1} + \frac{-1}{2^2 - 1} + \frac{-1}{2^3 - 1} + \frac{1}{2^{2\cdot 3} - 1}$$
$$= \frac{1}{1} - (\frac{1}{3} + \frac{1}{7}) + \frac{1}{63} = 1 - \frac{29}{63}.$$

Gandhiho algoritmus

- Uvažujme cez všetky delitele $d|P_k$ sumu

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1}.$$

- Napríklad, pre $k = 2$ je $P_k = 2 \cdot 3$ a suma je

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2^1 - 1} + \frac{-1}{2^2 - 1} + \frac{-1}{2^3 - 1} + \frac{1}{2^{2 \cdot 3} - 1}$$

$$= \frac{1}{1} - (\frac{1}{3} + \frac{1}{7}) + \frac{1}{63} = 1 - \frac{29}{63}.$$

Prvočíslo p_{k+1} sa zo sumy vypočíta takto:

Gandhiho algoritmus

- Uvažujme cez všetky delitele $d|P_k$ sumu

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1}.$$

- Napríklad, pre $k = 2$ je $P_k = 2 \cdot 3$ a suma je

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2^1 - 1} + \frac{-1}{2^2 - 1} + \frac{-1}{2^3 - 1} + \frac{1}{2^{2\cdot 3} - 1}$$

$$= \frac{1}{1} - (\frac{1}{3} + \frac{1}{7}) + \frac{1}{63} = 1 - \frac{29}{63}.$$

Prvočíslo p_{k+1} sa zo sumy vypočíta takto:

- (1) Od uvedenej sumy odčítaj $\frac{1}{2}$.

Gandhiho algoritmus

- Uvažujme cez všetky delitele $d|P_k$ sumu

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1}.$$

- Napríklad, pre $k = 2$ je $P_k = 2 \cdot 3$ a suma je

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2^1 - 1} + \frac{-1}{2^2 - 1} + \frac{-1}{2^3 - 1} + \frac{1}{2^{2\cdot 3} - 1}$$

$$= \frac{1}{1} - (\frac{1}{3} + \frac{1}{7}) + \frac{1}{63} = 1 - \frac{29}{63}.$$

Prvočíslo p_{k+1} sa zo sumy vypočíta takto:

- (1) Od uvedenej sumy odčítaj $\frac{1}{2}$.
- (2) Z výsledku urči logaritmus pri základe 2.

Gandhiho algoritmus

- Uvažujme cez všetky delitele $d|P_k$ sumu

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1}.$$

- Napríklad, pre $k = 2$ je $P_k = 2 \cdot 3$ a suma je

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2^1 - 1} + \frac{-1}{2^2 - 1} + \frac{-1}{2^3 - 1} + \frac{1}{2^{2\cdot 3} - 1}$$

$$= \frac{1}{1} - (\frac{1}{3} + \frac{1}{7}) + \frac{1}{63} = 1 - \frac{29}{63}.$$

Prvočíslo p_{k+1} sa zo sumy vypočíta takto:

- (1) Od uvedenej sumy odčítaj $\frac{1}{2}$.
- (2) Z výsledku urči logaritmus pri základe 2.
- (3) Odčítaj získaný výsledok od čísla 1.

Gandhiho algoritmus

- Uvažujme cez všetky delitele $d|P_k$ sumu

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1}.$$

- Napríklad, pre $k = 2$ je $P_k = 2 \cdot 3$ a suma je

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2^1 - 1} + \frac{-1}{2^2 - 1} + \frac{-1}{2^3 - 1} + \frac{1}{2^{2\cdot 3} - 1}$$

$$= \frac{1}{1} - (\frac{1}{3} + \frac{1}{7}) + \frac{1}{63} = 1 - \frac{29}{63}.$$

Prvočíslo p_{k+1} sa zo sumy vypočíta takto:

- (1) Od uvedenej sumy odčítaj $\frac{1}{2}$.
- (2) Z výsledku urči logaritmus pri základe 2.
- (3) Odčítaj získaný výsledok od čísla 1.
- (4) Z výsledku urči celú časť.

Gandhiho vzorec

Gandhiho vzorec

- Vzorec pre $(k+1)$-vé prvočíslo je

Gandhiho vzorec

- Vzorec pre $(k+1)$-vé prvočíslo je

$$p_{k+1} = \lfloor 1 - \log_2\left(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}\right)\rfloor.$$

Gandhiho vzorec

- Vzorec pre $(k+1)$-vé prvočíslo je

$$p_{k+1} = \lfloor 1 - \log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}) \rfloor.$$

- *Overme Gandhiho vzorec pre $k = 2$:*

Gandhiho vzorec

- Vzorec pre $(k+1)$-vé prvočíslo je

$$p_{k+1} = \lfloor 1 - \log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}) \rfloor.$$

- *Overme Gandhiho vzorec pre $k = 2$:*

$$\sum_{d|P_2} \frac{\mu(d)}{2^d - 1} = 1 - \frac{29}{63}.$$

Gandhiho vzorec

- Vzorec pre $(k+1)$-vé prvočíslo je

$$p_{k+1} = \lfloor 1 - \log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}) \rfloor.$$

- *Overme Gandhiho vzorec pre $k = 2$:*

$$\sum_{d|P_2} \frac{\mu(d)}{2^d - 1} = 1 - \frac{29}{63}.$$

$$-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2} - \frac{29}{63} \simeq 0.04.$$

Gandhiho vzorec

- Vzorec pre $(k+1)$-vé prvočíslo je

$$p_{k+1} = \lfloor 1 - \log_2\left(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}\right) \rfloor.$$

- *Overme Gandhiho vzorec pre $k = 2$:*

$$\sum_{d|P_2} \frac{\mu(d)}{2^d - 1} = 1 - \frac{29}{63}.$$

$$-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2} - \frac{29}{63} \simeq 0.04.$$

$$\log_2\left(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}\right) \simeq \log_2(0.04) \simeq -4.6.$$

Gandhiho vzorec

- Vzorec pre $(k+1)$-vé prvočíslo je

$$p_{k+1} = \lfloor 1 - \log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1})\rfloor.$$

