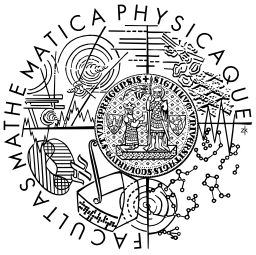

MATEMATICKO-FYZIKÁLNÍ
FAKULTA
Univerzita Karlova

**BAKALÁŘSKÁ PRÁCE**

Jaroslav Kroutil

# Krátké invertibilní prvky v cyklotomických okruzích

Katedra algebry

| | |
|---|---|
| Vedoucí bakalářské práce: | doc. Mgr. et Mgr. Jan Žemlička, Ph.D. |
| Studijní program: | Matematika |
| Studijní obor: | Matematika pro informační technologie |

Praha 2019

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Děkuji panu doc. Mgr. et Mgr. Janu Žemličkovi, Ph.D. za vedení, podnětné rady a jeho čas věnovaný konzultacím k této bakalářské práci. Děkuji dále své rodině a přátelům za podporu.

Název práce: Krátké invertibilní prvky v cyklotomických okruzích

Autor: Jaroslav Kroutil

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Katedra Algebry

Abstrakt: Tato bakalářská práce vychází z odborného článku, který pojednává o kritériu invertibility prvků ve speciálně volených cyklotomických okruzích. V této práci nejprve zopakujeme důležité pojmy a tvrzení z algebry, jež budeme potřebovat. Následně se budeme zabývat existencí nekonečně mnoha prvočísel splňujících podmínky, které využijeme k ireducibilnímu rozkladu cyklotomických polynomů. Na základě těchto polynomů definujeme cyklotomický okruh, ve kterém v závěru práce dokážeme invertibilitu prvků v závislosti na velikosti jejich normy.

Klíčová slova: cyklotomický okruh, mřížka, krátký vektor

Title: Short invertible elements in cyclotomic rings

Author: Jaroslav Kroutil

Department: Department of Algebra

Supervisor: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Department of Algebra

Abstract: This bachelor's thesis is based on an article about the criterion for invertibility of elements in special-chosen cyclotomic rings. In this thesis, we start with defining important terms and statements from algebra that we need. Then we will deal with the existence of infinitely many prime numbers which satisfy conditions that are used for irreducible decomposition of cyclotomic polynomials. Based on this polynomials we define cyclotomic rings and at the end of this thesis we prove invertibility of elements from this rings depending on the size of their norm.

Keywords: cyclotomic ring, lattice, short vector

# Obsah

# Úvod

V současné době dennodenně přicházíme do styku s šifrováním dat, ať už při přihlašování do banky, nebo při běžné komunikaci přes sociální sítě. K tomuto šifrování se hojně využívá kryptografie založená na problému diskrétního logaritmu a faktorizace. Tato kryptografie je běžnými počítači prakticky neprolomitelná a doposud stačilo na technologický vývoj počítačů reagovat pouhým zvětšováním čísel, se kterými kryptografické protokoly pracují. S očekávaným pokrokem v oblasti kvantových počítačů se však tento typ kryptografie zdá být ohrožen. Je proto potřeba nalézt jiný způsob šifrování, který by odolal i útokům vedeným z kvantového počítače. Jedním z možných způsobů se jeví kryptografie založená na mřížkách. K jejímu zavedení a následnému použití v praxi je ale potřeba kromě jiného definovat kryptografické primitivy, šifrovací a dešifrovací funkce a dokázat jejich bezpečnost. Tato formalizace vyžaduje v důkazech práci s okruhy $\mathbb{Z}_p[x]/(x^n + 1)$ v nichž potřebujeme o prvcích rozhodnout, zda jsou invertibilní.

V této práci se budeme zabývat kritériem pro invertibilitu prvků v cyklotomických okruzích (tj. faktorokruhy podle cyklotomických polynomů) v závislosti na jejich délce, kde délku chápeme jako velikost normy daného prvku. Invertibilita prvků okruhu $\mathbb{Z}_p[x]/(x^n + 1)$ je poté důsledkem věty, kterou dokážeme na konci této práce.

Struktura práce bude následující. V první kapitole připomeneme důležité pojmy a tvrzení z algebry, která budeme v této práci potřebovat. Ve druhé kapitole se budeme zabývat existencí nekonečně mnoha prvočísel, která splňují předpoklady, jež využijeme v následující kapitole. V další kapitole zadefinujeme cyklotomické polynomy a dokážeme některé jejich důležité vlastnosti. Na konci této kapitoly určíme, jak přesně vypadá ireducibilní rozklad námi požadovaných cyklotomických polynomů s využitím prvočísel z předcházející kapitoly. V poslední kapitole definujeme cyklotomické okruhy. Na závěr dokážeme invertibilitu prvků těchto okruhů za předpokladu, že mají malou délku.

# 1. Základní definice a věty

V první kapitole připomene základní pojmy a formulujeme potřebná tvrzení z algebry, teorie čísel a komutativních okruhů.

Symbolem $\varphi(n)$, kde $n \in \mathbb{N}$, budeme v celém textu značit *Eulerovou funkci*, jejíž výstupem je počet nesoudělných čísel s $n$.

*Grupou* rozumíme čtveřici $\mathbf{G} = (G, *, ', e)$, kde $G$ je neprázdná nosná množina, $*$ je binární operace, $'$ je unární operace, $e$ je konstanta a je splněno $\forall\, x, y, z \in G$:

$$x * (y * z) = (x * y) * z, \qquad x * e = e * x = x, \qquad x * x' = x' * x = e.$$

Značením $\mathbf{G}^*$ rozumíme grupu $\mathbf{G}$ s nosnou množinou všech invertibilních prvků z $G$, operacemi násobení a invertováním a konstantou 1. *Řádem prvku* $a$ rozumíme nejmenší kladnou mocninu $n$ takovou, že $a^n = e$. Pokud taková mocnina neexistuje, potom $\mathrm{ord}(a) = \infty$. *Řádem grupy* chápeme velikost její nosné množiny.

*Generátorem* cyklické grupy $\mathbf{G}$ je prvek $a \in G$ takový, že $\forall\, g \in G\ \exists\, n \in \mathbb{N} : a^n = g$.

Pro grupu $\mathbf{G}$ a její podgrupu $\mathbf{H}$ se množiny $aH = \{ah : h \in H\}$ nazývají *rozkladové třídy* podle podgrupy $\mathbf{H}$.

Podgrupa $\mathbf{N}$ grupy $\mathbf{G}$ se nazývá normální pokud splňuje

$$\forall a \in G : aH = Ha \quad \Leftrightarrow \quad \forall h \in H\ \forall a \in G : a * h * a' \in H$$

(tato ekvivalence plyne z (Stanovský, 2010, Tvrzení 18.7)). Pomocí normální podgrupy lze definovat *faktorgrupu* jejíž prvky jsou rozkladové třídy (ty jsou zároveň bloky ekvivalence díky úvaze v (Stanovský, 2010, s. 120)).

*Okruhem* rozumíme strukturu jenž je aditivní grupou spolu s operací násobení, která splňuje distributivitu. *Faktorokruhem* pak rozumíme okruh jehož prvky jsou rozkladové třídy podle ideálu. Jedná se opět o bloky ekvivalence. Řekneme, že prvky $a, b$ okruhu $R$ jsou kongruentní modulo $p \in R$, pokud platí $p|a - b$.

Generování hlavního ideálu $I$ prvkem $r$ budeme značit $I = (r)$.

Nyní zformulujeme jednoduché lemma o kongruencích, které dokážeme.

**Lemma 1.** *Nechť* $a, \tilde{a}, b, c \in \mathbb{Z}[x]$, $p \in \mathbb{Z}$, $a \not\equiv 0 \pmod p$. *Jestliže platí* $ab \equiv \tilde{a}c \pmod p$ *a* $a \equiv \tilde{a} \pmod p$, *potom* $b \equiv c \pmod p$.

*Důkaz.* Nejdříve využijeme definice kongruence

$$ab \equiv \tilde{a}c \pmod p \Rightarrow p|\tilde{a}c - ab \Rightarrow \tilde{a}c - ab \equiv 0 \pmod p.$$

Nyní vyjádříme rozdíl následovně $\tilde{a}c - ab = (\tilde{a} - a)c + (c - b)a$. Z předpokladu víme, že $\tilde{a} - a \equiv 0 \pmod p$ a tedy musí platit $(c-b)a \equiv 0 \pmod p$. Z předpokladů dále víme $a \not\equiv 0 \pmod p$ a tedy $c - b \equiv 0 \pmod p \Rightarrow b \equiv c \pmod p$. □

Zavedení pojmů a důkazy následujících vět a tvrzení 2 až 9 lze nalézt v (Stanovský, 2010).

**Věta 2** (Eulerova věta)**.** *Pro každé* $a \in \mathbb{N}$ *a* $n \in \mathbb{N}$ *splňující* $\mathrm{NSD(a, n)} = 1$, *platí*

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

*kde* $\varphi$ *je Eulerova funkce.*

**Věta 3** (Lagrangeova věta)**.** *Nechť* $\boldsymbol{H}$ *je podgrupa konečné grupy* $\boldsymbol{G}$*. Potom* $\mathrm{ord}(\boldsymbol{H}) \mid \mathrm{ord}(\boldsymbol{G})$*.*

**Věta 4** (Čínská zbytková věta)**.** *Mějme* $m_1, \ldots, m_n$ *po dvou nesoudělná přirozená čísla. Označme* $M = m_1 \cdot \ldots \cdot m_n$*. Pak pro libovolná celá čísla* $u_1, \ldots, u_n$ *existuje právě jedno* $x \in \{0, \ldots, M-1\}$*, které řeší soustavu kongruencí*

$$x \equiv u_1 \pmod{m_1}, \ \ldots \ , x \equiv u_n \pmod{m_n}.$$

**Tvrzení 5.** *Podgrupa cyklické grupy je cyklická grupa.*

**Tvrzení 6.** *Průnik podgrup je podgrupa.*

**Lemma 7.** *Buď* $\boldsymbol{G} = \langle a \rangle$ *cyklická grupa. Pak*

1. $\left\langle a^k, a^l \right\rangle = \left\langle a^{\mathrm{NSD(k,l)}} \right\rangle$*;*
2. *je-li* $|\boldsymbol{G}| = n$*, pak* $\left\langle a^k \right\rangle = \left\langle a^{\mathrm{NSD(k,n)}} \right\rangle$*.*

**Věta 8** (1. věta o izomorfismu grup)**.** *Nechť* $\boldsymbol{G}$ *a* $\boldsymbol{H}$ *jsou grupy a* $\gamma : \boldsymbol{G} \to \boldsymbol{H}$ *je homomorfismus grup. Potom*

$$\boldsymbol{G}/\boldsymbol{Ker}(\gamma) \simeq \boldsymbol{Im}(\gamma).$$

**Věta 9** (1. věta o izomorfismu okruhů)**.** *Nechť* $R$ *a* $S$ *jsou okruhy a* $\gamma : R \to S$ *je homomorfismus okruhů. Potom*

$$R/\mathrm{Ker}(\gamma) \simeq \mathrm{Im}(\gamma).$$

**Věta 10** (Dirichletova věta o aritmetické posloupnosti)**.** *Nechť* $h, k \in \mathbb{Z}, k > 0$ *a platí, že* $\mathrm{NSD(h,k)} = 1$*. Potom existuje nekonečně mnoho prvočísel* $p$ *splňujících* $p \equiv h \pmod{k}$*.*

Důkaz této věty lze nalézt v (Apostol, 1976).

