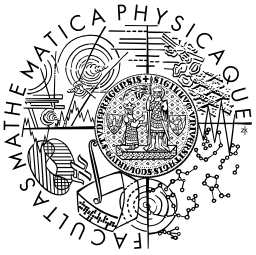

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Filip Miroslav Kucka

RSA v číselných tělesech a na mřížkách

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Vítězslav Kala, Ph.D.

Studijní program: Matematika

Studijní obor: Matematika pro informační technologie

Praha 2023

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

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

Týmto by som rád poďakoval svojmu vedúcemu práce, pánovi docentovi Mgr. Vítězslavu Kalovi Phd. za mimoriadnú trpezlivosť, ochotu, skvelé rady a pripomienky k práci. Rovnako by som chcel poďakovať rodine ktorá ma počas celého štúdia podporovala.

Název práce: RSA v číselných tělesech a na mřížkách

Autor: Filip Miroslav Kucka

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Vítězslav Kala, Ph.D., Katedra algebry

Abstrakt: Táto práca sa zaoberá algoritmom RSA popísaneho na číselných telesách a mriežkach. Konkrétne ide o rozšírenie článku High Dimensional RSA od autorov Zheng a Liu. V práci pomocou viet a príkladov dôkladne popisujeme teóriu potrebnú pre vytvorenie algoritmu, pričom využívame najmä poznatky z algebraickej teórie čísel a teórie mriežok. V druhej kapitole popisujeme RSA iba na číselných telesách, vysvetľujeme jeho problémy a potrebu prechodu do mreižok. V tretej kapitole dôkladne popisujeme vlastnosti ideálových matíc, definujeme vektorové násobenie v $\mathbb{R}^n$ a na konci dokazujeme okruhový izomorfizmus $K \simeq \mathbb{Q}^n \simeq M^*_{\mathbb{Q}}$. Vo štvrtej kapitole sa venujeme dôkazu okruhovému izomorfizmu $\mathbb{Z}[x]/(m_\theta(x)) \simeq \mathcal{O}_K \simeq \mathbb{Z}^n \simeq M^*_{\mathbb{Z}}$, definujeme ideálové mriežky a budujeme potrebnú teóriu nad mriežkami pre RSA. Záverečná kapitola obsahuje kompletný algoritmus aj s názorným príkladom.

Klíčová slova: RSA, číselné telesá, mriežky

Title: RSA in number fields and on lattices

Author: Filip Miroslav Kucka

Department: Department of Algebra

Supervisor: doc. Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: This thesis is focused on the RSA algorithm in number fields and on lattices. Specifically, we extend the work the authors Zheng and Liu in their article High Dimensional RSA. In the thesis we precisely describe all the theory required theory with theorems and examples using mostly Algebraic number theory and lattice theory. In the second chapter, we create the RSA only in number fields, we discuss its problems and the necessity of lattices. In the third chapter, we precisely describe and prove properties of ideal matrices, we define the vector multiplication in $\mathbb{R}^n$ and at the end ve prove the ring isomorphism $K \simeq \mathbb{Q}^n \simeq M^*_{\mathbb{Q}}$. In the fourth chapter, we prove the ring isomorphism $\mathbb{Z}[x]/(m_\theta(x)) \simeq \mathcal{O}_K \simeq \mathbb{Z}^n \simeq M^*_{\mathbb{Z}}$, we define ideal lattices and we create all the required theory over lattices for RSA. The last chapter consists of the complete RSA algorithm in number fields and on lattices and example.

Keywords: RSA, number fields, lattice

Obsah

Úvod

Šifra RSA, pomenovaná po svojich zakladateľoch Rivest, Shamir, Adleman, bola tajne vyvinutá v roku 1973 a verejne predstavená v roku 1977. RSA sa radí medzi asymetrické šifry, čo znamená, že pri šifrovaní a dešifrovaní sa na rozdiel od symetrických šifier používajú rozdielne kľúče. Napriek svojmu veku je RSA vo svojej pôvodnej podobe veľmi obľúbenou a často využívanou šifrou aj v súčasnosti napríklad v elektornickej pošte a pri digitálnom podpise. Svoju popularitu si drží vďaka jednoduchosti a veľkej bezpečnosti. Bezpečnosť RSA závisí hlavne na tom, že sme stále nenašli žiaden efektívny algoritmus na faktorizáciu veľkých čísel známy aj ako *RSA ploblém*.

S postupným vývojom kvantového počítača už nebude problémom faktorizovať veľké čísla v reálnom čase, čím sa RSA algoritmus a ďalšie asymetrické šifry a protokoly stanú nepoužitelné.

Kryptografovia si uvedomujú tento problém a tak sa v posledných rokoch začalo s popisovaním známych asymetrických šifier nad algebraickými štruktúrami ako napríklad číselné telesá a mriežky. Obvzlášť mriežky a teória mriežok v kryptografii bola predmetom intenzívneho výskumu posledné dve desaťročia. Výsledkom tohto výskumu je zatiaľ to, že neexistuje žiaden kvantový algoritmus pre šifry popísané pomocou tórie mriežok.

Samotné RSA nad číselnými telesami však nie je bezpečnejšia varianta od klasického RSA, pretože rozklad na prvoideály sa dá preniesť na rozklad normy daného ideálu/prvku na súčin prvočísel v $\mathbb{Z}$. To už je ale nad rámec tejto práce a pre viac detajlov odporúčame knihu Cohen (1996).

Našou úlohou v tejto práci je podrobne matematicky popísať RSA algoritmus na číselných telesách a mriežkach a ilustrovať ho na príkladoch, pričom hlavnou predlohou tejto práce bol článok Zheng a Liu (2022).

Kapitola 1 obsahuje prehľad základných definícií, tvrdení a viet z algebraickej teórie čísel a teórie mriežok.

V kapitole 2 bude naším cieľom vypracovať RSA algoritmus na číselných telesách, poukázať na jeho problémy a vytvoriť formálny prechod z číselných telies do teórie mriežok. V sekcii 2.2 dokážeme Eulerovu vetu pre ideály a popíšeme RSA, V sekcii 2.3 vysvetlíme problém takto popísaného RSA algoritmu na príklade číselného telesa $K = \mathbb{Q}(\sqrt{D})$ a v sekcii 2.4 definujeme zobrazenie medzi K a $\mathbb{Q}^n$ pre ktoré dokážeme že z každého ideálu v $\mathcal{O}_K$ vytvorí racionálnu mriežku.

Cieľom kapitoly 3 bude vytvoriť štvorcovú maticu H^*, ktorej množina stĺpcových vektorov bude tvoriť bázu mriežky vo výslednom RSA algoritme. V sekcii 3.2 formálne definujeme matice H a H^* aj s operáciou násobenia vektorov a vypracujeme ukážkové príklady. V sekcii 3.3 dokážeme základné vlastnosti H^*. V sekcii 3.4 ukážeme že na maticu $H^*(f)$ (kde $f \in \mathbb{R}^n$ sa môžeme dívať ako na polynom $t_f(H)$ stupňa najviac n, ktorý bude mať v premennej maticu H. To nám potom pomôže v sekcii 3.5 dokázať netriviálne vlastnosti H^*. Na záver v sekcii 3.6 dokážeme okruhový izomorfizmus $K \simeq \mathbb{Q}^n \simeq M^*_{\mathbb{Q}}$.

V kapitole 4 bude cieľom vybudovať potrebnú teóriu na vytvorenie RSA algoritmu na mriežkach. V sekcii 4.2 dokážeme izomorfizmus $\mathbb{Z}[x]/(m_\theta(x)) \simeq \mathcal{O}_K \simeq \mathbb{Z}^n \simeq M^*_{\mathbb{Z}}$. V sekcii 4.3 definujeme pojem *ideálova mriežka* a dokážeme tvrdenie

ktoré nám pre každý ideál v $\mathcal{O}_K$ zobrazí na ideálovú mriežku. V sekcii 4.4 ukážeme že pre obecné $\mathbb{Z}^n/\mathcal{L}$ existuje jednotný tvar množiny reprezentantov ak je báza mriežky $\mathcal{L}$ v Hermitovskej normálnej forme a v sekcii 4.5 dokážeme Eulerovu vetu pre mriežky.

Kapitola 5 obsahuje kompletne spísaný RSA algoritmus na číselných telesách a na mriežkach aj s názorným príkladom na ktorom ukážeme jeho fungovanie.

Náš vlastný prínos v tejto práci spočíva vo vypracovaní dôkazov tvrdení a viet ktoré vypracoval autor sám s pomocou vedúceho práce. Konkrétne ide o lemma 1.1.18 ktoré je v článku Zheng a Liu (2022) okomentované bez dôkazu ako jednoduchá vlastnosť číselných telies. V sekcii 2.3 sme vypracovali vlastný dôkaz o tvaroch všetkých množín reprezentantov pre faktorokruhy v telese $K = \mathbb{Q}(\sqrt{D})$, kdežto Zheng a Liu vo svojom článku dokazujú podobné tvrdenie pre jeden obecný tvar množín reprezentantov ktorý existuje v každom číselnom telese. Ďalej sme dokázali tvrdenie 2.4.2 dokazujúce izomorfizmus $\mathbb{Q}$-vektorových priestorov K a $\mathbb{Q}^n$, a tvrdenie 3.3.1 ktorým dokazujeme základné vastnosti matice H^* a izomorfizmus $\mathbb{R}$-vektorových priestorov $\mathbb{R}^n$ a $M^*_{\mathbb{R}}$ ktoré Zheng a Liu tieto vlastnosti komentujú bez dôkazu ako jednoduché cvičenie.

Lemata 3.4.3, 3.6.1 a 3.3.2 a veta 3.4.4 sú naše vlastné tvrdenia s vlastnými dôkazmi slúžiace ako pomocné tvrdenia pre zložitejšie vety. Veta 3.4.4 dokazuje izomorfizmus okruhov $\mathbb{R}^n(+,\odot)$ a $\mathbb{R}[x]/(m_\theta(x))(+,\cdot)$ pričom ani jedno z tvrdení Zheng a Liu vo svojom článku nespomínajú.

Lema 3.5.1 je na rozdiel od článku Zheng a Liu (2022) spracované podrobne. Špeciálne sme dokázali bod 3 ktorý v Zheng a Liu formálne nedokázali. Rovnako sme formálne dokázali vety 4.2.1, 4.4.2 dokazujúce izomorfizmus okruhov $\mathbb{Z}[x]/(m_\theta(x)) \simeq \mathcal{O}_K \simeq \mathbb{Z}^n \simeq M^*_{\mathbb{Z}}$ a tvar množiny reprezentantov pre obecné $\mathbb{Z}^n/\mathcal{L}$ a lema 4.4.1 ktoré tak isto Zheng a Liu formálne nedokázali.

Formálne sme pritom ešte dokázali dôsledok 4.3.3 a vypracovali príklady 1.1.24, 3.2.3, 3.2.5 a príklad v sekcii 5.2.

Dôkazy zvyšných tvrdení sú, až na malé úpravy, v pôvodnej forme.

1. Základné definície

V tejto kapitole zhrnieme základné definície a vlastnosti známe z algebraickej teórie čísel a teórie mriežok ktoré využijeme v tejto práci.

1.1 Algebraická teória čísel

Vety a definície z tejto sekcie je možné v pozmenenej forme nájsť v knihách Milne (2020), Stewart a Tall (2002) a Narkiewicz (1974).