- *Overme Gandhiho vzorec pre $k = 2$:*

$$\sum_{d|P_2} \frac{\mu(d)}{2^d - 1} = 1 - \frac{29}{63}.$$

$$-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2} - \frac{29}{63} \simeq 0.04.$$

$$\log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}) \simeq \log_2(0.04) \simeq -4.6.$$

$$p_3 = \lfloor 1 - (-4.6)\rfloor = \lfloor 5.6\rfloor = 5.$$

Gandhiho vzorec-prečo funguje

Gandhiho vzorec-prečo funguje

Pomocou nekonečného rozvoja

Gandhiho vzorec-prečo funguje

Pomocou nekonečného rozvoja

$$\frac{1}{2^d - 1} = \frac{1}{2^d} + \frac{1}{2^{2d}} + \frac{1}{2^{3d}} + \dots.$$

Gandhiho vzorec-prečo funguje

Pomocou nekonečného rozvoja

$$\frac{1}{2^d - 1} = \frac{1}{2^d} + \frac{1}{2^{2d}} + \frac{1}{2^{3d}} + \dots .$$

upravíme sumu

$$\sum_{d|P_k} \frac{\mu(d)}{2^d - 1} = \frac{1}{2^1 - 1} - \left(\frac{1}{2^{p_1} - 1} + \dots + \frac{1}{2^{p_k} - 1}\right) + \dots$$

na tvar $\left(\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \dots\right) - \left(\frac{1}{2^{p_1}} + \frac{1}{2^{2p_1}} + \frac{1}{2^{3p_1}} + \dots\right) -$

$$\left(\frac{1}{2^{p_2}} + \frac{1}{2^{2p_2}} + \frac{1}{2^{3p_2}} + \dots\right) - \dots - \left(\frac{1}{2^{p_k}} + \frac{1}{2^{2p_k}} + \frac{1}{2^{3p_k}} + \dots\right) + \dots$$

Gandhiho vzorec-prečo funguje

Pomocou nekonečného rozvoja

$$\frac{1}{2^d-1}=\frac{1}{2^d}+\frac{1}{2^{2d}}+\frac{1}{2^{3d}}+\dots.$$

upravíme sumu

$$\sum_{d|P_k}\frac{\mu(d)}{2^d-1}=\frac{1}{2^1-1}-\left(\frac{1}{2^{p_1}-1}+\dots+\frac{1}{2^{p_k}-1}\right)+\dots$$

na tvar $\left(\frac{1}{2}+\frac{1}{2^2}+\frac{1}{2^3}+\dots\right)-\left(\frac{1}{2^{p_1}}+\frac{1}{2^{2p_1}}+\frac{1}{2^{3p_1}}+\dots\right)-$

$$\left(\frac{1}{2^{p_2}}+\frac{1}{2^{2p_2}}+\frac{1}{2^{3p_2}}+\dots\right)-\dots-\left(\frac{1}{2^{p_k}}+\frac{1}{2^{2p_k}}+\frac{1}{2^{3p_k}}+\dots\right)+$$

Od sumy $\sum\frac{1}{2^n}$ sa odčítajú postupne všetky tie $\frac{1}{2^n}$, kde n je deliteľné prvočíslami $p_1, p_2, \dots, p_k$.

Gandhiho vzorec-dôkaz

Gandhiho vzorec-dôkaz

Keď teda od sumy $\sum \frac{1}{2^n}$ odoberieme prvý člen $\frac{1}{2}$, *Eratostenovo sito* nám hovorí, že prvý zostávajúci člen sumy $\sum \frac{1}{2^n}$ bude

Gandhiho vzorec-dôkaz

Keď teda od sumy $\sum \frac{1}{2^n}$ odoberieme prvý člen $\frac{1}{2}$, *Eratostenovo sito* nám hovorí, že prvý zostávajúci člen sumy $\sum \frac{1}{2^n}$ bude

$$\frac{1}{2^{p_{k+1}}} = 2^{-p_{k+1}} \ .$$

Gandhiho vzorec-dôkaz

Keď teda od sumy $\sum \frac{1}{2^n}$ odoberieme prvý člen $\frac{1}{2}$, *Eratostenovo sito* nám hovorí, že prvý zostávajúci člen sumy $\sum \frac{1}{2^n}$ bude

$$\frac{1}{2^{p_{k+1}}} = 2^{-p_{k+1}} \; .$$

Teda

$$log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1})$$

Gandhiho vzorec-dôkaz

Keď teda od sumy $\sum \frac{1}{2^n}$ odoberieme prvý člen $\frac{1}{2}$, *Eratostenovo sito* nám hovorí, že prvý zostávajúci člen sumy $\sum \frac{1}{2^n}$ bude

$$\frac{1}{2^{p_{k+1}}} = 2^{-p_{k+1}} \; .$$

Teda

$$log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1})$$

je o trochu väčšie ako $-p_{k+1}$.

Gandhiho vzorec-dôkaz

Keď teda od sumy $\sum \frac{1}{2^n}$ odoberieme prvý člen $\frac{1}{2}$, *Eratostenovo sito* nám hovorí, že prvý zostávajúci člen sumy $\sum \frac{1}{2^n}$ bude

$$\frac{1}{2^{p_{k+1}}} = 2^{-p_{k+1}} .$$

Teda

$$log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1})$$

je o trochu väčšie ako $-p_{k+1}$. Preto

$$1 - log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1})$$

je trochu menšie ako $1 + p_{k+1}$,

Gandhiho vzorec-dôkaz

Keď teda od sumy $\sum \frac{1}{2^n}$ odoberieme prvý člen $\frac{1}{2}$, *Eratostenovo sito* nám hovorí, že prvý zostávajúci člen sumy $\sum \frac{1}{2^n}$ bude

$$\frac{1}{2^{p_{k+1}}} = 2^{-p_{k+1}} \ .$$

Teda

$$log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1})$$

je o trochu väčšie ako $-p_{k+1}$. Preto

$$1 - log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1})$$

je trochu menšie ako $1 + p_{k+1}$, čiže

$$\lfloor 1 - log_2(-\frac{1}{2} + \sum_{d|P_k} \frac{\mu(d)}{2^d - 1}) \rfloor = p_{k+1}.$$

Pseudoprvočísla

Pseudoprvočísla

- Gandhiho algoritmus je nepoužiteľný pre praktické výpočty, pretože počet sčítancov v danej sume, ktoré odpovedajú deliteľom $d|P_k$ rastie s k exponenciálne a už pre $p_{25} = 97$ je tento počet viac ako 30 miliónov.