V této práci budeme dále potřebovat následující poznatky z teorie Komutativních okruhů. Jestliže $R$ je okruh, potom *R-modul* $M$ je abelovská grupa $\mathbf{M} = (M, +, -, 0)$ spolu se skalárním násobením $r \cdot m \in M$ pro $r \in R, m \in M$ splňující $\forall r, s \in R$ a $\forall m, n \in M$

$$r \cdot (m+n) = r \cdot m + r \cdot n, \quad r \cdot (s \cdot m) = (rs) \cdot m, \quad (r+s) \cdot m = r \cdot m + s \cdot m, \quad 1 \cdot m = m$$

Podmnožina $X$ modulu $F$ se nazývá *volnou bází*, jestliže $X$ generuje $F$ a jestliže pro každý modul $M$ a každý výběr prvků $a_x \in M, x \in X$, existuje homomorfismus $\psi : F \to M$ takový, že $\psi(x) = a_x$ pro každé $x \in X$. Mohutnosti této báze se říká *hodnost* a je jednoznačně určena díky (Drápal, 2006, Tvrzení I.4.7). *Volnou abelovskou grupu* chápeme jako $\mathbb{Z}$-modul s volnou bází.

**Tvrzení 11.** *Mějme* $\mathbb{Z}$ *obor hlavních ideálů, volnou abelovskou grupu* $A = \mathbb{Z}^n$ *a podgrupu* $B$ *grupy* $A$*. Potom existují jednoznačně určené ideály* $I_1 \supseteq I_2 \supseteq \ldots \supseteq I_n$ *okruhu* $\mathbb{Z}$ *takové, že pro některou volnou bázi* $e_1, \ldots, e_n$ *grupy* $A$ *platí*

$$B = I_1 e_1 + \ldots I_n e_n.$$

Toto tvrzení je přeformulováním (Drápal, 2006, Věta I.6.2). Ideály $I_i$ jsou hlavní a proto je můžeme zapsat pro nějaká $r_i$ jako $I_i = (r_i)$. S tímto značením formulujme další tvrzení jenž je přeformulováním (Drápal, 2006, Důsledek I.6.3).

**Tvrzení 12.** *Mějme $\mathbb{Z}$ obor hlavních ideálů, volnou abelovskou grupu $A = \mathbb{Z}^n$ a podgrupu $B$ grupy $A$. Poté lze nalézt volnou bázi $e_1, \ldots, e_n$ grupy $A$ a prvky $r_1, \ldots, r_n \in \mathbb{Z}$ takové, že $r_1 | r_2, \ldots, r_{n-1} | r_n$ a $M = \sum_{i=1}^{n} \mathbb{Z} r_i e_i$. Ať $k$ je nejvyšší takové, že $r_k \neq 0$, kde $0 \leq k \leq n$. Pak $r_1 e_1, \ldots, r_k e_k$ tvoří volnou bázi grupy $B$.*

**Důsledek 13.** *Nechť $A = \mathbb{Z}^n$ je volná abelovská grupa hodnosti $n$ a $B$ je její podgrupa. Nechť $A/B$ je konečná grupa. Potom $B$ je hodnosti $n$.*

*Důkaz.* Díky Tvrzení 12 stačí dokázat $k = n$. Předpokládejme tedy pro spor, že existuje prvek $r_j = 0$. Bez újmy na obecnosti předpokládejme $I_n = (r_n) = (0)$. Díky Tvrzení 11 tím pádem máme $B = I_1 e_1 + \ldots + I_n e_n = (r_1) e_1 + \ldots + (r_{n-1}) e_{n-1} + (0) e_n$. Vezměme si nyní prvek $t_1 e_n \in A$ a $t_2 e_n \in A$, kde $t_1$,$t_2$ jsou různá libovolná přirozená čísla. Ve faktorgrupě $A/B$ těmto dvěma prvkům přísluší různé rozkladové třídy a tedy $A/B$ je nekonečná, což je spor.

□

# 2. Nekonečně mnoho potřebných prvočísel

V hlavní větě této práce (Věta 35) se vyskytuje prvočíslo $p$ s konkrétními vlastnostmi. V této kapitole proto dokážeme existenci nekonečně mnoha těchto prvočísel (Tvrzení 16). Začneme ale nejprve dvěma pomocnými lemmaty, která k důkazu využijeme.

**Lemma 14.** *Nechť* $a \equiv 1 + 2^f \pmod{2^{f+1}}$ *pro* $f \geq 2$. *Potom* $\mathrm{ord}(a)$ *v grupě* $\mathbb{Z}^*_{2^e}$ *pro* $e \geq f$ *je roven* $2^{e-f}$.

Následující důkaz je podrobným rozepsáním a doplněním důkazu (Lyubashevsky a Seiler, 2018, Lemma 2.4).

*Důkaz.* Předpokládáme, že $a \equiv 1 + 2^f \pmod{2^{f+1}}$. To nám implikuje vyjádření $a = 1+2^f+c2^{f+1}$ pro nějaké $c \in \mathbb{Z}$. Tento tvar můžeme dále vytknutím $2^f$ upravit na $1 + 2^f(1 + 2c)$. Číslo $a$ lze tedy zapsat ve tvaru $a = 1 + 2^f k_1$, kde $k_1 = 1 + 2c$ je liché celé číslo.

Indukcí podle $j$ dokážeme, že $a^{2^j} = 1 + 2^{f+j}k_j$, pro $k_j \in \mathbb{Z}$ liché. Pro $j = 1$ platí

$$a^2 = (1 + 2^f k_1)^2 = 1 + 2^{f+1}k_1 + 2^{2f}k_1^2 = 1 + 2^{f+1}(k_1 + 2^{f-1}k_1^2) = 1 + 2^{f+1}k_2,$$

kde $k_2 = k_1 + 2^{f-1}k_1^2 \in \mathbb{Z}$ a jedná se o liché číslo.

V indukčním kroku předpokládejme, že rovnost platí pro $j$. Tedy $a^{2^j} = 1 + 2^{f+j}k_j$, kde $k_j$ je liché číslo. Nyní dokážeme, že poté rovnost platí také pro $j + 1$

$$a^{2^{j+1}} = 1 + 2^{f+j+1}(2^{f+j-1}k_j^2 + k_j).$$

Z indukčního předpokladu víme, že $k_j$ je liché číslo, naopak $2^{f+j-1}k_j^2$ je zjevně sudé a tedy jejich součet je liché číslo. Můžeme proto definovat $k_{j+1} = (2^{f+j-1}k_j^2 + k_j)$ a tedy $a^{2^{j+1}} = 1 + 2^{f+j+1}k_{j+1}$.

Pro volbu $j = e - f$ nyní dostáváme $a^{2^{e-f}} = 1 + 2^e k_{e-f} \equiv 1 \pmod{2^e}$.

Zbývá ověřit, že $\mathrm{ord}(a) = 2^{e-f}$ v grupě $\mathbb{Z}^*_{2^e}$. Nejprve předpokládejme $e = f$. Potom $a^1 \equiv 1 \pmod{2^e}$ a tedy řád $a$ musí být roven 1 (menší být nemůže).

Nyní pro spor nechť $\mathrm{ord}(a) < 2^{e-f}$, kde $e > f$. Označme $m = \mathrm{ord}(a)$. Z Lagrangeovy věty (Věta 3) plyne $m|2^{e-f}$ a tedy existuje $l \in \mathbb{N}$ takové, že $m = 2^l$, kde zároveň $l < e - f \Rightarrow f + l < e$. Pro volbu $j = l$ víme, že platí $a^{2^l} = 1 + 2^{f+l}k_l$. Z předpokladu pro spor máme $a^{2^l} \equiv 1 \pmod{2^e} \Rightarrow 2^e|2^{f+l}k_l$. To je ale spor, neboť $2^e > 2^{f+l}$ a $k_l$ je liché číslo.

□

**Lemma 15.** *Nechť* $p$ *je liché prvočíslo.*

*a) Pokud je* $g$ *generátorem grupy* $\mathbb{Z}^*_p$, *potom buď* $g$ *nebo* $g + p$ *je generátor v grupě* $\mathbb{Z}^*_{p^2}$.

*b) Pokud je* $g$ *generátorem grupy* $\mathbb{Z}^*_{p^2}$, *potom* $g$ *je generátorem grupy* $\mathbb{Z}^*_{p^k}$ *pro* $k \in \mathbb{N}$, $k \geq 2$.

Následující důkaz vychází z důkazu v (Baker, 2011).

*Důkaz.* (a) Nechť $m = \mathrm{ord}(g)$ v grupě $\mathbb{Z}_{p^2}^*$. Řád této grupy je $\varphi(p^2) = p(p-1)$. Z Lagrangeovy věty (Věta 3) plyne $m \mid p(p-1)$. Z $g^m \equiv 1 \pmod{p^2}$ plyne, že také $g^m \equiv 1 \pmod{p}$. Z předpokladu, že $g$ je generátor grupy $\mathbb{Z}_p^*$ plyne $p-1 \mid m$. Dohromady tedy buď $m = p-1$, nebo $m = p(p-1)$.

Uvažujme nyní prvek $g + p \in \mathbb{Z}_{p^2}^*$ (ten opravdu leží v grupě $\mathbb{Z}_{p^2}^*$, jelikož $\mathrm{NSD(g + p, p^2)} = 1$) a označme si $m' = \mathrm{ord}(g+p)$ v grupě $\mathbb{Z}_{p^2}^*$ . Opět z Lagrangeovy věty plyne $m' \mid p(p-1)$. Zároveň $(g+p)^{m'} \equiv 1 \pmod{p^2} \Rightarrow (g+p)^{m'} \equiv 1 \pmod{p}$ a tedy $g^{m'} \equiv 1 \pmod{p}$. O $g$ víme, že je generátor grupy $\mathbb{Z}_p^*$ a tedy z Lagrangeovy věty $p-1 \mid m'$ a proto $m' = p-1$, nebo $m' = p(p-1)$.

Pro spor předpokládejme, že $m = m' = p-1$. Využitím toho, že $m'$ je $\mathrm{ord}(g+p)$ v grupě $\mathbb{Z}_{p^2}^*$ získáváme

$$(g+p)^p = (g+p)(g+p)^{p-1} \equiv g + p \pmod{p^2}.$$

Z binomické věty plyne

$$(g+p)^p = g^p + pg^{p-1}p + \binom{p}{2} g^{p-2}p + \ldots + p^p \equiv g^p \pmod{p^2}.$$

Zároveň také platí

$$g^m = g^{p-1} \equiv 1 \pmod{p^2} \Rightarrow g^p \equiv g \pmod{p^2}.$$

Celkově máme $g + p \equiv g \pmod{p^2} \Rightarrow p \equiv 0 \pmod{p^2}$, což je spor. Tedy buď $m = p(p-1)$ nebo $m' = p(p-1)$, což znamená, že $g$ nebo $g+p$ je generátorem grupy $\mathbb{Z}_{p^2}^*$.

(b) Tuto část dokážeme indukcí podle $k$. Pro $k = 2$ tvrzení předpokládáme. V indukčním kroku předpokládejme, že $g$ je generátorem grupy $\mathbb{Z}_{p^k}^*$. Dokážeme, že poté $g$ je generátorem grupy $\mathbb{Z}_{p^{k+1}}^*$.

Označme $m = \mathrm{ord}(g)$ v grupě $\mathbb{Z}_{p^{k+1}}^*$. Z toho plyne $m | \varphi(p^{k+1}) = (p-1)p^k$, tedy $g^m \equiv 1 \pmod{p^{k+1}}$, z čehož zjevně $g^m \equiv 1 \pmod{p^k}$. To spolu s předpokladem, že $g$ je generátorem grupy $\mathbb{Z}_{p^k}^*$, implikuje $\varphi(p^k) = (p-1)p^{k-1} | m$. Dohromady tedy platí $(p-1)p^{k-1} | m$ a $m | (p-1)p^k$. Díky jednoznačnosti prvočíselných rozkladů jsou jedinými kandidáty $m = (p-1)p^{k-1}$, nebo $m = (p-1)p^k$. Pokud by $m = (p-1)p^{k-1}$ znamenalo by to, že $g$ není generátor grupy $\mathbb{Z}_{p^{k+1}}^*$, protože tato grupa má řád $\varphi(p^{k+1}) = (p-1)p^k$. Stačí tedy dokázat $g^{(p-1)p^{k-1}} \not\equiv 1 \pmod{p^{k+1}}$.

