

# Algoritmy teorie čísel

Radan Kučera, jarní semestr 2012

## Literatura: text v ISu čerpající z následujících zdrojů

1. Cassels J. W. S.: *An Introduction to Diophantine Approximation*, University Press, Cambridge, 1965.
2. Cohen H.: *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics 138, Springer–Verlag, Berlin, Heidelberg, New York 1993, kapitoly 8–10, (čtvrté aktualizované vydání 2000).
3. Dietzfelbinger M., *Primality Testing in Polynomial Time (From Randomized Algorithms to “Primes is in P”)*, LNCS 3000, Springer–Verlag Berlin, Heidelberg, New York 2004.
4. Knuth D.E., *The Art of Computer Programming, díl 2: Seminumerical Algorithms*, (druhé vydání), Addison-Wesley, Reading, Mass., 1981.
5. Lenstra A. K., Lenstra H. W. Jr.: *Algorithms in Number Theory*, v *Handbook of Theoretical Computer Science*, kapitola 12, Elsevier Science Publishers B.V., 1990.
6. Rosický J., *Algebra*, 4. vydání, skriptum MU, 2002.

## Pojem algoritmu

**Algoritmus** je metoda, která pro jistý typ vstupů dá po konečné době výstup, tedy odpověď na zadaný problém.

Při zadání algoritmu je nutno provést:

- ▶ dokázat správnost výstupu,
- ▶ odhadnout časovou náročnost,
- ▶ odhadnout paměťovou náročnost.

Časovou náročností rozumíme závislost délky výpočtu na délce vstupu, přitom délku vstupu měříme počtem bitů potřebných pro zápis zadání a délkou výpočtu rozumíme, jak dlouho trvá nejdelší výpočet pro danou délku vstupu.

*Příklad.* Pro vstup jednoho přirozeného čísla  $N$  je třeba  $1 + \lceil \log_2 N \rceil$  bitů.

Paměťovou náročnost budeme také měřit v bitech (u většiny algoritmů, se kterými se setkáme, nebude nutné se jí zabývat, neboť bude konstantní a zanedbatelně malá).

## Asymptotický odhad

Nechť  $(a_n)_{n=1}^{\infty}$ ,  $(b_n)_{n=1}^{\infty}$  jsou posloupnosti. Řekneme, že posloupnost  $(a_n)_{n=1}^{\infty}$  je řádu  $O(b_n)$ , jestliže platí

$$\limsup_{n \rightarrow \infty} \left| \frac{a_n}{b_n} \right| < \infty.$$

Řekneme, že posloupnost  $(a_n)_{n=1}^{\infty}$  je řádu  $o(b_n)$ , jestliže existuje

$$\lim_{n \rightarrow \infty} \frac{a_n}{b_n} = 0.$$

Protože se budeme zabývat algoritmy, jejichž cílem je rozložit přirozené číslo na prvočinitele, bude vstupem pro náš algoritmus jediné přirozené číslo  $N$ .

Dohodněme se, že  $\ln^k N$  bude znamenat  $(\ln N)^k$ . Kupříkladu tedy  $\ln^2 N = (\ln N)^2$ , nikoli  $\ln \ln N$ .

Definice. Řekneme, že algoritmus je polynomiálního času, jestliže čas, po který algoritmus poběží, najde-li na vstupu přirozené číslo  $N$ , je řádu  $o(\ln^k N)$  pro nějaké přirozené číslo  $k$ .

Řekneme, že algoritmus je lineárního (resp. kvadratického, resp. kubického) času, je-li tento čas řádu  $O(\ln N)$ , (resp.  $O(\ln^2 N)$ , resp.  $O(\ln^3 N)$ ).

Je-li tento čas řádu  $o(N^\alpha)$  pro každé kladné reálné číslo  $\alpha$  a přitom algoritmus není polynomiálního času, řekneme, že algoritmus je subexponenciálního času.

Konečně, jestliže existují kladná reálná čísla  $\alpha > \beta$  tak, že tento čas je řádu  $O(N^\alpha)$ , ale není řádu  $O(N^\beta)$ , řekneme, že algoritmus je exponenciálního času.