Pseudoprvočísla

- Gandhiho algoritmus je nepoužiteľný pre praktické výpočty, pretože počet sčítancov v danej sume, ktoré odpovedajú deliteľom $d|P_k$ rastie s k exponenciálne a už pre $p_{25} = 97$ je tento počet viac ako 30 miliónov. Sú *rýchlejšie spôsoby nájdenia prvočísel*:

Pseudoprvočísla

- Gandhiho algoritmus je nepoužiteľný pre praktické výpočty, pretože počet sčítancov v danej sume, ktoré odpovedajú deliteľom $d|P_k$ rastie s k exponenciálne a už pre $p_{25} = 97$ je tento počet viac ako 30 miliónov. Sú *rýchlejšie spôsoby nájdenia prvočísel*:
- (1) Nájdu sa čísla, ktoré sú s veľkou pravdepodobnosťou prvočísla.

Pseudoprvočísla

- Gandhiho algoritmus je nepoužiteľný pre praktické výpočty, pretože počet sčítancov v danej sume, ktoré odpovedajú deliteľom $d|P_k$ rastie s k exponenciálne a už pre $p_{25} = 97$ je tento počet viac ako 30 miliónov. Sú *rýchlejšie spôsoby nájdenia prvočísel*:
- (1) Nájdu sa čísla, ktoré sú s veľkou pravdepodobnosťou prvočísla.
- (2) Overí sa, že tieto čísla sú skutočne prvočísla.

Pseudoprvočísla

- Gandhiho algoritmus je nepoužiteľný pre praktické výpočty, pretože počet sčítancov v danej sume, ktoré odpovedajú deliteľom $d|P_k$ rastie s k exponenciálne a už pre $p_{25} = 97$ je tento počet viac ako 30 miliónov. Sú *rýchlejšie spôsoby nájdenia prvočísel*:
- (1) Nájdu sa čísla, ktoré sú s veľkou pravdepodobnosťou prvočísla.
- (2) Overí sa, že tieto čísla sú skutočne prvočísla.
- Na úlohu (1) sa používa *test* $n|2^n - 2$.

Pseudoprvočísla

- Gandhiho algoritmus je nepoužiteľný pre praktické výpočty, pretože počet sčítancov v danej sume, ktoré odpovedajú deliteľom $d|P_k$ rastie s k exponenciálne a už pre $p_{25} = 97$ je tento počet viac ako 30 miliónov. Sú *rýchlejšie spôsoby nájdenia prvočísel*:
- (1) Nájdu sa čísla, ktoré sú s veľkou pravdepodobnosťou prvočísla.
- (2) Overí sa, že tieto čísla sú skutočne prvočísla.
- Na úlohu (1) sa používa *test* $n|2^n - 2$. Spĺňajú ho všetky prvočísla (podľa Malej Fermatovej vety) a len málo neprvočísel (napr. $n = 341 = 11 \times 31$): tieto sa volajú *pseudoprvočísla.*

Pseudoprvočísla

- Gandhiho algoritmus je nepoužiteľný pre praktické výpočty, pretože počet sčítancov v danej sume, ktoré odpovedajú deliteľom $d|P_k$ rastie s k exponenciálne a už pre $p_{25} = 97$ je tento počet viac ako 30 miliónov. Sú *rýchlejšie spôsoby nájdenia prvočísel*:
- (1) Nájdu sa čísla, ktoré sú s veľkou pravdepodobnosťou prvočísla.
- (2) Overí sa, že tieto čísla sú skutočne prvočísla.
- Na úlohu (1) sa používa *test* $n|2^n - 2$. Spĺňajú ho všetky prvočísla (podľa Malej Fermatovej vety) a len málo neprvočísel (napr. $n = 341 = 11 \times 31$): tieto sa volajú *pseudoprvočísla.* Ak číslo n prejde testom $n|2^n - 2$, je s veľkou pravdepodobnosťou teda prvočíslo.

AKS algoritmus

AKS algoritmus

- K úlohe (2), overeniu, či dané číslo je naozaj prvočíslo, existuje mnoho metód a obrovský záujem o vývoj rýchlejších algoritmov.

AKS algoritmus

- K úlohe (2), overeniu, či dané číslo je naozaj prvočíslo, existuje mnoho metód a obrovský záujem o vývoj rýchlejších algoritmov.
- Otvorenou otázkou zostávalo, či existuje *polynomiálny algoritmus pre testovanie prvočíselnosti*:

AKS algoritmus

- K úlohe (2), overeniu, či dané číslo je naozaj prvočíslo, existuje mnoho metód a obrovský záujem o vývoj rýchlejších algoritmov.
- Otvorenou otázkou zostávalo, či existuje *polynomiálny algoritmus pre testovanie prvočíselnosti*: ktorého trvanie je polynomiálna funkcia počtu číslic daného čísla.

AKS algoritmus

- K úlohe (2), overeniu, či dané číslo je naozaj prvočíslo, existuje mnoho metód a obrovský záujem o vývoj rýchlejších algoritmov.
- Otvorenou otázkou zostávalo, či existuje *polynomiálny algoritmus pre testovanie prvočíselnosti*: ktorého trvanie je polynomiálna funkcia počtu číslic daného čísla.
- V roku 2002 *Agrawal-Kayal-Saxena* z Indian Institute of Technology šokovali svet nájdením takého algoritmu.

AKS algoritmus

- K úlohe (2), overeniu, či dané číslo je naozaj prvočíslo, existuje mnoho metód a obrovský záujem o vývoj rýchlejších algoritmov.
- Otvorenou otázkou zostávalo, či existuje *polynomiálny algoritmus pre testovanie prvočíselnosti*: ktorého trvanie je polynomiálna funkcia počtu číslic daného čísla.
- V roku 2002 *Agrawal-Kayal-Saxena* z Indian Institute of Technology šokovali svet nájdením takého algoritmu. AKS algoritmus prekvapuje relatívnou jednoduchosťou a jeho štartujúci bod je zovšeobecnenie M. Fermatovej vety:

AKS algoritmus

- K úlohe (2), overeniu, či dané číslo je naozaj prvočíslo, existuje mnoho metód a obrovský záujem o vývoj rýchlejších algoritmov.
- Otvorenou otázkou zostávalo, či existuje *polynomiálny algoritmus pre testovanie prvočíselnosti*: ktorého trvanie je polynomiálna funkcia počtu číslic daného čísla.
- V roku 2002 *Agrawal-Kayal-Saxena* z Indian Institute of Technology šokovali svet nájdením takého algoritmu. AKS algoritmus prekvapuje relatívnou jednoduchosťou a jeho štartujúci bod je zovšeobecnenie M. Fermatovej vety:
- ak $1 < a < p$, tak p je prvočíslo práve vtedy, keď koeficienty polynómu $(x-a)^p - (x^p - a)$ sú všetky deliteľné p.