Definícia 1.1.1. *Nech je S podokruh okruhu T. Prvok $v \in T$ je celistvý nad S, ak je koreňom nejakého monického polynómu v $S[x]$, teda $\exists f \in S[x]$: $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ a $f(v) = 0$.*

Definícia 1.1.2. *Teleso K je číselné teleso, ak je rozšírením konečného stupňa telesa $\mathbb{Q}$. Teda ak K je $\mathbb{Q}-$vektorový priestor konečnej dimenzie, pričom stupeň rozšírenia K je práve dimenzia K ako $\mathbb{Q}$-vektorového priestoru. To že K je telesovým rozšírením telesa $\mathbb{Q}$ budeme značiť $K/\mathbb{Q}$.*

Poznámka 1.1.3. Pre takto definované teleso K potom existuje celistvý prvok $\theta \in K$ taký že $K = \mathbb{Q}(\theta)$ a báza telesa K ako $\mathbb{Q}$-vektorového priestoru je báza $\{1,\theta,\ldots,\theta^{n-1}\}$. Minimálny polynóm pre θ budeme rozumieť polynóm $m_\theta(x) = x^n - m_{n-1}x^{n-1} - \ldots - m_1x - m_0 \in \mathbb{Z}[x]$ a $\{\theta_0, \theta_1, \theta_2, \ldots, \theta_{n-1}\}$ je n rôznych koreňov $m_\theta(x)$.

Od tejto chvíle bude v celej sekcii K označovať obecné číselné teleso pokiaľ nebude uvedené inač.

Veta 1.1.4. *Stewart a Tall (2002, veta 2.4) Nech $K = \mathbb{Q}(\theta)$ je číselné teleso stupňa n nad $\mathbb{Q}$. Potom existuje práve n rozdielných $\mathbb{Q}$-homomorfizmov $\sigma_i : K \to \mathbb{C}$(i = 0, ..., n-1). Prvky $\sigma_i(\theta) = \theta_i$ sú navzájom rozdielne korene minimálneho polynómu pre θ nad $\mathbb{Q}$.*

Definícia 1.1.5. *Okruh všetkých prvkov z K ktoré sú celistvé nad $\mathbb{Z}$ budeme označovať $\mathcal{O}_K$.*

Od tejto chvíle bude v celej sekcii $\mathcal{O}_K$ označovať obecný okruh celistvých prvkov telesa K pokiaľ nebude uvedené inač.

Definícia 1.1.6. *Ak K je číselné teleso, bázu $\alpha_1, \ldots, \alpha_n$ okruhu celistvých prvkov $\mathcal{O}_K$ ako $\mathbb{Z}$-modulu sa nazýva celistvá báza K.*

Veta 1.1.7. *Stewart a Tall (2002, veta 2.16) Pre každé číselné teleso K existuje celistvá báza.*

Obecne potom môžme celistvú bázu K brať ako $\{1,\theta,\ldots,\theta^{n-1}\}$. Zároveň rovnaká veta platí aj pre ideály $\mathcal{O}_K$.

Veta 1.1.8. *Stewart a Tall (2002, veta 5.9) Pre každý ideál $A \neq 0 \leq \mathcal{O}_K$ existuje celistvá báza $\{\alpha_1, \ldots, \alpha_n\}$ kde n je stupeň rozšírenia telesa K.*

Definícia 1.1.9. *Nech $A \leq \mathcal{O}_K$. Množinu reprezentantov S faktorokruhu $\mathcal{O}_K/A$ budeme rozumieť množinu reprezentantov každej ekvivalenčnej triedy $\mathcal{O}_K/A$.*

Veta 1.1.10. *Kala (2022, veta 4.3) Buď $D \neq 0,1$ bezštvorcové a $K = \mathbb{Q}(\sqrt{D})$. Potom*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] \text{ pre } D \equiv 2,3 \pmod 4 \\ \mathbb{Z}[(1+\sqrt{D})/2] \text{ pre } D \equiv 1 \pmod 4. \end{cases}$$

Analogicky $\mathcal{O}_K = \mathbb{Z}[\omega]$ kde $\omega \in \{\sqrt{D}, (1+\sqrt{D})/2\}$ podľa toho či $D \equiv 2,3 \pmod 4$ alebo $D \equiv 1 \pmod 4$.

Pri obecnom rozšírení číselných telies U/T sa nám hodí definovať *stopu* a *normu* prvku $a \in U$. Definícií týchto dvoch pojmov je viacero a všetky sú navzájom ekvivalentné. My však ponúkneme iba dve vyjadrenia stopy a normy ktoré budeme v tejto práci potrebovať.

Základnú definíciu sme se zvolili z Milne (2020, strana 31), ktorá je obecne definovaná nad okruhmi, no v tejto práci nám ju stačí definovať nad telesami.

Definícia 1.1.11. *Nech U/T je rozšírenie číselných telies stupňa n, $a \in U$, $\varphi_{(a)}$: $U \to U$ T-lineárne zobrazenie definované predpisom*

$$\varphi_{(a)}(x) = a \cdot x \quad \text{pre všetky} \quad x \in U.$$

a nech $M_{\varphi_{(a)}}$ matica zobrazenia $\varphi_{(a)}$. Potom definujeme stopu a normu prvku a ako stopu a determinant matice $M_{\varphi_{(a)}}$:

$$Tr(a) = Tr_{U/T}(a) = Tr(M_{\varphi_{(a)}}) \quad a \quad N(a) = N_{U/T}(a) = \det(M_{\varphi_{(a)}}).$$

Veta 1.1.12. *Milne (2020, dôsledok 2.20) Nech U/T je rozšírenie číselných telies stupňa n a nech $\sigma_1, \ldots, \sigma_n$ sú vzájomne odlišné T-homomorfizmy do $\mathbb{C}$. Potom pre stopu a normu prvku $a \in U$ platí*

$$Tr(a) = Tr_{U/T}(a) = \sum_{i=1}^{n} \sigma_i(a) \quad a \quad N(a) = N_{U/T}(a) = \prod_{i=1}^{n} \sigma_i(a).$$

Zároveň pre každé a,$b \in U$ platí:

- $Tr_{U/T}(a+b) = Tr_{U/T}(a) + Tr_{U/T}(b)$
- $N_{U/T}(a \cdot b) = N_{U/T}(a) \cdot N_{U/T}(b)$.

Definícia 1.1.13. *Nech $A \neq 0 \leq \mathcal{O}_K$ je ideál a a,$b \in \mathcal{O}_K$. Povieme že a je kongruentne b modulo A, budeme značiť*

$$a \equiv b \pmod A$$

ak $(a-b) \in A$.

Veta 1.1.14. *Stewart a Tall (2002, veta 5.20) Každý ideál v $\mathcal{O}_K$ je konečne generovaný a to najviac dvoma generátormi.*

Definícia 1.1.15. *Majme I a J ideály z $\mathcal{O}_K$. Povieme že I delí J ak existuje ideál H taký že $I \cdot H = J$*

Veta 1.1.16. *Stewart a Tall (2002, poznámka 5.7) Pre ideály I,$J \in \mathcal{O}_K$ máme $I|J \Leftrightarrow J \subset I$.*

Veta 1.1.17. *Stewart a Tall (2002, dôkaz vety 5.3) Ak je $A \leq \mathcal{O}_K$ nenulový ideál, potom je faktorokruh $\mathcal{O}_K/A$ konečný.*

Počet tried faktorokruhu $\mathcal{O}_K/A$ budeme označovať $N(A)$ a nazývať *norma*. Ak $A = \alpha\mathcal{O}_K$ je hlavný ideál, tak platí $N(A) = |N_{K/\mathbb{Q}}(\alpha)|$ kde $\alpha \in \mathcal{O}_K$. Ďalej platí $N(IJ) = N(I) \cdot N(J)$ kde I,J sú ideály v $\mathcal{O}_K$.

Lemma 1.1.18. *Pre prvoideál $P \neq 0 \leq \mathcal{O}_K$ a prvočíslo $p \in \mathbb{Z}$ sú nasledujúce podmienky ekvivalentné:*

1. $p \in P$
2. $\mathbb{Z} \cap P = p\mathbb{Z}$.

Dôkaz. (2) $\Rightarrow$ (1) Vieme že $\mathbb{Z} \cap P = p\mathbb{Z}$, z toho plynie $p \in P$.

(1) $\Rightarrow$ (2) Vieme že $p \in P$. P je ideál, takže obsahuje aj všetky násobky p a teda $p\mathcal{O}_K \subset P$. Pretože $\mathbb{Z} \subset \mathcal{O}_K$, potom $p\mathbb{Z} \subset \mathcal{O}_K$. Zároveň $p\mathbb{Z} \subset \mathbb{Z}$ a z toho potom dostávame $p\mathbb{Z} \subset \mathbb{Z} \cap P$.

Z toho že $p \in P \Rightarrow \mathbb{Z} \cap P \subset p\mathbb{Z}$. $p\mathbb{Z}$ je maximálny ideál v $\mathbb{Z}$, takže neexistuje žiadné prvočíslo $q \neq 1$,$p \in \mathbb{Z}$ také že $p\mathbb{Z} \subset q\mathbb{Z} \Rightarrow \mathbb{Z} \cap P = p\mathbb{Z}$. □

Veta 1.1.19. *Milne (2020, veta 3.35) Buď K číselné teleso. Potom každý nenulový ideál $A \leq \mathcal{O}_K$ vieme napísať ako*

$$A = P_1^{k_1} \dots P_n^{k_n}$$

kde P_i a P_j sú odlišné prvoideály pre všetky $i \neq j$ a $k_i \in \mathbb{N}$ pre $(1 \leq i \leq n)$, pričom tento rozklad je určený jednoznačne až na poradie.

Veta 1.1.20. *Narkiewicz (1974, veta 1.19) Buď $\mathcal{O}_K/A$ faktorokruh kde A je nenulový ideál, potom počet invertibilných prvkov $\mathcal{O}_K/A$ vieme vyjadriť ako*

$$\varphi(A) = N(A) \prod_{P|A} (1 - (1/N(P))$$

kde súčin vedieme cez všetky prvoideály P ktoré delia ideál A. Navyše ak $\alpha \in \mathcal{O}_K$ a $\alpha\mathcal{O}_K + A = 1$, potom

$$\alpha^{\varphi(A)} \equiv 1 \pmod{A}.$$

Pri obecných ideáloch okruhu $\mathcal{O}_K$ nás budú zaujímať dve čísla a to *stupeň vetvenia* a *stupeň inercie*.

Vieme že faktorokruh $\mathcal{O}_K/P$ kde P je prvoideál je konečný. Navyše je $\mathcal{O}_K/P$ konečné teleso pre ktore platí $\mathbb{Z}/p\mathbb{Z} \subset \mathcal{O}_K/P$. Takže $\mathcal{O}_K/P$ je rozšírenie konečného stupňa telesa $\mathbb{F}_p$.

Definícia 1.1.21. *Nech n je stupeň rozšírenia K a $P \leq \mathcal{O}_K$ je prvoideál, potom stupeň inercie faktorokruhu $\mathcal{O}_K/P$ definujeme ako dimenziu $\mathbb{F}_p$-vektorového priestoru $\mathcal{O}_K/P$ a budeme ho značiť ako*

$$f = dim_{\mathbb{F}_p}(\mathcal{O}_K/P).$$

Potom platí že

$$N(P) = |\mathcal{O}_K/P| = |\mathbb{F}_p^{dim_{\mathbb{F}_p}(\mathcal{O}_K/P)}| = |\mathbb{F}_p|^f = p^f, \quad 1 \leq f \leq n.$$

Definícia 1.1.22. *Nech $p \in \mathbb{Z}$ je prvočíslo a $p\mathcal{O}_K = P_1^{e_1} P_2^{e_2} \dots P_g^{e_g}$ je prvoideálový rozklad. Stupeň vetvenia prvoideálu P_i potom budeme rozumieť číslo e_i.*

Nasledujúca veta nám dáva vzťah medzi číslami e_i a f_i pre $i \in \{1, \dots, g\}$.

