Diskrétní matematika – 2. týden
Elementární teorie čísel – kongruence a prvočísla

Lukáš Vokřínek

Masarykova univerzita
Fakulta informatiky

jaro 2020

Obsah přednášky

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant
  Matematika drsně a svižně, *e*-text na
  `www.math.muni.cz/Matematika_drsne_svizne`.

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant **Matematika drsně a svižně**, *e*-text na `www.math.muni.cz/Matematika_drsne_svizne`.
- Michal Bulant, výukový text k přednášce **Elementární teorie čísel**, `http://is.muni.cz/el/1431/podzim2012/M6520/um/main-print.pdf`
- Jiří Herman, Radan Kučera, Jaromír Šimša, **Metody řešení matematických úloh**. MU Brno, 2001.
- William Stein, **Elementary Number Theory: Primes, Congruences, and Secrets**, Springer, 2008. Dostupné na `http://wstein.org/ent/ent.pdf`
- Radan Kučera, výukový text k přednášce **Algoritmy teorie čísel**, `http://www.math.muni.cz/~kucera/texty/ATC10.pdf`

Plán přednášky

Pojem kongruence byl zaveden Gaussem. Ačkoliv je to pojem velice jednoduchý, jeho důležitost a užitečnost v teorii čísel je nedocenitelná; projevuje se zejména ve stručných a přehledných zápisech některých i velmi komplikovaných úvah.

Pojem kongruence byl zaveden Gaussem. Ačkoliv je to pojem velice jednoduchý, jeho důležitost a užitečnost v teorii čísel je nedocenitelná; projevuje se zejména ve stručných a přehledných zápisech některých i velmi komplikovaných úvah.

Definice

Jestliže dvě celá čísla a, b mají při dělení přirozeným číslem m týž zbytek r, kde $0 \leq r < m$, nazývají se a, b *kongruentní modulo* m (též *kongruentní podle modulu* m), což zapisujeme takto:

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

V opačném případě řekneme, že a, b nejsou kongruentní modulo m, a píšeme

$$a \not\equiv b \pmod{m}.$$

Lemma

Pro libovolná $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ *jsou následující podmínky ekvivalentní:*

1. $a \equiv b \pmod{m}$,
2. $a = b + mt$ *pro vhodné* $t \in \mathbb{Z}$,
3. $m \mid a - b$.

Základní vlastnosti kongruencí

Přímo z definice plyne, že kongruence podle modulu m je reflexivní (tj. $a \equiv a \pmod{m}$ platí pro každé $a \in \mathbb{Z}$), symetrická (tj. pro každé $a, b \in \mathbb{Z}$ z $a \equiv b \pmod{m}$ plyne $b \equiv a \pmod{m}$) a tranzitivní (tj. pro každé $a, b, c \in \mathbb{Z}$ z $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$ plyne $a \equiv c \pmod{m}$) relace, jde tedy o *ekvivalenci*.

Základní vlastnosti kongruencí

Přímo z definice plyne, že kongruence podle modulu m je reflexivní (tj. $a \equiv a \pmod{m}$ platí pro každé $a \in \mathbb{Z}$), symetrická (tj. pro každé $a, b \in \mathbb{Z}$ z $a \equiv b \pmod{m}$ plyne $b \equiv a \pmod{m}$) a tranzitivní (tj. pro každé $a, b, c \in \mathbb{Z}$ z $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$ plyne $a \equiv c \pmod{m}$) relace, jde tedy o *ekvivalenci*. Dokážeme nyní další vlastnosti:

- **Kongruence** podle téhož modulu **můžeme sčítat**. Libovolný sčítanec můžeme přenést s opačným znaménkem z jedné strany kongruence na druhou. **K libovolné straně** kongruence **můžeme přičíst** jakýkoliv **násobek modulu.**

- **Kongruence** podle téhož modulu **můžeme násobit**. Obě strany kongruence je možné **umocnit na totéž přirozené číslo**. Obě strany kongruence je možné **vynásobit stejným celým číslem**.

