Diskrétní matematika – 3. týden
Elementární teorie čísel – prvočísla a kongruence

Jan Slovák

Masarykova univerzita
Fakulta informatiky

jaro 2014

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

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 věty plyne 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. □

Naznačili jsme, jak "hustě" se mezi přirozenými čísla prvočísla vyskytují. Přesněji (i když "pouze" asymptoticky) to popisuje velmi důležitá tzv. "Prime Number Theorem" (uvádíme bez důkazu):

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.

Naznačili jsme, jak "hustě" se mezi přirozenými čísla prvočísla vyskytují. Přesněji (i když "pouze" asymptoticky) to popisuje velmi důležitá tzv. "Prime Number Theorem" (uvádíme bez důkazu):

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 $\sum_{p \in P} \frac{1}{p} = \infty$. (důkaz v textu, relativně složitý).

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 (protože $\sum_n \frac{1}{n^2} = \frac{\pi^2}{6}$).

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

Plán přednášky

Aritmetické funkce

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

Definice

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 $\mu(1) = 1$.

Aritmetické funkce

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

Definice

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* $\sum_{d|n} \mu(d) = 0$.

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

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

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

Definice

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

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

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:

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

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

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

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

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

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

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

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 $\sum_{d|n} \varphi(d) = n$.

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*

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

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.

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 $\varphi(72)$.

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

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

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

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

Plán přednášky

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) □

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

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

Úplná a redukovaná soustava zbytků

Definice

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

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.

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.

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*

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

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

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

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

Řád čísla

S Eulerovou funkcí a Eulerovou větou úzce souvisí důležitý pojem *řád čísla modulo m*:

Řád čísla

S Eulerovou funkcí a Eulerovou větou úzce souvisí důležitý pojem *řád čísla modulo m*:

Definice

Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$ $(a, m) = 1$. *Řádem čísla a modulo m* rozumíme nejmenší přirozené číslo n splňující

$$a^n \equiv 1 \pmod{m}.$$

Poznámka

To, že je řád definován, plyne z Eulerovy věty – pro každé číslo nesoudělné s modulem je totiž jistě jeho řád nejvýše roven $\varphi(m)$. Jak později uvidíme, velmi důležitá jsou právě ta čísla, jejichž **řád je roven právě** $\varphi(m)$ – tato čísla nazýváme primitivními kořeny modulo m a hrají důležitou roli mj. při řešení binomických kongruencí.

Poznámka

To, že je řád definován, plyne z Eulerovy věty – pro každé číslo nesoudělné s modulem je totiž jistě jeho řád nejvýše roven $\varphi(m)$. Jak později uvidíme, velmi důležitá jsou právě ta čísla, jejichž **řád je roven právě** $\varphi(m)$ – tato čísla nazýváme primitivními kořeny modulo m a hrají důležitou roli mj. při řešení binomických kongruencí.

Příklad

Pro libovolné $m \in \mathbb{N}$ má číslo 1 modulo m řád 1. Číslo -1 má řád

- 1 pro $m = 1$ nebo $m = 2$
- 2 pro $m > 2$

Příklad

Určete řád čísla 2 modulo 7.

Příklad

Určete řád čísla 2 modulo 7.

Řešení

$$2^1 = 2 \not\equiv 1 \pmod 7$$
$$2^2 = 4 \not\equiv 1 \pmod 7$$
$$2^3 = 8 \equiv 1 \pmod 7$$

Řád čísla 2 modulo 7 je tedy roven 3. □

Uveďme nyní několik zásadních tvrzení udávajících vlastnosti řádu čísla modulo m:

Lemma

Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. *Jestliže* $a \equiv b \pmod{m}$, *pak obě čísla* a, b *mají stejný řád modulo* m.

Uveďme nyní několik zásadních tvrzení udávajících vlastnosti řádu čísla modulo m:

Lemma

Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. *Jestliže* $a \equiv b \pmod{m}$, *pak obě čísla* a, b *mají stejný řád modulo* m.

Důkaz.

Umocněním kongruence $a \equiv b \pmod{m}$ na n-tou dostaneme $a^n \equiv b^n \pmod{m}$, tedy $a^n \equiv 1 \pmod{m} \iff b^n \equiv 1 \pmod{m}$. □

Lemma

Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Je-li řád čísla a modulo m roven $r \cdot s$, (kde $r, s \in \mathbb{N}$), pak řád čísla a^r modulo m je roven s.

Lemma

Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Je-li řád čísla a modulo m roven $r \cdot s$, (kde $r, s \in \mathbb{N}$), pak řád čísla a^r modulo m je roven s.

Důkaz.

Protože žádné z čísel $a, a^2, a^3, \ldots, a^{rs-1}$ není kongruentní s 1 modulo m, není ani žádné z čísel $a^r, a^{2r}, a^{3r}, \ldots, a^{(s-1)r}$ kongruentní s 1. Platí ale $(a^r)^s \equiv 1 \pmod{m}$, proto je řád a^r modulo m roven s. □

Poznámka

Opak obecně neplatí – z toho, že řád čísla a^r modulo m je roven s ještě neplyne, že řád čísla a modulo m je $r \cdot s$.