Fermatove čísla

Fermatove čísla

- $F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots.$

Fermatove čísla

- $F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots.$
- $F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,$ $F_4 = 65537$, F_5 Fermat nespočítal.

Fermatove čísla

- $F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots.$
- $F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,$
  $F_4 = 65537$, F_5 Fermat nespočítal.

Fermatove čísla

- $F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots.$
- $F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,$
  $F_4 = 65537,$ F_5 Fermat nespočítal.
- *Fermat (1640)*: F_n sú všetky prvočísla.

Fermatove čísla

- $F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots.$
- $F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,$
  $F_4 = 65537$, F_5 Fermat nespočítal.
- *Fermat (1640)*: F_n sú všetky prvočísla.
- *Euler (1732)*: $F_5 = 641 \times 6700417$.

Fermatove čísla

- $F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots.$
- $F_0 = 3,\; F_1 = 5,\; F_2 = 17,\; F_3 = 257,$
  $F_4 = 65537$, F_5 Fermat nespočítal.
- *Fermat (1640)*: F_n sú všetky prvočísla.
- *Euler (1732)*: $F_5 = 641 \times 6700417$.
- Všetky ďalšie známe F_n sú zložené!

Fermatove čísla

- $F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots.$
- $F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,$
  $F_4 = 65537$, F_5 Fermat nespočítal.
- *Fermat (1640)*: F_n sú všetky prvočísla.
- *Euler (1732)*: $F_5 = 641 \times 6700417$.
- Všetky ďalšie známe F_n sú zložené!
- U F_{11} sa pozná úplná faktorizácia,

Fermatove čísla

- $F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots.$
- $F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,$ $F_4 = 65537$, F_5 Fermat nespočítal.
- *Fermat (1640)*: F_n sú všetky prvočísla.
- *Euler (1732)*: $F_5 = 641 \times 6700417$.
- Všetky ďalšie známe F_n sú zložené!
- U F_{11} sa pozná úplná faktorizácia, o F_{33} sa nevie, či je zložené.

Fermatove čísla

- $F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots$.
- $F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,$ $F_4 = 65537$, F_5 Fermat nespočítal.
- *Fermat (1640)*: F_n sú všetky prvočísla.
- *Euler (1732)*: $F_5 = 641 \times 6700417$.
- Všetky ďalšie známe F_n sú zložené!
- U F_{11} sa pozná úplná faktorizácia, o F_{33} sa nevie, či je zložené. Ale F_{303088} je zložené s faktorom
$$3 \times 2^{303093} + 1.$$

Fermatove čísla

- $F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots.$
- $F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,$ $F_4 = 65537$, F_5 Fermat nespočítal.
- *Fermat (1640)*: F_n sú všetky prvočísla.
- *Euler (1732)*: $F_5 = 641 \times 6700417.$
- Všetky ďalšie známe F_n sú zložené!
- U F_{11} sa pozná úplná faktorizácia, o F_{33} sa nevie, či je zložené. Ale F_{303088} je zložené s faktorom
$$3 \times 2^{303093} + 1.$$
- *Eisensteinova hypotéza (1844)*: Fermatových prvočísel je nekonečne veľa.

Nekonečne mnoho prvočísel

Nekonečne mnoho prvočísel

Ďalšie dôkazy nekonečného počtu prvočísel:

Nekonečne mnoho prvočísel

Ďalšie dôkazy nekonečného počtu prvočísel:

- *Euler*: $\sum \frac{1}{p} = \infty$.

Nekonečne mnoho prvočísel

Ďalšie dôkazy nekonečného počtu prvočísel:

- *Euler*: $\sum \frac{1}{p} = \infty$.

Nekonečne mnoho prvočísel

Ďalšie dôkazy nekonečného počtu prvočísel:

- *Euler*: $\sum \frac{1}{p} = \infty$.
- *Goldbach*: stačí nájsť nekonečne veľa po dvoch nesúdeliteľných čísel:

Nekonečne mnoho prvočísel

Ďalšie dôkazy nekonečného počtu prvočísel:

- *Euler*: $\sum \frac{1}{p} = \infty$.
- *Goldbach*: stačí nájsť nekonečne veľa po dvoch nesúdeliteľných čísel: takými sú *Fermatove čísla*

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots.$$

Nekonečne mnoho prvočísel

Ďalšie dôkazy nekonečného počtu prvočísel:

- *Euler*: $\sum \frac{1}{p} = \infty$.
- *Goldbach*: stačí nájsť nekonečne veľa po dvoch nesúdeliteľných čísel: takými sú *Fermatove čísla*

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \dots .$$

- 2 ich nedelí; predpokladajme, že $p > 2$ delí F_n, potom

Nekonečne mnoho prvočísel

Ďalšie dôkazy nekonečného počtu prvočísel:

- *Euler*: $\sum \frac{1}{p} = \infty$.
- *Goldbach*: stačí nájsť nekonečne veľa po dvoch nesúdeliteľných čísel: takými sú *Fermatove čísla*

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots.$$

- 2 ich nedelí; predpokladajme, že $p > 2$ delí F_n, potom

$$2^{2^n} \equiv -1 \pmod{p},$$

Nekonečne mnoho prvočísel

Ďalšie dôkazy nekonečného počtu prvočísel:

- *Euler*: $\sum \frac{1}{p} = \infty$.
- *Goldbach*: stačí nájsť nekonečne veľa po dvoch nesúdeliteľných čísel: takými sú *Fermatove čísla*

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \ldots .$$

- 2 ich nedelí; predpokladajme, že $p > 2$ delí F_n, potom

$$2^{2^n} \equiv -1 \pmod{p},$$

$$F_{n+k} = (2^{2^n})^{2^k} + 1 \equiv 2 \pmod{p},$$

Nekonečne mnoho prvočísel

Ďalšie dôkazy nekonečného počtu prvočísel:

- *Euler*: $\sum \frac{1}{p} = \infty$.
- *Goldbach*: stačí nájsť nekonečne veľa po dvoch nesúdeliteľných čísel: takými sú *Fermatove čísla*

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2, 3, \dots .$$

- 2 ich nedelí; predpokladajme, že $p > 2$ delí F_n, potom

$$2^{2^n} \equiv -1 \pmod{p},$$

$$F_{n+k} = (2^{2^n})^{2^k} + 1 \equiv 2 \pmod{p},$$

teda p nedelí F_{n+k}.