- **Kongruence** podle téhož modulu **můžeme násobit**. Obě strany kongruence je možné **umocnit na totéž přirozené číslo**. Obě strany kongruence je možné **vynásobit stejným celým číslem**.
- **Obě strany** kongruence **můžeme vydělit jejich společným dělitelem**, jestliže je tento dělitel **nesoudělný s modulem.**

- **Kongruence** podle téhož modulu **můžeme násobit**. Obě strany kongruence je možné **umocnit na totéž přirozené číslo**. Obě strany kongruence je možné **vynásobit stejným celým číslem**.
- **Obě strany** kongruence **můžeme vydělit jejich společným dělitelem**, jestliže je tento dělitel **nesoudělný s modulem.**
- Obě strany kongruence i její modul můžeme současně vynásobit tímtéž přirozeným číslem.

- **Kongruence** podle téhož modulu **můžeme násobit**. Obě strany kongruence je možné **umocnit na totéž přirozené číslo**. Obě strany kongruence je možné **vynásobit stejným celým číslem**.
- **Obě strany** kongruence **můžeme vydělit jejich společným dělitelem**, jestliže je tento dělitel **nesoudělný s modulem.**
- Obě strany kongruence i její modul můžeme současně vynásobit tímtéž přirozeným číslem.
- Obě strany kongruence i její modul můžeme vydělit jejich společným kladným dělitelem.

- **Kongruence** podle téhož modulu **můžeme násobit**. Obě strany kongruence je možné **umocnit na totéž přirozené číslo**. Obě strany kongruence je možné **vynásobit stejným celým číslem**.
- **Obě strany** kongruence **můžeme vydělit jejich společným dělitelem**, jestliže je tento dělitel **nesoudělný s modulem.**
- Obě strany kongruence i její modul můžeme současně vynásobit tímtéž přirozeným číslem.
- Obě strany kongruence i její modul můžeme vydělit jejich společným kladným dělitelem.
- **Jestliže kongruence** $a \equiv b$ **platí podle modulů** $m_1, \ldots, m_k$, **platí i podle modulu, kterým je nejmenší společný násobek** $[\mathbf{m_1}, \ldots, \mathbf{m_k}]$ **těchto čísel.**

- **Kongruence** podle téhož modulu **můžeme násobit**. Obě strany kongruence je možné **umocnit na totéž přirozené číslo**. Obě strany kongruence je možné **vynásobit stejným celým číslem**.
- **Obě strany** kongruence **můžeme vydělit jejich společným dělitelem**, jestliže je tento dělitel **nesoudělný s modulem.**
- Obě strany kongruence i její modul můžeme současně vynásobit tímtéž přirozeným číslem.
- Obě strany kongruence i její modul můžeme vydělit jejich společným kladným dělitelem.
- **Jestliže kongruence** $a \equiv b$ **platí podle modulů** $m_1, \ldots, m_k$, **platí i podle modulu, kterým je nejmenší společný násobek** $[\mathbf{m_1}, \ldots, \mathbf{m_k}]$ **těchto čísel.**
- Jestliže kongruence platí podle modulu m, platí podle libovolného modulu d, který je dělitelem čísla m.

- **Kongruence** podle téhož modulu **můžeme násobit**. Obě strany kongruence je možné **umocnit na totéž přirozené číslo**. Obě strany kongruence je možné **vynásobit stejným celým číslem**.
- **Obě strany** kongruence **můžeme vydělit jejich společným dělitelem**, jestliže je tento dělitel **nesoudělný s modulem.**
- Obě strany kongruence i její modul můžeme současně vynásobit tímtéž přirozeným číslem.
- Obě strany kongruence i její modul můžeme vydělit jejich společným kladným dělitelem.
- **Jestliže kongruence** $a \equiv b$ **platí podle modulů** $m_1, \ldots, m_k$, **platí i podle modulu, kterým je nejmenší společný násobek** $[\mathbf{m_1}, \ldots, \mathbf{m_k}]$ **těchto čísel.**
- Jestliže kongruence platí podle modulu m, platí podle libovolného modulu d, který je dělitelem čísla m.
- Jestliže je jedna strana kongruence a modul dělitelný nějakým celým číslem, musí být tímto číslem dělitelná i druhá strana.