Např pro $m = 13$ máme:

$a = 3$, $a^2 = 9 \pmod{13}$, $a^3 = 27 \equiv 1 \pmod{13} \Rightarrow 3$ má řád 3 mod 13.

$b = -4$, $b^2 = 16 \not\equiv 1 \pmod{13}$, $b^3 = -64 \equiv 1 \pmod{13} \Rightarrow -4$ má řád 3 mod 13.

Přitom $(-4)^2 = 16 \equiv 3 \pmod{13}$ má stejný řád 3 jako číslo 3, ale číslo -4 nemá řád $2 \cdot 3$.

Přesný popis závislosti řádu na exponentu dávají následující 2 věty:

Věta

Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Označme r řád čísla a modulo m. Pak pro libovolná $t, s \in \mathbb{N} \cup \{0\}$ platí

$$a^t \equiv a^s \pmod{m} \iff t \equiv s \pmod{r}.$$

Důkaz.

Bez újmy na obecnosti lze předpokládat, že $t \geq s$. Vydělíme-li číslo $t - s$ číslem r se zbytkem, dostaneme $t - s = q \cdot r + z$, kde $q, z \in \mathbb{N}_0, 0 \leq z < r$.

"$\Leftarrow$" Protože $t \equiv s \pmod{r}$, máme $z = 0$, a tedy $a^{t-s} = a^{qr} = (a^r)^q \equiv 1^q \pmod{m}$. Vynásobením obou stran kongruence číslem a^s dostaneme tvrzení.

"$\Rightarrow$" Z $a^t \equiv a^s \pmod{m}$ plyne $a^s \cdot a^{qr+z} \equiv a^s \pmod{m}$. Protože je $a^r \equiv 1 \pmod{m}$, je rovněž $a^{qr+z} \equiv a^z \pmod{m}$. Celkem po vydělení obou stran kongruence číslem a^s (které je nesoudělné s modulem), dostáváme $a^z \equiv 1 \pmod{m}$. Protože $z < r$, plyne z definice řádu, že $z = 0$, a tedy $r \mid t - s$. □

Zřejmým důsledkem předchozí věty a Eulerovy věty je následující tvrzení

Důsledek

Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Označme r řád čísla a modulo m.

1. *Pro libovolné $n \in \mathbb{N} \cup \{0\}$ platí*

$$a^n \equiv 1 \pmod{m} \iff r \mid n.$$

2. $r \mid \varphi(m)$

Následující věta je zobecněním předchozího Lemmatu.

Věta

Nechť $m, n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. *Je-li řád čísla* a *modulo* m *roven* $r \in \mathbb{N}$, *je řád čísla* a^n *modulo* m *roven* $\frac{r}{(n,r)}$.

Následující věta je zobecněním předchozího Lemmatu.

Věta

Nechť $m, n \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$. Je-li řád čísla a modulo m roven $r \in \mathbb{N}$, je řád čísla a^n modulo m roven $\frac{r}{(n,r)}$.

Důkaz.

Protože $\frac{r \cdot n}{(r,n)} = [r, n]$, což je zřejmě násobek r, máme

$$(a^n)^{\frac{r}{(r,n)}} = a^{[r,n]} \equiv 1 \pmod{m}$$

(plyne z předchozího Důsledku, neboť $r \mid [r, n]$). Na druhou stranu, je-li $k \in \mathbb{N}$ libovolné takové, že $(a^n)^k = a^{n \cdot k} \equiv 1 \pmod{m}$, dostáváme ($r$ je řád a), že $r \mid n \cdot k$ a dále víme, že $\frac{r}{(n,r)} \mid \frac{n}{(n,r)} \cdot k$ a díky nesoudělnosti čísel $\frac{r}{(n,r)}$ a $\frac{n}{(n,r)}$ dostáváme $\frac{r}{(n,r)} \mid k$. Proto je $\frac{r}{(n,r)}$ řádem čísla a^n modulo m. □

Poslední z této řady tvrzení dává do souvislosti řády dvou čísel a řád jejich součinu:

Lemma

Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. Jestliže a je řádu r a b je řádu s modulo m, kde $(r, s) = 1$, pak číslo $a \cdot b$ je řádu $r \cdot s$ modulo m.

Poslední z této řady tvrzení dává do souvislosti řády dvou čísel a řád jejich součinu:

Lemma

Nechť $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$. Jestliže a je řádu r a b je řádu s modulo m, kde $(r, s) = 1$, pak číslo $a \cdot b$ je řádu $r \cdot s$ modulo m.

Důkaz.

Označme δ řád čísla $a \cdot b$. Pak $(ab)^\delta \equiv 1 \pmod{m}$ a umocněním obou stran kongruence dostaneme $a^{r\delta} b^{r\delta} \equiv 1 \pmod{m}$. Protože je r řádem čísla a, je $a^r \equiv 1 \pmod{m}$, tj. $b^{r\delta} \equiv 1 \pmod{m}$, a proto $s \mid r\delta$. Z nesoudělnosti r a s plyne $s \mid \delta$. Analogicky dostaneme i $r \mid \delta$, a tedy (opět s využitím nesoudělnosti r, s) $r \cdot s \mid \delta$. Obráceně zřejmě platí $(ab)^{rs} \equiv 1 \pmod{m}$, proto $\delta \mid rs$. Celkem tedy $\delta = rs$. □