Pojem superprvočísla

Pojem superprvočísla

S P. Maličkým sme skúmali nasledujúci pojem:

Pojem superprvočísla

S P. Maličkým sme skúmali nasledujúci pojem:

- *Superprvočíslom* je prvočíslo, ktorého všetky cifry (v dekadickom zápise) sú prvočísla.

Pojem superprvočísla

S P. Maličkým sme skúmali nasledujúci pojem:

- *Superprvočíslom* je prvočíslo, ktorého všetky cifry (v dekadickom zápise) sú prvočísla.

Pojem superprvočísla

S P. Maličkým sme skúmali nasledujúci pojem:

- *Superprvočíslom* je prvočíslo, ktorého všetky cifry (v dekadickom zápise) sú prvočísla.
- *Superprvočísla do tisíc* sú: 2, 3, 5, 7, 23, 37, 53, 73, 223, 227, 233, 257, 277, 337, 353, 373, 523, 557, 577, 727, 733, 757, 773.

Pojem superprvočísla

S P. Maličkým sme skúmali nasledujúci pojem:

- *Superprvočíslom* je prvočíslo, ktorého všetky cifry (v dekadickom zápise) sú prvočísla.
- *Superprvočísla do tisíc* sú: 2, 3, 5, 7, 23, 37, 53, 73, 223, 227, 233, 257, 277, 337, 353, 373, 523, 557, 577, 727, 733, 757, 773.

Nech *P_k je počet k-ciferných superprvočísel*:

k	P_k	**k**	P_k	**k**	P_k
1	4	**6**	389	**11**	214432
2	4	**7**	1325	**12**	781471
3	15	**8**	4643	**13**	2884201
4	38	**9**	16623	**14**	10687480
5	128	**10**	59241	**15**	39838489

Nekonečne mnoho superprvočísel?

Nekonečne mnoho superprvočísel?

Vyslovujeme hypotézy:

Nekonečne mnoho superprvočísel?

Vyslovujeme hypotézy:

Hypotéza 1: **Superprvočísel je nekonečne veľa.**

Nekonečne mnoho superprvočísel?

Vyslovujeme hypotézy:

Hypotéza 1: **Superprvočísel je nekonečne veľa.**

Hypotéza 2: **Pre každé $k > 0$ existuje k-ciferné superprvočíslo.**

Nekonečne mnoho superprvočísel?

Vyslovujeme hypotézy:
Hypotéza 1: **Superprvočísel je nekonečne veľa.**

Hypotéza 2: **Pre každé $k > 0$ existuje k-ciferné superprvočíslo.**
Zosilnené superprvočísla budú tie, kde naviac každá dvojica po sebe idúcich cifier dáva prvočíslo. Prvých 7 aspoň trojciferných je:

Nekonečne mnoho superprvočísel?

Vyslovujeme hypotézy:

Hypotéza 1: **Superprvočísel je nekonečne veľa.**

Hypotéza 2: **Pre každé $k > 0$ existuje k-ciferné superprvočíslo.**

Zosilnené superprvočísla budú tie, kde naviac každá dvojica po sebe idúcich cifier dáva prvočíslo. Prvých 7 aspoň trojciferných je: 373, 237373, 537373, 5373737, 53737373, 53737373737, 237373737373.

Nekonečne mnoho superprvočísel?

Vyslovujeme hypotézy:
Hypotéza 1: **Superprvočísel je nekonečne veľa.**

Hypotéza 2: **Pre každé $k > 0$ existuje k-ciferné superprvočíslo.**
Zosilnené superprvočísla budú tie, kde naviac každá dvojica po sebe idúcich cifier dáva prvočíslo. Prvých 7 aspoň trojciferných je: 373, 237373, 537373, 5373737, 53737373, 53737373737, 237373737373.
Vychádzajú tri typy zosilnených superprvočísel:

1. 23 a n kópií 73, prvé je 237373 ($n = 2$);
2. 53 a n kópií 73, prvé je 537373 ($n = 2$);
3. 5 a n kópií 37, prvé je 5373737 ($n = 3$).

Nekonečne mnoho superprvočísel?

Vyslovujeme hypotézy:
Hypotéza 1: **Superprvočísel je nekonečne veľa.**

Hypotéza 2: **Pre každé $k > 0$ existuje k-ciferné superprvočíslo.**
Zosilnené superprvočísla budú tie, kde naviac každá dvojica po sebe idúcich cifier dáva prvočíslo. Prvých 7 aspoň trojciferných je:
373, 237373, 537373, 5373737, 53737373, 53737373737, 237373737373.
Vychádzajú tri typy zosilnených superprvočísel:

1. 23 a n kópií 73, prvé je 237373 ($n = 2$);
2. 53 a n kópií 73, prvé je 537373 ($n = 2$);
3. 5 a n kópií 37, prvé je 5373737 ($n = 3$).

Hypotéza 3: **Pre každý z typov (1),(2), (3) existuje nekonečne veľa zosilnených superprvočísel.**

Zovšeobecnená Dirichletova postupnosť (GDS)

Zovšeobecnená Dirichletova postupnosť (GDS)

- **Dirichletova veta**: *Ak a, b sú nesúdeliteľné, tak existuje nekonečne veľa prvočísel v rámci aritmetickej postupnosti*

$$a, a+b, a+2b, a+3b, \ldots .$$

Zovšeobecnená Dirichletova postupnosť (GDS)

- **Dirichletova veta**: *Ak a, b sú nesúdeliteľné, tak existuje nekonečne veľa prvočísel v rámci aritmetickej postupnosti*
$$a, a+b, a+2b, a+3b, \ldots.$$
- *Zovšeobecnenou Dirichletovou postupnosťou (GDS)* sme nazvali postupnosť $(x_n)_{n=0}^{\infty}$ definovanú rekurzívnym vzťahom

$$x_{n+1} = ax_n + b$$

kde a, b a x_0 sú celé čísla a $D(b, ax_0) = 1$.