Veta 1.1.23. *Milne (2020, veta 3.34) Nech n je stupeň rozšírenia telesa K, $p \in \mathbb{Z}$ je prvočíslo a $p\mathcal{O}_K = P_1^{e_1} P_2^{e_2} \dots P_g^{e_g} \leq \mathcal{O}_K$ je prvoideálový rozklad. Potom*

$$\sum_{i=1}^{g} e_i f_i = n$$

kde e_i udáva stupeň vetvenia P_i a f_i udáva stupeň inercie P_i.

Platnosť tejto vety spolu s definíciami stupňa inercie a vetvenia si ukážeme na nasledujúcom príklade.

Príklad 1.1.24. Majme číselné teleso $\mathbb{Q}[i]$ stupňa $n = 2$, potom $\mathcal{O}_K = \mathbb{Z}[i]$. Prvočíslo 2 sa v $\mathbb{Z}[i]$ dá napísať ako $2 = (1+i)^2$. Potom prvoideálový rozklad ideálu $2\mathbb{Z}[i]$ je $2\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i]$ a teda stupeň vetvenia $e = 2$.

Teraz si vezmeme faktorokruh $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$. Podľa lemma 1.1.18 $2 \in (1+i)\mathbb{Z}[i]$. Teleso $\mathbb{Z}[i]/(1+i)\mathbb{Z}[i]$ obsahuje presne dve triedy a to $[0]$ a $[1]$. Podľa definície 1.1.21 platí že $N(1+i) = 2^f$ a teda $f = 1$. Podľa vety 1.1.23 plati $e \cdot f = 2 \cdot 1 = 2 = n$.

Prvočíslo 3 je prvočiniteľ v $\mathbb{Z}[i]$ a tak stupeň vetvenia $e = 1$. Faktorokruh $\mathbb{Z}[i]/3\mathbb{Z}[i]$ má 9 tried tvaru $\{[u+iv]\}$ kde u,$v \in \{0,1,2\}$. a teda $N(3) = 9 = 3^2$ z čoho plynie že stupeň inercie je 2. Podľa vety 1.1.23 platí $e \cdot f = 1 \cdot 2 = 2 = n$.

Prvočíslo 5 vieme v $\mathbb{Z}[i]$ napísať ako $5 = (2+i)(2-i)$. Potom $5\mathbb{Z}[i] = (2+i)\mathbb{Z}[i] \cdot (2-i)\mathbb{Z}[i]$ je prvoideálovy rozklad, takže $e_1 = e_2 = 1$. Pre $\mathbb{Z}[i]/(2+i)\mathbb{Z}[i]$, $\mathbb{Z}[i]/(2-i)\mathbb{Z}[i]$ platí $N(2+i) = 5$ a $N(2-i) = 5$. Ich triedy sú $\{[0],[1],[2],[3],[4]\}$. Podľa vety 1.1.23 potom platí $\sum_{i=1}^{2} e_i f_i = 1 \cdot 1 + 1 \cdot 1 = 2$.

Na vytvorenie dobre pracujúceho RSA algoritmu, je výhodné ak platí $K = \mathbb{Q}(\theta)$ a $\mathcal{O}_K = \mathbb{Z}[\theta]$ kde

$$\mathbb{Z}[\theta] = \left\{ \sum_{i=0}^{n-1} a_i \theta^i \mid a_i \in \mathbb{Z} \right\}.$$

Potom budeme mať istotu že $K = \mathbb{Q}(\theta)$ a $\mathcal{O}_K$ budú mať rovnakú celistvú bázu $\{1,\theta,\dots,\theta^{n-1}\}$. Ak by sme napriklad vzali číselné teleso $K = \mathbb{Q}(\sqrt{5})$, tak podľa Kala (2022, veta 4.3) je celistvá báza rovná $\{1, (1+\sqrt{5})/2\}$. Bez tejto podmienky by sme si museli celistvú bázu pre každé $\mathcal{O}_K$ vypočítat zvlášť.

Číselné telesá pre ktoré toto platí sú napríklad:

- $K = \mathbb{Q}(\sqrt{D})$ kde $D \in \mathbb{Z}$ nie je štvorec a $D \equiv 2, 3 \pmod 4$.
- $K = \mathbb{Q}(\xi_n)$ kde $\xi_n = e^{2\pi i/n}$ je primitívna n-tá odmocnina z 1.
- $K = \mathbb{Q}(\xi_n + \xi_n^{-1})$ kde $K \subset \mathbb{R}$ je maximálne reálne podteleso $\mathbb{Q}(\xi_n)$.

1.2 Teória mriežok

Vety a definície z tejto sekcie je možné v pozmenenej forme nájsť v prácach Micciancio (2001) a Cohen (1996).

Definícia 1.2.1. *Mriežka je diskrétna aditívná podgrupa $\mathbb{R}^n$, inač povedané, je to podmnožina $\Lambda \subset \mathbb{R}^n$ pre ktorú platí*

1. *Λ je podgrupou $\mathbb{R}^n(+)$.*
2. *$\exists\ \epsilon \geq 0$, také že každé dva body $x \neq y \in \Lambda$ sú vzdialené aspoň o ϵ, teda $\|x - y\| \geq \epsilon$, kde $\|x - y\|$ znamená euklidovskú normu v priestore $\mathbb{R}^n$.*

Definícia 1.2.2. *Nech $b_1, b_2, \ldots, b_k \in \mathbb{R}^n$ sú lineárne nezávislé vektory v $\mathbb{R}^n$. Potom mriežka generovana B= $[b_1, b_2, \ldots, b_k]$ je množina*

$$\mathcal{L}(B) = \{Bx : x \in \mathbb{Z}^k\} = \{\sum_{i=1}^{k} x_i \cdot b_i : x_i \in \mathbb{Z}\}$$

všetkých celočíselných lineárných kombinácií stĺpcových vektorov B. Množina B sa nazýva báza mriežky $\mathcal{L}(B)$. Čísla n a k sa nazývajú dimenzia a hodnosť mriežky. Ak $n = k$ tak povieme že mriežka $\mathcal{L}(B)$ má plnú hodnosť.

V tejto práci budeme pracovať iba s bázami $B \subset \mathbb{R}^n$ ktoré majú plnú hodnosť. Ak $B \subset \mathbb{Q}^n$ potom mriežku $\mathcal{L}(B) \subset \mathbb{Q}^n$ nazveme *racionálna mriežka* a ak $B \subset \mathbb{Z}^n$ potom mriežku $\mathcal{L}(B) \subset \mathbb{Z}^n$ nazveme *celočíselná mriežka.*

Definícia 1.2.3. *Pre ľubovoľnú postupnosť lineárne nezávislých vektorov $B = [b_1, \ldots, b_n] \subset \mathbb{R}^n$ definujeme ortogonálnu postupnosť vektorov $B^* = [b_1^*, \ldots, b_n^*] \subset \mathbb{R}^n$ iteratívnym vzorcom*

$$b_i^* = b_i - \sum_{j<i} \mu_{ij} b_j^* \text{ kde } \mu_{ij} = \langle b_i, b_j^* \rangle / \langle b_j^*, b_j^* \rangle.$$

Definícia 1.2.4. *Majme bázu $B = [b_1, b_2, \ldots, b_n] \subset \mathbb{R}^n$, potom rovnobežnosten asociovaný s B definujeme ako množinu bodov*

$$\mathcal{P}(B) = B[0, 1)^n = \{\sum_{i=1}^{n} x_i \cdot b_i : 0 \leq x_i < 1\}.$$

Poznámka 1.2.5. Micciancio (2010, sekcia 4.1) Nech $\mathcal{L} = \mathcal{L}(B) \subset \mathbb{R}^n$ je mriežka $B \subset \mathbb{R}^n$ je báza a B^* je ortogonálna báza z B. Vieme že $\mathcal{P}(B^*)$ je polootvorená množina. Všimnime si, že môžeme pomocou $\{\mathcal{P}(B^*) + v, v \in \mathcal{L}(B)\}$ pokryť celý priestor $\mathbb{R}^n$. Špeciálne pre každý vektor $x \in \mathbb{R}^n$ existuje jednoznačne určený vektor $v \in \mathcal{L}(B)$ taký že $x \in v + \mathcal{P}(B^*)$.

Definícia 1.2.6. *Nech $B = [b_1, b_2, \ldots, b_k] \subset \mathbb{R}^n$ je báza $\mathcal{L}(B)$. Potom determinant* $\det(\mathcal{L}(B))$ *je definovaný ako n-dimenzionálny objem rovnobežnostenu asociovaného s B*

$$\det(\mathcal{L}(B)) = vol(\mathcal{P}(B)) = \prod_{i=1}^{k} ||b_i^*||.$$

Navyše ak B má plnú hodnosť, potom $\det(\mathcal{L}(B)) = \det(B)$.

Definícia 1.2.7. *Nech $\mathcal{L}(B) \subset \mathbb{R}^n$ je mriežka a u,v $\in \mathbb{R}^n$. Povieme že u je kongruentne v modulo $\mathcal{L}(B)$, budeme značiť*

$$u \equiv v \pmod{\mathcal{L}(B)}$$

ak $(u - v) \in \mathcal{L}(B)$.

Definícia 1.2.8. *Regulárna matica $H = (h_{ij}) \in \mathbb{Z}^{n\times n}$ je v Hermitovskej normálnej forme ak*

1. *H je horná trojuholníková matica.*
2. *Pre každé $1 \leq i \leq n$ platí $h_{ii} > 0$.*
3. *Pre každé $i \leq j$ platí $0 \leq h_{ij} < h_{ii}$.*

Definícia 1.2.9. *Celočíselná štvorcová matica M rádu n ktorej determinant je ± 1 na nazýva unimodulárna matica. Grupu unimodulárnych matic rádu n budeme značiť $GL_n(\mathbb{Z})$.*

Veta 1.2.10. *Micciancio (2001, str. 2, veta 1) Nech B a C sú dve rozdielne bázy. Potom $\mathcal{L}(B) = \mathcal{L}(C)$ práve vtedy ak existuje matica $U \in GL_n(\mathbb{Z})$ taká že $B = CU$.*

Veta 1.2.11. *Cohen (1996, str. 67, veta 2.4.3) Nech $A \in \mathbb{Z}^{n\times n}$ je regulárna matica. Potom existuje jednoznačne určená matica $B \in \mathbb{Z}^{n\times n}$ v HNF pre ktorú platí $B = AU$, kde $U \in GL_n(\mathbb{Z})$.*

2. RSA v číselných telesách

2.1 Úvod

V tejto kapitole si popíšeme klasický RSA algoritmus pomocou číselných telies, popíšeme problém výberu množiny reprezentantov v číselných telesách a ukážeme vzťah medzi číselnými telesami a mriežkami.

Pripomeňme že K označuje číselné teleso, $\mathcal{O}_K \subset K$ je okruh celistvých prvkov, $N(A)$ označuje normu a $\varphi(A)$ označuje počet invertibilných prvkov faktorokruhu $\mathcal{O}_K/A$. V celej tejto kapitole bude platiť že ideál $A = PQ$ kde P,$Q \leq \mathcal{O}_K$ budú dva odlišné prvoideály. Zároveň budeme používať značenie (G, H) = NSD(G, H).

2.2 RSA a Eulerova veta pre ideály

V tejto časti si dokážeme vetu ktorá nám pomôže zobecniť RSA nad ľubovoľným číselným telesom K.