Příklad. Později se setkáme s algoritmy, jejichž čas je řádu

$$O(e^{c(\ln N)^a(\ln \ln N)^b}),$$

kde  $a$ ,  $b$ ,  $c$  jsou kladná reálná čísla, přičemž  $a + b = 1$ . Tyto algoritmy jsou subexponenciálního času.

# Pravděpodobnostní algoritmy

Budeme pracovat s algoritmy, jejichž průběh výpočtu závisí na jistém zdroji náhodných čísel. Je zde možnost (pravděpodobnosti nula), že jejich běh nikdy neskončí, přesto zkušenosti ukazují, že tyto algoritmy jsou často efektivnější než ostatní a mnohdy jsou jediné, které máme k dispozici.

Na druhé straně rozhodně nebudeme nazývat algoritmem metodu, produkující výsledek, který je s vysokou pravděpodobností správný. Je podstatné, že algoritmus v okamžiku zastavení dává pouze správné výsledky (odhlédneme-li od případných chyb člověka či počítače při provádění výpočtu).

## Počítání s velkými čísly

Budeme předpokládat, že máme k dispozici software, ve kterém je možné provádět základní algebraické operace s čísly, majícími řekněme 1000 dekadických cifer (MATHEMATICA, MAPLE, PARI-GP a podobně).

Taková čísla jsou zapsána v poziční soustavě o vhodném základu a operace jsou prováděny podobně jako jsme to zvyklí dělat na papíře s dekadickými čísly. Vhodný základ je mocnina dvou: čas potřebný pro vstup a výstup je pouze zanedbatelná část celkové doby výpočtu a obvykle je dominován časem pro fyzický zápis.

**Sčítání** a **odčítání** má lineární časovou náročnost.

**Násobení malou konstantou** má také lineární časovou náročnost.

**Obecné násobení** a **dělení se zbytkem** má kvadratickou časovou náročnost.

(Jsou známy algoritmy pro násobení a dělení  $n$ bitových čísel, které dosahují menší časové náročnosti než „metoda tužky a papíru“.

Schönhage a Strassen popsali metodu jen s  $O(n \cdot \ln n \cdot \ln \ln n)$  bitových operací. Avšak tyto rafinované metody jsou rychlejší až pro čísla mající alespoň několik set dekadických cifer.)

## Výpočet největšího společného dělitele

Často budeme potřebovat spočítat největší společný dělitel dvou přirozených čísel.

Naivní řešení: rozlož obě čísla na součin prvočísel a poté vynásob společné činitele.

Tento postup je vhodný jen pro velmi malá čísla (řekněme do 100) nebo v případě, že víme, že některé z daných čísel je prvočíslo (pak stačí provést jen jedno dělení se zbytkem).

Mnohem výhodnější je výpočet největšího společného dělitele pomocí Euklidova algoritmu, který je nejen nejstarší, ale asi i nejdůležitější algoritmus teorie čísel.



# Euklidův algoritmus

**Algoritmus (Euklidův).** Pro daná nezáporná celá čísla  $a, b$  algoritmus najde jejich největší společný dělitel.

1. [Jsi hotov?] Je-li  $b = 0$ , pak vytiskni  $a$  jako odpověď a skonči.
2. [Euklidovský krok] Polož  $r \leftarrow a \bmod b$ ,  $a \leftarrow b$ ,  $b \leftarrow r$  a jdi na 1.

Věta. 1. Je-li  $1 \leq a \leq N$ ,  $1 \leq b \leq N$ , pak počet Euklidovských kroků v předchozím algoritmu je roven nejvýše

$$\left\lceil \frac{\ln(\sqrt{5}N)}{\ln \frac{1+\sqrt{5}}{2}} \right\rceil - 2 \approx 2,078 \ln N + 1,672.$$

2. Průměrný počet Euklidovských kroků v předchozím algoritmu pro  $a, b \in \{1, \dots, N\}$  je roven přibližně

$$\frac{12 \ln 2}{\pi^2} \ln N + 0,14 \approx 0,843 \ln N + 0,14.$$

## Časová náročnost Euklidova algoritmu

Podle věty je počet kroků algoritmu lineární v  $\ln N$ .