Zovšeobecnená Dirichletova postupnosť (GDS)

- **Dirichletova veta**: *Ak a, b sú nesúdeliteľné, tak existuje nekonečne veľa prvočísel v rámci aritmetickej postupnosti*
$$a, a+b, a+2b, a+3b, \ldots.$$
- *Zovšeobecnenou Dirichletovou postupnosťou (GDS)* sme nazvali postupnosť $(x_n)_{n=0}^{\infty}$ definovanú rekurzívnym vzťahom
$$x_{n+1} = ax_n + b$$
kde a, b a x_0 sú celé čísla a $D(b, ax_0) = 1$.
- Pre $\mathbf{a} = \mathbf{1}$ z nej dostaneme **Dirichletovu postupnosť** vyššie. Predpokladáme, že $a \notin \{-1, 0, 1\}$ and $b \neq -(a-1)x_0$.
- *Naším cieľom bolo nájsť podmienky, aby GDS obsahovala iba konečne veľa prvočísel.*

Príklad a prvá podmienka pre GDS

Príklad a prvá podmienka pre GDS

- Položme v GDS $x_0 = 3$, $a = 5$ a $b = 1$. Potom

Príklad a prvá podmienka pre GDS

- Položme v GDS $x_0 = 3$, $a = 5$ a $b = 1$. Potom $(x_n)_{n=0}^{\infty} = 3, 16, 81, 406, 2031, 10156, 50781, \ldots$ a **všetky členy** x_{2n} **sú násobky** 3.

Príklad a prvá podmienka pre GDS

- Položme v GDS $x_0 = 3$, $a = 5$ a $b = 1$. Potom $(x_n)_{n=0}^{\infty} = 3, 16, 81, 406, 2031, 10156, 50781, \ldots$ a **všetky členy** x_{2n} **sú násobky** 3. Máme $x_1 = 16$ a **všetky členy** x_{2n+1} **sú násobky** 2.

Príklad a prvá podmienka pre GDS

- Položme v GDS $x_0 = 3$, $a = 5$ a $b = 1$. Potom

  $(x_n)_{n=0}^{\infty} = \ 3, 16, 81, 406, 2031, 10156, 50781, ...$

  a **všetky členy** x_{2n} **sú násobky** 3. Máme $x_1 = 16$ a **všetky členy** x_{2n+1} **sú násobky** 2.
- GDS $(x_n)_{n=0}^{\infty}$ môže mať teda rozklad na k podpostupností s vlastnými deliteľmi:

  $$x_{kn} \quad = a^k x_{k(n-1)} + (a^{k-1} + \cdots + a + 1)b,$$
  $$x_{kn+1} = a^k x_{k(n-1)+1} + (a^{k-1} + \cdots + a + 1)b,$$
  $$\ldots\ldots$$

Príklad a prvá podmienka pre GDS

- Položme v GDS $x_0 = 3$, $a = 5$ a $b = 1$. Potom
  $(x_n)_{n=0}^{\infty} = 3, 16, 81, 406, 2031, 10156, 50781, \ldots$
  a **všetky členy** x_{2n} **sú násobky** 3. Máme
  $x_1 = 16$ a **všetky členy** x_{2n+1} **sú násobky** 2.
- GDS $(x_n)_{n=0}^{\infty}$ môže mať teda rozklad na k podpostupností s vlastnými deliteľmi:
  $$x_{kn} = a^k x_{k(n-1)} + (a^{k-1} + \cdots + a + 1)b,$$
  $$x_{kn+1} = a^k x_{k(n-1)+1} + (a^{k-1} + \cdots + a + 1)b,$$
  $\ldots\ldots$
- Ak nejaké $d_j > 1$ delí $\mathbf{A_k} := a^{k-1} + \cdots + a + 1$ a delí prvý člen x_j, tak d_j delí členy $(x_{kn+j})_{n=0}^{\infty}$.

Príklad a prvá podmienka pre GDS

- Položme v GDS $x_0 = 3$, $a = 5$ a $b = 1$. Potom $(x_n)_{n=0}^{\infty} = 3, 16, 81, 406, 2031, 10156, 50781, \ldots$ a **všetky členy** x_{2n} **sú násobky** 3. Máme $x_1 = 16$ a **všetky členy** x_{2n+1} **sú násobky** 2.
- GDS $(x_n)_{n=0}^{\infty}$ môže mať teda rozklad na k podpostupností s vlastnými deliteľmi:
$$x_{kn} = a^k x_{k(n-1)} + (a^{k-1} + \cdots + a + 1)b,$$
$$x_{kn+1} = a^k x_{k(n-1)+1} + (a^{k-1} + \cdots + a + 1)b,$$
$$\ldots\ldots$$
- Ak nejaké $d_j > 1$ delí $\mathbf{A_k} := a^{k-1} + \cdots + a + 1$ a delí prvý člen x_j, tak d_j delí členy $(x_{kn+j})_{n=0}^{\infty}$. V príklade $k = 2$, $A_2 = 6$, t.j. $D(A_2, x_0) = 3$, $D(A_2, x_1) = 2$. Máme prvú podmienku:

Príklad a prvá podmienka pre GDS

- Položme v GDS $x_0 = 3$, $a = 5$ a $b = 1$. Potom
  $$(x_n)_{n=0}^{\infty} = 3, 16, 81, 406, 2031, 10156, 50781, \ldots$$
  a **všetky členy** x_{2n} **sú násobky** 3. Máme $x_1 = 16$ a **všetky členy** x_{2n+1} **sú násobky** 2.
- GDS $(x_n)_{n=0}^{\infty}$ môže mať teda rozklad na k podpostupností s vlastnými deliteľmi:
  $$\begin{aligned} x_{kn} &= a^k x_{k(n-1)} + (a^{k-1} + \cdots + a + 1)b, \\ x_{kn+1} &= a^k x_{k(n-1)+1} + (a^{k-1} + \cdots + a + 1)b, \\ &\ldots\ldots \end{aligned}$$
- Ak nejaké $d_j > 1$ delí $\mathbf{A_k} := a^{k-1} + \cdots + a + 1$ a delí prvý člen x_j, tak d_j delí členy $(x_{kn+j})_{n=0}^{\infty}$. V príklade $k = 2$, $A_2 = 6$, t.j. $D(A_2, x_0) = 3$, $D(A_2, x_1) = 2$. Máme prvú podmienku:
- *(P1) GDS má konečne veľa prvočísel, ak*
  $$(\exists k \geq 2)(\forall j \in \{0, \ldots, k-1\})(\exists d_j > 1) d_j | D(A_k, x_j).$$

Ďalšie podmienky pre GDS

Ďalšie podmienky pre GDS

- *GDS má konečne veľa prvočísel, ak*

$(P2)$ $a = c^4,\ b = 4d^4(1-c^4),\ x_0 = \left(\alpha^4 + 4d^4\right)$

$(P3)$ $a = c^4,\ b = d^4(1-c^4),\ x_0 = \left(4\alpha^4 + d^4\right),$

kde $c \geq 2,\ d \geq 1, \alpha \geq 1$ sú celé čísla.