Pro spor předpokládejme $g^{(p-1)p^{k-1}} \equiv 1 \pmod{p^{k+1}}$. Nyní použijeme Eulerovu větu (Věta 2) pro $n = p^{k-1}$ a $a = g$. K tomu potřebujeme ověřit nesoudělnost $g$ a $p^{k-1}$, tedy $g \in \mathbb{Z}_{p^k}^* \Rightarrow \mathrm{NSD(g, p^k)} = 1 \Rightarrow \mathrm{NSD(g, p^{k-1})} = 1$.

Získáváme tak kongruenci $g^{(p-1)p^{k-2}} \equiv 1 \pmod{p^{k-1}}$ a tedy $g^{(p-1)p^{k-2}} = 1 + ap^{k-1}$ pro nějaké $a \in \mathbb{Z}$. Umocněním obou stran na $p$-tou a použitím binomické věty získáme

$$\begin{aligned} g^{(p-1)p^{k-1}} = (1 + ap^{k-1})^p &= 1 + \binom{p}{1} ap^{k-1} + \binom{p}{2} a^2 p^{2k-2} + \cdots + \binom{p}{p} a^p p^{p(k-1)} \\ &\equiv 1 + ap^k \pmod{p^{k+1}}. \end{aligned}$$

Z předpokladu pro spor a binomického rozvoje

$$g^{(p-1)p^{k-1}} \equiv 1 \equiv 1 + ap^k \pmod{p^{k+1}} \Rightarrow ap^k \equiv 0 \pmod{p^{k+1}} \Rightarrow p|a.$$

Kongruenci získanou použitím Eulerovy věty výše tedy můžeme díky $p|a$ dále rozepsat jako

$$g^{(p-1)p^{k-2}} = 1 + ap^{k-1} \equiv 1 \pmod{p^k}.$$

To je ale spor s předpokladem indukce, že $g$ je generátorem grupy $\mathbb{Z}^*_{p^k}$, neboť jsme nalezli menší mocninu než je řád této grupy, pro kterou platí $g^{(p-1)p^{k-2}} \equiv 1 \pmod{p^k}$. Tedy $m \neq (p-1)p^{k-1}$ a proto $m = (p-1)p^k = \mathrm{ord}(g)$ v grupě $\mathbb{Z}^*_{p^{k+1}}$. □

Pro prvočíslo $p = 2$ část (b) v Lemmatu 15 neplatí, neboť pro $\mathbb{Z}^*_{2^2}$ máme generátor prvek $g = 3$, ovšem například pro $k = 3$ grupa $\mathbb{Z}^*_8$ není cyklická.

**Tvrzení 16.** *Nechť $m = \prod_{i=1}^n p_i^{e_i}$, kde $p_i$ jsou po dvou různá prvočísla a $n, e_i \in \mathbb{N}$, $e_i \geq 1$. Nechť $z = \prod_{i=1}^n p_i^{f_i}$, kde $f_i \in \mathbb{N}$ splňuje $1 \leq f_i \leq e_i$. Navíc nechť platí implikace, pokud $8|m$, pak $4|z$. Potom existuje nekonečně mnoho prvočísel $p$, které splňují $p \equiv 1 \pmod{z}$ a $\mathrm{ord}(p) = m/z$ v multiplikativní grupě modulo $m$.*

Následující důkaz je podrobným rozepsáním a doplněním důkazu (Lyubashevsky a Seiler, 2018, Theorem 2.5).

*Důkaz.* Začneme tím, že pro každé prvočíslo $p_i$ nalezneme $a_i$ splňující $a_i \equiv 1 \pmod{p_i^{f_i}}$ a $\mathrm{ord}(a_i) = p_i^{e_i - f_i}$ v grupě $\mathbb{Z}^*_{p_i^{e_i}}$, tedy $a_i^{p_i^{e_i-f_i}} \equiv 1 \pmod{p_i^{e_i}}$. Díky tomu poté nalezneme $a \in \mathbb{Z}$, ne nutně prvočíslo, splňující závěr věty.

Uvažujme nejprve pouze lichá prvočísla $p_i$. Protože grupa $\mathbb{Z}^*_{p_i}$ je cyklická, existuje generátor $g$ této grupy. Z Lemmatu 15 víme, že potom $g$, nebo $g + p_i$ je generátorem grupy $\mathbb{Z}^*_{p_i^k}$ $\forall k \in \mathbb{N}, k \geq 2$. Označme tedy $g'$ tento společný generátor grupy $\mathbb{Z}^*_{p_i^{e_i}}$. V grupě $\mathbb{Z}^*_{p_i^{f_i}}$ platí $(g')^{(p_i-1)p_i^{f_i-1}} \equiv 1 \pmod{p_i^{f_i}}$, díky Eulerově větě (Věta 2), kde $(p_i - 1)p_i^{f_i-1}$ je řád prvku $g'$. Dává proto smysl definovat $a_i = (g')^{(p_i-1)p_i^{f_i-1}} \pmod{p_i^{e_i}}$. Stejnou úvahou získáme řád $(p_i - 1)p_i^{e_i-1}$ generátoru $g'$ v grupě $\mathbb{Z}^*_{p_i^{e_i}}$. Nás nyní zajímá řád prvku $a_i$ v grupě $\mathbb{Z}^*_{p_i^{e_i}}$. Tedy hledáme nejmenší $k_i$ takové, že $a_i^{k_i} = \left((g')^{(p_i-1)f_i-1}\right)^{k_i} \equiv 1 \pmod{p_i^{e_i}}$. Již víme, že řád $g'$ v grupě $\mathbb{Z}^*_{p_i^{e_i}}$ je $(p_i - 1)p_i^{e_i-1}$ a tedy

$$k_i = \frac{(p_i - 1)p_i^{e_i-1}}{(p_i - 1)p_i^{f_i-1}} = p_i^{e_i-f_i}.$$

Nyní uvažujme prvočíslo $p_1 = 2$. Předpokládejme, že $8|m$. Pro exponent $e_1$ v rozkladu $m$ na součin prvočísel tedy platí $e_1 \geq 3$. Ze znění tvrzení díky tomu máme $4|z$ a tedy $f_1 \geq 2$.

Volme v Lemmatu 14 $f = 2$ a $e = e_1$. Tím získáme prvek $5 \equiv 1 + 2^2 \pmod{2^3}$, pro který platí $\mathrm{ord}(5) = 2^{e_1-2}$ v grupě $\mathbb{Z}^*_{2^{e_1}}$. Zároveň můžeme ale také volit $e = f_1$, tím získáme $\mathrm{ord}(5) = 2^{f_1-2}$ v grupě $\mathbb{Z}^*_{2^{f_1}}$. Definujme proto $a_1 = 5^{2^{f_1-2}}$. Řad tohoto prvku v grupě $\mathbb{Z}^*_{2^{e_1}}$ je potom díky stejné úvaze jako v části důkazu pro lichá prvočísla roven

$$k_1 = \frac{(2-1)2^{e_1-1}}{(2-1)2^{f_i-1}} = 2^{e_1-f_1}.$$

Tím pádem pro prvočíslo 2 splňuje prvek $a_1$ pro $e_1 \geq 3$ a $f_1 \geq 2$ stejné podmínky jako prvky $a_i$ pro lichá prvočísla.

Nyní případ, kdy $e_1 = 2$ a tedy $f_1 = 1$ nebo $f_1 = 2$. Začněme s $f_1 = 1$. Lze snadno nahlédnout, že prvek $a_1 = 3^{2^0}$ splňuje požadované podmínky, tedy platí $3 \equiv 1 \pmod 2$ a $\mathrm{ord}(3) = 2^{2-1}$ v grupě $\mathbb{Z}^*_{2^2}$. Pro $f_2 = 2$ budeme volit $a_1 = 1$, protože v tomto případě $a_1 \equiv 1 \pmod{2^2}$ a $\mathrm{ord}(a_1) = 1$ v grupě $\mathbb{Z}^*_{2^2}$.

Jako poslední zbývá případ $e_1 = 1 \Rightarrow f_1 = 1$. V tomto případě stačí volit $a_1 = 1$.

Celkově tedy máme pro všechna prvočísla $p_i$ prvky $a_i$, které splňují podmínky $a_i \equiv 1 \pmod{p_i^{f_i}}$ a $\mathrm{ord}(a_i) = p_i^{e_i - f_i}$.

Nyní můžeme použít Čínskou zbytkovou větu (Věta 4)pro nalezení celého čísla $a$ splňujícího $a \equiv a_i \pmod{p_i^{e_i}}$ $\forall i \in \{1, \ldots, n\}$. Z této volby plyne $a \equiv a_i \pmod{p_i^{f_i}}$. My ale víme $a_i \equiv 1 \pmod{p_i^{f_i}}$ a tedy $a \equiv 1 \pmod{p_i^{f_i}}$. Existují tedy $r_i \in \mathbb{N}$ splňující

$$a - 1 = r_1 p_1^{f_1} = r_2 p_2^{f_2} = \ldots = r_n p_n^{f_n}.$$

Navíc díky vzájemné nesoudělnosti prvočísel můžeme $a - 1$ vydělit $z$ beze zbytku a tedy platí $a - 1 = c \prod_{i=1}^{n} p_i^{f_i} = cz$ pro nějaké $c \in \mathbb{N}$. Tím máme splněno $a \equiv 1 \pmod z$.

Nyní dokážeme $\mathrm{ord}(a) = \frac{m}{z}$ v grupě $\mathbb{Z}^*_m$. Prvek $a$ leží v grupě $\mathbb{Z}^*_m$ díky vztahu $a \equiv a_i \equiv 1 \pmod{p_i^{f_i}} \equiv 1 \pmod{p_i}$ a tedy výraz $\mathrm{ord}(a)$ v grupě $\mathbb{Z}^*_m$ má smysl.

Začneme umocněním $a \equiv a_i \pmod{p_i^{e_i}}$ na $m/z$, tedy

$$a^{m/z} \equiv a_i^{m/z} = a_i^{\prod_{j=1}^{n} p_j^{e_j - f_j}} = \left(a_i^{p_i^{e_i - f_i}}\right)^{\prod_{j=1, j\neq i}^{n} p_j^{e_j - f_j}} \equiv 1 \pmod{p_i^{e_i}} \tag{2.1}$$

Existují tedy $t_i \in \mathbb{N}$ takové, že

$$a^{m/z} - 1 = t_1 p_1^{e_1} = \ldots = t_n p_n^{e_n}$$

a tedy opět díky vzájemné nesoudělnosti prvočísel $p_i$, existuje nějaké $d \in \mathbb{N}$ pro které platí $a^{m/z} - 1 = dm$. Pro ověření, že se skutečně jedná o řád, je potřeba ověřit, že mocnina $\frac{m}{z}$ je nejmenší taková.

Označme $q_i = \mathrm{ord}(a_i) = p_i^{e_i - f_i}$ v grupě $\mathbb{Z}^*_{p_i^{e_i}}$. V rovnosti (2.1) jsme dokázali $a^{m/z} \equiv 1 \pmod{p_i^{e_i}}$ a víme, že $a \equiv a_i \pmod{p_i^{e_i}}$, tedy dohromady $a_i^{m/z} \equiv 1 \pmod{p_i^{e_i}}$. Proto $m/z$ musí obsahovat nějaký násobek $q_i$ pro každé $i = 1, \ldots, n$. Nejmenší takové číslo je $\mathrm{NSN}(\mathrm{q_1}, \ldots, \mathrm{q_n}) = \mathrm{NSN}(\mathrm{p_1^{e_1 - f_1}}, \ldots, \mathrm{p_n^{e_n - f_n}})$, což je právě $m/z$.

Nyní použijeme Dirichletovu věto o aritmetické posloupnosti (Věta 10). Je potřeba ověřit předpoklad, že $\mathrm{NSD(a, m)} = 1$. To ale zjevně platí, neboť $a \in \mathbb{Z}^*_m \Leftrightarrow \mathrm{NSD(a, m)} = 1$. Tedy díky této větě existuje nekonečně mnoho prvočísel $p$ tvaru $a + lm$, kde $l \in \mathbb{N}$. Tato prvočísla zjevně splňují $p \equiv 1 \pmod z$. Pro získání řádu $p$ v grupě $\mathbb{Z}^*_m$ stačí ověřit (díky výpočtu tohoto řádu výše), že $p \equiv a_i \pmod{p_i^{e_i}}$, což ale opět zjevně platí.

