Diskrétní matematika B – 2. týden
Elementární teorie čísel – Kongruence

Michal Bulant

Masarykova univerzita
Fakulta informatiky

jaro 2019

Obsah přednášky

1. Literatura

2. Rozložení prvočísel
   - Asymptotické chování prvočísel

3. Kongruence
   - Základní vlastnosti kongruencí
   - Aritmetické funkce
   - Eulerova funkce φ

4. Fermatova a Eulerova věta
   - Malá Fermatova věta, Eulerova věta

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant, *Matematika drsně a svižně*, MU Brno, 2013, 774 s. (též jako e-text).
- *Předmětové záložky v IS MU*
- Michal Bulant, výukový text k přednášce **Elementární teorie čísel**, `http://is.muni.cz/el/1431/podzim2014/M6520/um/main-print.pdf`
- 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/ATC2014.pdf`

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.

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.

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. Bez důkazu uvedeme podstatně silnější tvrzení.

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.

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.

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 $k \in \mathbb{N}_0$.

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.

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.

Věta

Je-li P množina všech prvočísel, pak $\sum_{p\in P} \frac{1}{p} = \infty$.

Důkaz.

Buď n libovolné přirozené číslo a $p_1, \ldots, p_{\pi(n)}$ všechna prvočísla nepřevyšující n. Položme

$$\lambda(n) = \prod_{i=1}^{\pi(n)} \left(1 - \frac{1}{p_i}\right)^{-1}.$$

Jednotlivé činitele lze chápat jako součet geometrické řady, proto

$$\lambda(n) = \prod_{i=1}^{\pi(n)} \left(\sum_{\alpha_i=0}^{\infty} \frac{1}{p_i^{\alpha_i}}\right) = \sum \frac{1}{p_1^{\alpha_1} \cdots p_{\pi(n)}^{\alpha_{\pi(n)}}},$$

kde sčítáme přes všechny $\pi(n)$-tice nezáporných celých čísel $(\alpha_1, \ldots, \alpha_{\pi(n)})$.

Důkaz.

Protože každé číslo nepřevyšující n se rozkládá pouze na prvočísla z množiny $\{p_1, \ldots, p_{\pi(n)}\}$, je určitě každé takové číslo v tomto součtu zahrnuto. Tedy $\lambda(n) > 1 + \frac{1}{2} + \cdots + \frac{1}{n}$, a protože harmonická řada diverguje , je i $\lim_{n\to\infty} \lambda(n) = \infty$.
S využitím rozvoje funkce $\ln(1+x)$ do mocninné řady dále dostáváme

$$\ln \lambda(n) = -\sum_{i=1}^{\pi(n)} \ln\left(1 - \frac{1}{p_i}\right) = \sum_{i=1}^{\pi(n)} \sum_{m=1}^{\infty} (m p_i^m)^{-1} =$$

$$= p_1^{-1} + \cdots + p_{\pi(n)}^{-1} + \sum_{i=1}^{\pi(n)} \sum_{m=2}^{\infty} (m p_i^m)^{-1}.$$

Důkaz.

$$\ln \lambda(n) = p_1^{-1} + \cdots + p_{\pi(n)}^{-1} + \sum_{i=1}^{\pi(n)} \sum_{m=2}^{\infty} (m p_i^m)^{-1}.$$

Protože vnitřní součet lze shora odhadnout jako

$$\sum_{m=2}^{\infty} (m p_i^m)^{-1} < \sum_{m=2}^{\infty} p_i^{-m} = \\ = p_i^{-2} \left(1 - p_i^{-1}\right)^{-1} \leq 2 p_i^{-2},$$

umíme shora odhadnout i divergující posloupnost $\ln \lambda(n) < \sum_{i=1}^{\pi(n)} p_i^{-1} + 2 \sum_{i=1}^{\pi(n)} p_i^{-2}$. Druhý součet přitom zřejmě konverguje (viz konvergence řady $\sum_{n=1}^{\infty} n^{-2}$), proto musí nutně divergovat první součet $\sum_{i=1}^{\pi(n)} p_i^{-1}$, což jsme chtěli dokázat. □

Příklad

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

x	$\pi(x)$	$x/\ln(x)$	rel. chyba	Li(x)	rel. chyba
100	25	21,7	0,13	29,1	0,04
1000	168	144,7	0,13	176,6	0,01
10000	1229	1085,7	0,11	1245,1	0,002
100000	9592	8685,9	0,09	9628,8	0,0004
500000	41538	38102,9	0,08	41605,2	0,0001

$Li(x) = \int_2^x \frac{\mathrm{d}t}{\ln t}$ značí tzv. logaritmický integrál a za předpokladu tzv. Riemannovy hypotézy platí odhad

$$|\pi(x) - Li(x)| = O(\sqrt{x}\ln x).$$

Kongruence

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. $m \mid a - b$.