Každý krok vyžaduje dlouhé dělení, které je kvadratického času.

Proto se zdá, že je tento algoritmus kubického času.

V průběhu výpočtu jsou však  $a$ ,  $b$  stále menší a menší, proto je možné průběžně snižovat potřebný počet cifer v poziční soustavě.

Při výpočtu Euklidovského kroku  $a = bq + r$  je časová náročnost  $O((\ln a)(1 + \ln q))$ , tedy celkový čas je omezen řádem

$$O((\ln N)((\sum \ln q) + O(\ln N))).$$

Ale

$$\sum \ln q = \ln \prod q \leq \ln N,$$

a tedy při pečlivém naprogramování jde o algoritmus kvadratického času.

## Binární verze Euklidova algoritmu

Místo dlouhého dělení je užito odčítání a dělení 2 (realizované posunem). Základem poziční soustavy musí být mocnina 2.

**Algoritmus (Binární NSD).** Pro daná nezáporná celá čísla  $a$ ,  $b$  algoritmus najde jejich největší společný dělitel.

- [Jednou zredukuj velikost] Je-li  $a < b$ , vyměň  $a$  s  $b$ . Je-li  $b = 0$ , pak vytiskni  $a$  jako odpověď a skonči. Jinak (tj. pro  $b \neq 0$ ) polož  $r \leftarrow a \bmod b$ ,  $a \leftarrow b$ ,  $b \leftarrow r$ .*
- [Spočítej mocninu 2] Je-li  $b = 0$ , pak vytiskni  $a$  jako odpověď a skonči. Jinak polož  $k \leftarrow 0$  a dokud budou  $a$  i  $b$  sudá, opakuj  $k \leftarrow k + 1$ ,  $a \leftarrow a/2$ ,  $b \leftarrow b/2$ .*
- [Odstraň přebytečné mocniny 2] Je-li  $a$  sudé, opakuj  $a \leftarrow a/2$ , dokud bude  $a$  sudé. Jinak, je-li  $b$  sudé, opakuj  $b \leftarrow b/2$ , dokud bude  $b$  sudé.*
- [Odečti] (Nyní jsou obě  $a$  i  $b$  lichá.) Polož  $t \leftarrow \frac{a-b}{2}$ . Je-li  $t = 0$ , vytiskni  $2^k \cdot a$  jako odpověď a skonči.*
- [Cyklus] Dokud bude  $t$  sudé, opakuj  $t \leftarrow t/2$ . Pak, je-li  $t > 0$ , polož  $a \leftarrow t$ , jinak polož  $b \leftarrow -t$  a jdi na 4.*

## Rozšířená verze Euklidova algoritmu

Označme  $d$  největší společný dělitel celých čísel  $a$ ,  $b$ , pak existují celá čísla  $u$ ,  $v$  tak, že  $d = ua + vb$  (tzv. Bezoutova rovnost).

V některých aplikacích budeme potřebovat spočítat nejen  $d$ , ale i čísla  $u$ ,  $v$ , proto si uvedeme algoritmus pro jejich výpočet.

**Algoritmus (Rozšířený Euklidův).** Pro daná nezáporná celá čísla  $a$ ,  $b$  algoritmus najde trojici celých čísel  $(u, v, d)$  takovou, že  $d$  je největší společný dělitel čísel  $a$ ,  $b$  a platí  $d = ua + vb$ .