□

Důkaz Tvrzení 16 nám dává návod na přesný výpočet prvočísla $p$ ze znění tohoto tvrzení. Pro ilustraci se podívejme na následující příklad.

**Příklad 1.** *Nechť* $m = 540 = 2^2 \cdot 3^3 \cdot 5$ *a* $z = 90 = 2 \cdot 3^2 \cdot 5$. *Určete, jak vypadají prvočísla* $p$, *pro která platí* $p \equiv 1 \pmod{90}$ *a* $\mathrm{ord}(p) = 6$ *v grupě* $\mathbb{Z}^*_{540}$.

*Řešení.* Budeme postupovat přesně podle důkazu Tvrzení 16. Označíme si $m = \prod_{i=1}^{3} p_i^{e_i}$ a $z = \prod_{i=1}^{3} p_i^{f_i}$, kde $p_1 = 2$, $p_2 = 3$, $p_3 = 5$.

Nejprve nalezneme pro každé prvočíslo $p_i$ prvek $a_i$ takový, že $a_i \equiv 1 \pmod{p_i^{f_i}}$ a $\mathrm{ord}(a_i) = p_i^{e_i - f_i}$ v grupě $\mathbb{Z}^*_{p_i^{e_i}}$. Konkrétně tedy chceme

$$\begin{aligned} a_1 &\equiv 1 \pmod 2 \ \text{ a } \ \mathrm{ord}(a_1) = 2 \text{ v grupě } \mathbb{Z}^*_4 \\ a_2 &\equiv 1 \pmod 9 \ \text{ a } \ \mathrm{ord}(a_2) = 3 \text{ v grupě } \mathbb{Z}^*_{27} \\ a_3 &\equiv 1 \pmod 5 \ \text{ a } \ \mathrm{ord}(a_3) = 1 \text{ v grupě } \mathbb{Z}^*_5 \end{aligned}$$

Prvočíslo $p_1$ je sudé a proto dle důkazu můžeme volit $a_1 = 3$ pro $e_1 = 2$ a $f_1 = 1$. Požadavek $\mathrm{ord}(3) = 2$ v grupě $\mathbb{Z}^*_4$ je tímto splněn.

Nyní prvočíslo $p_2$. To je liché, a tedy dle důkazu potřebujeme najít generátor $g$ grupy $\mathbb{Z}^*_3$. Tím je například 2. Potom víme, že buď 2 nebo $2+3$ je generátorem $\mathbb{Z}^*_9$. Postupným mocněním ověříme, že 2 je generátorem grupy $\mathbb{Z}^*_9$ a tedy můžeme pomocí něj definovat prvek $a_2 = 10$, protože $2^6 \equiv 10 \pmod{27}$. Řád 2 v grupě $\mathbb{Z}^*_{27}$ je z důkazu roven $k = 3$ a tedy požadavek na řád prvku $a_2$ je splněn.

Zbývá prvočíslo $p_3$. Požadujeme, aby řád prvku $a_3$ byl v grupě $\mathbb{Z}^*_5$ roven jedné. Takový prvek je pouze neutrální prvek, a tedy $a_3 = 1$.

Nyní použijeme Čínskou zbytkovou větu pro nalezení $a$ splňující

$$a \equiv 3 \pmod 4 \qquad a \equiv 10 \pmod{27} \qquad a \equiv 1 \pmod 5.$$

Toto $a$ je ve tvaru $91 + 540t$, kde $t \in \mathbb{Z}$. Tedy pro $t = 0$ definujme $a = 91$. Tento prvek opravdu splňuje $a \equiv 1 \pmod z$ a $\mathrm{ord}(a) = m/z \pmod m$, konkrétně $91 \equiv 1 \pmod{90}$ a $\mathrm{ord}(91) = 6$ v grupě $Z^*_{540}$.

Číslo 91 není prvočíslo, ovšem díky Dirichletově větě máme nekonečně mnoho prvočísel $p$ ve tvaru $91 + l540$, kde $l \in \mathbb{N}$. Prvočíslo získáme například pro $l \in [1{,}10]$ v případech, kdy $l = 1, 2, 4, 5, 6, 9$.

□

# 3. Cyklotomické polynomy

V této kapitole se seznámíme s cyklotomickými polynomy, dokážeme některé potřebné vlastnosti a první část o ireducibilitě rozkladu cyklotomického polynomu z Věty 35. V celé kapitole uvažujeme všechna tělesa komutativní.

## 3.1 Základní vlastnosti

**Definice 1.** *Je-li $\boldsymbol{K}$ libovolné těleso, pak rozkladové nadtěleso polynomu $x^n - 1 \in \boldsymbol{K}[x]$ nad tělesem $\boldsymbol{K}$ se nazývá* $n$-té cyklotomické těleso *nad $\boldsymbol{K}$ a označuje se $\boldsymbol{K}^{(n)}$. Množina všech kořenů polynomu $x^n - 1$ v $\boldsymbol{K}^{(n)}$ se značí $\boldsymbol{E}^{(n)}$. Prvky $\boldsymbol{E}^{(n)}$ nazýváme* $n$-té odmocniny z jedné.

**Tvrzení 17.** *Nechť $n \in \mathbb{N}$ a $\boldsymbol{K}$ je těleso charakteristiky $p$, kde $p$ je prvočíslo splňující $p \nmid n$. Potom $x^n - 1$ má v $\boldsymbol{K}^{(n)}$ jednoduché kořeny a $\boldsymbol{E}^{(n)}$ je cyklická podgrupa řádu $n$ multiplikativní grupy $\left(\boldsymbol{K}^{(n)}\right)^*$ tělesa $\boldsymbol{K}^{(n)}$.*

Důkaz tohoto tvrzení lze nalézt v (Barto a Tůma, 2008, s. 23).

**Důsledek 18.** *Protože kořeny $x^n - 1$ v $\boldsymbol{K}^{(n)}$ jsou navzájem různé, platí*

$$x^n - 1 = \prod_{\xi \in \boldsymbol{E}^{(n)}} (x - \xi).$$

**Definice 2.** *Nechť $n \in \mathbb{N}$ a $\boldsymbol{K}$ je těleso charakteristiky 0, nebo $p$, kde $p$ je prvočíslo splňující $p \nmid n$. Pak libovolný generátor $\boldsymbol{E}^{(n)}$ (neboli prvek řádu $n$) nazýváme* primitivní $n$-tá odmocnina z 1 *nad $\boldsymbol{K}$.*

**Definice 3.** *Nechť $n \in \mathbb{N}$ a $\boldsymbol{K}$ je těleso charakteristiky 0, nebo $p$, kde $p$ je prvočíslo splňující $p \nmid n$. Pak polynom*

$$Q_n(x) = \prod_{\xi \text{ je primitivní } n\text{-tá odmocnina z } 1} (x - \xi)$$

*se nazývá* $n$-tý cyklotomický polynom *nad $\boldsymbol{K}$.*

Mějme tedy $\xi$ generátor grupy $\mathbf{E}^{(n)}$. Každý prvek $\mathbf{E}^{(n)}$ je roven $\xi^i$ pro $i \in \{0, \ldots, n-1\}$. Berme postupně tyto prvky $\xi^i$. Díky Lemma 7 víme, že pokud platí, $\mathrm{NSD(i, n)} = 1$, potom oba prvky generují stejnou podgrupu (v tomto případě přímo grupu $\mathbf{E}^{(n)}$). Prvků, pro které toto platí, je zjevně z Eulerovy funkce právě $\varphi(n)$. Tedy cyklotomický polynom $Q_n$ můžeme zapsat ve tvaru

$$Q_n(x) = \prod_{i=1}^{\varphi(n)} (x - \xi_i),$$

kde $\xi_1, \ldots, \xi_{\varphi(n)}$ jsou primitivní $n$-té odmocniny z 1 v tělese $\mathbf{K}$.

**Tvrzení 19.** *Nechť $n \in \mathbb{N}$ a $\boldsymbol{K}$ je těleso charakteristiky 0, nebo $p$, kde $p$ je prvočíslo splňující $p \nmid n$. Pak platí*

$$x^n - 1 = \prod_{d \mid n} Q_d(x).$$

*Důkaz.* Díky Tvrzení 17 víme, že existuje $n$ kořenů v grupě $\mathbf{E}^{(n)}$. Zároveň také víme, že existuje prvek $\xi \in \mathbf{E}^{(n)}$ takový, že $\langle \xi \rangle = \mathbf{E}^{(n)}$, a tedy

$$\begin{aligned} x^n - 1 &= \prod_{i=1}^{n} (x - \xi^i) \\ &= \prod_{d|n} \prod_{1 \le i \le n, \mathrm{NSD(i,n)}=d} (x - \xi^i) \\ &= \prod_{d|n} \prod_{1 \le i \le \frac{n}{d}, \mathrm{NSD(i,\frac{n}{d})}=1} (x - \xi^{id}) \\ &= \prod_{d|n} Q_{\frac{n}{d}}(x) = \prod_{d|n} Q_d(x). \end{aligned}$$

□

## 3.2 Cyklotomické polynomy nad tělesem charakteristiky $p$ a $0$

*Značení.* Označme $Q_n^0$ cyklotomický polynom $Q_n$ nad tělesem $\mathbb{Q}$ a $Q_n^p$ cyklotomický polynom $Q_n$ nad tělesem $\mathbb{Z}_p$.

**Důsledek 20.** *Cyklotomický polynom $Q_n^0(x)$ má koeficienty v $\mathbb{Z}$, a tedy $Q_n^0(x) \in \mathbb{Z}[x]$. Cyklotomický polynom $Q_n^p(x)$ má koeficienty v $\mathbb{Z}_p$, a tedy $Q_n^p(x) \in \mathbb{Z}_p[x]$.*

Následující důkaz je inspirován důkazem v (Barto a Tůma, 2008, s. 24).

*Důkaz.* Nejprve dokážeme, že $Q_n^0(x) \in \mathbb{Q}[x]$. Důkaz provedeme indukcí podle $n$. Pro $n = 1$ platí $Q_1^0(x) = x - 1 \in \mathbb{Z}[x]$. Předpokládejme nyní, že tvrzení platí pro všechna $d < n$. Z Tvrzení 19 máme rovnost $x^n - 1 = \prod_{d|n} Q_d^0(x)$ a tedy můžeme vyjádřit $Q_n^0$ následovně

$$Q_n^0(x) = \frac{x^n - 1}{\prod_{d|n, d<n} Q_d^0(x)}.$$

Cyklotomické polynomy $Q_d^0$ jsou z indukčního předpokladu v $\mathbb{Z}[x]$. Jejich součin má vedoucí koeficient 1 a tedy pokud se na zlomek podíváme jako dělení se zbytkem, získáme opět polynom z $\mathbb{Z}[x]$ se zbytkem 0.

Nyní, že $Q_n^p(x) \in \mathbb{Z}_p[x]$. Důkaz provedeme opět indukcí. Pro $n = 1$ zjevně $Q_1^p(x) = x - 1 \in \mathbb{Z}_p[x]$. Nechť pro každé $d < n$ tvrzení platí. Cyklotomický polynom $Q_n^p(x)$ můžeme opět zapsat jako

$$Q_n^p(x) = \frac{x^n - 1}{\prod_{d|n, d<n} Q_d^p(x)},$$

a díky dělení se zbytkem v $\mathbb{Z}_p[x]$ získáváme opět polynom z $\mathbb{Z}_p[x]$.