Naším cieľom je napísať RSA algoritmus v číselných telesách fungujúci na rovnakom princípe ako klasické RSA. Na to si budeme musieť dokázať platnosť Eulerovej vety pre ideály číselných telies, teda že pre ľubovoľné $\alpha \in \mathcal{O}_K$, $k \geq 0$ a ideal $A = PQ \in \mathcal{O}_K$. platí

$$\alpha^{k\varphi(A)+1} \equiv \alpha \pmod{A}.$$

Toto si dokážeme v nasledujúcej vete.

Veta 2.2.1. *Nech $A = PQ \leq \mathcal{O}_K$, potom pre každé $\alpha \in \mathcal{O}_K$ a $k \geq 0$ platí*

$$\alpha^{k\varphi(A)+1} \equiv \alpha \pmod{A}. \tag{2.1}$$

Dôkaz. Nech $\alpha \in \mathcal{O}_K$. Vetu chceme dokázať pre každé α, takže musíme vyriešiť prípady kedy $\alpha \notin A$, $\alpha \in A$ a kedy $\alpha \in P$ alebo $\alpha \in Q$.

Ak $\alpha \notin A$ potom $(\alpha\mathcal{O}_K, A) = 1$, a (2.1) plynie okamžite z vety 1.1.20. Ak $\alpha \in A$, potom $\alpha\mathcal{O}_K \subset A$ a $(\alpha\mathcal{O}_K, A) = A$. Z toho (2.1) plynie triviálne. Ostáva už len vyriešiť $(\alpha\mathcal{O}_K, A) = P$ a $(\alpha\mathcal{O}_K, A) = Q$, teda prípady kedy $\alpha \in P$ alebo $\alpha \in Q$.

BÚNO uvažujme $(\alpha\mathcal{O}_K, A) = P$, druhý prípad sa dokáže analogicky. Z toho že $(\alpha\mathcal{O}_K, A) = P$ plynie že P je najmenší spoločný deliteľ ideálov $\alpha\mathcal{O}_K$ a A. Takže $P \mid \alpha\mathcal{O}_K$ a zároveň $P \mid A$. Tým pádom Q nedelí ideál $\alpha\mathcal{O}_K$ z čoho plynie $(\alpha\mathcal{O}_K, Q) = 1$. Z vety 1.1.20 potom platí

$$\alpha^{\varphi(Q)} \equiv 1 \pmod{Q}.$$

Z čoho potom plynie

$$\alpha^{k\varphi(Q)} \equiv 1 \pmod{Q}, \quad \forall k \in \mathbb{Z}, \quad k \geq 0.$$

Takže $\alpha^{k\varphi(Q)} \in 1 + Q$. Z toho potom existuje $\beta \in Q$ také že

$$\alpha^{k\varphi(Q)} = 1 + \beta$$

Z toho potom platí

$$\alpha^{k\varphi(A)+1} = \alpha + \alpha\beta \quad \Rightarrow \quad \alpha^{k\varphi(A)+1} \equiv \alpha \pmod{A}$$

pretože $\alpha \in P$ a $\beta \in Q \Rightarrow \alpha\beta \in A$. □

Vďaka tejto vete máme istotu dešifrovania a nič nám nebráni prepísať klasické RSA do jazyka číselných telies.

Parametre	$n \geq 1$ je prirodzené číslo, $K/\mathbb{Q}$ je číselné teleso stupňa n, $\mathcal{O}_K \subset K$ okruh celistvých prvkov nad K. P a Q sú dva prvoideály $\mathcal{O}_K$, $A = PQ$, $\mathcal{O}_K/A$, je faktorokruh, S je množina reprezentantov $\mathcal{O}_K/A$, $\varphi(A)$ je počet invertibilných prvkov $\mathcal{O}_K/A$, $1 \leq e,d \leq \varphi(A)$ sú prirodzené čísla také že $ed \equiv 1 \pmod{\varphi(A)}$.
Verejné kľúče	Ideál A a prirodzené číslo e.
Súkromné kľúče	Prvoideály P, Q a prirodzené číslo d.
Šifrovanie	Pre ľubovoľnú správu $\alpha \in S$ a pre šifrovaný text c platí $c \equiv \alpha^e \pmod{A}$.
Dešifrovanie	$c^d \equiv \alpha^{de} \equiv \alpha \pmod{A}$.

Tabuľka 2.1: RSA v číselných telesách

Z tabuľky 2.1 ľahko nahliadneme že ak $n = 1$, tak tabuľka vyššie popisuje klasické RSA.

Problémom tohto algoritmu je, že na rozdiel od klasického RSA, množina reprezentantov S nemá jednotný tvar pre obecný faktorokruh $\mathcal{O}_K/A$. Takže pre každý $\mathcal{O}_K/A$ si musíme S spočítať nanovo.

Tomuto problému sa budeme venovať v ďalšej sekcii.

2.3 Množina reprezentantov S

V tejto sekcii popíšeme všetky množiny reprezentantov číselného telesa $K = \mathbb{Q}(\sqrt{D})$ kde $D \neq 0, 1$ nie je štvorec a ukážeme si vhodnú množinu reprezentantov S ktorá existuje v každom telese K.

V celej tejto sekcii bude $K = \mathbb{Q}(\sqrt{D})$ kde $D \neq 0, 1$ nie je štvorec a $\mathcal{O}_K = \mathbb{Z}[\omega]$ kde $\omega \in \{\sqrt{D}, (1 + \sqrt{D})/2\}$ rovnako ako vo vete 1.1.10. Zároveň pripomenieme že $A = PQ \leq \mathcal{O}_K$ je prvoideálový rozklad.

V obecnom RSA je množinu reprezentantov $\mathbb{Z}/N\mathbb{Z} = \{0, \ldots, N-1\}$, čo je zároveň jediná možnosť. Pre RSA v číselných telesách miesto $\mathbb{Z}/N\mathbb{Z}$ musíme brať $\mathcal{O}_K/A$, pričom množina reprezentantov nie je daná jednoznačne, ale závisí na prvoideáloch A.

V nasledujúcej vete dokážeme že v prípade $K = \mathbb{Q}(\sqrt{D})$ existujú tri odlišné množiny reprezentantov pre obecný faktorokruh $\mathcal{O}_K/A$. Tretí bod nasledujúcej vety ostáva bez dôkazu, pretože ide o zložitejšie tvrdenie.

Veta 2.3.1. *Buď $D \neq 0{,}1 \in \mathbb{Z}$ bezštvorcové, $K = \mathbb{Q}(\sqrt{D})$ a nech $\{1, \omega\} \subset \mathcal{O}_K = \mathbb{Z}[\omega]$ je celistvá báza K kde ω rovnaké ako vo vete 1.1.10. Nech p,$q \in \mathbb{Z}$ sú rozdielne prvočísla, $A = PQ$ kde P a Q sú rozdielne prvoideály také že*

1. *$N(P) = p^2$, $N(Q) = q^2$ a nech*

$$S = \{a_0 + a_1\omega |\ a_0, a_1 \in \mathbb{Z}, 0 \leq a_0, a_1 < pq\}.$$

   Potom S je množina reprezentantov faktorokruhu $\mathcal{O}_K/A$.

2. *$N(P) = p$, $N(Q) = q$ a nech*

$$S = \{a \mid a \in \mathbb{Z}, 0 \leq a < pq\}.$$

   Potom S je množina reprezentantov faktorokruhu $\mathcal{O}_K/A$.

3. *$N(P) = p^2$, $N(Q) = q$ a nech*

$$S = \{a + b\omega |\ a, b \in \mathbb{Z}, 0 \leq a < pq, 0 \leq b < p\}.$$

   Potom S je množina reprezentantov faktorokruhu $\mathcal{O}_K/A$.

Dôkaz. (1) Majme zobrazenie

$$\begin{aligned} \psi : S &\to \mathcal{O}_K/A \\ a + b\omega &\mapsto (a + b\omega) + A. \end{aligned}$$

Vidíme že $|\mathcal{O}_K/A| = N(A) = N(PQ) = N(P)N(Q) = p^2q^2 = |S|$, takže S a $\mathcal{O}_K/A$ majú rovnakú veľkosť. Keďže $N(P) = p^2$ a $N(Q) = q^2 \Rightarrow p \in P$ a $q \in Q$ $\Rightarrow pq \in A$. Pretože $\{1, \omega\}$ je celistvá báza $\mathcal{O}_K$, tak môžeme napísať

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega.$$

Kde miesto $\mathbb{Z}$ si môžeme vziať skalár $m_i \in \mathbb{Z}$ pre ľubovoľne $i \in \{0, 1\}$ a príslušný prvok $m_0 + m_1\omega$ bude vždy ležat v $\mathcal{O}_K$. Majme ľubovoľný prvok $\alpha = \alpha_0 + \alpha_1\omega \in \mathcal{O}_K$, kde $\alpha_i \in \mathbb{Z}$, α_i potom môžeme vydeliť so zvyškom ako $\alpha_i = a_ipq + r_i$, kde $0 \leq r_i < pq$. Z tohto zápisu vidíme že

$$\alpha = \alpha_0 + \alpha_1\omega = (a_0pq + r_0) + (a_1pq + r_1)\omega \equiv r_0 + r_1\omega \pmod{A}.$$

Takže pre každé $\alpha \in \mathcal{O}_K$ platí $\alpha \in (r_0 + r_1\omega) + A = \psi(r_0 + r_1\omega)$, pričom $0 \leq r_0$,$r_1 < pq \Rightarrow \psi$ je surjektivné zobrazenie medzi rovnako veľkými konečnými množinami, takže ψ je bijekcia a tým je dôkaz hotový.

(2) Potrebujeme ukázať že existuje bijektivné zobrazenie medzi S a $\mathcal{O}_K/A$. Majme zobrazenie

$$\begin{aligned} \psi : S &\to \mathcal{O}_K/A \\ a &\mapsto a + A. \end{aligned}$$

Najprv ukážeme že ψ je prosté, teda že $\forall\, a,b \in S : \psi(a) = \psi(b) \Rightarrow a = b$.

Nech teda $\psi(a) = \psi(b) \Rightarrow a + A = b + A \Rightarrow a \equiv b \pmod{A}$ pre nejaké $a,b \in S$. Potom $a - b \in A$. Keďže $a,b \in \mathbb{Z} \Rightarrow a - b \in \mathbb{Z}$. Keďže $N(P) = p$ a $N(Q) = q \Rightarrow p \in P$ a $q \in Q \Rightarrow pq \in A$. Takže $a - b \in (A \cap \mathbb{Z}) = pq\mathbb{Z} \Rightarrow a \equiv b \pmod{pq} \Rightarrow a = b$.

Rovnosť $(A \cap \mathbb{Z}) = pq\mathbb{Z}$ platí pretože $pq\mathbb{Z} \subset (A \cap \mathbb{Z})$ vďaka tomu že $pq \in A$ ako sme si rozmysleli vyššie. Ak $n \in (A \cap \mathbb{Z}) \Rightarrow n \in \mathbb{Z}$ a $n \in A$. Pretože $A = PQ \Rightarrow P|A$ a $Q|A$. Z vety 1.1.16 plynie že $A \subset P$ a $A \subset Q \Rightarrow n \in P$ a $n \in Q \Rightarrow p|n$ a $q|n \Rightarrow pq|n \Rightarrow (A \cap \mathbb{Z}) \subset pq\mathbb{Z}$.

ψ je teda prosté. Zároveň platí $|\mathcal{O}_K/A| = N(A) = N(PQ) = N(P)N(Q) = pq = |S|$. ψ je tak prosté zobrazenie medzi dvoma rovnako veľkými konečnými množinami $\Rightarrow \psi$ je bijekcia a tým je dôkaz dokončený.

