

# Diskrétní matematika – 3. týden

## Elementární teorie čísel – Eulerova věta, řád prvku

Lukáš Vokřínek

Masarykova univerzita  
Fakulta informatiky

jaro 2020

# Obsah přednášky

- 1 Prvočísla
  - Poznámky
  - Dělitelé znovu
  - Rozložení prvočísel
- 2 Aritmetické funkce
  - Eulerova funkce  $\varphi$
- 3 Malá Fermatova věta, Eulerova věta

## Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant  
**Matematika drsně a svižně**, e-text na  
[www.math.muni.cz/Matematika\\_drsne\\_svizne](http://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](http://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

- 1 Prvočísla
  - Poznámky
  - Dělitelé znovu
  - Rozložení prvočísel
- 2 Aritmetické funkce
  - Eulerova funkce  $\varphi$
- 3 Malá Fermatova věta, Eulerova věta

# Připomenutí – věta o jednoznačném rozkladu

## Věta

*Libovolné přirozené číslo  $n \geq 2$  je možné vyjádřit jako součin prvočísel, přičemž je toto vyjádření jediné, nebereme-li v úvahu pořadí činitelů. (Je-li  $n$  prvočíslo, pak jde o „součin“ jednoho prvočísla.)*

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

# 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](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?

$$n \longmapsto p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

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*<sup>1</sup>, je sub-exponenciální časové složitosti  $O(e^{1.9(\log N)^{1/3}(\log \log N)^{2/3}})$ .

<sup>1</sup>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*<sup>1</sup>, 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 sestavit počítače s dostatečným počtem qubits – jak je to obtížné, lze vysledovat z toho, že v roce 2001 se IBM podařilo pomocí kvantového počítače rozložit číslo 15 a v roce 2012 byl dosažen další faktorizační rekord rozkladem čísla 21.

<sup>1</sup>Pro podrobnosti navštivte M8190 Algoritmy teorie čísel 

# RSA Challenge

## Poznámka

Že 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).

$$n = p \cdot q \quad \rightarrow \text{najít } p, q \text{ těžké}$$

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 dřívějšíka 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  $m_1 \leq n_1, m_2 \leq n_2, \dots, m_k \leq n_k$ .

$$p \mid a \Rightarrow p = p_1 \cdot \dots \cdot p_k$$

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 dřívějšíka intuitivně známý) postup na výpočet největšího společného dělitele dvou čísel ze znalosti jejich rozkladu na prvočísla.

## Důsledek

- Každý kladný dělitel čísla  $a = p_1^{n_1} \cdots p_k^{n_k}$  je tvaru  $p_1^{m_1} \cdots p_k^{m_k}$ , 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  $\tau(a) = (n_1 + 1)(n_2 + 1) \cdots (n_k + 1)$  kladných dělitelů, jejichž součet je

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

dělitelé!

jsou

$$P_1^{n_1} \dots P_k^{n_k}$$

$$P_1^{m_1} \dots P_k^{m_k}$$

$(n_1+1) \dots (n_k+1)$   
možností

$$\left\{ \begin{array}{l} 0 \leq m_1 \leq n_1 \leftarrow n_1+1 \text{ možností} \\ \vdots \\ 0 \leq m_k \leq n_k \leftarrow n_k+1 \text{ mož.} \end{array} \right.$$

dělitelů

součet

je  $(1 + P_1 + \dots + P_1^{n_1}) \dots (1 + P_k + \dots + P_k^{n_k})$

// L možností součet ✓

$$\frac{P_1^{n_1+1} - 1}{P_1 - 1}$$

## Důsledek (Pokr.)

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

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

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

minimální  
exponenty

# 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.*



$$\frac{p_i^{k+1} - 1}{p_i - 1} \stackrel{p_i=2}{=} 2^{k+1} - 1$$

$n$  sude' dokonale' cislo

$$n = 2^k \cdot l \quad \begin{array}{l} \text{liche} \\ \text{prvocislo} \end{array} \quad 2^{k+1} - 1$$

$$2n = \sigma(n) = \frac{(2^{k+1} - 1) \cdot \sigma(l)}{2^{k+1} - 1} \cdot l$$

$$\frac{2^{k+1} \cdot l}{2^{k+1} - 1} \cdot l$$

$$2^{k+1} - 1 \mid 2^{k+1} \cdot l$$

= rozd.