Důkaz.

"(1)⇒(3)" Jestliže $a = q_1 m + r$, $b = q_2 m + r$, pak $a - b = (q_1 - q_2)m$.
"(3)⇒(2)" Jestliže $m \mid a - b$, pak existuje $t \in \mathbb{Z}$ tak, že $m \cdot t = a - b$, tj. $a = b + mt$.
"(2)⇒(1)" Jestliže $a = b + mt$, pak z vyjádření $b = mq + r$ plyne $a = m(q + t) + r$, tedy a i b mají při dělení číslem m týž zbytek r, tj. $a \equiv b \pmod{m}$. □

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**.
- **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.

Řešení

Protože $5^2 = 25 \equiv -1 \pmod{26}$, platí
$5^{20} \equiv (-1)^{10} = 1 \pmod{26}$, a tedy zbytek po dělení čísla 5^{20} číslem 26 je jedna.

Příklad

Dokažte, že pro libovolné $n \in \mathbb{N}$ je $37^{n+2} + 16^{n+1} + 23^n$ dělitelné sedmi.

Řešení

Platí $37 \equiv 16 \equiv 23 \equiv 2 \pmod{7}$, a tedy podle základních vlastností platí

$$37^{n+2}+16^{n+1}+23^n \equiv 2^{n+2}+2^{n+1}+2^n = 2^n(4+2+1) \equiv 0 \pmod{7}.$$

Příklad

Dokažte, že číslo $n = (835^5 + 6)^{18} - 1$ je dělitelné číslem 112.

Řešení

Rozložíme $112 = 7 \cdot 16$. Protože $(7, 16) = 1$, stačí ukázat, že $7 \mid n$ a $16 \mid n$. Platí $835 \equiv 2 \pmod 7$, a tedy

$$n \equiv (2^5 + 6)^{18} - 1 = 38^{18} - 1 \equiv 3^{18} - 1 = \\ = 27^6 - 1 \equiv (-1)^6 - 1 = 0 \pmod 7,$$

proto $7 \mid n$. Podobně $835 \equiv 3 \pmod{16}$, a tedy

$$n \equiv (3^5 + 6)^{18} - 1 = (3 \cdot 81 + 6)^{18} - 1 \equiv (3 \cdot 1 + 6)^{18} - 1 = \\ = 9^{18} - 1 = 81^9 - 1 \equiv 1^9 - 1 = 0 \pmod{16},$$

proto $16 \mid n$. Celkem tedy $112 \mid n$, což jsme měli dokázat.

Příklad

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

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

Řešení

Podle binomické věty platí

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + \binom{p}{p-1} a b^{p-1} + b^p.$$

Dále, protože $p \mid \binom{p}{k}$ pro libovolné $k \in \{1, \ldots, p-1\}$ (*dokažte*!), platí $\binom{p}{k} \equiv 0 \pmod{p}$, odkud plyne tvrzení.

Aritmetické funkce

Aritmetickou funkcí zde rozumíme funkci, jejímž definičním oborem je množina přirozených čísel.

Definice (Möbiova funkce)

Rozložme přirozené číslo n na prvočísla: $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Hodnotu *Möbiovy funkce* $\mu(n)$ definujeme rovnu 0, pokud pro některé i platí $\alpha_i > 1$ a rovnu $(-1)^k$ v opačném případě. Dále definujeme $\mu(1) = 1$.

Příklad

$\mu(4) = \mu(2^2) = 0, \mu(6) = \mu(2 \cdot 3) = (-1)^2, \mu(2) = \mu(3) = -1.$

Dokážeme nyní několik důležitých vlastností Möbiovy funkce, zejména tzv. *Möbiovu inverzní formuli*.

Lemma

Pro $n \in \mathbb{N} \setminus \{1\}$ *platí* $\sum_{d|n} \mu(d) = 0$.

Důkaz.