(3) Bez dôkazu. □

Pre obecné teleso K so stupňom rozšírenia n sa s rastúcim n počet rôznych množín reprezentantov zvyšuje a hľadať pre každý ideál A množinu reprezentantov by bolo značne náročné. Riešením tohto problému je zvoliť pevný tvar množiny reprezentantov pre obecné K. Podľa Zheng a Liu (2022) by to mohla byť množina

$$S = \left\{ \sum_{i=1}^{n} a_i \alpha_i \mid 0 \leq a_i < pq,\, a_i \in \mathbb{Z},\, 1 \leq i \leq n \right\}. \tag{2.2}$$

Jednalo by sa teda o zobecnenie bodu (1) vo vete 2.3.1, pričom by pre P, Q platilo $N(P) = p^n$ a $N(Q) = q^n$. Takéto prvoideály vieme nájsť v každom telese K stupňa n a navyše sa táto množina najviac podobá množine reprezentantov klasického RSA ako si ukážeme v nasledujúcom príklade.

Príklad 2.3.2. Nech K je číselné teleso stupňa n nad $\mathbb{Q}$, $A = PQ \leq \mathcal{O}_K$ kde $N(P) = p^n$ a $N(Q) = q^n$ a $\mathcal{O}_K/A$ je faktorokruh. Vďaka vete 1.1.20 potom jednoducho spočítame

$$\varphi(A) = \varphi(P) \cdot \varphi(Q) = \varphi(p\mathcal{O}_K)\varphi(q\mathcal{O}_K) = (p^n - 1) \cdot (q^n - 1)$$

Podľa vety 2.2.1 pre ľubovoľné $a \in \mathbb{Z}$ dostávame

$$a^{k(p^n-1)(q^n-1)+1} \equiv a \pmod{pq}, \quad k \in \mathbb{Z}, \quad k \geq 0.$$

Keďže S z 2.2 je množina reprezentantov pre $\mathcal{O}_K/A$ a $\alpha = \sum_{i=1}^{n} a_i \alpha_i \in S$. Môžeme napísať vektor α ako $\alpha = (a_1,a_2,\ldots,a_n) \in \mathbb{Z}_{pq}^n$. Nech pre čísla $m = pq$, $1 \leq e, d < (p^n - 1)(q^n - 1)$ platí že

$$ed \equiv 1 \pmod{(p^n - 1)(q^n - 1)}.$$

Potom pre každú správu $\alpha = (a_1,a_2,\cdots,a_n)$, použijeme verejný kľúč (m,e) na šifrovanie a súkromný kľúč (p,q,d) na dešifrovanie pre každé a_i zvlášť, v konečnom dôsledku ide iba o viacnásobné použitie klasického RSA.

Ku koncu práce ukážeme že prepisom algoritmu pomocou mriežok dokážeme nájsť jednoznačný tvar rozkladovej triedy ktorý bude vyhovovať každému faktorokruhu $\mathcal{O}_K/A$.

2.4 Vzťah medzi K a $\mathbb{Q}^n$

RSA algoritmus nad číselnými telesami máme už obstojne popísaný. Z praktických dôvodov je ale lepšie prepísať tento algoritmus pomocou teórie mriežok. V tejto sekcii si ukážeme že sa na ideály v číselných telesách dá dívať obecne ako na racionálne mriežky.

Na začiatok si vytvoríme zobrazenie ktorým prepojíme K a $\mathbb{Q}^n$. Definícia 1.1.2 nám umožňuje vyjadriť si K ako

$$K = \mathbb{Q}(\theta) = \left\{ \sum_{i=0}^{n-1} a_i \theta^i \mid a_i \in \mathbb{Q} \right\}.$$

Z tohto zápisu už je jednoduché nájsť zobrazenie medzi K a $\mathbb{Q}^n$ ktoré nám prevedie racionálne koeficienty a_i na n-zložkové racionálne vektory.

Definícia 2.4.1. *Majme číselné teleso $K = \mathbb{Q}(\theta)$ stupňa n nad $\mathbb{Q}$ a vektorový priestor $\mathbb{Q}^n$, potom definujeme zobrazenie τ: $K \to \mathbb{Q}^n$ predpisom*

$$\alpha = \sum_{i=0}^{n-1} a_i \theta^i \in K \xrightarrow{\tau} \tau(\alpha) = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} \in \mathbb{Q}^n \quad kde \quad a_i \in \mathbb{Q}.$$

Z definície j ejednoduché nahliadnuť že zobrazenie τ je bijekcia.

Tvrdenie 2.4.2. *Buď K číselné teleso stupňa n nad $\mathbb{Q}$. Potom je zobrazenie $\tau : K \to \mathbb{Q}^n$ definované ako v 2.4.1 je izomorfizmom $\mathbb{Q}$-vektorových priestorov.*

Dôkaz. Najprv si ukážeme že zobrazenie τ je bijekcia. Majme $\tau(\alpha)$, $\tau(\beta) \in \mathbb{Q}^n$ také že $\tau(\alpha) = \tau(\beta)$. Potom platí

$$\begin{aligned} \tau(\alpha) = \tau(\beta) \Rightarrow \tau(\alpha) - \tau(\beta) = 0 \Rightarrow \tau(\alpha - \beta) = 0 \Rightarrow \tau(\gamma) = 0 \\ \Rightarrow \gamma = 0 \Rightarrow \alpha - \beta = 0 \Rightarrow \alpha = \beta. \end{aligned}$$

Z definície 1.1.2 je K $\mathbb{Q}$-vektorový priestor dimenzie n. $\mathbb{Q}^n$ je rovnako vektorový priestor dimenzie n. τ je teda bijekcia pretože ide o prosté zobrazenie medzi vektorovými priestormi rovnakej konečnej dimenzie.

Teraz ukážeme že $\tau(\alpha+\beta) = \tau(\alpha)+\tau(\beta)$ a $\tau(r\alpha) = r\tau(\alpha)$ pre všetky α,$\beta \in K$ a $r \in \mathbb{Q}$.

$$\tau(\alpha + \beta) = (a_0 + b_0, \ldots, a_n + b_n)^T = (a_0, \ldots, a_n)^T + (b_0, \ldots, b_n)^T = \tau(\alpha) + \tau(\beta).$$

a

$$\tau(r\alpha) = (ra_0, \ldots, ra_n)^T = r(a_0, \ldots, a_n)^T = r\tau(\alpha).$$

a tým dostávame izomorfizmus K a $\mathbb{Q}^n$ ako $\mathbb{Q}$-vektorových priestorov. □

Neskôr si ukážeme že K a $\mathbb{Q}^n$ sú izomorfné ako okruhy. Zobrazenie τ nám zároveň z každého nenulového ideálu $A < \mathcal{O}_K$ vytvorí racionálnu mriežku $\mathcal{L} \subset \mathbb{Q}^n$ čo si dokážeme v nasledujúcom lemmate.

Lemma 2.4.3. *Nech $A < \mathcal{O}_K$ kde $A \neq 0$. Potom $\tau(A)$ je racionálna mriežka.*

Dôkaz. Nech $\{\beta_1, \beta_2, \ldots, \beta_n\} \subset A$ je celistvá báza $K/\mathbb{Q}$. Potom A môžeme napísať ako

$$A = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \cdots + \mathbb{Z}\beta_n.$$

Použitim τ dostávame

$$\tau(A) = \mathbb{Z}\tau(\beta_1) + \mathbb{Z}\tau(\beta_2) + \cdots + \mathbb{Z}\tau(\beta_n).$$

Keďže vektory $\beta_1, \beta_2, \ldots, \beta_n$ sú lineárne nezávislé $\Rightarrow$ $\tau(\beta_1), \tau(\beta_2), \ldots, \tau(\beta_n)$ sú lineárne nezávislé vektory v $\mathbb{Q}^n$. Označme si $B = \{\tau(\beta_1), \tau(\beta_2), \ldots, \tau(\beta_n)\} \subset \mathbb{Q}^n$ a podľa definície 1.2.2 potom platí

$$\tau(A) = \mathcal{L}(B) = \{Bx : x \in \mathbb{Z}^n\}.$$

□

3. Ideálové matice

3.1 Úvod

V tejto kapitole si vytvoríme a dôkladne popíšeme vhodnú regulárnu štvorcovú maticu spolu so všetkými, pre túto prácu potrebnými, vlastnosťami. Množina stĺpcových vektorov tejto matice nám bude slúžiť ako báza pre mriežku $\mathcal{L}$ vo výslednom RSA algoritme. Rovnako dokážeme vlastnosti tejto matice, ktoré využieme pre popis RSA pomocou mriežok a nakoniec si dokážeme izomorfizmus $K \simeq \mathbb{Q}^n \simeq M^*_{\mathbb{Q}}$.

Pripomeňme že $K = \mathbb{Q}(\theta)$ kde θ je celistvý prvok ktorého minimálny polynóm je $m_\theta(x) = x^n - m_{n-1}x^{n-1} - \ldots - m_1 x - m_0 \in \mathbb{Z}[x]$. V celej tejto kapitole vektory $e_1, e_2, \ldots, e_n \in \mathbb{R}^n$ budú označovať vektory kanonickej bazy $\mathbb{R}^n$.

3.2 Definície

V tejto sekcii si definujeme základné pojmy ktoré budeme používať v priebehu celej kapitoly a ukážeme si ich využitie na základných príkladoch.

Definícia 3.2.1. *Nech θ je celistvý prvok a $m_\theta(x)$ je minimálny polynóm čísla θ, rotačnú maticu vzhľadom k $m_\theta(x)$ budeme rozumieť maticu*

$$H = H_{m_\theta} = \begin{pmatrix} 0 & \cdots & 0 & m_0 \\ & & & m_1 \\ & I_{n-1} & & \vdots \\ & & & m_{n-1} \end{pmatrix} \in \mathbb{Z}^{n\times n},$$

kde I_{n-1} je jednotková matica dimenzie $n-1$

Vyššie spomenutá matica H je zaujímava najmä tromi vlastnosťami. Je regulárna, jej charakteristický polynóm je rovný $m_\theta(x)$ a ako si onedlho ukážeme jej k-tá mocnina sa k vektorom správa rovnako ako k-tá mocnina čísla θ voči prvkom $\alpha \in K$. Maticu H spolu s jej mocninami využijeme pri definícií takzvanej. *ideálovej matice.*

Definícia 3.2.2. *Nech θ je celistvý prvok. Majme maticu H priradená minimálnemu polynómu $m_\theta(x)$. Ideálovú maticu $H^*(f)$ generovanú vektorom $f \in \mathbb{R}^n$ budeme rozumieť maticu*

$$H^*(f) = \left(f, Hf, \ldots, H^{n-1}f\right)_{n\times n} \in \mathbb{R}^{n\times n}$$

a priestor všetkych ideálových matíc nad $\mathbb{R}$ a $\mathbb{Q}$ označíme ako

$$M^*_{\mathbb{R}} = \{H^*(f) |\ f \in \mathbb{R}^n\} \subset \mathbb{R}^{n\times n} \text{ a } M^*_{\mathbb{Q}} = \{H^*(f) |\ f \in \mathbb{Q}^n\} \subset \mathbb{Q}^{n\times n}.$$

Príklad 3.2.3. Majme teleso $\mathbb{Q}(\sqrt[4]{3})$ kde $\theta = \sqrt[4]{3}$, potom minimálny polynóm pre $\sqrt[4]{3}$ je $m_\theta(x) = x^4 - 3$ a rotačná matica je tvaru

$$H = \begin{pmatrix} 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Následne si zvoľme vektor $f = \begin{pmatrix} 2 \\ 3 \\ 0 \\ -4 \end{pmatrix} \in \mathbb{R}^4$, čo je podľa 2.4.1 vektorová reprezentácia prvku $\alpha = 2 + 3\sqrt[4]{3} - 4\sqrt[4]{27} \in \mathbb{Q}(\sqrt[4]{3})$. Podľa 3.2.2 je matica $H^*(f)$ definovaná ako

$$H^* f = \begin{pmatrix} 2 & -12 & 0 & 9 \\ 3 & 2 & -12 & 0 \\ 0 & 3 & 2 & -12 \\ -4 & 0 & 3 & 2 \end{pmatrix}$$