Poznámka

Některé vlastnosti kongruencí jsme již používali, aniž bychom si toho povšimli – například příklad z minulého týdne lze přeformulovat do tvaru "jestliže $a \equiv 1 \pmod{m}$, $b \equiv 1 \pmod{m}$, pak také $ab \equiv 1 \pmod{m}$", což je speciální případ zpředhozího tvrzení.

Nejde o náhodu. Libovolné tvrzení používající kongruence můžeme snadno přepsat pomocí dělitelnosti. Užitečnost kongruencí tedy netkví v tom, že bychom pomocí nich mohli řešit úlohy, které bez nich řešit nejsme schopni, ale v tom, že jde o velmi vhodný způsob zápisu. Osvojíme-li si ho, výrazně tím zjednodušíme jak vyjadřování, tak i některé úvahy. Je to typický jev: v matematice hraje vhodná symbolika velmi závažnou úlohu.

Příklad

Nalezněte zbytek po dělení čísla 5^{20} číslem 26.

Příklad

Nalezněte zbytek po dělení čísla 5^{20} číslem 26.

Příklad

Dokažte, že pro libovolné prvočíslo p a libovolná $a, b \in \mathbb{Z}$ platí

$$a^p + b^p \equiv (a+b)^p \pmod{p}.$$

Příklad

Nalezněte zbytek po dělení čísla 5^{20} číslem 26.

Příklad

Dokažte, že pro libovolné prvočíslo p a libovolná $a, b \in \mathbb{Z}$ platí

$$a^p + b^p \equiv (a+b)^p \pmod{p}.$$

Příklad

Najděte "inverzi" k číslu 39 modulo 47, tj. najděte x takové, že $39 \cdot x \equiv 1 \pmod{47}$.

Plán přednášky

PRIMES is in P

Poznámka

Již jsme se zmínili, že je složité o velkých číslech s jistotou rozhodnout, jde-li o prvočíslo (na druhou stranu je o naprosté většině složených čísel snadné prokázat, že jsou skutečně složená). Přesto se v roce 2002 podařilo indickým matematikům (Agrawal, Saxena, Kayal: `http://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf`) dokázat, že problém prvočíselnosti je možné rozhodnout algoritmem s časovou složitostí polynomiálně závislou na počtu cifer vstupního čísla. Nic podobného se zatím nepodařilo v otázce rozkladu čísla na prvočísla (třebaže se obecně nevěří, že je to možné, exaktní důkaz zatím nebyl podán).

Is FACTOR in P?

Nic podobného se zatím nepodařilo v otázce rozkladu čísla na prvočísla (třebaže se obecně nevěří, že je to možné, exaktní důkaz zatím nebyl podán). Nejrychlejší obecně použitelný faktorizační algoritmus, tzv. *síto v číselném tělese*[1], je sub-exponenciální časové složitosti $O(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}})$.

[1] Pro podrobnosti navštivte M8190 Algoritmy teorie čísel

Is FACTOR in P?

Nic podobného se zatím nepodařilo v otázce rozkladu čísla na prvočísla (třebaže se obecně nevěří, že je to možné, exaktní důkaz zatím nebyl podán). Nejrychlejší obecně použitelný faktorizační algoritmus, tzv. *síto v číselném tělese*[1], je sub-exponenciální časové složitosti $O(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}})$.