$$\Rightarrow 2^{k+1} - 1 \mid l \Rightarrow l = \frac{(2^{k+1} - 1) \cdot m}{2^{k+1} - 1} \cdot l$$

$$2^{k+1} \cdot \frac{(2^{k+1} - 1) \cdot m}{2^{k+1} - 1} = \frac{(2^{k+1} - 1) \cdot \sigma((2^{k+1} - 1) \cdot m)}{2^{k+1} - 1}$$

$\rightarrow$   $l + m$  — jsou dva delitele  $l$   
 $m=1$   $l$  je prvo cislo

## Mersenneho prvočísla a dokonalá čísla

S pojmem *součet všech kladných dělitelů čísla  $a$*  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.*

Na druhou stranu popsat lichá dokonalá čísla se dodnes nepodařilo, resp. **dodnes se neví, jestli vůbec nějaké liché dokonalé číslo existuje.**

# Hledání velkých prvočísel

$2^{ab} - 1$  je del.  $2^a - 1$  / *nikdy od  $1, 2^{ab} - 1$*   
 $2^a \equiv 1 \pmod{2^a - 1} \xrightarrow{(\cdot)^b} 2^{ab} \equiv 1, \underline{\underline{2^{ab} - 1 \equiv 0}}$   $\wedge$  prvočíslo  $\uparrow\uparrow$

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

# Hledání velkých prvočísel

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

## 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  $M_p = 2^p - 1$  prvočísló, právě tehdy, když  $M_p$  dělí  $s_{p-2}$ .

*dělení se 25*

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<sup>2</sup>, 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).

max. zhruba 29 mil. cifer

<sup>2</sup>Viz např. titulek iDnes z 6. února 2013: *Největší známé prvočíslu na světě má 17 milionů číslic a je k ničemu*

# 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?

*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  $p_1, p_2, \dots, p_n$ . Položme  $N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$ . Toto číslo je buď samo prvočíslem nebo je dělitelné nějakým prvočíslem různým od  $p_1, \dots, p_n$  (čísla  $p_1, \dots, p_n$  totiž dělí číslo  $N - 1$ ), což je spor.  $\square$

$$2, 3, 5 \quad \longrightarrow \quad 2 \cdot 3 \cdot 5 + 1 = 31$$

$$2, 3, 5, 7 \quad \longrightarrow \quad 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$$

# Prvočísel je nekonečně mnoho

## Věta (Eukleidés)

*Mezi přirozenými čísly existuje nekonečně mnoho prvočísel.*

## Důkaz.

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

## 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 prvočíslu.

# Prvočísel je vcelku hodně

## Příklad

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

## Řešení

Označme  $p$  libovolné prvočíslu 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  $p < n!$ . Prvočíslu  $p$  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 prvočísllo  $p$  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  $(n+1)! + 2$ ,  $(n+1)! + 3$ ,  $\dots$ ,  $(n+1)! + (n+1)$ .  
 Mezi těmito  $n$  po sobě jdoucími čísly není žádné prvočíslo, protože pro libovolné  $k \in \{2, 3, \dots, n+1\}$  platí  $k \mid (n+1)!$ , a tedy  $k \mid (n+1)! + k$ , a proto  $(n+1)! + k$  nemůže být prvočíslo.  $\square$

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.

$$4m+1, 4m+3, \cancel{4m+2} \quad \leftarrow 2 \text{ jinak nic}$$

### 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  $1 \cdot m + a, 2 \cdot m + a, 3 \cdot m + a, \dots$  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  $k \in \mathbb{N}_0$ .

*podobně pro  $4k+3$*

## Řešení

Předpokládejme naopak, že existuje pouze konečně mnoho prvočísel tohoto tvaru a označme je  $p_1 = 2, p_2 = 5, p_3 = 11, \dots, p_n$ . Položme  $N = 3p_2 \cdot p_3 \cdot \dots \cdot p_n + 2$ . Rozložíme-li  $N$  na součin prvočísel, musí v tomto rozkladu vystupovat aspoň jedno prvočíсло  $p$  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. Prvočíсло  $p$  ovšem nemůže být žádné z prvočísel  $p_1, p_2, \dots, p_n$ , 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  $\# \{2 \leq p \leq x\}$

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

power je cca  $\frac{1}{\ln x}$

tj. podíl funkcí  $\pi(x)$  a  $x/\ln x$  se pro  $x \rightarrow \infty$  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  $x \rightarrow \infty$  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

$$\frac{|\pi(x) - x/\ln(x)|}{\pi(x)} = 9\%$$



# Plán přednášky

- 1 Prvočísla
  - Poznámky
  - Dělitelé znovu
  - Rozložení prvočísel
- 2 Aritmetické funkce
  - Eulerova funkce  $\varphi$
- 3 Malá Fermatova věta, Eulerova věta