Rozborom jednotlivých stĺpcov matice $H^*(f)$ môžeme nahliadnuť že i-tý stĺpec tejto matice pre $i \in \{1,dots, 4\}$ odpovedá súčinu $\theta^{i-1}\alpha$. Prvý stĺpec je jasný, pre stĺpce 2, 3 a 4 potom platí

$$H(f) = \begin{pmatrix} -12 \\ 2 \\ 3 \\ 0 \end{pmatrix} \xrightarrow{t^{-1}} \sqrt[4]{3}(2 + 3\sqrt[4]{3} - 4\sqrt[4]{27}) = -12 + 2\sqrt[4]{3} + 3\sqrt[4]{9}$$

$$H^2 f = \begin{pmatrix} 0 \\ -12 \\ 2 \\ 3 \end{pmatrix} \xrightarrow{t^{-1}} \sqrt[4]{9}(2 + 3\sqrt[4]{3} - 4\sqrt[4]{27}) = -12\sqrt[4]{3} + 2\sqrt[4]{9} + 3\sqrt[4]{27}$$

$$H^3 f = \begin{pmatrix} 9 \\ 0 \\ -12 \\ 2 \end{pmatrix} \xrightarrow{t^{-1}} \sqrt[4]{27}(2 + 3\sqrt[4]{3} - 4\sqrt[4]{27}) = 9 - 12\sqrt[4]{9} + 2\sqrt[4]{27}$$

kde t je bijektívné zobrazenie definované v 2.4.1.

Definícia 3.2.4. *Buď θ celistvý prvok a $m_\theta(x)$ jeho minimálny polynóm. Buď H rotačná matica priradená k $m_\theta(x)$. Potom pre ľubvoľné dva vektory f, $g \in \mathbb{R}^n$ definujeme $\odot$-súčin ako*

$$f \odot g = H^*(f)g$$

a n-tú mocninu f ako

$$f^{\odot n} = \overbrace{f \odot f \cdots \odot f}^{n-krát}, n \in \mathbb{N}$$

Príklad 3.2.5. Buď θ rovnaká ako v príklade 3.2.3 Zvoľme si $f = \begin{pmatrix} 2 \\ 3 \\ 0 \\ -4 \end{pmatrix} \in \mathbb{R}^4$ a $g = \begin{pmatrix} -4 \\ 2 \\ 1 \\ 1 \end{pmatrix} \in \mathbb{R}^4$. Potom $\odot$-súčin $f \odot g$ spočítame ak

$$f \odot g = H^*(f)g = \begin{pmatrix} 2 & -12 & 0 & 9 \\ 3 & 2 & -12 & 0 \\ 0 & 3 & 2 & -12 \\ -4 & 0 & 3 & 2 \end{pmatrix} \begin{pmatrix} -4 \\ 2 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} -23 \\ -20 \\ -4 \\ 21 \end{pmatrix}.$$

Keďže vektory f a g sú vektorové reprezentácie prvkov $\alpha = 2 + 3\sqrt[4]{3} - 4\sqrt[4]{27} \in \mathbb{Q}(\sqrt[4]{3})$ a $\beta = -4 + 2\sqrt[4]{3} + \sqrt[4]{9} + \sqrt[4]{27} \in \mathbb{Q}(\sqrt[4]{3})$, priamym výpočtom nahliadneme že $\odot$-súčin je vektorová operácia ktorá dáva koeficienty prvku $\alpha \cdot \beta$, teda

$$\begin{aligned} \alpha \cdot \beta &= (2 + 3\sqrt[4]{3} - 4\sqrt[4]{27}) \cdot (-4 + 2\sqrt[4]{3} + \sqrt[4]{9} + \sqrt[4]{27}) \\ &= -23 - 20\sqrt[4]{3} - 4\sqrt[4]{9} + 9\sqrt[4]{27}. \end{aligned}$$

3.3 Základné vlastnosti ideálových matíc

V tejto sekcii si dokážeme pár základných vlastností matice H^*.

Lemma 3.3.1. *Nech $\mathbb{R}^n$ je vektorový priestor, $M^*_{\mathbb{R}}(+)$ je priestor reálnych ideálových matic a nech $f, g \in \mathbb{R}^n$ sú vektory. Potom*

1. $H^*(f) = 0 \Leftrightarrow f = 0$
2. $H^*(f + g) = H^*(f) + H^*(g)$
3. $H^*(rf) = rH^*(f) \quad pre \quad r \in \mathbb{R}$
4. $H^*(f) = H^*(g) \Leftrightarrow f = g$

Navyše zobrazenie H^*: $\mathbb{R}^n \to M^*_{\mathbb{R}}$ nám dáva izomorfizmus $\mathbb{R}$-vektorových priestorov.

Dôkaz. (1) ($\Rightarrow$) $H^*(f)$ je nulová matica. Z definície 3.2.2 prvý stĺpcový vektor $H^*(f)$ je práve vektor $f \Rightarrow f = 0$.

($\Leftarrow$) plynie triviálne z definície 3.2.2.

(2) Majme $H^*(f + g)$. Podľa definície 3.2.2 platí

$$\begin{aligned} H^*(f + g) &= (f + g, H(f + g), \ldots, H^{n-1}(f + g)) \\ &= (f, Hf, \ldots, H^{n-1}f) \\ &+ (g, Hg, \ldots, H^{n-1}g) \\ &= H^*(f) + H^*(g). \end{aligned}$$

(3) Dokážeme priamym výpočtom

$$\begin{aligned} H^*(rf) &= (rf, H(rf), \ldots, H^{n-1}(rf)) \\ &= (rf, r(Hf), \ldots, r(H^{n-1}f)) \\ &= r(f, Hf, \ldots, H^{n-1}f) \\ &= rH^*(f). \end{aligned}$$

(4) $H^*(f) = H^*(g) \Leftrightarrow H^*(f) - H^*(g) = 0$. Podľa bodu (2) ale vieme že $H^*(f) - H^*(g) = 0 \Leftrightarrow H^*(f - g) = 0$. Podľa (1) potom dostávame $H^*(f - g) = 0 \Leftrightarrow f - g = 0 \Leftrightarrow f = g$.

($Izomorfizmus$) Z bodov (2) a (3) hneď dostávame že H^* nám dáva homomorfizmus vektorových priestorov nad $\mathbb{R}$. Z bodu (4) dostávame že H^* je prosté. Zároveň z bodu (4) plynie že každá matica $H^*(f) \in M^*_{\mathbb{R}}$ je jednoznačne určená vektorom $f \in \mathbb{R}^n$, takže H^* je surjektívné. □

O zobrazení H^*: $\mathbb{R}^n \to M^*_{\mathbb{R}}$ si ku koncu kapitoly dokážeme že nám dáva izomorfizmus $\mathbb{R}^n \simeq M^*_{\mathbb{R}}$ okruhov.

Lemma 3.3.2. *Buď θ celistvý prvok a $m_\theta(x)$ jeho minimálny polynóm. Nech H je rotačná matica k $m_\theta(x)$ a $e_1 = (1,0,\ldots,0) \in \mathbb{R}^n$. Potom*

$$H^k e_1 = e_{k+1} \quad pre \quad 0 \leq k \leq n-1.$$

Dôkaz. Budeme dokazovať indukciou podľa k. Pre $k = 0$ platí $I_n e_1 = e_1$ a pre $k = 1$ platí $He_1 = e_2$, čo je hneď vidieť z definície 3.2.1. Chceme aby to platilo pre obecné k. Z indukčného predpokladu to platí pre $k-1$, teda platí $H^{k-1}e_1 = e_k$. Pre výraz $H^k e_1$ potom dostávame

$$H^k e_1 = H(H^{k-1}e_1) = He_k = e_{k+1}.$$

Kde posledná rovnosť platí pretože v indukčnom predpoklade vektor e_k nikdy nie je vektor e_n. Takže z definície 3.2.1 matice H nám súčin He_k dá práve $k+1$-vý vektor kanonickej báze. □

Lemma 3.3.3. *Buď τ definované ako v definícii 2.4.1, potom platí*

$$\begin{cases} \tau\left(\theta^k\right) = e_{k+1}, \ 0 \leq k \leq n-1 \\ H^*(e_k) = H^{k-1}, \ 1 \leq k \leq n \end{cases}$$

Dôkaz. $\tau\left(\theta^k\right) = e_{k+1}$ plynie triviálne z definície 2.4.1. Časť $H^*(e_k) = H^{k-1}$ dokážeme indukciou. Rozpísaním definície a pomocou lemmatu 3.3.2 nahliadneme že

$$\begin{aligned} H^*(e_1) &= (e_1, He_1, \ldots, H^{n-1}e_1) \\ &= (e_1, e_2, e_3, \ldots, e_n) = I_n. \end{aligned}$$

Predpokládajme že platí $H^*(e_{k-1}) = H^{k-2}$, pre k ≥ 2. Z definície 3.2.1 je vidieť že k-tý stĺpec matice H je rovný e_{k+1} pre $1 \leq k \leq n-1$ a teda platí $e_k = H(e_{k-1})$, z toho dostávame

$$\begin{aligned} H^*(e_k) &= \left(H(e_{k-1}), H^2(e_{k-1}), \cdots, H^n(e_{k-1})\right) \\ &= H\left(e_{k-1}, H(e_{k-1}), \cdots, H^{n-1}(e_{k-1})\right) \\ &= HH(e_{k-1}) = HH^{k-2} = H^{k-1}. \end{aligned}$$

□

Z kapitoly 2 už vieme že zobrazenie τ: $K \to \mathbb{Q}^n$ nám dáva izomorfizmus medzi K a $\mathbb{Q}^n$ ako $\mathbb{Q}$ vektorových priestorov. Nasledújúcou vetou si dokážeme že τ nám dáva $K \simeq \mathbb{Q}^n$ ako izomorfizmus okruhov.

Veta 3.3.4. *Buď $K = \mathbb{Q}(\theta)$ a nech $\odot$-súčin je definovaný rovnako ako v 3.2.4. Majme zobrazenie τ: $K \to \mathbb{Q}^n$ definované rovnako ako v 2.4.1, potom pre každé dva prvky $\alpha, \beta \in K$ platí*

$$\tau(\alpha \cdot \beta) = \tau(\alpha) \odot \tau(\beta).$$

Navyše zobrazenie τ nám dáva izomorfizmus okruhov $K(+,\cdot) \simeq \mathbb{Q}^n(+, \odot)$.