□

**Důsledek 21.** *Nechť $n \in \mathbb{N}$, $p$ je prvočíslo splňující $p \nmid n$. Poté platí*

$$Q_n^p(x) \equiv Q_n^0(x) \pmod{p}.$$

*Důkaz.* Důkaz provedeme indukcí podle $n$. Pro $n = 1$ tvrzení platí, neboť

$$Q_1^p(x) \equiv x - 1 \equiv Q_1^0(x) \pmod{p}.$$

Předpokládejme nyní, že tvrzení platí pro všechna $d < n$, tedy

$$\prod_{d|n, d<n} Q_d^p(x) \equiv \prod_{d|n, d<n} Q_d^0(x) \pmod{p}.$$

Zjevně platí $x^n - 1 \equiv x^n - 1 \pmod{p}$, a proto díky Tvrzení 19

$$Q_n^p(x) = \prod_{d|n, d<n} Q_d^p(x) \equiv Q_n^0(x) \prod_{d|n, d<n} Q_d^0(x) \pmod{p}.$$

Tím máme splněny předpoklady Lemmatu 1, a tedy $Q_n^p(x) \equiv Q_n^0(x) \pmod{p}$. □

**Věta 22.** *Cyklotomické polynomy nad $\mathbb{Q}$ jsou ireducibilní.*

Důkaz věty lze nalézt v (Weintraub, 2000).

## 3.3 Ireducibilní rozklad nad tělesem charakteristiky $p$

**Definice 4.** Möbiova funkce *je zobrazení $\mu : \mathbb{N} \to \{-1, 0, 1\}$, které je definované*

$$\mu(n) = \begin{cases} 1 & \text{pokud } n = 1 \\ (-1)^k & \text{pokud } n \text{ je součinem } k \text{ různých prvočísel} \\ 0 & \text{pokud } p^2 \mid n \text{ pro nějaké prvočíslo } p \end{cases}$$

**Lemma 23.** *Pro libovolné $n \in \mathbb{N}$ platí*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ pokud } n = 1 \\ 0 \text{ pokud } n > 1 \end{cases}$$

Následující důkaz je podrobnějším sepsáním na základě (Barto a Tůma, 2008, s. 29).

*Důkaz.* Pro $n = 1$ je lemma zřejmé. Nechť tedy $n > 1$ a $n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$ je prvočíselný rozklad. Platí-li $d|n$, potom existují $m_i \in \mathbb{Z}$, $0 \leq m_i \leq k_i$ pro $i \in \{1, \ldots, n\}$ taková, že

$$d = \prod_{i=1}^{l} p_i^{m_i}.$$

Pokud ale existuje $j \in \{1, \ldots, n\}$ takové, že $m_j > 1$, potom $\mu(d) = 0$, a tedy takový dělitel celkový součet neovlivní. Zajímají nás proto pouze dělitelé tvaru

$$d = \prod_{i=1}^{l} p_i^{t_i},$$

kde $t_i \in \{0, 1\}$. Sumu $\sum_{d|n} \mu(d)$ ze znění lemmatu tedy můžeme rozepsat následovně

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{d=p_i} \mu(d) + \sum_{\substack{d=p_i p_j \\ i \neq j}} \mu(d) + \sum_{\substack{d=p_i p_j p_k \\ i \neq j \neq k \neq i}} \mu(d) + \ldots + \mu\left(\prod_{i=1}^{l} p_i\right)$$
$$= 1 - \binom{l}{1} + \binom{l}{2} - \binom{l}{3} + \ldots + (-1)^l \binom{l}{l} = (1-1)^l = 0$$

□

**Věta 24** (Möbiova inverzní formule)**.** *Nechť* $\boldsymbol{G} = (G, \cdot, ^{-1}, 1)$ *je multiplikativní komutativní grupa a* $H, h : \mathbb{N} \to G$ *dvě zobrazení. Mějme*

$$\forall n \in \mathbb{N} : \; H(n) = \prod_{d|n} h(d),$$

*potom*

$$\forall n \in \mathbb{N} : \; h(n) = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)}.$$

Následující důkaz pro multiplikativní grupu vychází z důkazu pro aditivní grupu v (Barto a Tůma, 2008, s. 29).

*Důkaz.*

$$\prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d|n} \left(\prod_{c|\frac{n}{d}} h(c)\right)^{\mu(d)} = \prod_{c|n} \left(\prod_{d|\frac{n}{c}} h(c)\right)^{\mu(d)}$$

První rovnost jsme získali z předpokladu věty a druhou díky pozorování $cd|n \Leftrightarrow c|n \;\&\; d|\frac{n}{c}$. Zafixujme nyní $c$. Potom lze výraz

$$\left(\prod_{d|\frac{n}{c}} h(c)\right)^{\mu(d)}$$

za poslední rovností rozepsat jako

$$h(c)^{\mu(d_1)} \cdot \ldots \cdot h(c)^{\mu(d_m)} = h(c)^{\sum_{d|\frac{n}{c}} \mu(d)},$$

kde pro $d_1, \ldots, d_m$ platí $d_i|\frac{n}{c}$. Z Lemmatu 23 víme, že součet $\sum_{d|\frac{n}{c}} \mu(d) = 0$ kromě případu, kdy $\frac{n}{c} = 1 \Rightarrow n = c$. Tedy jediný součin různý od jedné je součin přes $c = n$, a tedy

$$\prod_{c|n} \left(\prod_{d|\frac{n}{c}} h(c)\right)^{\mu(d)} = h(n).$$

□

**Tvrzení 25.** *Nechť* $n \in \mathbb{N}$ *a* $p$ *prvočíslo, pro nějž platí* $p \nmid n$*. Potom lze cyklotomický polynom* $Q_n^p(x)$ *zapsat ve tvaru*

$$Q_n^p(x) = \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}.$$

*Důkaz.* Díky Tvrzení 19 víme, že $x^n - 1 = \prod_{d|n} Q_n^p(x)$. Definujme funkce $H(n)$ a $h(n)$ z Věty 24 $H(n) = x^n - 1$ a $h(n) = Q_n^p(x)$. Tedy díky této větě získáváme přesně tvrzení důsledku

$$h(n) = \prod_{d|n} H\left(\frac{n}{d}\right)^{\mu(d)} = Q_n^p(x) = \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}.$$

□

V Příkladu 1 jsem určili, jak vypadají prvočísla $p$. Zvolme tedy jedno konkrétní, například $p = 91 + 540 = 631$ a spočítejme následující příklad.

**Příklad 2.** *Určete cyklotomický polynom $Q_{540}^{631}(x)$.*

*Řešení.* K řešení tohoto příkladu využijeme Tvrzení 25. Z něj vidíme, že cyklotomický polynom můžeme zapsat jako součin přes všechny dělitele $d$ čísla $540 = 2^2 \cdot 3^3 \cdot 5$. Ovšem tito dělitelé se zároveň vyskytují jako argument funkce $\mu(d)$. Tato funkce z definice nabývá nenulových hodnot pouze v případech, kdy prvek $d$ neobsahuje ve svém prvočíselném rozkladu nějaké prvočíslo na vyšší mocninu než 1. Zajímají nás proto pouze dělitelé $1, 2, 3, 5, 2 \cdot 3 = 6, 3 \cdot 5 = 15, 2 \cdot 5 = 10, 2 \cdot 3 \cdot 5 = 30$.

$$\begin{aligned} Q_{540}^{631}(x) &= \left(x^{540} - 1\right)^{\mu(1)} \cdot \left(x^{270} - 1\right)^{\mu(2)} \cdot \left(x^{180} - 1\right)^{\mu(3)} \cdot \left(x^{108} - 1\right)^{\mu(5)} \cdot \\ &\quad \cdot \left(x^{90} - 1\right)^{\mu(6)} \cdot \left(x^{36} - 1\right)^{\mu(15)} \cdot \left(x^{54} - 1\right)^{\mu(10)} \cdot \left(x^{18} - 1\right)^{\mu(30)} \\ &= \frac{(x^{540} - 1) \cdot (x^{90} - 1) \cdot (x^{36} - 1) \cdot (x^{54} - 1)}{(x^{270} - 1) \cdot (x^{180} - 1) \cdot (x^{108} - 1) \cdot (x^{18} - 1)} \\ &= x^{144} + x^{126} - x^{90} - x^{72} - x^{54} + x^{18} + 1. \end{aligned}$$

□

**Definice 5.** *Definujeme funkci*

$$\delta(n) = \prod_{p|n,\ p \text{ je prvočíslo}} p.$$

**Důsledek 26.** *Nechť $n \in \mathbb{N}$ a $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ je prvočíselný rozklad. Nechť $p$ je prvočíslo pro nějž platí $p \nmid n$. Potom můžeme cyklotomický polynom $Q_n^p(x)$ přepsat jako*

$$Q_n^p(x) = Q_{\delta(n)}^p\left(x^{\frac{n}{\delta(n)}}\right).$$

*Důkaz.* Cyklotomický polynom $Q_n^p$ přepíšeme pomocí Tvrzení 25

$$Q_n^p(x) = \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}.$$

Všimneme si, že pokud $d|n$ a $d \nmid \delta(n)$, potom je z definice $\mu(d) = 0$, a tedy stačí počítat pouze s děliteli $\delta(n)$

$$\prod_{d|\delta(n)} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)} = \prod_{d|\delta(n)} \left(\left(x^{\frac{n}{\delta(n)}}\right)^{\frac{\delta(n)}{d}} - 1\right)^{\mu(d)} = Q_{\delta(n)}^p\left(x^{\frac{n}{\delta(n)}}\right).$$

□

**Lemma 27.** *Nechť $m = \prod_{i=1}^{n} p_i^{e_i}$, kde $p_i$ jsou po dvou různá prvočísla a $n, e_i \in \mathbb{N}$, $e_i \geq 1$. Nechť $z = \prod_{i=1}^{n} p_i^{f_i}$, kde $f_i \in \mathbb{N}$ splňuje $1 \leq f_i \leq e_i$. Potom*

$$Q_m^p(x) = Q_z^p\left(x^{\frac{m}{z}}\right) \quad a \quad \frac{m}{z} = \frac{\varphi(m)}{\varphi(z)}.$$

Následující důkaz vychází z důkazu (Lyubashevsky a Seiler, 2018, Lemma 2.2).

*Důkaz.* Z definice funkce $\delta$ zjevně platí $\delta(m) = \delta(z)$. Využijeme Důsledku 26, a tedy

$$Q_m^p(x) = Q_{\delta(m)}^p\left(x^{\frac{m}{\delta(m)}}\right) = Q_{\delta(z)}^p\left(x^{\frac{m}{\delta(z)}}\right) = Q_{\delta(z)}^p\left(\left(x^{\frac{m}{z}}\right)^{\frac{z}{\delta(z)}}\right) = Q_z^p\left(x^{\frac{m}{z}}\right).$$

Cyklotomický polynom $Q_m^p(x)$ má stupeň $\varphi(m)$. Cyklotomický polynom $Q_z^p(x^{m/z})$ má stupeň $(m\varphi(z))/z$. Jelikož jsem již dokázali rovnost mezi nimi, musí platit $m/z = \varphi(m)/\varphi(z)$.

□

**Tvrzení 28.** *Nechť $m = \prod_{i=1}^{n} p_i^{e_i}$, kde $p_i$ jsou po dvou různá prvočísla a $n, e_i \in \mathbb{N}$, $e_i \geq 1$. Nechť $z = \prod_{i=1}^{n} p_i^{f_i}$, kde $f_i \in \mathbb{N}$ splňuje $1 \leq f_i \leq e_i$. Pokud je $p$ prvočíslo, pro nějž platí $p \equiv 1 \pmod{z}$ a $\mathrm{ord}(p) = m/z$ v grupě $\mathbb{Z}_m^*$, potom lze vyjádřit $Q_m^p(x)$ jakožto součin*

$$Q_m^p(x) = \prod_{j=1}^{\varphi(z)} x^{m/z} - r_j$$

*pro různá $r_j \in \mathbb{Z}_p^*$, kde $x^{m/z} - r_j$ jsou ireducibilní v $\mathbb{Z}_p[x]$.*

Následující důkaz je podrobným doplněním a rozepsáním důkazu (Lyubashevsky a Seiler, 2018, Theorem 2.3).

*Důkaz.* Díky Lemmatu 27 získáváme

$$Q_m^p(x) = Q_z^p\left(x^{\frac{m}{z}}\right) = \prod_{i=1}^{\varphi(z)} x^{\frac{m}{z}} - r_i,$$

kde $r_1 \ldots, r_{\varphi(z)}$ jsou různé primitivní $z$-té odmocniny z jedné.