Poznámka

Peter Shor v roce 1994 vymyslel algoritmus, který faktorizuje v kubickém čase (tj. $O((\log N)^3)$) na kvantovém počítači. Je k tomu nicméně třeba sestrojit počítače s dostatečným počtem qubits – jak je to obtížné, lze vysledovat z toho, ze v roce 2001 se IBM podařilo pomocí kvantového počítače rozložit číslo 15 a v roce 2012 byl dosažen další faktorizační rekord rozkladem čísla 21.

[1] Pro podrobnosti navštivte M8190 Algoritmy teorie čísel

RSA Challenge

Poznámka

Ⓡe je problém rozkladu přirozeného čísla na prvočísla výpočetně složitý, o tom svědčí i (již neplatná) výzva učiněná v roce 1991 firmou RSA Security (viz `http://www.rsasecurity.com/rsalabs/node.asp?id=2093`). Pokud se komukoliv podařilo rozložit čísla označená podle počtu cifer jako RSA-100, . . . , RSA-704, RSA-768, . . . , RSA-2048, mohl obdržet 1 000,. . . , 30 000, 50 000, . . . , resp. 200 000 dolarů (číslo RSA-100 rozložil v témže roce Arjen Lenstra, číslo RSA-704 bylo rozloženo v roce 2012, některá dosud rozložena nebyla).

Díky jednoznačnosti rozkladu na prvočísla jsme schopni (se znalostí tohoto rozkladu) snadno odpovědět i na otázky ohledně počtu či součtu dělitelů konkrétního čísla. Stejně snadno dostaneme i (z dřívějška intuitivně známý) postup na výpočet největšího společného dělitele dvou čísel ze znalosti jejich rozkladu na prvočísla.

Důsledek

- *Každý kladný dělitel čísla* $a = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$ *je tvaru* $p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}$, *kde* $m_1, \ldots, m_k \in \mathbb{N}_0$ *a* $m_1 \leq n_1$, $m_2 \leq n_2$, $\ldots$, $m_k \leq n_k$.

Díky jednoznačnosti rozkladu na prvočísla jsme schopni (se znalostí tohoto rozkladu) snadno odpovědět i na otázky ohledně počtu či součtu dělitelů konkrétního čísla. Stejně snadno dostaneme i (z dřívějška intuitivně známý) postup na výpočet největšího společného dělitele dvou čísel ze znalosti jejich rozkladu na prvočísla.

Důsledek

- *Každý kladný dělitel čísla* $a = p_1^{n_1} \cdot \dots \cdot p_k^{n_k}$ *je tvaru* $p_1^{m_1} \cdot \dots \cdot p_k^{m_k}$, *kde* $m_1, \dots, m_k \in \mathbb{N}_0$ *a* $m_1 \leq n_1$, $m_2 \leq n_2$, $\dots$, $m_k \leq n_k$.
- *Číslo* a *má tedy právě* $\tau(a) = (n_1 + 1)(n_2 + 1) \cdot \dots \cdot (n_k + 1)$ *kladných dělitelů, jejichž součet je*

$$\sigma(a) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \dots \frac{p_k^{n_k+1} - 1}{p_k - 1}.$$

Důsledek (Pokr.)

- *Jsou-li* $p_1, \ldots, p_k$ *navzájem různá prvočísla a* $n_1, \ldots, n_k, m_1, \ldots, m_k \in \mathbb{N}_0$ *a označíme-li* $r_i = \min\{n_i, m_i\}$, $t_i = \max\{n_i, m_i\}$ *pro každé* $i = 1, 2, \ldots, k$, *platí*

$$(p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}, p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}) = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k},$$

$$[p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}, p_1^{m_1} \cdot \ldots \cdot p_k^{m_k}] = p_1^{t_1} \cdot \ldots \cdot p_k^{t_k}.$$

Mersenneho prvočísla a dokonalá čísla

S pojmem *součet všech kladných dělitelů čísla a* souvisí pojem tzv. *dokonalého čísla a*, které splňuje podmínku $\sigma(a) = 2a$, resp. slovně: *součet všech kladných dělitelů čísla a menších než a samotné je roven číslu a*.
Takovými čísly jsou např. $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$, 496 a 8128 (jde o všechna dokonalá čísla menší než 10 000).