Dôkaz. Nech $\beta = \beta_0 + \beta_1\theta + \cdots + \beta_{n-1}\theta^{n-1}$, kde $\beta_i \in \mathbb{Q}$. Ľahko nahliadneme že

$$\theta\beta = \beta_0\theta + \beta_1\theta^2 + \cdots + \beta_{n-1}\theta^n.$$

Číslo θ^n si vďaka minimálnemu polynómu $m_\theta(x)$ môžeme napísať ako

$$\theta^n = m_{n-1}\theta^{n-1} + \cdots + m_1\theta + m_0.$$

Z toho potom dostávame

$$\begin{aligned}\beta_0\theta + \cdots + \beta_{n-1}\theta^n = \beta_{n-1}m_0 + (\beta_0 + \beta_{n-1}m_1)\theta + \ldots \\ + (\beta_{n-2} + \beta_{n-1}m_{n-1})\theta^{n-1}.\end{aligned}$$

Obecne potom platí $\tau(\theta\beta) = H(\tau(\beta))$ a

$$\tau(\theta^k\beta) = H^k(\tau(\beta)), \quad 0 \leq k \leq n-1$$

Majme $\alpha = \alpha_0 + \alpha_1\theta + \cdots + \alpha_{n-1}\theta^{n-1}$, potom z lemma3.3.3 dostávame

$$\tau(\alpha\beta) = \sum_{k=0}^{n-1} \alpha_k \tau(\theta^k\beta) = \sum_{k=0}^{n-1} \alpha_k H^k(\tau(\beta)) = H^*(\tau(\alpha))\tau(\beta) = \tau(\alpha) \odot \tau(\beta).$$

($Izomorfizmus$) Na to aby sme ukázali izomorfizmus musí pre ľubovoľné $\alpha, \beta \in K$ platiť $\tau(\alpha+\beta) = \tau(\alpha)+\tau(\beta)$ a $\tau(\alpha\cdot\beta) = \tau(\alpha)\odot\tau(\beta)$. Časť o sčítaní a bijekciu τ nám dokazuje lemma 2.4.2 a časť o násobení sme si dokázali vyššie. □

Veta vyššie nám teda dokazuje prvý okruhový izomorfizmus tejto kapitoly. Nás ale bude zaujímať ešte izomorfizmus týchto telies s množinou $M^*_{\mathbb{Q}}$ ktorý si necháme až na koniec tejto kapitoly.

3.4 Faktorokruh $\mathbb{R}[x]/(m_\theta(x))$

Doteraz sme v tejto kapitole pracovali výhradne s vektormi z $\mathbb{R}^n$, v ďalšom priebehu kapitoly sa nám ale bude hodiť pracovať s polynomamiálnou reprezentáciou daných vektorov. Preto si teraz zavedieme zobrazenie ktoré nam umožní previesť vektory do ich polynomiálnej reprezentacie a späť.

Definícia 3.4.1. *Buď θ celistvý prvok a $m_\theta(x)$ jeho minimálny polynóm stupňa n. Zavedieme zobrazenie t medzi $\mathbb{R}^n$ a $\mathbb{R}[x]/(m_\theta(x))$ predpisom*

$$f = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} \in \mathbb{R}^n \xrightarrow{t} t_f(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} \in \mathbb{R}[x]/(m_\theta(x)).$$

a môžeme písať $t(f) = t_f(x)$.

Z takto definovaného zobrazenia a obecnej definície faktorokruhu vidíme že t je bijekcia a zároveň zachováva sčítanie, teda $t(f + g) = t(f) + t(g)$ pre všetky f,$g \in \mathbb{R}^n$.

V tejto sekcii dokážeme izomorfizmus okruhov $\mathbb{R}^n(+,\odot) \simeq \mathbb{R}[x]/(m_\theta(x))(+,\cdot)$. Tento izomorfizmus sa nám potom bude hodiť v ďalšej kapitole o mriežkach.

Polynomiálny pohľad na reálne vektory sa nám bude hodiť ako aparát na jednoduchšie dokazovanie netriviálnych vlastností ideálových matíc kde sa na matice $H^*(f)$ budeme môcť dívať ako na polynómy tvaru $t_f(H) = f_0 I_n + f_1 H + \cdots + f_{n-1}H^{n-1}$.

Kedže $m_\theta(x)$ je charakteristický polynóm H, podľa Caley - Hamiltonovej vety platí

$$m_\theta(H) = 0, \text{ alebo } H^n = m_0 + m_1 H + \cdots + m_{n-1}H^{n-1}. \tag{3.1}$$

Takže všetky rotačné matice $H^k (k \geq 0)$ sú ideálové matice, špeciálne jednotková matica $I_n = H^*(e_1)$ je ideálová matica.

Lemma 3.4.2. *Pre ľubovoľný vektor $f \in \mathbb{R}^n$, môžeme ideálovu maticu $H^*(f)$ napísať ako*

$$H^*(f) = t_f(H) = f_0 I_n + f_1 H + \cdots + f_{n-1}H^{n-1}$$

Navyše, ak $F(x) \in \mathbb{R}[x]$ a $F(x) \equiv t_f(x) \pmod{m_\theta(x)}$, tak $t_f(H) = F(H)$.

Dôkaz. f môžeme napísať ako $f = f_0 e_1 + f_1 e_2 + \cdots + f_{n-1}e_{n-1}$, a z lem 3.3.1 a 3.3.3 dostávame

$$\begin{aligned} H^*(f) &= f_0 H^*(e_1) + f_1 H^*(e_2) + \cdots + f_{n-1}H^*(e_n) \\ &= f_0 I_n + f_1 H + \cdots + f_{n-1}H^{n-1} = f(H) \end{aligned}$$

Predpokladajme že $F(x) \equiv t_f(x) \pmod{m_\theta}$, pretože $F(x) = t_f(x) + g(x)m_\theta(x)$, kde $g(x) \in \mathbb{R}[x]$ a teda $F(H) = t_f(H) + g(H)m_\theta(H)$ ale práve vďaka 3.1 platí $m_\theta(H) = 0$ a teda $F(H) = t_f(H)$ □

Pre dôkaz izomorfizmu $\mathbb{R}^n(+,\odot) \simeq \mathbb{R}[x]/(m_\theta(x))(+,\cdot)$ si ešte dokážeme jedno pomocné lema.

Lemma 3.4.3. *Buď θ celistvý prvok a $m_\theta(x)$ jeho minimálny polynóm. Nech H je rotačná matica priradená k $m_\theta(x)$, $g \in \mathbb{R}^n$ a t je zobrazenie definované rovnako ako v 3.4.1. Potom*

$$t(H^k g) = x^k t_g(x) \quad pre \quad 0 \leq k \leq n-1.$$

Dôkaz. Dôkaz spravíme indukciou.

Pre $k = 0$ platí $t(I_n g) = t(g) = t_g(x) = x^0 t_g(x)$.

Pre $k = 1$ platí

$$\begin{aligned} t(H(g)) &= g_{n-1}m_0 + (g_0 + g_{n-1}m_1)x + \cdots + (g_{n-2} + g_{n-1}m_{n-1})x^{n-1} \\ &= g_0 x + g_1 x^2 + \cdots + g_{n-1}(m_0 x^{n-1} + \cdots + m_{n-1}x^{n-1}) \\ &= g_0 x + g_1 x^2 + \cdots + g_{n-1}x^n \\ &= x t_g(x). \end{aligned}$$

Chceme to dokázať pre k. Z indukčného predpokladu $t(H^{k-1}g) = x^{k-1}t_g(x)$. Vieme že t je bijekcia, takže platí $H^{k-1}g = t^{-1}(x^{k-1}t_g(x))$.

Označme si $t^{-1}(x^{k-1}t_g(x)) = a \in \mathbb{R}^n$. Potom

$$\begin{aligned} t(H^k g) &= t(H(H^{k-1}g)) = t(Ha) \\ &= a_{n-1}m_0 + (a_0 + a_{n-1}m_1)x + \cdots + (a_{n-2} + a_{n-1}m_{n-1})x^{n-1} \\ &= a_0 x + a_1 x^2 + \cdots + a_{n-1}(m_0 x^{n-1} + \cdots + m_{n-1}x^{n-1}) \\ &= a_0 x + a_1 x^2 + \cdots + a_{n-1}x^n \\ &= x t_a(x) = x t_a(x) = x t(a) \\ &= x t(t^{-1}(x^{k-1}t_g(x))) = x(x^{k-1}t_g(x)) = x^k t_g(x). \end{aligned}$$

□

Veta 3.4.4. *Buď θ celistvý prvok a $m_\theta(x)$ jeho minimálny polynóm stupňa n a buď $\odot$ definované ako v 3.2.4. Potom $t : \mathbb{R}^n(+,\odot) \to \mathbb{R}[x]/(m_\theta(x))(+,\cdot)$ je izomorfizmus okruhov.*

Dôkaz. Z definície 3.4.1 vieme že t je bijekcia a $t(f+g) = t(f) + t(g)$ pre všetky $f,g \in \mathbb{R}^n$. Na izomorfizmus okruhov ešte musíme ukázať platnosť $t(f \odot g) = t(f) \cdot t(g)$ pre všetky $f,g \in \mathbb{R}^n$.

Pre násobenie platí

$$\begin{aligned} t(f \odot g) &= \sum_{i=0}^{n-1} f_i t(H^i g) \overset{3.4.3}{=} \sum_{i=0}^{n-1} f_i (\sum_{j=0}^{n-1} g_j x^j) x^i = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f_i g_j x^{j+i}. \\ &= \sum_{i=0}^{2n-2} (\sum_{j+k=i} f_j g_k) x^i = (\sum_{i=0}^{n-1} f_i x^i) \cdot (\sum_{j=0}^{n-1} g_j x^j) = t(f) \cdot t(g). \end{aligned}$$

□

Priamym dôsledkom vety 3.4.4 nasledujúce lema.

Lemma 3.4.5. *Nech f a g sú ľubovoľné vektory z $\mathbb{R}^n$ a nech $f(x), g(x)$ sú k ním príslušné polynómy, potom platí*

$$t(f \odot g) \equiv f(x)g(x) \pmod{m_\theta(x)}$$

3.5 Netriviálne vlastnosti ideálových matíc

V tejto sekcii bude

$$V_{m_\theta} = \left[\theta_j^i\right]_{0\le i,j\le n-1} \quad kde \quad \det\left(V_{m_\theta}\right) \neq 0$$

značiť Vandermontovu maticu kde $\{\theta_0, \theta_1, \theta_2, \ldots, \theta_{n-1}\}$ je n rôznych koreňov minimálneho polynómu $m_\theta(x)$ prvku $\theta \in K$ kde K je číselné teleso.

Lemma 3.5.1. *Pre ľubovoľné vektory* $f = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{n-1} \end{pmatrix} \in \mathbb{R}^n$, $g = \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{n-1} \end{pmatrix} \in \mathbb{R}^n$, *platia nasledujúce vlastnosti ideálových matíc:*

1. $H^*(f)H^*(g) = H^*(g)H^*(f)$
2. $H^*(f)H^*(g) = H^*(H^*(f)g)$
3. $H^*(f) = V_{m_\theta}^{-1} diag\{t_f(\theta_0), t_f(\theta_1), \ldots, t_f(\theta_{n-1})\}V_{m_\theta}$
4. $\det\left(H^*(f)\right) = \prod_{i=0}^{n-1} t_f(\theta_i)$
5. *Ak* $f \neq 0 \in \mathbb{Q}^n$ *tak* $H^*(f)$ *je invertibilná matica a*

$$\left(H^*(f)\right)^{-1} = H^*(u)$$

kde $u(x) \in \mathbb{Q}[x]$ *je jediný polynóm taký že* $u(x)f(x) \equiv 1 \pmod{m_\theta(x)}$ *v* $\mathbb{Q}[x]$

Dôkaz. (1) Z lema 3.3.3 platí že

$$H^*(f)H^*(g) = t_f(H)t_g(H) = t_g(H)t_f(H) = H^*(g)H^*(f)$$

(2) $H^*(H^*(f)g) \overset{3.4.2}{=} H^*(t_f(H)g) = H^*\left(\sum_{k=0}^{n-1} f_k H^k g\right)$. Pretože H^* pracuje iba s vektormi môžeme sumu aj s koeficientami f_k vybrať. Potom platí

$$H^*\left(\sum_{k=0}^{n-1} f_k H^k g\right) = \sum_{k=0}^{n-1} f_k \left(H^*(H^k g)\right).$$

Keďže $H^k g$ je vektor, môžeme podľa definicie 3.2.2 rozpísať $H^*(H^k g)$ ako

$$\begin{aligned} H^*(H^k g) &= (H^k g, H^{k+1} g, \ldots, H^{n-1+k} g)_{n\times n} \\ &= H^k(g, H^1 g, \ldots, H^{n-1} g)_{n\times n} = H^k(H^*(g)) \end{aligned}$$

Výsledok predchádzajúcich úprav dosadíme do sumy a dostávame

$$\sum_{k=0}^{n-1} f_k \left(H^*(H^k(g))\right) = \sum_{k=0}^{n-1} f_k \left(H^k(H^*(g))\right) = \sum_{k=0}^{n-1} f_k H^k(H^*(g)).$$

Čo potom môžme napísať ako

$$\sum_{k=0}^{n-1} f_k H^k(H^*(g)) = (\sum_{k=0}^{n-1} f_k H^k)(H^*(g)) = t_f(H)(H^*(g)) \overset{3.4.2}{=} H^*(f)H^*(g).$$

(3) Vieme že $m_\theta(x)$ je minimálny polynóm θ. Z poznámky 1.1.3 vieme že číselné teleso K si vieme vyjadriť ako $K = \mathbb{Q}(\theta)$ a že $\{\theta_0, \ldots, \theta_{n-1}\}$ kde $\theta_0 = \theta$ je n rôznych koreňov $m_\theta(x)$.