Ďalšie podmienky pre GDS

- *GDS má konečne veľa prvočísel, ak*

$(P2)$ $a = c^4,\ b = 4d^4(1-c^4),\ x_0 = \left(\alpha^4 + 4d^4\right)$

$(P3)$ $a = c^4,\ b = d^4(1-c^4),\ x_0 = \left(4\alpha^4 + d^4\right),$

kde $c \geq 2,\ d \geq 1, \alpha \geq 1$ sú celé čísla.

Dôvodom je *identita Sophie Germain*

$$x^4 + 4y^4 = (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2)$$
$$= \left((x+y)^2 + y^2\right)\left((x-y)^2 + y^2\right),$$ s ktorou máme v

Ďalšie podmienky pre GDS

- *GDS má konečne veľa prvočísel, ak*

(P2) $a = c^4,\ b = 4d^4(1 - c^4),\ x_0 = \left(\alpha^4 + 4d^4\right)$

(P3) $a = c^4,\ b = d^4(1 - c^4),\ x_0 = \left(4\alpha^4 + d^4\right)$,

kde $c \geq 2$, $d \geq 1, \alpha \geq 1$ sú celé čísla.

Dôvodom je *identita Sophie Germain*

$$x^4 + 4y^4 = (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2)$$
$$= \left((x+y)^2 + y^2\right)\left((x-y)^2 + y^2\right),$$ s ktorou máme v

(P2) $x_n = \alpha^4 c^{4n} + 4d^4 = \left((\alpha c^n + d)^2 + d^2\right)\left((\alpha c^n - d)^2 + d^2\right)$;

(P3) $x_n = 4\alpha^4 c^{4n} + d^4 = \left((d + \alpha c^n)^2 + c^{2n}\right)\left((d - \alpha c^n)^2 + \alpha^2 c^{2n}\right)$

Ďalšie podmienky pre GDS

- *GDS má konečne veľa prvočísel, ak*

$$(P2)\quad a = c^4,\ b = 4d^4(1-c^4),\ x_0 = \left(\alpha^4 + 4d^4\right),$$

$$(P3)\quad a = c^4,\ b = d^4(1-c^4),\ x_0 = \left(4\alpha^4 + d^4\right),$$

kde $c \geq 2$, $d \geq 1, \alpha \geq 1$ sú celé čísla.

Dôvodom je *identita Sophie Germain*

$$x^4 + 4y^4 = (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2)$$
$$= \left((x+y)^2 + y^2\right)\left((x-y)^2 + y^2\right),$$ s ktorou máme v

$$(P2)\ x_n = \alpha^4 c^{4n} + 4d^4 = \left((\alpha c^n + d)^2 + d^2\right)\left((\alpha c^n - d)^2 + d^2\right);$$

$$(P3)\ x_n = 4\alpha^4 c^{4n} + d^4 = \left((d + \alpha c^n)^2 + c^{2n}\right)\left((d - \alpha c^n)^2 + \alpha^2 c^{2n}\right)$$

Faktory v zátvorkách sú väčšie ako 1 okrem prípadu $d = 1, \alpha = 1$ a $n = 0$.

Zovšeobecnená Dirichletova veta

Zovšeobecnená Dirichletova veta

S *identitou Sophie Germain* súvisí aj podmienka

Zovšeobecnená Dirichletova veta

S *identitou Sophie Germain* súvisí aj podmienka

- *GDS má konečne veľa prvočísel, ak*

  $$(P4)\quad a = c^m,\ b = d^m(c^m - 1),\ x_0 = \left(\alpha^m - d^m\right),$$

  kde $d \neq 0, c \notin \{-1, 0, 1\}, \alpha \neq 0$ sú celé čísla.

Zovšeobecnená Dirichletova veta

S *identitou Sophie Germain* súvisí aj podmienka

- *GDS má konečne veľa prvočísel, ak*

  $$(P4)\quad a = c^m,\ b = d^m(c^m - 1),\ x_0 = \left(\alpha^m - d^m\right),$$

  kde $d \neq 0, c \notin \{-1, 0, 1\}, \alpha \neq 0$ sú celé čísla.
- Ďalšie dve podmienky *(P5)*, *(P6)* sa týkajú *(zovšeobecnených) Mersennových čísel* $\frac{a^n - 1}{a - 1}$, kde $a \notin \{-1, 0, 1\}$, ktoré sú prvočísla iba ak n samotné je prvočíslo (a aj to nastáva iba pre konečne veľa n).

Zovšeobecnená Dirichletova veta

S *identitou Sophie Germain* súvisí aj podmienka

- *GDS má konečne veľa prvočísel, ak*

  $(P4)\ \ a = c^m,\ b = d^m(c^m - 1),\ x_0 = (\alpha^m - d^m),$

  kde $d \neq 0, c \notin \{-1, 0, 1\}, \alpha \neq 0$ sú celé čísla.
- Ďalšie dve podmienky *(P5)*, *(P6)* sa týkajú *(zovšeobecnených) Mersennových čísel* $\frac{a^n - 1}{a - 1}$, kde $a \notin \{-1, 0, 1\}$, ktoré sú prvočísla iba ak n samotné je prvočíslo (a aj to nastáva iba pre konečne veľa n).