1. [Inicializace] Polož  $u \leftarrow 1$ ,  $d \leftarrow a$ . Je-li  $b = 0$ , polož  $v \leftarrow 0$ , vytiskni  $(u, v, d)$  jako odpověď a skonči. Jinak polož  $v_1 \leftarrow 0$  a  $v_3 \leftarrow b$ .
2. [Jsi hotov?] Je-li  $v_3 = 0$ , pak polož  $v \leftarrow \frac{d-au}{b}$ , vytiskni  $(u, v, d)$  jako odpověď a skonči.
3. [Euklidovský krok] Současně  $q \leftarrow \lfloor \frac{d}{v_3} \rfloor$ ,  $t_3 \leftarrow d \bmod v_3$ . Pak polož  $t_1 \leftarrow u - qv_1$ ,  $u \leftarrow v_1$ ,  $d \leftarrow v_3$ ,  $v_1 \leftarrow t_1$ ,  $v_3 \leftarrow t_3$  a jdi na 2.

Hodnoty proměnných  $d$ ,  $v_3$ ,  $t_3$  nezávisí na hodnotách ostatních proměnných. Přeznačíme-li je  $a$ ,  $b$ ,  $r$ , dostaneme původní Euklidův algoritmus, tedy tento algoritmus vždy skončí, a to se správným  $d$ .

## Důkaz správnosti rozšířené verze Euklidova algoritmu

Zavedeme proměnné  $v_2$ ,  $t_2$ ,  $v$ , které nebudou nikdy použity pro výpočet hodnot původních proměnných. Před krokem 2 vždy platí

$$at_1 + bt_2 = t_3, \quad au + bv = d, \quad av_1 + bv_2 = v_3.$$

**Algoritmus (Upravený rozšířený Euklidův).** Pro daná nezáporná celá čísla  $a$ ,  $b$  algoritmus najde trojici celých čísel  $(u, v, d)$  takovou, že  $d$  je největší společný dělitel čísel  $a$ ,  $b$  a platí  $d = ua + vb$ .

1. [Inicializace] Polož  $u \leftarrow 1$ ,  $d \leftarrow a$ . Je-li  $b = 0$ , polož  $v \leftarrow 0$ , vytiskni  $(u, v, d)$  jako odpověď a skonči. Jinak polož  $v_1 \leftarrow 0$ ,  $v_3 \leftarrow b$ ,  $t_1 \leftarrow 0$ ,  $t_2 \leftarrow 0$ ,  $t_3 \leftarrow 0$ ,  $v \leftarrow 0$ ,  $v_2 \leftarrow 1$ .
2. [Jsi hotov?] Je-li  $v_3 = 0$ , pak polož  $v \leftarrow \frac{d-au}{b}$ , vytiskni  $(u, v, d)$  jako odpověď a skonči.
3. [Euklidovský krok] Současně  $q \leftarrow \lfloor \frac{d}{v_3} \rfloor$ ,  $t_3 \leftarrow d \bmod v_3$ . Pak polož  $t_1 \leftarrow u - qv_1$ ,  $u \leftarrow v_1$ ,  $d \leftarrow v_3$ ,  $v_1 \leftarrow t_1$ ,  $v_3 \leftarrow t_3$ ,  $t_2 \leftarrow v - qv_2$ ,  $v \leftarrow v_2$ ,  $v_2 \leftarrow t_2$  a jdi na 2.

# Nezbytný aparát z algebry a elementární teorie čísel

## Kongruence

Definice. Necht'  $m \in \mathbb{N}$ ,  $a, b \in \mathbb{Z}$ . Řekneme, že  $a$  je kongruentní s  $b$  podle modulu  $m$ , píšeme  $a \equiv b \pmod{m}$ , jestliže  $m \mid a - b$ .

Věta 1. Necht'  $m \in \mathbb{N}$ ,  $a, b, c, d \in \mathbb{Z}$ . Jestliže  $a \equiv b \pmod{m}$ ,  $c \equiv d \pmod{m}$ , pak platí  $a + c \equiv b + d \pmod{m}$ ,  $a - c \equiv b - d \pmod{m}$ ,  $ac \equiv bd \pmod{m}$ .

Věta 2. Necht'  $m, k \in \mathbb{N}$ ,  $a, b \in \mathbb{Z}$ . Pak platí  $a \equiv b \pmod{m}$  právě tehdy, když  $ak \equiv bk \pmod{mk}$ .