Mersenneho prvočísla a dokonalá čísla

S pojmem *součet všech kladných dělitelů čísla a* souvisí pojem tzv. *dokonalého čísla a*, které splňuje podmínku $\sigma(a) = 2a$, resp. slovně: *součet všech kladných dělitelů čísla a menších než a samotné je roven číslu a*.
Takovými čísly jsou např. $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$, 496 a 8128 (jde o všechna dokonalá čísla menší než 10 000).

Poznámka

Lze ukázat, že sudá dokonalá čísla jsou v úzkém vztahu s tzv. *Mersenneho prvočísly*. Platí totiž: *a je sudé dokonalé číslo, právě když je tvaru* $a = 2^{q-1} \cdot (2^q - 1)$, *kde* $2^q - 1$ *je prvočíslo.*

Mersenneho prvočísla jsou právě prvočísla tvaru $2^k - 1$. Bez zajímavosti není ani to, že právě Mersenneho prvočísla jsou mezi všemi prvočísly nejlépe „vidět“ – pro Mersenneho čísla existuje poměrně jednoduchý a rychlý postup, jak ověřit, že jde o prvočísla.

Hledání velkých prvočísel

Proto není náhodou, že největší známá prvočísla jsou obvykle tvaru $2^k - 1$ (viz např. `http://www.utm.edu/research/primes/largest.html`). Jakkoliv může být hledání největšího známého prvočísla chápáno jako pochybná zábava bez valného praktického užitku[2], jednak posunuje hranice matematického poznání a zdokonaluje použité metody (a často i hardware), jednak může přinést benefit i samotným objevitelům (Electronic Frontier Foundation vypsala odměny EFF Cooperative Computing Awards za nalezení prvočísla majícího alespoň $10^6, 10^7, 10^8$ a 10^9 číslic – odměny 50, resp. 100 tisíc $ za první dvě kategorie byly vyplaceny v letech 2000, resp. 2009 – v obou případech projektu GIMPS – na další odměny si ještě zřejmě nějaký čas počkáme).

[2] Viz např. titulek iDnes z 6.února 2013: *Největší známé prvočíslo na světě*

Hledání velkých prvočísel

Proto není náhodou, že největší známá prvočísla jsou obvykle tvaru $2^k - 1$ (viz např. `http://www.utm.edu/research/primes/largest.html`).
Jakkoliv může být hledání největšího známého prvočísla chápáno jako pochybná zábava bez valného praktického užitku[2], jednak posunuje hranice matematického poznání a zdokonaluje použité metody (a často i hardware), jednak může přinést benefit i samotným objevitelům (Electronic Frontier Foundation vypsala odměny EFF Cooperative Computing Awards za nalezení prvočísla majícího alespoň $10^6, 10^7, 10^8$ a 10^9 číslic – odměny 50, resp. 100 tisíc $ za první dvě kategorie byly vyplaceny v letech 2000, resp. 2009 – v obou případech projektu GIMPS – na další odměny si ještě zřejmě nějaký čas počkáme).
Na druhou stranu popsat lichá dokonalá čísla se dodnes nepodařilo, resp. **dodnes se neví, jestli vůbec nějaké liché dokonalé číslo existuje**.

[2] Viz např. titulek iDnes z 6.února 2013: *Největší známé prvočíslo na světě*

Jak testovat Mersenneho prvočísla?

Přestože zatím nemáme jasno v tom, jak efektivně implementovat použité operace, ani neumíme dokázat jeho správnost, uveďme si pro ilustraci test, kterým lze zjistit, je-li dané Mersenneho číslo prvočíslem.