Zapíšeme-li n ve tvaru $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, pak všechny dělitele d čísla n jsou tvaru $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$, kde $0 \leq \beta_i \leq \alpha_i$ pro všechna $i \in \{1, \ldots, k\}$. Proto

$$\begin{aligned}
\sum_{d|n} \mu(d) &= \sum_{\substack{(\beta_1,\ldots,\beta_k)\in(\mathbb{N}\cup\{0\})^k \\ 0\leq\beta_i\leq\alpha_i}} \mu(p_1^{\beta_1} \cdots p_k^{\beta_k}) = \\
&= \sum_{(\beta_1,\ldots,\beta_k)\in\{0,1\}^k} \mu(p_1^{\beta_1} \cdots p_k^{\beta_k}) \\
&= \binom{k}{0} + \binom{k}{1} \cdot (-1) + \binom{k}{2} \cdot (-1)^2 + \cdots + \binom{k}{k} \cdot (-1)^k \\
&= \big(1 + (-1)\big)^k = 0.
\end{aligned}$$

S Möbiovou funkcí úzce souvisí pojem *Dirichletův součin* (konvoluce):

Definice

Buďte f, g aritmetické funkce. Jejich *Dirichletův součin* je definován předpisem

$$(f \circ g)(n) = \sum_{d|n} f(d) \cdot g\left(\tfrac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1) \cdot g(d_2).$$

Lemma

Dirichletův součin je asociativní.

Důkaz.

$$((f \circ g) \circ h)(n) = \sum_{d_1 d_2 d_3 = n} f(d_1) \cdot g(d_2) \cdot h(d_3) = (f \circ (g \circ h))(n)$$

□

Příklad

Definujme dvě pomocné funkce $\mathbb{I}$ a I předpisem $\mathbb{I}(1) = 1$, $\mathbb{I}(n) = 0$ pro všechna $n > 1$, resp. $I(n) = 1$ pro všechna $n \in \mathbb{N}$. Pak pro každou aritmetickou funkci f platí:

$$f \circ \mathbb{I} = \mathbb{I} \circ f = f \quad \text{a} \quad (I \circ f)(n) = (f \circ I)(n) = \sum_{d|n} f(d).$$

Dále platí $I \circ \mu = \mu \circ I = \mathbb{I}$, neboť

$$(I \circ \mu)(n) = \sum_{d|n} I(d)\mu(\tfrac{n}{d}) = \sum_{d|n} I(\tfrac{n}{d})\mu(d) =$$
$$= \sum_{d|n} \mu(d) = 0 \quad \text{pro všechna } n > 1$$

podle lemmatu za definicí Möbiovy funkce (pro $n = 1$ je tvrzení zřejmé).

Věta (Möbiova inverzní formule)

Nechť je aritmetická funkce F definovaná pomocí aritmetické funkce f předpisem $F(n) = \sum_{d|n} f(d)$. Pak lze funkci f vyjádřit ve tvaru

$$f(n) = \sum_{d|n} \mu(\tfrac{n}{d}) \cdot F(d).$$

Důkaz.

Vztah $F(n) = \sum_{d|n} f(d)$ lze jiným způsobem zapsat jako $F = f \circ I$. Proto $F \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ \mathbb{I} = f$, což je tvrzení věty. □

Definice

Multiplikativní funkcí přirozených čísel rozumíme takovou aritmetickou funkci, která splňuje, že pro všechny dvojice **nesoudělných** čísel $a, b \in \mathbb{N}$ platí

$$f(a \cdot b) = f(a) \cdot f(b).$$

Příklad

Multiplikativními funkcemi jsou např. funkce $f(n) = \sigma(n)$, $f(n) = \tau(n)$, či $f(n) = \mu(n)$ nebo, jak brzy dokážeme i tzv. Eulerova funkce $f(n) = \varphi(n)$.

Eulerova funkce

Definice

Nechť $n \in \mathbb{N}$. Definujme Eulerovu funkci φ předpisem

$$\varphi(n) = |\{a \in \mathbb{N} \,|\, 0 < a \leq n, (a, n) = 1\}|$$

Příklad

$\varphi(1) = 1, \varphi(5) = 4, \varphi(6) = 2$, je-li p prvočíslo, je zřejmě $\varphi(p) = p - 1$.

Nyní dokážeme několik důležitých tvrzení o funkci φ:

Lemma

Nechť $n \in \mathbb{N}$. Pak $\sum_{d|n} \varphi(d) = n$.

Důkaz.

Uvažme n zlomků

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n}.$$

Zkrátíme-li zlomky na základní tvar a seskupíme podle jmenovatelů, snadno dostaneme právě uvedené tvrzení. □

Věta

Nechť $n \in \mathbb{N}$, jehož rozklad je tvaru $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Pak

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

Důkaz.