Věta 3. Necht'  $m \in \mathbb{N}$ ,  $a, b, k \in \mathbb{Z}$ . Jestliže  $ak \equiv bk \pmod{m}$  a navíc  $(m, k) = 1$ , pak platí  $a \equiv b \pmod{m}$ .

Věta 4. Necht'  $a, b \in \mathbb{Z}$ . Pak existuje  $x \in \mathbb{Z}$  splňující kongruenci  $ax \equiv b \pmod{m}$  právě tehdy, když  $(a, m) \mid b$ .

Věta 5 (Čínská zbytková věta). Necht'  $m_1, m_2 \in \mathbb{N}$ ,  $(m_1, m_2) = 1$ . Pak pro libovolná  $x_1, x_2 \in \mathbb{Z}$  existuje  $x \in \mathbb{Z}$  splňující  $x \equiv x_1 \pmod{m_1}$ ,  $x \equiv x_2 \pmod{m_2}$ .

## Okruh zbytkových tříd modulo $m$

Definice. Pro libovolné  $m \in \mathbb{N}$  a libovolné  $a \in \mathbb{Z}$  definujeme zbytkovou třídu modulo  $m$  obsahující číslo  $a$  předpisem

$$[a]_m = \{b \in \mathbb{Z}; b \equiv a \pmod{m}\},$$

jde tedy o množinu všech celých čísel dávajících stejný zbytek po dělení číslem  $m$  jako číslo  $a$ . Množinu všech těchto tříd značíme

$$\mathbb{Z}/m\mathbb{Z} = \{[a]_m; a \in \mathbb{Z}\}.$$

Z věty 1 plyne, že na  $\mathbb{Z}/m\mathbb{Z}$  lze definovat operace  $+$  a  $\cdot$  pomocí reprezentantů, tj.

$$[a]_m + [b]_m = [a + b]_m, \quad [a]_m \cdot [b]_m = [a \cdot b]_m,$$

a že vůči těmto operacím tvoří  $\mathbb{Z}/m\mathbb{Z}$  komutativní okruh o  $m$  prvcích, který nazýváme okruh zbytkových tříd modulo  $m$ .

## Eulerova funkce $\varphi$

Definice. Je-li  $R$  okruh, označme  $R^\times$  jeho (multiplikativní) grupu jednotek (neboli invertibilních prvků), tj.

$$R^\times = \{a \in R; \exists b \in R : ab = 1\},$$

kde 1 značí jedničku okruhu  $R$ . Charakteristika okruhu  $R$  je nejmenší  $n \in \mathbb{N}$  splňující  $n \cdot 1 = \underbrace{1 + 1 + \dots + 1}_n = 0$  (tj. součet  $n$  kopií  $1 \in R$  je roven  $0 \in R$ ), pokud alespoň jedno takové  $n$  existuje. V opačném případě řekneme, že  $R$  je okruh charakteristiky nula.

Definice. Pro libovolné  $m \in \mathbb{N}$  je  $\varphi(m)$  definováno jako počet čísel z množiny  $\{1, 2, \dots, m\}$ , která jsou nesoudělná s  $m$ . Tato funkce  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  se nazývá Eulerova.

Příklad. Charakteristika okruhu  $\mathbb{Z}/m\mathbb{Z}$  je  $m$ . Podle věty 4 platí

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{[a]_m; a \in \mathbb{Z}, (a, m) = 1\},$$

je tedy  $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$ .



## Vlastnosti Eulerovy funkce $\varphi$

Věta 6. Pro libovolná  $m_1, m_2 \in \mathbb{N}$  taková, že  $(m_1, m_2) = 1$ , platí  $\varphi(m_1 m_2) = \varphi(m_1) \varphi(m_2)$ .