Jak testovat Mersenneho prvočísla?

Přestože zatím nemáme jasno v tom, jak efektivně implementovat použité operace, ani neumíme dokázat jeho správnost, uveďme si pro ilustraci test, kterým lze zjistit, je-li dané Mersenneho číslo prvočíslem.

Lucas-Lehmerův test

Definujme posloupnost $(s_n)_{n=0}^{\infty}$ rekurzívně předpisem $s_0 = 4, s_{n+1} = s_n^2 - 2$.
Pak je číslo $M_p = 2^p - 1$ prvočíslo, právě tehdy, když M_p dělí s_{p-2}.

Rozložení prvočísel

Nyní se budeme snažit zodpovědět následující otázky:

1. Je prvočísel nekonečně mnoho?

Rozložení prvočísel

Nyní se budeme snažit zodpovědět následující otázky:

1. Je prvočísel nekonečně mnoho?
2. Je prvočísel nekonečně mnoho v každé (nebo aspoň některé) aritmetické posloupnosti?

Rozložení prvočísel

Nyní se budeme snažit zodpovědět následující otázky:

1. Je prvočísel nekonečně mnoho?
2. Je prvočísel nekonečně mnoho v každé (nebo aspoň některé) aritmetické posloupnosti?
3. Jak jsou prvočísla rozložena mezi přirozenými čísly?

Rozložení prvočísel

Nyní se budeme snažit zodpovědět následující otázky:

1. Je prvočísel nekonečně mnoho?
2. Je prvočísel nekonečně mnoho v každé (nebo aspoň některé) aritmetické posloupnosti?
3. Jak jsou prvočísla rozložena mezi přirozenými čísly?

Rozložení prvočísel

Nyní se budeme snažit zodpovědět následující otázky:

1. Je prvočísel nekonečně mnoho?
2. Je prvočísel nekonečně mnoho v každé (nebo aspoň některé) aritmetické posloupnosti?
3. Jak jsou prvočísla rozložena mezi přirozenými čísly?

> *There are two facts about the distribution of prime numbers. The first is that, [they are] the most arbitrary and ornery objects studied by mathematicians: they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behavior, and that they obey these laws with almost military precision.*
>
> *Don Zagier*

Prvočísel je nekonečně mnoho

Věta (Eukleidés)

Mezi přirozenými čísly existuje nekonečně mnoho prvočísel.

Prvočísel je nekonečně mnoho

Věta (Eukleidés)

Mezi přirozenými čísly existuje nekonečně mnoho prvočísel.

Důkaz.

Předpokládejme, že prvočísel je konečně mnoho a označme je $p_1, p_2, \ldots, p_n$. Položme $N = p_1 \cdot p_2 \ldots p_n + 1$. Toto číslo je buď samo prvočíslem nebo je dělitelné nějakým prvočíslem různým od $p_1, \ldots, p_n$ (čísla $p_1, \ldots, p_n$ totiž dělí číslo $N - 1$), což je spor. □

Prvočísel je nekonečně mnoho

Věta (Eukleidés)

Mezi přirozenými čísly existuje nekonečně mnoho prvočísel.

Důkaz.

Předpokládejme, že prvočísel je konečně mnoho a označme je $p_1, p_2, \ldots, p_n$. Položme $N = p_1 \cdot p_2 \ldots p_n + 1$. Toto číslo je buď samo prvočíslem nebo je dělitelné nějakým prvočíslem různým od $p_1, \ldots, p_n$ (čísla $p_1, \ldots, p_n$ totiž dělí číslo $N - 1$), což je spor. □

Poznámka

Existuje mnoho variant důkazů nekonečnosti prvočísel z různých oblastí matematiky, uveďme ještě alespoň některá tvrzení, z nichž zároveň získáme alespoň částečnou informaci o rozložení prvočísel mezi přirozenými čísly.