Hypotéza (Zovšeobecnená Dirichletova veta): **Nech a, b a x_0 sú celé čísla a $D(b, ax_0) = 1$.** *Nech GDS $(x_n)_{n=0}^{\infty}$ daná vzťahom*

$$x_{n+1} = ax_n + b$$

nespĺňa žiadnu z podmienok (P1)-(P6). **Potom GDS obsahuje nekonečne veľa prvočísel.**

Mersennove a Fermatove prvočísla

Mersennove a Fermatove prvočísla

- Pre $x_0 = 0, a = 2, b = 1$ je v GDS $x_n = 2^n - 1$, čo je prvočíslo, iba ak n je prvočíslo, kedy x_n je tzv. *Mersennovo prvočíslo*.

Mersennove a Fermatove prvočísla

- Pre $x_0 = 0, a = 2, b = 1$ je v GDS $x_n = 2^n - 1$, čo je prvočíslo, iba ak n je prvočíslo, kedy x_n je tzv. *Mersennovo prvočíslo*.
- Vidieť, že podmienka *(P1)* neplatí, lebo $A_k = 2^k - 1$ a $x_1 = 1$ nemajú sp. deliteľa $d > 1$. Tiež podmienky *(P2)–(P6)* neplatia.

Mersennove a Fermatove prvočísla

- Pre $x_0 = 0, a = 2, b = 1$ je v GDS $x_n = 2^n - 1$, čo je prvočíslo, iba ak n je prvočíslo, kedy x_n je tzv. *Mersennovo prvočíslo*.
- Vidieť, že podmienka *(P1)* neplatí, lebo $A_k = 2^k - 1$ a $x_1 = 1$ nemajú sp. deliteľa $d > 1$. Tiež podmienky *(P2)–(P6)* neplatia.
- Z našej Zovšeobecnenej Dirichletovej vety (ako hypotézy) vyplýva známa hypotéza, že *Mersennových prvočísel je nekonečne veľa*.

Mersennove a Fermatove prvočísla

- Pre $x_0 = 0, a = 2, b = 1$ je v GDS $x_n = 2^n - 1$, čo je prvočíslo, iba ak n je prvočíslo, kedy x_n je tzv. *Mersennovo prvočíslo*.
- Vidieť, že podmienka *(P1)* neplatí, lebo $A_k = 2^k - 1$ a $x_1 = 1$ nemajú sp. deliteľa $d > 1$. Tiež podmienky *(P2)–(P6)* neplatia.
- Z našej Zovšeobecnenej Dirichletovej vety (ako hypotézy) vyplýva známa hypotéza, že *Mersennových prvočísel je nekonečne veľa*.
- Pre $x_0 = 2, a = 2, b = -1$ je v GDS $x_n = 2^n + 1$, čo je prvočíslo, iba ak $n = 2^k$, kedy x_n je *Fermatovo prvočíslo*.

Mersennove a Fermatove prvočísla

- Pre $x_0 = 0, a = 2, b = 1$ je v GDS $x_n = 2^n - 1$, čo je prvočíslo, iba ak n je prvočíslo, kedy x_n je tzv. *Mersennovo prvočíslo*.
- Vidieť, že podmienka *(P1)* neplatí, lebo $A_k = 2^k - 1$ a $x_1 = 1$ nemajú sp. deliteľa $d > 1$. Tiež podmienky *(P2)–(P6)* neplatia.
- Z našej Zovšeobecnenej Dirichletovej vety (ako hypotézy) vyplýva známa hypotéza, že *Mersennových prvočísel je nekonečne veľa*.
- Pre $x_0 = 2, a = 2, b = -1$ je v GDS $x_n = 2^n + 1$, čo je prvočíslo, iba ak $n = 2^k$, kedy x_n je *Fermatovo prvočíslo*. Teraz $A_k = 2^k - 1$, $x_0 = 2$ a *(P1)–(P6)* neplatia.

Mersennove a Fermatove prvočísla

- Pre $x_0 = 0, a = 2, b = 1$ je v GDS $x_n = 2^n - 1$, čo je prvočíslo, iba ak n je prvočíslo, kedy x_n je tzv. *Mersennovo prvočíslo*.
- Vidieť, že podmienka *(P1)* neplatí, lebo $A_k = 2^k - 1$ a $x_1 = 1$ nemajú sp. deliteľa $d > 1$. Tiež podmienky *(P2)–(P6)* neplatia.
- Z našej Zovšeobecnenej Dirichletovej vety (ako hypotézy) vyplýva známa hypotéza, že *Mersennových prvočísel je nekonečne veľa*.
- Pre $x_0 = 2, a = 2, b = -1$ je v GDS $x_n = 2^n + 1$, čo je prvočíslo, iba ak $n = 2^k$, kedy x_n je *Fermatovo prvočíslo*. Teraz $A_k = 2^k - 1$, $x_0 = 2$ a *(P1)–(P6)* neplatia.
- Z našej Zovšeobecnenej Dirichletovej vety (ako hypotézy) vyplýva teda hypotéza, že *Fermatových prvočísel je nekonečne veľa*.

Literatúra po roku 2000

[1] Folkmar Borneman, PRIMES is in P: a breakthrough for “Everyman”, Notices of AMS 50 (2003), 545-552.

[2] J. Brian Conrey, The Riemann hypothesis, Notices of AMS 50 (2003), 341-353.

[3] John Derbyshire, Prime Obsession, Joseph Henry Press, Washington, DC, 2003.

[4] Apostolos Doxiadis, Uncle Petros and Goldbach’s conjecture, Bloomsbury, New York, 2000.

[5] Paolo Ribenboim, My numbers, my friends, Springer, New York, 2000.

[6] Marcus du Sautoy, The Music of the Primes, Harper Collins, 2003.

[7] Karl Sabbagh, The Riemann Hypothesis: the greatest unsolved problems in mathematics, Farrar, Strauss and Giroux, 2003.

Webovské zdroje

[1] Historické kapitoly k prvočíslam:
http://www-groups.dcs.st-and.ac.uk/
history/HistTopics/Prime numbers.html
[2] Výskum k prvočíslam:
http://www.utm.edu/research/primes
[3] Výpočtové aspekty prvočíselných problémov:
http://www.olemiss.edu/mathed/pow/powold.
[4] Prvočíselné úlohy pre školákov:
http://www.bwctc.northants.sch.uk/html/
master/maths/autumn99/primech.htm
[5] Prvočíselné hypotézy:
http://www.primepuzzles.net/conjectures/index.html
[6] Hľadanie veľkých prvočísel:
http://primes.utm.edu/primes/background/finding.php
[7] Relácia o prvočíslach na BBC radio:
http://www.bbc.co.uk/radio4/science/another53.shtml