Prvky $r_j$ leží v $\mathbb{Z}_p^*$, díky následující úvaze. Z předpokladu $p \equiv 1 \pmod{z}$ víme, že $z|p-1$, a tedy existuje $l = \frac{p-1}{z}$. Grupa $\mathbb{Z}_p^*$ je cyklická s generátorem $g$, proto $g^{zl} \equiv 1 \pmod{p}$, kde $zl$ je řád $g$. Označme si $r = g^l$. Potom $\mathrm{ord}(r) = z$. Máme tedy prvek $r \in \mathbb{Z}_p^*$ řádu $z$, který generuje podgrupu $\mathbf{G}$ řádu $z$, která je cyklická. Všimneme si, že prvek $r^i$, kde $i \in \mathbb{N}$, $i \leq z$ generuje díky Lemmatu 7 grupu $\mathbf{G}$ právě tehdy, když $\mathrm{NSD(i, z)} = 1$. Takových prvků je právě $\varphi(z)$. Celkově tedy máme podgrupu $\mathbf{G}$ grupy $\mathbb{Z}_p^*$, která má $z$ prvků a počet generátorů $\mathbf{G}$ je právě $\varphi(z)$. Nosná množina grupy $\mathbf{G}$ je tedy množinou všech kořenů polynomu $x^z - 1$, a tedy z definice se jedná o $\mathbf{E}^{(z)}$. Označíme-li si generátory grupy $\mathbf{G}$ jako $r_1, \ldots, r_{\varphi(z)}$, jsou tyto prvky primitivní $z$-té odmocniny z jedné v grupě $\mathbb{Z}_p^*$.

Zbývá ověřit, že $x^{m/z} - r_i$ jsou ireducibilní polynomy v $\mathbb{Z}_p[x]$ pro každé $i \in \{1, \ldots, \varphi(z)\}$. Bez újmy na obecnosti předpokládejme $i = 1$. Pro spor předpokládejme, že $x^{m/z} - r_1$ je reducibilní a ireducibilní polynom $f \in \mathbb{Z}_p[x]$ splňuje

$f \mid x^{m/z} - r_1$. Označme $d$ stupeň polynomu $f$. Platí, že $d < \frac{m}{z}$. Polynom $f$ definuje kořenové nadtěleso $\mathbb{Z}_p$ stupně $d$, tedy těleso $\mathbb{F}_{p^d}$, které je izomorfní $\mathbb{Z}_p[x]/(f(x))$. Pro multiplikativní grupu od něj odvozenou platí $\mathrm{ord}(\mathbb{F}^*_{p^d}) = p^d - 1$ , a tedy všechny prvky $t \in \mathbb{Z}^*_{p^d}$ splňují rovnost $t^{p^d-1} - 1 = 0$. To lze rozšířit na všechny prvky $\mathbb{F}_{p^d}$. Platí tedy $\forall t \in \mathbb{F}_{p^d} : t^{p^d} - t = 0$. Rovnost $t^{p^d} - t = 0$ platí díky izomorfismu také v tělese $Z_p[x]/(f(x))$, z čehož plyne $f | x^{p^d} - x$. Díky předpokladu a $\mathrm{ord}(p) = \frac{m}{z}$ v grupě $\mathbb{Z}^*_m$ a $d < \frac{m}{z}$ víme, že $p^d \equiv b \pmod m$, kde $b \not\equiv 1 \pmod m$. Můžeme tedy $p^d$ zapsat ve tvaru $p^d = am + b$ pro nějaké $a \in \mathbb{Z}_m \setminus \{0\}$. Proto platí

$$x^{p^d} - x = x^{am+b} - x = x\left(x^{am+b-1} - 1\right).$$

Polynom $f$ je ireducibilní v $\mathbb{Z}_p[x]$, a tedy jeho kořenem zjevně není 0. Tedy $f | x^{am+b-1} - 1$. Odtud plyne, že kořen polynomu $f$ musí mít nad $\mathbb{Z}_p$ řád, který dělí $am + b - 1$. Zároveň byl polynom $f$ zvolen jako dělitel $x^{m/z} - r_1$, a tedy $f | Q^p_m$. Pro cyklotomický polynom $Q^p_m$ platí

$$Q^p_m(x) = \prod_{i=1}^{\varphi(m)} x - c_i,$$

kde $c_i$ jsou primitivní $m$-té odmocniny z jedné nad tělesem $\mathbb{Z}_p$, a tedy řád kořenů $f$ musí dělit $m$.

Označme v tělese $k$ řád libovolného kořene polynomu $f$. Dohromady pro něj platí $k | m$ a $k | am + b - 1$, kde $b \neq 1$. To je spor, a tedy $x^{m/z} - r_1$ je ireducibilní. □

Pokračujme nyní v příkladech 1 a 2.

**Příklad 3.** *Nechť $m = 540 = 2^2 \cdot 3^3 \cdot 5$, $z = 90 = 2 \cdot 3^2 \cdot 5$ a $p = 631$. Určete ireducibilní rozklad v $\mathbb{Z}_{631}[x]$ následujícího cyklotomického polynomu*

$$Q^0_{540}(x) = x^{144} + x^{126} - x^{90} - x^{72} - x^{54} + x^{18} + 1.$$

*Řešení.* Důkaz Tvrzení 28 nám opět dává návod jak postupovat. Dle důkazu definujme $l = (p-1)/z = 7$. Grupa $\mathbb{Z}^*_{631}$ je cyklická (řádu 630), a tedy existuje její generátor $g$. Ten nalezneme postupným procházením prvků a testováním, zda $g^k \not\equiv 1 \pmod{631}$, kde $k | 630$. Generátorem je například prvek 3.

Označme si tedy $r = g^l = 3^7 \equiv 294 \pmod{631}$. Prvek $r$ generuje 90-ti prvkovou podgrupu $\mathbf{G}$ grupy $\mathbb{Z}^*_{631}$. Nás nyní zajímají generátory této podgrupy. Jedná se totiž o primitivní $z$-té odmocniny z jedné v tělese $\mathbb{Z}^*_{631}$. Prvek $r^i$ je generátorem $\mathbf{G} \Leftrightarrow \mathrm{NSD(i, z)} = 1$, a tedy generátory grupy $\mathbf{G}$ jsou prvky $r^i$, kde $i \in \{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 77, 79, 83, 87, 89\}$. Označme tuto množinu $M$. Platí tedy, že

$$Q^{631}_{540}(x) = \prod_{i \in M} x^6 - 294^i \pmod{631}$$

je ireducibilní rozklad cyklotomického polynomu $Q^{631}_{540}$ v $\mathbb{Z}_{631}[x]$.

□

# 4. Cyklotomické okruhy a invertibilní prvky

## 4.1 Cyklotomické okruhy a jejich aditivní grupy

**Definice 6.** Cyklotomickým okruhem *rozumíme faktorokruh* $\mathbb{Z}[x]/(Q_m^0(x))$ *respektive* $\mathbb{Z}_p[x]/(Q_m^p(x))$*, kde* $(Q_m^0(x))$ *je ideál v okruhu* $\mathbb{Z}[x]$ *generovaný cyklotomickým polynomem* $Q_m^0(x)$ *respektive* $(Q_m^p(x))$ *je ideál v okruhu* $\mathbb{Z}_p[x]$ *generovaný cyklotomickým polynomem* $Q_m^p(x)$*.*

*Značení.* Výrazem $R_m$ budeme značit cyklotomický okruh $\mathbb{Z}[x]/(Q_m^0(x))$. Výrazem $R_{m,p}$ budeme značit cyklotomický okruh $\mathbb{Z}_p[x]/(Q_m^p(x))$.

Připomeňme, že každý okruh lze chápat jako aditivní grupu, pokud se omezíme pouze na operace + a −. Zároveň každý ideál $I$ v okruhu $R$ je zároveň normální podgrupou aditivní grupy od okruhu odvozené.

*Značení.* Aditivní grupu okruhu $R$ budeme značit $R^+$.

Přímým důsledkem je poté následující lemma.

**Lemma 29.** *Cyklotomické okruhy lze chápat jako následující aditivní grupy* $R_m^+ = \mathbb{Z}[x]^+/(Q_m^0)$ *a* $R_{m,p}^+ = \mathbb{Z}_p[x]^+/(Q_m^p)$*.*

Uvažujme nyní $n \in \mathbb{N}$ a aditivní grupu $\mathbb{Z}^n = (\mathbb{Z}^n, +, -, 0^n)$. Její prvky jsou $n$-rozměrné vektory. V $\mathbb{Z}^n$ jsou operace + a − definovány následovně. Nechť $a$,$b \in \mathbb{Z}^n$, $a = (a_0, \ldots, a_{n-1}), b = (b_0, \ldots, b_{n-1})$.

$$\begin{aligned} a + b &= (a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1}) \\ -a &= (-a_0, -a_1, \ldots, -a_{n-1}) \end{aligned}$$

**Lemma 30.** *Pro aditivní grupy odvozené od cyklotomických okruhů platí* $R_m^+ \simeq \mathbb{Z}^{\varphi(m)}$ *a* $R_{m,p}^+ \simeq \mathbb{Z}_p^{\varphi(m)}$*.*

*Důkaz.* Nejprve dokážeme $R_m^+ \simeq \mathbb{Z}^{\varphi(m)}$. Mějme polynom $g = \sum_{i=0}^{n} g_i x^i \in \mathbb{Z}[x]^+$. Uvažujme následující zobrazení

$$\begin{aligned} \psi : \mathbb{Z}[x]^+ &\to \mathbb{Z}^{\varphi(m)} \\ g(x) &\mapsto \left(g_0, \ldots, g_{\varphi(m)-1}\right). \end{aligned}$$

Pokud je $n < \varphi(m) - 1$, definujeme koeficienty $g_{n+1} = g_{n+2} = \ldots = g_{\varphi(m)-1} = 0$. Toto zobrazení je zjevně grupový homomorfismus. Nyní definujme zobrazení $\gamma$ následovně

$$\begin{aligned} \gamma : \mathbb{Z}[x]^+ &\to \mathbb{Z}^{\varphi(m)} \\ f(x) &\mapsto \psi\left(f \pmod{Q_m^0}\right). \end{aligned}$$

Toto zobrazení je grupový homomorfismus, neboť $\forall a$,$b \in \mathbb{Z}[x]^+$ platí

$$\begin{aligned} \gamma(a+b) &= \psi\left(a + b \pmod{Q_m^0}\right) = \psi\left(a \pmod{Q_m^0} + b \pmod{Q_m^0}\right) \\ &= \psi\left(a \pmod{Q_m^0}\right) + \psi\left(b \pmod{Q_m^0}\right) \\ &= \gamma(a) + \gamma(b). \end{aligned}$$

Obraz tohoto homomorfismu je zřejmě na $\mathbb{Z}^{\varphi(m)}$, neboť stačí volit polynomy v $\mathbb{Z}[x]^+$ stupně menšího než $\varphi(m)$. Pro jádro platí $\gamma(a) = 0 \Leftrightarrow a \pmod{Q_m^0} = 0 \Leftrightarrow a \in (Q_m^0)$, a tedy $\mathrm{Ker}(\gamma) = (Q_m^0)$. Celkově proto můžeme použít první větu o izomorfismu grup (Věta 8), a tedy

$$R_m^+ \simeq \mathbb{Z}^{\varphi(m)}.$$

Izomorfismus $R_{m,p}^+ \simeq \mathbb{Z}_p^{\varphi(m)}$ se dokáže obdobně, jen budeme volit homomorfismy $\psi : \mathbb{Z}_p[x]^+ \to \mathbb{Z}_p^{\varphi(m)}$ a $\gamma : \mathbb{Z}_p[x]^+ \to \mathbb{Z}_p^{\varphi(m)}$.

□

**Definice 7.** *Aditivní diskrétní podgrupa $L$ v $\mathbb{R}^n$ se nazývá* mřížka*, pokud existují vektory $b_1, \ldots, b_m \in L$ takové, že*

$$L = \sum_{i=1}^{m} \mathbb{Z} b_i = \left\{ \sum_{i=1}^{m} x_i b_i : x_1, \ldots, x_m \in \mathbb{Z} \right\}.$$

*Vektory $b_1, \ldots, b_m$ se nazývají bází mřížky $L$. Pokud platí $n = m$ mluvíme o mřížce plné hodnosti.*

**Definice 8.** Determinantem *mřížky $L \subseteq \mathbb{Z}^n$ plné hodnosti rozumíme velikost faktorgrupy $\mathbb{Z}^n/L$, tedy* $\det(L) = |\mathbb{Z}^n/L|$.