Prvočísel je vcelku hodně

Příklad

Pro celé $n > 2$ existuje mezi čísly n a $n!$ alespoň jedno prvočíslo.

Prvočísel je vcelku hodně

Příklad

Pro celé $n > 2$ existuje mezi čísly n a $n!$ alespoň jedno prvočíslo.

Řešení

Označme p libovolné prvočíslo dělící číslo $n! - 1$ (takové existuje podle Základní věty aritmetiky, protože $n! - 1 > 1$). Kdyby $p \leq n$, muselo by p dělit číslo $n!$ a nedělilo by $n! - 1$. Je tedy $n < p$. Protože $p \mid (n! - 1)$, platí $p \leq n! - 1$, tedy $p < n!$. Prvočíslo p splňuje podmínky úlohy. □

Prvočísel je vcelku hodně

Příklad

Pro celé $n > 2$ existuje mezi čísly n a $n!$ alespoň jedno prvočíslo.

Řešení

Označme p libovolné prvočíslo dělící číslo $n! - 1$ (takové existuje podle Základní věty aritmetiky, protože $n! - 1 > 1$). Kdyby $p \leq n$, muselo by p dělit číslo $n!$ a nedělilo by $n! - 1$. Je tedy $n < p$. Protože $p \mid (n! - 1)$, platí $p \leq n! - 1$, tedy $p < n!$. Prvočíslo p splňuje podmínky úlohy. □

Z této věty rovněž vyplývá nekonečnost prvočísel, její tvrzení je ale velice slabé. Následující tvrzení, uvedené bez důkazu, je podstatně silnější.

Věta (Čebyševova, Bertrandův postulát)

Pro libovolné číslo $n > 1$ existuje alespoň jedno prvočíslo p splňující $n < p < 2n$.

Prvočísel je vcelku málo

Příklad

Dokažte, že pro libovolné přirozené číslo n existuje n po sobě jdoucích přirozených čísel, z nichž žádné není prvočíslo.

Prvočísel je vcelku málo

Příklad

Dokažte, že pro libovolné přirozené číslo n existuje n po sobě jdoucích přirozených čísel, z nichž žádné není prvočíslo.

Řešení

Zkoumejme čísla $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$. Mezi těmito n po sobě jdoucími čísly není žádné prvočíslo, protože pro libovolné $k \in \{2, 3, \ldots, n+1\}$ platí $k \mid (n+1)!$, a tedy $k \mid (n+1)!+k$, a proto $(n+1)!+k$ nemůže být prvočíslo. □

Prvočísla jsou relativně rovnoměrně rozložena v tom, smyslu, že v libovolné „rozumné“ aritmetické posloupnosti je jich nekonečně mnoho. Například zbytek 1 po dělení čtyřmi, stejně jako zbytek 3 po dělení čtyřmi dá vždy nekonečně mnoho prvočísel (zbytek 0 nedá samozřejmě žádné a zbytek 2 pouze jediné). Obdobná situace je pak při uvažování zbytků po dělení libovolným jiným přirozeným číslem, jak uvádí následující věta, jejíž důkaz je ovšem velmi obtížný.

Prvočísla jsou relativně rovnoměrně rozložena v tom, smyslu, že v libovolné „rozumné“ aritmetické posloupnosti je jich nekonečně mnoho. Například zbytek 1 po dělení čtyřmi, stejně jako zbytek 3 po dělení čtyřmi dá vždy nekonečně mnoho prvočísel (zbytek 0 nedá samozřejmě žádné a zbytek 2 pouze jediné). Obdobná situace je pak při uvažování zbytků po dělení libovolným jiným přirozeným číslem, jak uvádí následující věta, jejíž důkaz je ovšem velmi obtížný.

Věta (Dirichletova o prvočíslech v aritmetické posloupnosti)

Jsou-li a, m nesoudělná přirozená čísla, existuje nekonečně mnoho přirozených čísel k tak, že $mk + a$ je prvočíslo. Jinými slovy, mezi čísly $1 \cdot m + a, 2 \cdot m + a, 3 \cdot m + a, \ldots$ existuje nekonečně mnoho prvočísel.