S využitím předchozího lemmatu a Möbiovy inverzní formule dostáváme

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n - \frac{n}{p_1} - \cdots - \frac{n}{p_k} + \cdots + (-1)^k \frac{n}{p_1 \cdots p_k} =$$

$$= n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

□

Poznámka

Předchozí výsledek lze obdržet i bez použití Möbiovy inverzní formule pomocí principu inkluze a exkluze na základě zjištění počtu čísel soudělných s n v určitém intervalu.

Důsledek

Nechť $a, b \in \mathbb{N}$, $(a, b) = 1$. *Pak*

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Poznámka

Rovněž toto tvrzení lze odvodit nezávisle na základě poznatku $(n, ab) = 1 \iff (n, a) = 1 \wedge (n, b) = 1$. Spolu se snadno odvoditelným výsledkem

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1) \cdot p^{\alpha-1}$$

pak lze odvodit vztah pro výpočet φ již třetím způsobem.

Příklad

Vypočtěte $\varphi(72)$.

Řešení

$72 = 2^3 \cdot 3^2 \implies \varphi(72) = 72 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 24$, alternativně $\varphi(72) = \varphi(8) \cdot \varphi(9) = 4 \cdot 6 = 24$. □

Příklad

Dokažte, že $\forall n \in \mathbb{N} : \varphi(4n + 2) = \varphi(2n + 1)$.

Řešení

$\varphi(4n + 2) = \varphi(2 \cdot (2n + 1)) = \varphi(2) \cdot \varphi(2n + 1) = \varphi(2n + 1)$. □

Malá Fermatova věta

Tato tvrzení patří mezi nejdůležitější výsledky elementární teorie čísel.

Věta (Fermatova, Malá Fermatova)

Nechť $a \in \mathbb{Z}$, p prvočíslo, $p \nmid a$. Pak

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

Důkaz.

Tvrzení vyplyne jako snadný důsledek Eulerovy věty. Dá se ale dokázat i přímo (např. matematickou indukcí nebo kombinatoricky) □

Důsledek

Nechť $a \in \mathbb{Z}$, p prvočíslo. Pak

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

Příklad (Důkaz Malé Fermatovy věty)

Kombinatorický důkaz jde na věc poněkud „od lesa“: podobně jako v úlohách využívajících Burnsideovo lemma máme za úkol určit počet náhrdelníků dané délky (ty vzniknou navlečením několika šperků na šňůrku a jejím svázáním) vytvořených z několika typů šperků s tím, že nerozlišujeme náhrdelníky, které je možné na sebe převést otočením (a liší se tedy jen tím, kde je zavázaný „uzlík“). Snadno si lze rozmyslet, že navlékáme-li n šperků, lze v některých konstelacích převést náhrdelník sám na sebe při otočení o určitý počet šperků. Předpokládejme nyní, že máme a typů šperků a požadovaný počet použitých šperků na jeden náhrdelník je dán prvočíslem p. Zřejmě pro každý náhrdelník využívající alespoň dvou typů šperků dostáváme různým umístěním uzlíku p různých p-tic šperků na šňůrce (což ale není případ náhrdelníků sestavených pouze z jednoho typu šperku). Vidíme tedy, že počet různých náhrdelníků je roven

$$\frac{a^p - a}{p} + a,$$

což zejména znamená, že musí platit $p \mid a^p - a$.

Příklad

Například pro hodnoty $a = 2, p = 5$ tak určujeme počet náhrdelníků dvou typů šperků (A, B) délky pět. Dáme-li ze všech 2^5 různě navlečených šňůrek stranou 2 náhrdelníky tvořené pouze jedním typem $(AAAAA, BBBBB)$, pak dále máme $\frac{2^5-2}{5} = 6$ náhrdelníků, které na sebe nelze převést otáčením $(ABBBB, AABBB, AAABB, AAAAB, ABABB, AABAB)$.

Úplná a redukovaná soustava zbytků

Definice

Úplná soustava zbytků modulo m je libovolná m-tice čísel po dvou nekongruentních modulo m (nejčastěji $0, 1, \ldots, m-1$).
Redukovaná soustava zbytků modulo m je libovolná $\varphi(m)$-tice čísel nesoudělných s m a po dvou nekongruentních modulo m.