# Aritmetické funkce

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

$f: \mathbb{N} \rightarrow \mathbb{Z}$  *nebo  $\mathbb{N}$  nebo obecně*

## Definice

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

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

$$f(n) = f(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2} \dots p_k^{\alpha_k})$$

*nesoudělné*

$$= \dots = \underline{\underline{f(p_1^{\alpha_1}) \dots f(p_k^{\alpha_k})}}$$

$\Rightarrow f$  určena hodnotami na  $\boxed{p^\alpha}$

# Aritmetické funkce

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

## 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  $f(n) = \sigma(n)$ ,  $f(n) = \tau(n)$  nebo, jak brzy dokážeme i tzv. Eulerova funkce  $f(n) = \varphi(n)$ .

$$\underbrace{(\alpha_1 + 1) \cdots (\alpha_k + 1)}_{\tau(p_1^{\alpha_1})} \cdots \underbrace{(\alpha_k + 1)}_{\tau(p_k^{\alpha_k})}$$

# Eulerova funkce

## Definice

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

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

*vlastnost  
 zb. třídy  
 $a \pmod n$*

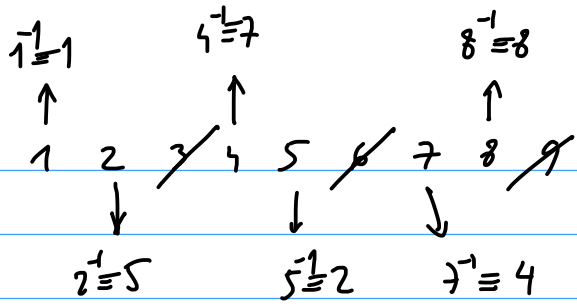
(lépe počet zbytkových tříd nesoudělných s  $n$  nebo také těch, které mají modulo  $n$  inverzi).

$n=6$   
 $1^{-1} \equiv 1 \pmod{6}$   
 $5^{-1} \equiv 5 \pmod{6}$

1	<del>2</del>	<del>3</del>	<del>4</del>	5	<del>6</del>
7	8	9	10	11	12
⋮	⋮	⋮	⋮	⋮	⋮

$\varphi(6) = 2$   
 $(2, 6) = (8, 6)$   
 $= (14, 6)$   
 $= \dots$

$$n = 9 = 3^2$$
$$\varphi(n) = 6$$



# Eulerova funkce

## Definice

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

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

(lépe počet zbytkových tříd nesoudělných s  $n$  nebo také těch, které mají modulo  $n$  inverzi).

## Příklad

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

$$\varphi(p) = p - 1.$$

$1 \ 2 \ \dots \ p-1$   ~~$p$~~   
nesoud.

Nyní dokážeme několik důležitých tvrzení o funkci  $\varphi$ :

### Lemma

*Platí  $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1) = p^\alpha(1 - \frac{1}{p})$ .*

$$\underline{\text{Pr.}} \quad 9 = 3^2$$

Nyní dokážeme několik důležitých tvrzení o funkci  $\varphi$ :

### Lemma

Platí  $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1) = p^\alpha(1 - \frac{1}{p})$ .

### Důkaz.

Mezi čísla  $\{1, \dots, p^\alpha\}$  jsou soudělná s  $p^\alpha$  právě násobky  $p$ , tedy

$$1 \cdot p, 2 \cdot p, \dots, p^{\alpha-1} \cdot p$$

a těch je  $p^{\alpha-1}$ . Nesoudělných je proto  $p^\alpha - p^{\alpha-1}$ . □



za dvířku

## Věta

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

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

$$\begin{aligned} \varphi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) &= \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) \\ &= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \cdots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right) \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

## Věta

Eulerova funkce  $\varphi$  je multiplikatívní.

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.

Nechť  $a, b$  jsou nesoudělná. Připomeňme bijekci

$$x \pmod{a \cdot b} \longmapsto (x \pmod{a}, x \pmod{b})$$

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

Stačí proto ukázat, že  $x \pmod{a \cdot b}$  má inverzi, právě když obě složky obrazu mají inverzi – takových dvojic je totiž přesně  $\varphi(a) \cdot \varphi(b)$ . To je ale jasné z CRT. — Chinese remainder theorem  $\square$

$x \pmod{a \cdot b}$  ma' inverzi

$\Leftrightarrow x \pmod{a}$   
 $x \pmod{b}$  naji inverzi

$$x \cdot x^{-1} \equiv 1 \pmod{a \cdot b} \Rightarrow \begin{cases} x \cdot x^{-1} \equiv 1 \pmod{a} \\ x \cdot x^{-1} \equiv 1 \pmod{b} \end{cases}$$

$$x \cdot w \equiv 1 \pmod{a \cdot b} \Leftrightarrow \begin{cases} x \cdot y \equiv 1 \pmod{a} \\ x \cdot z \equiv 1 \pmod{b} \end{cases}$$

↓  
 $w \equiv y \pmod{a} \quad w \equiv z \pmod{b}$

podle CRT odp.  
w (a·b)

## Příklad

Vypočtete  $\varphi(72)$ .