Důkaz. Zobrazení  $\{1, 2, \dots, m_1\} \times \{1, 2, \dots, m_2\} \rightarrow \{1, 2, \dots, m_1 m_2\}$  přiřadí dvojici  $(x_1, x_2) \in \{1, 2, \dots, m_1\} \times \{1, 2, \dots, m_2\}$  číslo  $y \in \{1, 2, \dots, m_1 m_2\}$  splňující  $y \equiv x_1 \pmod{m_1}$ ,  $y \equiv x_2 \pmod{m_2}$  (číslo  $y$  je kongruentní s číslem  $x$  z věty 5 modulo  $m_1 m_2$ ). Toto zobrazení je bijekce a platí  $(y, m_1 m_2) = 1$  právě když  $(x_1, m_1) = 1$  a  $(x_2, m_2) = 1$ .

Věta 7. Pro libovolné  $m \in \mathbb{N}$  platí

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right)$$

kde  $p$  probíhá v součinu všechna prvočísla dělicí  $m$ .

Důkaz. Zřejmé, je-li  $m$  mocninou prvočísla. Pro obecné  $m$  plyne z věty 6 indukcí vzhledem k počtu prvočísel dělicích  $m$ .

## Lagrangeova, Eulerova a malá Fermatova věta

Definice. Necht'  $G$  je grupa,  $a \in G$ . Pokud neexistuje žádné  $n \in \mathbb{N}$  s vlastností  $a^n = 1$ , řekneme, že řád prvku  $a$  je  $\infty$ . V opačném případě nejmenší  $n \in \mathbb{N}$  s touto vlastností se nazývá řád prvku  $a$ . Naproti tomu řádem grupy  $G$  rozumíme počet  $|G|$  jejích prvků (je-li konečná).

Věta 8 (Lagrangeova věta). Je-li  $G$  konečná grupa, pak řád libovolného prvku  $a \in G$  je přirozené číslo, které je dělitelem řádu  $|G|$  grupy  $G$ . Platí tedy  $a^{|G|} = 1$ .

Důsledek (Eulerova věta). Pro libovolná  $m \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ , taková, že  $(a, m) = 1$ , platí

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

Důsledek (malá Fermatova věta). Pro libovolné prvočíslo  $p$  a libovolné  $a \in \mathbb{Z}$  nedělitelné  $p$  platí

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

## Řád čísla $a$ modulo $m$

Věta 9. Necht' jsou  $m \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ , taková, že  $(a, m) = 1$ . Označme

$$e = \min\{n \in \mathbb{N}; a^n \equiv 1 \pmod{m}\}.$$

Pak pro libovolná  $r, s \in \mathbb{N} \cup \{0\}$  platí

$$a^r \equiv a^s \pmod{m}, \quad \text{právě když } r \equiv s \pmod{e}.$$

Důkaz. Lze předpokládat, že  $r > s$ . Vydělme  $r - s$  číslem  $e$  se zbytkem:  $r - s = qe + z$  pro  $q, z \in \mathbb{Z}$ ,  $0 \leq z < e$ . Pak  $a^{r-s} = (a^e)^q \cdot a^z \equiv a^z \pmod{m}$ . Odtud plyne  $a^{r-s} \equiv 1 \pmod{m}$ , právě když  $z = 0$ .

Definice. Číslo  $e$  z předchozí věty se nazývá řád čísla  $a$  modulo  $m$ . Je to vlastně řád prvku  $[a]_m$  v grupě  $(\mathbb{Z}/m\mathbb{Z})^\times$ .

## Konečná tělesa

Věta 10. Charakteristika konečného tělesa je prvočíslo.

Věta 11. Bud'  $R$  konečné těleso charakteristiky  $p$ . Pak počet prvků tělesa  $R$  je mocninou prvočísla  $p$ .

Věta 12. Necht'  $p$  je prvočíslo a  $n \in \mathbb{N}$ . Pak existuje těleso o  $p^n$  prvcích.

Věta 13. Libovolná dvě konečná tělesa o stejném počtu prvků jsou izomorfní.

Věta 14. Bud'  $R$  konečné těleso o  $p^n$  prvcích. Pak  $R^\times$  je cyklická grupa o  $p^n - 1$  prvcích. Každý prvek  $r \in R$  je jednoduchým kořenem polynomu  $x^{p^n} - x \in \mathbb{F}_p[x]$ .