Lemma

Nechť $x_1, x_2, \ldots, x_{\varphi(m)}$ tvoří redukovanou soustavu zbytků modulo m. Je-li $a \in \mathbb{Z}$, $(a, m) = 1$ pak i čísla $a \cdot x_1, \ldots, a \cdot x_{\varphi(m)}$ tvoří redukovanou soustavu zbytků modulo m.

Důkaz.

Protože $(a, m) = 1$ a $(x_i, m) = 1$, platí $(a \cdot x_i, m) = 1$. Kdyby pro nějaká i, j platilo $a \cdot x_i \equiv a \cdot x_j \pmod{m}$, po vydělení obou stran kongruence číslem a nesoudělným s m dostaneme $x_i \equiv x_j \pmod{m}$. □

Eulerova věta

Věta (Eulerova)

Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$, $(a, m) = 1$. *Pak*

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

Důkaz.

Buď $x_1, x_2, \ldots, x_{\varphi(m)}$ libovolná redukovaná soustava zbytků modulo m. Podle předchozího lemmatu je i $a \cdot x_1, \ldots, a \cdot x_{\varphi(m)}$ redukovaná soustava zbytků modulo m. Platí tedy, že pro každé i existuje j ($i, j \in \{1, 2, \ldots, \varphi(m)\}$) tak, že $a \cdot x_i \equiv x_j \pmod{m}$. Vynásobením dostáváme
$(a \cdot x_1) \cdot (a \cdot x_2) \cdots (a \cdot x_{\varphi(m)}) \equiv x_1 \cdot x_2 \cdots x_{\varphi(m)} \pmod{m}$. Po úpravě

$$a^{\varphi(m)} \cdot x_1 \cdot x_2 \cdots x_{\varphi(m)} \equiv x_1 \cdot x_2 \cdots x_{\varphi(m)} \pmod{m}$$

a po vydělení číslem $x_1 \cdot x_2 \cdots x_{\varphi(m)}$ dostaneme požadované. □

Kryptografická motivace

RSA

Ron Rivest, Adi Shamir, Leonard Adleman (1977; C. Cocks,GCHQ – 1973)

- každý účastník A potřebuje dvojici klíčů – veřejný V_A a soukromý S_A
- generování klíčů: zvolí dvě velká prvočísla p, q, vypočte $n = pq$, $\varphi(n) = (p-1)(q-1)$ [n je veřejné, ale $\varphi(n)$ nelze snadno spočítat]
- zvolí **veřejný klíč** e a ověří, že $(e, \varphi(n)) = 1$
- např. pomocí Euklidova algoritmu spočítá **tajný klíč** d tak, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
- zašifrování numerického *kódu* zprávy M: $C = C_e(M) \equiv M^e \pmod{n}$
- dešifrování šifry C: $OT = D_d(C) \equiv C^d \pmod{n}$

Příklad

- **Generování klíče.** Alice vybere prvočísla $p = 2357, q = 2551$ a vypočte $n = p \cdot q = 6012707$ a $\varphi(n) = (p-1)(q-1) = 6007800$. Alice zvolí $e = 3674911$ a pomocí Euklidova algoritmu vypočte $d = 422191$ ($e \cdot d \equiv 1 \pmod{\varphi(n)}$). Soukromý klíč Alice je d, veřejný pak (n, e).
- Chce-li Bob poslat Alici zprávu $m = 5234673$, pomocí modulárního umocňování vypočte

$$c \equiv m^e \equiv 5234673^{3674911} \equiv 3650502 \pmod{n},$$

  a tu odešle Alici.
- Alice zprávu dešifruje díky výpočtu

$$c^d \equiv 3650502^{422191} \equiv 5234673.$$

Velikost klíčů

Jak velké klíče (pro RSA) je vhodné volit? Data, chráněná klíčem s délkou 1024 bitů jsou chráněna před útočníkem, který nemá k dispozici enormní zdroje.
Takový odhad učinili např. Shamir & Tromer (2003) při konstrukci hypotetického zařízení TWIRL. Navrhli hardwarové zařízení v ceně desítek milionů dolarů, které by bylo schopné rozložit 1024-bitový RSA klíč přibližně za rok. Podobně Franke et al (2005) odhadli cenu takového zařízení na cca 200 milionů dolarů. Další odhady ukazují, že pokud chceme bezpečně chránit svá data (řádově) na 10-20 let dopředu, měli bychom vystačit s klíčem délky 2048 bitů.

Zdroj: `http://www.javamex.com/tutorials/cryptography/rsa_key_length.shtml`