### Příklad

Vypočtete  $\varphi(72)$ .

### Řešení

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

### Příklad

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

## Příklad

Vypočtete  $\varphi(72)$ .

## Řešení

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

## Příklad

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

## Řešení

$$\varphi(4n + 2) = \varphi(2 \cdot (2n + 1)) = \cancel{\varphi(2)} \cdot \varphi(2n + 1) = \varphi(2n + 1). \quad \square$$

$$\varphi(2) = 2 - 1 = 1$$

# Plán přednášky

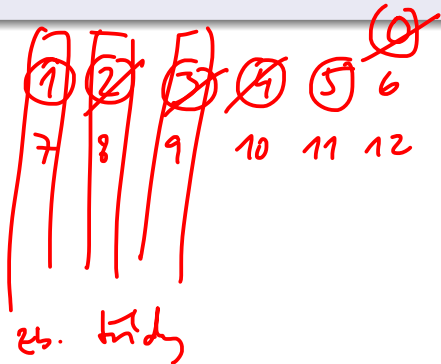
- 1 Prvočísla
  - Poznámky
  - Dělitelé znovu
  - Rozložení prvočísel
- 2 Aritmetické funkce
  - Eulerova funkce  $\varphi$
- 3 Malá Fermatova věta, Eulerova věta



# Úplná a redukovaná soustava zbytků

## Definice

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



# Úplná a redukovaná soustava zbytků

## Definice

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

*Redukovaná soustava zbytků* modulo  $m$  je libovolná  $\varphi(m)$ -tice čísel nesoudělných s  $m$  a po dvou nekongruentních modulo  $m$ .

1, 5 (6)  
1, 2, 4, 5, 7, 8 (9)

# Úplná a redukovaná soustava zbytků

## Definice

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

Redukovaná soustava zbytků modulo  $m$  je libovolná  $\varphi(m)$ -tice čísel nesoudělných s  $m$  a po dvou nekongruentních modulo  $m$ .

## Lemma

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

$x_1 \longrightarrow a \cdot x_1$   
 $x_2 \longrightarrow a \cdot x_2$   
 $x_3 \longrightarrow a \cdot x_3$   
 $\vdots$

*ruční poznámky:*  
 různé třídy  $\longrightarrow$  různé třídy  
 $a \cdot x_i \equiv a \cdot x_j$   
 $\Downarrow$   
 $x_i \equiv x_j$   
 $x_i x_i^{-1} \equiv 1$   
 $(a \cdot x_i)(a^{-1} \cdot x_i^{-1}) \equiv 1$

# Úplná a redukovaná soustava zbytků

## Definice

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

*Redukovaná soustava zbytků modulo  $m$  je libovolná  $\varphi(m)$ -tice čísel nesoudělných s  $m$  a po dvou nekongruentních modulo  $m$ .*

## Lemma

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

Eul. věta

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \Rightarrow a \cdot \underbrace{a^{\varphi(m)-1}}_{a^{-1}} \equiv 1$$

## 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.

Bud'  $x_1, x_2, \dots, x_{\varphi(m)}$  libovolná redukovaná soustava zbytků modulo  $m$ . Podle předchozího lemmatu je i  $a \cdot x_1, \dots, a \cdot x_{\varphi(m)}$  redukovaná soustava zbytků modulo  $m$ . Platí tedy, že pro každé  $i$  existuje  $j$  ( $i, j \in \{1, 2, \dots, \varphi(m)\}$ ) 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

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

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

$$m = 9$$

$$a \equiv 2$$

 $x_i$  $a \cdot x_i$ 

1

1

2

2

4

4

5

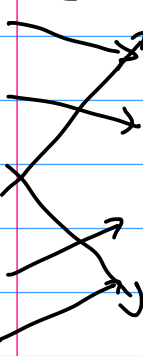
5

7

7

8

8

 $2x$  $(m)$

# 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*

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

$$\varphi(p) = p - 1$$



# 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

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

*lepší!*

## Důsledek

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

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

# 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

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

Handwritten notes illustrating the definition and properties of the order of a number modulo m:

$1 \ a \ a^2 \ a^3 \ \dots \ a^n \ a^{n+1} \ a^{n+2} \ \dots \ a^{2n}$   
 $\parallel \quad \parallel \quad \parallel \quad \dots \quad \parallel$   
 $1 \quad a \quad a^2 \quad \dots \quad a^n$   
 $\parallel \quad \parallel \quad \parallel \quad \dots \quad \parallel$   
 $1 \quad a \quad a^2 \quad \dots \quad a^{n-1}$

$a^i \equiv a^j \iff i \equiv j \pmod{n}$   
 $a^{i-j} \equiv 1 \iff n \mid i-j$

Navigation icons:

## 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.

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

## 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  $m > 2$

$$-1 \equiv 1 \quad (2)$$

## Příklad

Určete řád čísla 2 modulo 7.

### Příklad

Určete řád čísla 2 modulo 7.

### Řešení

$$2^0 = 1$$

$$2^1 = 2$$

$$2^2 = 4$$

$$2^3 = 8 = 1$$

$$2^4 = 2$$

$$2^5 = 4$$

$$2^1 = 2 \not\equiv 1 \pmod{7}$$

$$2^2 = 4 \not\equiv 1 \pmod{7}$$

$$2^3 = 8 \equiv 1 \pmod{7}$$

E.v.

$$a^{\varphi(7)} \equiv 1 \pmod{7}$$

$$a^6 \equiv 1 \pmod{7}$$

$$3^3 \equiv 6 \pmod{7} \quad \square$$

Řád čísla 2 modulo 7 je tedy roven 3.

!

řád 3 je 6  
 $\Rightarrow$  3 je prim. hořek

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

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



$$r \mid t-s \stackrel{\text{def}}{=} t \equiv s \pmod{r}$$

$$\begin{array}{l} a \equiv b \pmod{m} \Rightarrow a^k \equiv b^k \pmod{m} \\ t \equiv s \pmod{\varphi(m)} \Rightarrow a^t \equiv a^s \pmod{m} \\ \text{nebo } r \end{array}$$



## 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  $r \mid \varphi(m)$

$\triangleleft r = \varphi(m)$  --- primitivní kořen

$$a^{\varphi(m)} \equiv 1 \equiv a^0$$

$$\Rightarrow \varphi(m) \equiv 0$$

$$\Leftrightarrow r \mid \varphi(m)$$

(no d 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  $\frac{r}{(n,r)}$ .*

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

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

(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  $m$ .

$$\begin{aligned}
 (a \cdot b)^{\delta} &\equiv 1 \\
 a^{\delta} \cdot b^{\delta} &\equiv 1 \Rightarrow a^{r\delta} b^{r\delta} \equiv 1 \\
 &\Rightarrow b^{r\delta} \equiv 1 \Rightarrow \underline{s \mid r\delta} \\
 &\hspace{15em} \text{nesoud} \\
 &\Rightarrow \underline{s \mid \delta} \\
 &\hspace{15em} \text{nesoud} \\
 \text{symetricky } r \mid \delta &\Rightarrow \underline{r \cdot s \mid \delta}
 \end{aligned}$$

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  $\delta$  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  $\delta = rs$ . □

## Důsledek

*Nechť  $m \in \mathbb{N}$  a  $r$  je nejmenší společný násobek všech řádů modulo  $m$ . Pak existuje číslo řádu  $r$  modulo  $m$ .*

## Důsledek

*Nechť  $m \in \mathbb{N}$  a  $r$  je nejmenší společný násobek všech řádů modulo  $m$ . Pak existuje číslo řádu  $r$  modulo  $m$ .*

## Důkaz.

Stačí pro  $a$  řádu  $s$ ,  $b$  řádu  $t$  najít prvek řádu  $[s, t]$ . Nechť  $d = (s, t)$ , pak tímto prvkem je  $a^d \cdot b$ . □



## Důsledek

*Nechť  $m \in \mathbb{N}$  a  $r$  je nejmenší společný násobek všech řádů modulo  $m$ . Pak existuje číslo řádu  $r$  modulo  $m$ .*

## Důkaz.

Stačí pro  $a$  řádu  $s$ ,  $b$  řádu  $t$  najít prvek řádu  $[s, t]$ . Nechť  $d = (s, t)$ , pak tímto prvkem je  $a^d \cdot b$ . □

## Věta

*Nechť  $p \in \mathbb{N}$  je prvočíslo. Pak existuje prvek řádu  $p - 1$  modulo  $p$ , tzv. primitivní kořen.*