## 4.2 Invertibilita prvků z cyklotomického okruhu

V celé této kapitole budeme uvažovat čísla $m, z, p$ splňující předpoklady Tvrzení 28.

**Definice 9.** *Nechť $Q_m$ je $m$-tý cyklotomický polynom nad $\mathbb{Z}$ a $\xi_1, \ldots, \xi_{\varphi(m)} \in \mathbb{C}$ jsou kořeny tohoto polynomu. Potom definujeme matici $V_m$ o rozměrech $\varphi(m) \times \varphi(m)$ jako Vardemondovu matici pro prvky $\xi_1, \ldots, \xi_{\varphi(m)}$.*

$$V_m = \begin{pmatrix} 1 & \xi_1 & \xi_1^2 & \cdots & \xi_1^{\varphi(m)-1} \\ 1 & \xi_2 & \xi_2^2 & \cdots & \xi_2^{\varphi(m)-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \xi_{\varphi(m)} & \xi_{\varphi(m)}^2 & \cdots & \xi_{\varphi(m)}^{\varphi(m)-1} \end{pmatrix}$$

**Definice 10.** *Nechť $w \in R_m$ respektive $R_{m,p}$, $w = \sum_{i=0}^{\varphi(m)-1} w_i x^i$, kde $w_i \in \mathbb{Z}$ respektive $\mathbb{Z}_p$. Za předpokladu, že koeficienty $w_i$ budeme chápat jako reálná čísla, definujeme následující dvě normy*

$$\|w\|_\infty = \max_{i \in \{0,\ldots,\varphi(m)-1\}} |w_i| \qquad \|w\| = \sqrt{\sum_{i=0}^{\varphi(m)-1} |w_i|^2}.$$

*Značení.* Velikost nejkratšího nenulového vektoru mřížky $L$ v normě $\|\cdot\|$ budeme značit $\lambda_1(L)$.

*Poznámka.* Nenulový vektor v mřížce zjevně existuje (například bázové vektory). Nalezení nejkratšího nenulového vektoru je ovšem *NP*-těžký problém a doposud není znám žádný algoritmus, který by jej našel pro obecnou hodnost mřížky. Viz. (Stanovský a Barto, 2011, s. 163).

**Lemma 31.** *Pro prvek $w \in \mathbb{R}_{m,p}$ platí $\|w\| \leq \sqrt{\varphi(m)}\,\|w\|_\infty$.*

*Důkaz.* Nechť pro $j \in \{0, \ldots, \varphi(m)-1\}$ platí $\|w\|_\infty = |w_j|$. Potom

$$\|w\| = \sqrt{\sum_{i=0}^{\varphi(m)-1} |w_i|^2} \leq \sqrt{\sum_{i=0}^{\varphi(m)-1} |w_j|^2} = \sqrt{\varphi(m)|w_j|^2} = \sqrt{\varphi(m)}\,\|w\|_\infty .$$

□

**Definice 11.** *Nechť $V_m$ je matice, příslušná cyklotomickému polynomu $Q_m$ nad $\mathbb{Z}$. Potom definujeme $\sigma_1(m)$ následovně*

$$\sigma_1(m) = \max_{u \in \mathbb{C}^{\varphi(m)}} \frac{\|V_m u\|}{\|u\|}.$$

*Poznámka.* Díky (Barto a Tůma, 2019, Tvrzení 10.37) je takto definovaná hodnota $\sigma_1(m)$ největší singulární hodnota matice $V_m$.

**Lemma 32.** *Nechť $L$ je mříží plné hodnosti v $R_m$. Potom platí vztah*

$$\lambda_1(L) \geq \frac{\sqrt{\varphi(m)}}{\sigma_1(m)} \cdot p^{\frac{1}{\varphi(z)}}.$$

Toto lemma je citací (Lyubashevsky a Seiler, 2018, Lemma 2.7). Jeho důkaz vyžaduje hlubší znalosti teorie komutativní algebry, které jsou nad rámec této práce.

**Tvrzení 33.** *Nechť $m = \prod_{i=1}^{n} p_i^{e_i}$, kde $p_i$ jsou po dvou různá prvočísla a $n, e_i \in \mathbb{N}$, $e_i \geq 1$. Nechť $z = \prod_{i=1}^{n} p_i^{f_i}$, kde $f_i \in \mathbb{N}$ splňuje $1 \leq f_i \leq e_i$. Nechť $p$ je prvočíslo, pro nějž platí $p \equiv 1 \pmod{z}$ a $\mathrm{ord}(p) = m/z$ v grupě $\mathbb{Z}_m^*$. Nechť $y \in R_{m,p}$. Pokud*

$$0 < \|y\| < \frac{\sqrt{\varphi(m)}}{\sigma_1(m)} p^{\frac{1}{\varphi(z)}},$$

*potom $y$ je invertibilní v $R_{m,p}$.*

Následující důkaz je podrobným zpracováním důkazu (Lyubashevsky a Seiler, 2018, Lemma 3.1).

*Důkaz.* Díky Tvrzení 28 máme ireducibilní rozklad $Q_m^p = \prod_{j=1}^{\varphi(z)} x^{m/z} - r_j$ v $\mathbb{Z}_p[x]$, kde $r_j \in \mathbb{Z}_p^*$.

Pro spor uvažujme, že $y$ není invertibilní. Potom existuje $\mathrm{NSD}(\mathrm{y}, \mathrm{Q_m^p}) = f$, kde $f \in R_{m,p}$ a $f \neq 1$. Pokud totiž $\mathrm{NSD}(\mathrm{y}, \mathrm{Q_m^p}) = 1$, pak existují Bézoutovy koeficienty (díky tomu, že $\mathbb{Z}_p[x]$ je Eukleidovský obor) $a$,$b \in \mathbb{Z}_p[x]$ takové, že $1 = ay + bQ_m^p$, a tedy $1 \equiv ay \pmod{Q_m^p}$, kde $a$ je inverz. Protože známe ireducibilní rozklad polynomu $Q_m^p$, obsahuje $f$ ve svém ireducibilním rozkladu $x^{m/z} - r_j$

pro alespoň jedno $j$. Zvolme tedy jedno takové $j$ a definujme následující dvě množiny

$$L = \left\{u \in R_m : u \pmod p \equiv 0 \pmod{x^{m/z} - r_j}\right\},$$

$$L_p = \left\{u \in R_{m,p} : u \equiv 0 \pmod{x^{m/z} - r_j}\right\}.$$

$L$ je zjevně aditivní grupa. Součet dvou prvků z $L$ leží v $L$, $0 \in L$ a pokud $f \in L$, potom také $-f \in L$. Navíc $\forall r \in R_m\ \forall u \in L$ platí $ru \in L$, a tedy $L$ je ideál v $R_m$. Obdobně $L_p$ je ideálem v $R_{m,p}$.

Z Lemmatu 30 máme izomorfismus $R_m^+ \simeq \mathbb{Z}^{\varphi(m)}$. Množina $L$ je podgrupou $R_m^+$, a tedy také $Z^{\varphi(m)}$. Nás nyní zajímá $|R_m/L|$. K tomu dokážeme izomorfismus $R_m/L \simeq R_{m,p}/L_p$.

Díky Důsledku 21 je zobrazení $R_m \to R_{m,p}, [a] \mapsto [a \pmod p]$ homomorfismus okruhů, a tedy je následující zobrazení $\psi$ je taktéž homomorfismem.

$$\begin{aligned}\psi : R_m &\to R_{m,p}/L_p \\ [a] &\mapsto [a \pmod p] + L_p\end{aligned}$$

$\psi$ je zjevně na, neboť každý polynom z $R_{m,p}$ leží také v $R_m$. Jádro tohoto homomorfismu je rovno $L$, protože $\forall a \in R_m$ platí $\psi(a) = [0] + L_p \Leftrightarrow a \pmod p \equiv 0 \pmod{x^{m/z} - r_j} \Leftrightarrow a \in L$. Tím máme splněny předpoklady 1. věty o izomorfismu okruhů (Věta 9), a tedy

$$R_m/L \simeq R_{m,p}/L_p \Rightarrow |R_m/L| = |R_{m,p}/L_p| = |R_{m,p}|/|L_p|,$$

kde druhá rovnost plyne z Lagrangeovy věty (Věta 3).

Nyní určíme velikosti $R_{m,p}$ a $L_p$. Díky Lemma 30 platí $R_{m,p}^+ \simeq \mathbb{Z}_p^{\varphi(m)}$, a tedy zjevně $|\mathbb{Z}_p^{\varphi(m)}| = p^{\varphi(m)}$. Pro určení velikosti $L_p$ uvažujme $h \in L_p$. Pro každé $i \in \{1, \ldots, \varphi(z)\}$ víme, že polynomy $x^{m/z} - r_i$ jsou ireducibilní v $\mathbb{Z}_p[x]$. Můžeme proto využít Čínskou zbytkovou větu. Tím získáme právě jeden polynom $h' \in R_{m,p}$ splňující $h' \equiv h \pmod{x^{m/z} - r_i}$ pro každé $i \in \{1, \ldots, \varphi(z)\}$. Díky této jednoznačnosti můžeme určit počet vektorů $h$. Víme, že $h \pmod{x^{m/z} - r_j} \equiv 0$. Zároveň $\forall i \in \{1, \ldots, \varphi(z)\}, i \neq j$ může být $h \pmod{x^{m/z} - r_i}$ kongruentní libovolnému polynomu z $R_{m,p}$ stupně menšího než $\frac{m}{z}$. Těch je $p^{m/z}$, a tedy celkově počet polynomů $h$ je roven $p^{(\varphi(z)-1)m/z}$.

$$|R_m/L| = \frac{|R_{m,p}|}{|L_p|} = \frac{p^{\varphi(m)}}{p^{\frac{m}{z}(\varphi(z)-1)}} = p^{\varphi(m)-\varphi(m)+\frac{m}{z}} = p^{\frac{m}{z}} = p^{\frac{\varphi(m)}{\varphi(z)}}$$

Díky tomu můžeme využít Důsledku 13, a tedy $L$ je mříží plné hodnosti $\varphi(m)$. Máme tedy $\det(L) = p^{m/z}$. Díky Lemmatu 32 platí

$$\lambda_1(L) \geq \frac{\sqrt{\varphi(m)}}{\sigma_1(m)} \cdot p^{\frac{1}{\varphi(z)}}.$$

Díky předpokladu pro spor ze začátku důkazu víme, že $y \equiv 0 \pmod{x^{m/z} - r_j}$, a tedy $y \in L_p$. Zároveň $y$ je nenulový vektor, neboť pro něj platí z předpokladu věty $0 < \|y\| < \frac{\sqrt{\varphi(m)}}{\sigma_1(m)} p^{1/\varphi(z)}$. Celkově tedy

$$0 < \|y\| < \frac{\sqrt{\varphi(m)}}{\sigma_1(m)} p^{\frac{1}{\varphi(z)}} \leq \lambda_1(L),$$

což je spor s minimalitou $\lambda_1(L)$.