Definice. Pro libovolné prvočíslo  $p$  a libovolné  $n \in \mathbb{N}$  označme  $\mathbb{F}_{p^n}$  těleso o  $p^n$  prvcích.

Poznámka. Pro libovolné prvočíslo  $p$  je  $\mathbb{Z}/p\mathbb{Z}$  těleso, můžeme tedy položit  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ . Avšak  $\mathbb{Z}/p^n\mathbb{Z}$  je těleso pouze pro  $n = 1$ . Proto pro žádné  $n > 1$  nejsou  $\mathbb{F}_{p^n}$  a  $\mathbb{Z}/p^n\mathbb{Z}$  izomorfní!

## Konstrukce konečných těles $\mathbb{F}_{p^n}$ pro prvočíslo $p$ a $n > 1$

Zvolíme libovolný normovaný ireducibilní polynom  $h \in \mathbb{F}_p[x]$  stupně  $n$ . To, že takový polynom existuje pro každé prvočíslo  $p$  a každé přirozené číslo  $n$ , lze dokázat pomocí vět 12 a 14; to, že není podstatné, který z nich vybereme, plyne z věty 13. Pak  $\mathbb{F}_{p^n}$  konstruujeme jako faktorokruh okruhu polynomů  $\mathbb{F}_p[x]$  podle ideálu generovaného polynomem  $h$ . Prvky tohoto faktorokruhu jsou třídy rozkladu množiny polynomů  $\mathbb{F}_p[x]$ . V každé třídě leží právě jeden polynom stupně menšího než  $n$ . Proto, označíme-li  $\alpha$  třídu obsahující polynom  $x$ , lze psát

$$\mathbb{F}_{p^n} = \{g(\alpha); g(x) \in \mathbb{F}_p[x], \text{st } g < n\}.$$

V tělese  $\mathbb{F}_{p^n}$  pak sčítáme a násobíme prvky jako polynomiální výrazy v  $\alpha$  s tím, že po násobení musíme někdy eliminovat vyšší mocniny  $\alpha$ . To děláme tak, že  $\alpha^n$  vyjádříme pomocí nižších mocnin  $\alpha$  využitím toho, že  $h(\alpha) = 0$ .

## Grupa jednotek okruhu zbytkových tříd $(\mathbb{Z}/m\mathbb{Z})^\times$

Je-li  $p$  prvočíslo, je  $\mathbb{Z}/p\mathbb{Z}$  těleso, a tedy podle věty 14 je  $(\mathbb{Z}/p\mathbb{Z})^\times$  grupa cyklická. Pro  $n > 1$  však není  $\mathbb{Z}/p^n\mathbb{Z}$  těleso, a proto nelze věty 14 použít.

Věta 15. Je-li  $p$  liché prvočíslo a  $n \in \mathbb{N}$  libovolné, pak  $(\mathbb{Z}/p^n\mathbb{Z})^\times$  je cyklická grupa.

Poznámka. Pro  $p = 2$  a  $n > 2$  cyklickou grupu nedostáváme: například  $(\mathbb{Z}/8\mathbb{Z})^\times$  je necyklická čtyřprvková grupa.

Definice. Necht'  $p$  je liché prvočíslo,  $n \in \mathbb{N}$ ,  $[g]_{p^n}$  generátor grupy  $(\mathbb{Z}/p^n\mathbb{Z})^\times$ . Pak  $g$  nazýváme **primitivní kořen modulo  $p^n$** .

Poznámka. Libovolné  $g \in \mathbb{Z}$  je primitivní kořen modulo  $p^n$  právě tehdy, když platí: pro každé  $a \in \mathbb{Z}$  nedělitelné  $p$  existuje jediné  $k \in \{1, 2, \dots, (p-1)p^{n-1}\}$  tak, že  $a \equiv g^k \pmod{p^n}$ .

Věta 16 (Wilsonova věta). Necht'  $n \in \mathbb{N}$ ,  $n > 1$ . Pak  $n$  je prvočíslo, právě když platí  $(n-1)! \equiv -1 \pmod{n}$ .