Uveďme proto alespoň důkaz ve speciálním případě.

Prvočísel tvaru $3k + 2$ je nekonečně mnoho

Příklad

Dokažte, že existuje nekonečně mnoho prvočísel tvaru $3k + 2$, kde $k \in \mathbb{N}_0$.

Prvočísel tvaru $3k + 2$ je nekonečně mnoho

Příklad

Dokažte, že existuje nekonečně mnoho prvočísel tvaru $3k + 2$, kde $k \in \mathbb{N}_0$.

Řešení

Předpokládejme naopak, že existuje pouze konečně mnoho prvočísel tohoto tvaru a označme je $p_1 = 2$, $p_2 = 5$, $p_3 = 11$, $\ldots$, p_n. Položme $N = 3p_2 \cdot p_3 \cdot \cdots \cdot p_n + 2$. Rozložíme-li N na součin prvočísel, musí v tomto rozkladu vystupovat aspoň jedno prvočíslo p tvaru $3k + 2$, neboť v opačném případě by bylo N součinem prvočísel tvaru $3k + 1$ (uvažte, že N není dělitelné třemi), a tedy podle dřívějšího příkladu by bylo i N tvaru $3k + 1$, což není pravda. Prvočíslo p ovšem nemůže být žádné z prvočísel $p_1, p_2, \ldots, p_n$, jak plyne z tvaru čísla N, a to je spor.

Asymptotické chování prvočísel

Z tvrzení uvedených v této kapitole je možné si udělat hrubou představu o tom, jak "hustě" se mezi přirozenými čísla prvočísla vyskytují. Přesněji (i když "pouze" asymptoticky) to popisuje velmi důležitá tzv. "Prime Number Theorem":

Věta (Prime Number Theorem, věta o hustotě prvočísel)

Nechť $\pi(x)$ udává počet prvočísel menších nebo rovných číslu $x \in \mathbb{R}$. Pak

$$\pi(x) \sim \frac{x}{\ln x},$$

tj. podíl funkcí $\pi(x)$ a $x/\ln x$ se pro $x \to \infty$ limitně blíží k 1.

Asymptotické chování prvočísel

Z tvrzení uvedených v této kapitole je možné si udělat hrubou představu o tom, jak "hustě" se mezi přirozenými čísla prvočísla vyskytují. Přesněji (i když "pouze" asymptoticky) to popisuje velmi důležitá tzv. "Prime Number Theorem":

Věta (Prime Number Theorem, věta o hustotě prvočísel)

Nechť $\pi(x)$ udává počet prvočísel menších nebo rovných číslu $x \in \mathbb{R}$. Pak

$$\pi(x) \sim \frac{x}{\ln x},$$

tj. podíl funkcí $\pi(x)$ a $x/\ln x$ se pro $x \to \infty$ limitně blíží k 1.

Poznámka

To, jak jsou prvočísla hustě rozmístěna v množině přirozených čísel, rovněž udává Eulerův výsledek $\sum_{p \in P} \frac{1}{p} = \infty$. Přitom např. $\sum_{n \in \mathbb{N}} \frac{1}{n^2} = \frac{\pi^2}{6}$, což znamená, že prvočísla jsou v $\mathbb{N}$ rozmístěna „hustěji“ než druhé mocniny.

Příklad

O tom, jak odpovídá asymptotický odhad $\pi(x) \sim x/\ln(x)$,
v některých konkrétních příkladech vypovídá následující tabulka:

x	$\pi(x)$	$x/\ln(x)$	relativní chyba
100	25	21.71	0.13
1000	168	144.76	0.13
10000	1229	1085.73	0.11
100000	9592	8685.88	0.09
500000	41538	38102.89	0.08