□

**Tvrzení 34.** *Nechť $m = \prod_{i=1}^{n} p_i^{e_i}$, kde $p_i$ jsou po dvou různá prvočísla a $n, e_i \in \mathbb{N}$, $e_i \geq 1$. Nechť $z = \prod_{i=1}^{n} p_i^{f_i}$, kde $f_i \in \mathbb{N}$ splňuje $1 \leq f_i \leq e_i$. Nechť $p$ je prvočíslo, pro nějž platí $p \equiv 1 \pmod{z}$ a $\operatorname{ord}(p) = m/z$ v grupě $\mathbb{Z}_m^*$. Nechť $y \in R_{m,p}$, pro nějž platí*

$$y = \sum_{j=0}^{\varphi(m)-1} y_j x^j.$$

*Pro každé $0 \leq i < \varphi(m)/\varphi(z) - 1$ definujeme*

$$y_i' = \sum_{j=0}^{\varphi(z)-1} y_{j\cdot\varphi(m)/\varphi(z)+i} x^j.$$

*Potom pokud existuje $y_i'$ invertibilní v $R_{z,p}$, potom je $y$ invertibilní v $R_{m,p}$.*

Důkaz vychází z úvahy a důkazu z (Lyubashevsky a Seiler, 2018, s. 217, 218)

*Důkaz.* Z Lemmatu 27 máme rovnost

$$\frac{\varphi(m)}{\varphi(z)} = \frac{m}{z}.$$

Díky Tvrzení 28 víme, že cyklotomický polynom $Q_m^p(x)$ se v $R_{m,p}$ rozkládá právě na $\varphi(z)$ ireducibilních členů, které jsou tvaru $x^{m/z} - r_j$. Nechť $y$ leží v $\mathbb{R}_{m,p}$ a je tedy tvaru

$$y = \sum_{i=0}^{\varphi(m)-1} y_i x^i,$$

kde $\forall i \in \{0, \ldots, \varphi(m) - 1\}$ prvky $y_i \in \mathbb{Z}_p$. Pro $0 \leq i < \varphi(m)/\varphi(z) - 1$ máme definováno

$$y_i' = \sum_{j=0}^{\varphi(z)-1} y_{j\cdot\varphi(m)/\varphi(z)+i} x^j.$$

Pomocí takto definovaných $y_i'$ můžeme vyjádřit $y$.

$$\begin{aligned}
\sum_{i=0}^{\varphi(m)/\varphi(z)-1} y_i' \left(x^{\frac{\varphi(m)}{\varphi(z)}}\right) x^i &= \sum_{i=0}^{\varphi(m)/\varphi(z)-1} \sum_{j=0}^{\varphi(z)-1} y_{j\varphi(m)/\varphi(z)+i} \left(x^{\varphi(m)/\varphi(z)}\right)^j x^i \\
&= \sum_{i=0}^{\varphi(m)/\varphi(z)-1} \sum_{j=0}^{\varphi(z)-1} y_{j\varphi(m)/\varphi(z)+i} x^{j\varphi(m)/\varphi(z)+i} \\
&= \sum_{j=0}^{\varphi(m)-1} y_j x^j.
\end{aligned}$$

Díky tomuto vyjádření $y$ pomocí $y_i'$ můžeme snadno spočítat $y \pmod{x^{m/z} - r_j}$, kde $x^{m/z} - r_j$ je ireducibilní dělitel polynomu $Q_m^p(x)$. Tedy

$$y \pmod{x^{\frac{m}{z}} - r_j} = \sum_{i=0}^{m/z-1} y_i'(r_j)\, x^i.$$

Díky úvaze na začátku důkazu Věty 33 víme, že $y$ je invertibilní v $R_{m,p}$ právě tehdy, když $\forall j \in \{0, \ldots, \varphi(z)\}$ platí $y \pmod{x^{m/z} - r_j} \not\equiv 0$. Díky tomu a vyjádření $y \pmod{x^{m/z} - r_j}$ stačí nalézt $i$ takové, že $y_i'(r_j) \pmod p \not\equiv 0 \; \forall j \in \{0, \ldots, \varphi(z)\}$.

Z předpokladu věty máme invertibilitu $y_i'$ v $R_{z,p}$. Podíváme se na vyjdření cyklotomického polynomu $Q_z^p(x)$. Zkombinujeme vyjádření $Q_m^p(x) = \prod_{j=0}^{\varphi(z)} x^{m/z} - r_j$ a vztah $Q_m^p(x) = Q_z^p(x^{m/z})$ z Lemmatu 27

$$Q_m^p\left(x^{\frac{z}{m}}\right) = \prod_{j=0}^{\varphi(z)} \left(x^{\frac{z}{m}}\right)^{\frac{m}{z}} - r_j = \prod_{j=0}^{\varphi(z)} x - r_j = Q_z^p\left(\left(x^{\frac{z}{m}}\right)^{\frac{m}{z}}\right) = Q_z^p(x),$$

a tedy

$$Q_z^p(x) = \prod_{j=0}^{\varphi(z)} x - r_j$$

Máme tedy ireducibilní rozklad $Q_z^p$. Prvek $y_i'$ je opět díky Čínské zbytkové větě invertibilní právě tehdy když $y_i' \pmod{x - r_j} \not\equiv 0 \pmod p \; \forall j \in \{0, \ldots, \varphi(z)\}$. Což je ekvivalentní zápisu $y_i'(r_j) \not\equiv 0 \pmod p$.

Nalezli jsme tedy $i$ takové, že $y_i'(r_j) \pmod p \not\equiv 0 \; \forall j \in \{0, \ldots, \varphi(z)\}$, a tedy $y$ je invertibilní v $R_{m,p}$.

□

## 4.3 Hlavní věta

**Věta 35.** *Nechť $m = \prod_{i=1}^n p_i^{e_i}$, kde $p_i$ jsou po dvou různá prvočísla a $n, e_i \in \mathbb{N}$, $e_i \geq 1$. Nechť $z = \prod_{i=1}^n p_i^{f_i}$, kde $f_i \in \mathbb{N}$ splňuje $1 \leq f_i \leq e_i$. Pokud je $p$ prvočíslo, pro nějž platí $p \equiv 1 \pmod z$ a $\operatorname{ord}(p) = m/z$ v grupě $\mathbb{Z}_m^*$, potom lze vyjádřit $Q_m^p(x)$ jakožto součin*

$$Q_m^p(x) = \prod_{j=1}^{\varphi(z)} x^{m/z} - r_j$$

*pro různá $r_j \in \mathbb{Z}_p^*$, kde $x^{m/z} - r_j$ jsou ireducibilní v $\mathbb{Z}_p[x]$. Každý prvek $y \in R_{m,p}$, který splňuje*

$$0 < \|y\| < \frac{\sqrt{\varphi(m)}}{\sigma_1(m)} p^{\frac{1}{\varphi(z)}}$$

*nebo*

$$0 < \|y\|_\infty < \frac{1}{\sigma_1(z)} p^{\frac{1}{\varphi(z)}}$$

*je invertibilní v $R_{m,p}$.*

Následující důkaz vychází z důkazu (Lyubashevsky a Seiler, 2018, Theorem 1.1)

*Poznámka.* Prvky, jejichž norma splňuje alespoň jednu z nerovností Věty 35 budeme nazývat *krátkými vektory*.

*Důkaz.* Díky Tvrzení 28 máme požadovaný rozklad $Q_m^p(x)$ na ireducibilní polynomy v $\mathbb{Z}_p[x]$. Díky Tvrzení 33 máme dokázanou invertibilitu prvků $y$ splňujícího první vztah ze znění věty. Zbývá dokázat invertibilitu prkvu $y$ splňujícího druhý vztah. Nechť tedy $y$ tento vztah splňuje.

Jak jsme si již rozmysleli v důkazu Tvrzení 34 $Q_z^p(x) = \prod_{j=0}^{\varphi(z)} x - r_j$ je ireducibilní rozklad v $\mathbb{Z}_p[x]$.

Definujme nyní $y_i'$ stejně jako v Tvrzení 34. Jelikož předpokládáme, že $0 < \|y\|_\infty < \frac{1}{\sigma_1(z)} p^{1/\varphi(z)}$, platí také podle Lemma 31 vztah $\|y\| < \frac{\sqrt{\varphi(z)}}{\sigma_1(z)} \cdot p^{1/\varphi(z)}$, a tedy $\forall i \in \{0, \ldots, \varphi(m) - 1\}$ platí

$$\|y_i'\| < \frac{\sqrt{\varphi(z)}}{\sigma_1(z)} \cdot p^{1/\varphi(z)}.$$

$0 < \|y\|_\infty$, a tedy existuje $i$ takové, že $0 < \|y_i'\|$. Zároveň $y_i' \in R_{z,p}$, což díky Tvrzení 33 znamená, že $y_i'$ je invertibilní v $R_{z,p}$, a tedy díky Tvrzení 34 je $y$ invertibilní v $R_{m,p}$.

□

# Závěr

V práci jsme se věnovali podrobnému doplnění a zpracování článku Lyubashevsky a Seiler (2018), jehož hlavním přínosem je pro nás stanovení kritéria invertibility prvků v cyklotomických okruzích. Tohoto doplnění jsme dosáhli s vyjímkou Lemmatu 32 jehož důkaz vyžaduje hlubší znalosti komutativní algebry, které jsou nad rámec této práce.

Dokázané kritérium invertibility lze využít k důkazům některých vlastností kryptografie na mřížkách (jak je zmíněno v motivaci v úvodu). Toto kritérium je ovšem užitečné také z výpočetního hlediska. Stačí nám pouze jednou určit největší singulární hodnoty matic $V_m$ a $V_z$ a poté lze s velmi malou výpočetní složitostí díky Větě 35 o libovolném prvku s malou normou ukázat, že je invertibilní.

Celkově jsme v první kapitole připomněli důležité pojmy z algebry, teorie čísel a komutativních okruhů, které jsme dále hojně používali. Celou druhou kapitolu jsme věnovali otázce existence nekonečně mnoha prvočísel, která byla volena tak, abychom je mohli v další kapitole využít. Na začátku třetí kapitoly jsme se seznámili s cyklotomickými polynomy a dokázali některé jejich důležité vlastnosti. Následně jsme se věnovali vztahu cyklotomických polynomů nad tělesy charakteristiky 0 a prvočíselné charakteristiky. Na to jsme navázali ukázkou ireducibilního rozkladu cyklotomického polynomu se specifickými předpoklady, přičemž jsme využili prvočísla z druhé kapitoly. V poslední kapitole jsme na začátku definovali cyklotomické okruhy a dokázali některé jejich vlastnosti. Poté jsme ukázali, že některé prvky z cyklotomického okruhu mající malou normu, jsou invertibilní. Nakonec jsme dokázali hlavní větu této práce, tedy že prvky cyklotomického okruhu splňující alespoň jednu z nerovností Věty 35, jsou invertibilní.

Naše práce se nevěnuje konkrétnímu využití dokázaného kritéria invertibility prvků v kryptografii, jak bylo zmíněno v motivaci. Toto uplatnění by mohlo být námětem k dalšímu podrobnějšímu zkoumání.

# Seznam použité literatury


Apostol, T. (1976). *Introduction to Analytic Number Theory.* Undergraduate Texts in Mathematics. Springer-Verlag, New York. ISBN 0-387-90163-9. doi: 10.1007/978-1-4757-5579-4. URL https://doi.org/10.1007/978-1-4757-5579-4.

Baker, M. (2011). Notes on Primitive Roots. URL http://people.math.gatech.edu/~mbaker/pdf/primroots.pdf.

Barto, L. a Tůma, J. (2008). Konečná tělesa. URL http://www.karlin.mff.cuni.cz/~barto/student/SkriptaKonTel.pdf.

Barto, L. a Tůma, J. (2019). Lineární algebra. URL http://www.karlin.mff.cuni.cz/~barto/LinAlg/skripta_la6.pdf.

Drápal, A. (2006). Komutativní okruhy. URL http://www.karlin.mff.cuni.cz/~zemlicka/11-12/komalg.pdf.

Lyubashevsky, V. a Seiler, G. (2018). Short, Invertible Elements in Partially Splitting Cyclotomic Rings and Applications to Lattice-Based Zero-Knowledge Proofs. *Advances in Cryptology – EUROCRYPT 2018*, pages 204–224. URL https://doi.org/10.1007/978-3-319-78381-9_8.

Stanovský, D. (2010). *Základy algebry.* MatfyzPress. ISBN 978-80-7378-105-7.

Stanovský, D. a Barto, L. (2011). *Počítačová algebra.* MatfyzPress. ISBN 978-80-7378-340-2.

Weintraub, S. (2000). Several Proofs of the Irreducibility of the Cyclotomic Polynomials. URL https://www.lehigh.edu/~shw2/c-poly/several_proofs.pdf.