Prvočísla

Michal „Kenny“ Rolínek

Na přednášce si povíme všechno možné o prvočíslech. Dozvíte se, kam sahají naše znalosti o nich a taky, kam už nedosáhnou. Můžete se těšit na hezká prvočísla i na hezké příklady s nimi. Taky si řekneme, k čemu jsou prvočísla dobrá v úlohách.

Rozložení prvočísel

- Prvočísel je nekonečně mnoho.
- Úseky bez prvočísel jsou libovolně dlouhé.
- Prvočísla řidnou logaritmicky (Čebyšev).
- Prvočísel tvaru $4n + 1$ je nekonečně mnoho.
- Prvočísel tvaru $qn + 1$, kde q je prvočíslo je nekonečně mnoho.
- Prvočísel tvaru $an + b$, kde $(a, b) = 1$ je nekonečně mnoho (Dirichlet).
- Mezi n a $2n$ existuje prvočíslo pro $n \geq 2$ (Bertrand).
- (Hypotéza) Existuje nekonečně mnoho prvočísel tvaru $n^2 + 1$ (popřípadě si dosaď svůj oblíbený nerozložitelný polynom).
- (Hypotéza) Mezi n^2 a $(n + 1)^2$ existuje prvočíslo pro $n \geq 2$ (opět si můžeš dosadit různé mocniny).

Příklad 1. Ukažte, že existuje nekonečně mnoho prvočísel obsahující vaše rodné číslo (nepřerušené).

Příklad 2. Ukažte, že existuje nekonečně mnoho prvočísel začínajících vaším rodným číslem (v nejhorším použijte některou z hypotéz).

Počítání s prvočísly

Taky máte pocit, že počítání s přirozenými čísly je otrava? Zkusme si počítat s čísly $\{0, 1, 2 \ldots p - 1\}$ a uvidíme, že i zde vše krásně funguje.

- Sčítání, odčítání a násobení je úplně bez problému.
- Překvapivě se tu i dělení chová slušně.
- $a^p \equiv a \pmod{p}$ (Fermat).
- $(p - 1)! \equiv -1 \pmod{p}$ (Wilson).

Příklad 3. Najděte všechny prvočísla p, pro něž je číslo

$$\binom{p}{0}^2 + \binom{p}{1}^2 + \cdots + \binom{p}{p}^2$$

dělitelné číslem p^3.

Příklad 4. Sečtěte řadu

$$\frac{1}{2} + \frac{2}{3} + \cdots + \frac{p-2}{p-1} \pmod{p}.$$

Příklad 5. Vyřešte kongruenci

$$(1+2)(1+2+3)\ldots(1+2+\cdots+p-1) \equiv 2002 \pmod{p}$$

Otevřené problémy

- Riemannova hypotéza: O ní podrobněji až na přednášce
- Goldbachova hypotéza: Každé sudé číslo větší než 2 lze zapsat jakou součet dvou prvočísel.
- Slabá Goldbachova hypotéza: Každé liché prvočíslo větší než 5 lze zapsat jakou součet tří prvočísel.
- Prvočíselná dvojčata: Existuje nekonečně mnoho prvočíselných dvojčat.
- Existuje nekonečně mnoho Fermatových, Mersennovských, Fibonacciovských prvočísel.

Zajímavosti, novinky

- Existuje polynom (27 proměnných), jehož kladné hodnoty jsou právě všechna prvočísla (1947).
- Prvočísla se dají testovat v polynomiálním čase (2002).
- Prvočísla tvoří aritmetické posloupnosti libovolné délky (2004).
- Číslo $0{,}2357111317\ldots$ je iracionální (Erdos).
- Posloupnost $a_n = \sqrt{24n+1}$ obsahuje všechna prvočísla.
- Přirozená čísla lze přeuspořádat tak, aby součet žádné souvislé konečné podposloupnosti nebyl prvočíselný (na přednášce kdyžtak dovysvětlím).

Následuje několik zajímavých prvočísel (ovšem některá si nechám až na přednášku):

$$42^{42} + \pi(42)$$
$$120^{120} - 119^{119}$$
$$6163, 61603, 616003, 6160003$$
$$7^7 + 11^7 + 13^7$$
$$555555555551111111111$$
$$77777677777$$