Z definície 3.2.1 vieme že charakteristický polynóm matice H je práve $m_\theta(x)$, takže vlastné čísla matice H sú presne čísla $\{\theta_0, \ldots, \theta_{n-1}\}$. Vlastný vektor vlastného čísla θ_i spočítame ako riešenie sústavy $\ker(H - \theta_i I_n)$. Priamym výpočtom zistíme že

$$\begin{aligned}
x(H - \theta_i I_n) = 0 &\Leftrightarrow xH - (x\theta_i I_n) = 0 \\
&\Leftrightarrow (x_2, \ldots, x_n, m_0x_1 + \cdots + m_{n-1}x_n) - (\theta_i x_1, \ldots, \theta_i x_n) = 0 \\
&\Leftrightarrow (x_2 - \theta_i x_1, \ldots, x_n - \theta_i x_{n-1}, m_0x_1 + \cdots + (m_{n-1} - \theta_i)x_n) = 0 \\
&\Leftrightarrow x_2 - \theta_i x_1 = 0,\ x_3 - \theta_i x_2 = 0, \\
&\ldots, m_0x_1 + \cdots + (m_{n-1} - \theta_i)x_n = 0 \\
&\Leftrightarrow x_2 = \theta_i x_1,\ x_3 = \theta_i x_2, \\
&\ldots, m_0x_1 + \cdots + m_{n-1}x_n = \theta_i x_n.
\end{aligned}$$

Ak zvolíme $x_1 = 1$, potom $x_2 = \theta_i$, $x_3 = \theta_i^2$, $\ldots$, $x_n = \theta_i^{n-1}$ a $m_0 + \cdots + m_{n-1}\theta_i^{n-1} = \theta_i^n$. Riešením je teda práve pre jediný vektor

$$x = (1, \theta_i, \ldots, \theta_i^{n-1}) \quad pre\ všetky \quad i = 0, \ldots, n-1$$

čo je práve i-tý riadkový vektor Vandermontovej matice V_{m_θ} . Keďže má matica H n rôznych vlastných čísel $\Rightarrow$ H je diagonalizovatelná, takže ju môžeme napísať ako

$$H = V_{m_\theta}^{-1} diag\{\theta_0, \theta_1, \ldots, \theta_{n-1}\} V_{m_\theta}.$$

Odtiaľ z lema 3.4.2 plynie že

$$H^*(f) = t_f(H) = V_{m_\theta}^{-1} diag\{t_f(\theta_0), t_f(\theta_1), \ldots, t_f(\theta_{n-1})\} V_{m_\theta}.$$

(4) Vďaka vete o súčine determinantu matíc dostávame

$$\begin{aligned}
\det\left(H^*(f)\right) &= \det\left(V_{m_\theta}^{-1} diag\{t_f(\theta_0), t_f(\theta_1), \ldots, t_f(\theta_{n-1})\} V_{m_\theta}\right) \\
&= \det\left(V_{m_\theta}^{-1}\right) \det\left(diag\{t_f(\theta_0), t_f(\theta_1), \ldots, t_f(\theta_{n-1})\}\right) \det\left(V_{m_\theta}\right) \\
&= \det\left(diag\{t_f(\theta_0), t_f(\theta_1), \ldots, t_f(\theta_{n-1})\}\right) \\
&= \prod_{i=0}^{n-1} t_f(\theta_i).
\end{aligned}$$

(5) Keďže $f \in \mathbb{Q}^n$, $f \neq 0$ a $m_\theta(x)$ je ireducibilný polynóm v $\mathbb{Q}[x]$ tak máme

$$(t_f(x), m_\theta(x)) = 1$$

v $\mathbb{Q}[x]$, potom podľa Bezútových koeficientov existujú $u(x), v(x) \in \mathbb{Q}[x]$ také že

$$u(x)t_f(x) + v(x)m_\theta(x) = 1 \Rightarrow u(x)t_f(x) \equiv 1 \pmod{m_\theta(x)}$$

Z lemma 3.4.5 platí

$$t_f(x)u(x) = t(f \odot u) \equiv 1 \pmod{m_\theta(x)}$$

Aplikáciou t^{-1} a využitím toho že $t^{-1}(1) = e_1 \in \mathbb{R}^n$ dostávame

$$f \odot u \equiv e_1 \pmod{m_\theta(x)} \quad \Rightarrow \quad f \odot u = e_1$$

Ak na rovnicu $f \odot u = e_1$ použijeme zobrazenie H^* tak dostávame

$$H^*(f \odot u) = H^*(H^*(f)u) = H^*(f)H^*(u) = H^*(e_1) = I_n.$$

Z čoho potom plynie

$$(H^*(f))^{-1} = H^*(u).$$

□

3.6 Izomorfizmus $K \simeq \mathbb{Q}^n \simeq M^*_{\mathbb{Q}}$

Lemma 3.6.1. *Nech $\varphi : K \to K$ je zobrazenie definované predpisom $\varphi(\alpha) = \theta\alpha$ pre ľubovoľné $\alpha \in K$, potom*

1. *φ je $\mathbb{Q}$-lineárne zobrazenie*
2. *Maticou tohto lineárného zobrazenia je práve matica H.*

Dôkaz. (1) Prvú časť dokážeme priamym overením definície lineárneho zobrazenia. Majme ľubovoľné $\alpha, \beta \in K$ a $a \in \mathbb{R}$, chceme aby platilo $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$ a $\varphi(a\alpha) = a\varphi(\alpha)$. Sčítanie platí pretože

$$\varphi(\alpha) + \varphi(\beta) = \theta\alpha + \theta\beta = \theta(\alpha + \beta) = \varphi(\alpha + \beta).$$

Násobenie skalárom sa dokáže rovanko

$$\varphi(a\alpha) = \theta(a\alpha) = \theta a\alpha = a(\theta\alpha) = a\varphi(\alpha).$$

(2) Z poznámky 1.1.3 vieme že báza telesa $K = \mathbb{Q}(\theta)$ ako $\mathbb{Q}$-vektorového priestoru je báza $\{1,\theta,\cdots,\theta^{n-1}\}$. Majme teda maticu M_φ zobrazenia φ vzhľadom k báze $\{1,\theta,\ldots,\theta^{n-1}\}$.

Z predpisu φ pre každé $\theta^i \in K$ pre $(0 \leq i \leq (n-2))$ platí $\tau(\theta^i) = e_{i+1}$. Potom musí platiť $M_\varphi \cdot e_{i+1} = e_{i+2} = \tau(\theta^{i+1})$.

Pri prvku θ^{n-1} nám zobrazenie φ dáva

$$\varphi(\theta^{n-1}) = \theta^n = m_{n-1}\theta^{n-1} + \cdots + m_1\theta + m_0$$

pričom posledná rovnosť plynie z toho že θ je koreňom minimálneho polynómu a teda θ^n môžeme napísať ako lineárnu kombináciu predchádzajúcich mocnín θ^i. Takže pre maticu M_φ a vektor $e_n = \tau(\theta^{n-1})$ musí platiť

$$M_\varphi \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} m_0 \\ m_1 \\ \vdots \\ m_{n-1} \end{pmatrix} = \tau(\theta^n).$$

Ak si vezmeme všetky obrazy po násobení matice M_φ s e_i, tak ľahko nahliadneme že $M_\varphi = H$. □

Lemma 3.6.1 je posledným pomocným tvrdením ktoré potrebujeme pre dôkaz hlavnej vety celej kapitoly.

Veta 3.6.2. *Buď θ celistvý prvok a $m_\theta(x) \in \mathbb{Z}[x]$ jeho minimálny polynóm stupňa n. Buď $\odot$ definované ako v 3.2.4. Buď $K = \mathbb{Q}(\theta)$ číselné teleso stupňa n nad $\mathbb{Q}$. Potom*

$$K(+,\cdot) \simeq \mathbb{Q}^n(+,\odot) \simeq M^*_{\mathbb{Q}}(+,\cdot).$$

sú izomorfné ako okruhy. Navyše, nech $\alpha \in K$, $Tr(\alpha)$ a $N(\alpha)$ sú stopa a norma α, potom platí

$$Tr(\alpha) = Tr(H^*(\tau(\alpha))) \text{ a } N(\alpha) = \det(H^*(\tau(\alpha)))$$

Dôkaz. Izomorfizmus $K \simeq \mathbb{Q}^n$ dostavame vďaka vete 3.3.4. Lema 3.3.1 vieme že $H^* : \mathbb{R}^n \to M^*_{\mathbb{R}}$ nám dáva izomorfizmus aditívných grup $\mathbb{R}^n$ a $M^*_{\mathbb{R}}$, takže platí

$$H^*(\tau(\alpha) + \tau(\beta)) = H^*(\tau(\alpha)) + H^*(\tau(\beta)).$$

Z lematu 3.5.1 bodu (2) dostávame

$$H^*(\tau(\alpha) \odot \tau(\beta)) = H^*(\tau(\alpha))H^*(\tau\beta)).$$

Takže platí $\mathbb{R}^n \simeq M^*_{\mathbb{R}}$ ako okruhy. Zúžením H^* na racionálne čísla potom platí $\mathbb{Q}^n \simeq M^*_{\mathbb{Q}}$ a z toho potom plynie $K \simeq \mathbb{Q}^n \simeq M^*_{\mathbb{Q}}$.

Teraz dokážeme časť o stope a norme. Vďaka lematu 3.6.1 vieme že zobrazenie $\varphi(\alpha) = \theta\alpha$ je $\mathbb{Q}$-lineárne zobrazenie pre $K/\mathbb{Q}$ a rovnako že H je matica tohto zobrazenia voči baze $\{1,\theta,\theta^2,\ldots,\theta^{n-1}\}$. Potom z definície 1.1.11 pre stopu dostávame

$$Tr(\theta) = \phi_{n-1} = Tr(H) \quad a \quad Tr(\theta^k) = Tr(H^k); \quad 1 \leq k \leq n-1.$$

Nech $\alpha = \alpha_0 + \alpha_1\theta + \cdots + \alpha_{n-1}\theta^{n-1} \in K$, potom dostávame

$$Tr\left(\alpha\right) = \sum_{k=0}^{n-1} \alpha_k Tr\left(\theta^k\right) = \sum_{k=0}^{n-1} \alpha_k Tr\left(H^k\right) = Tr\left(\sum_{k=0}^{n-1} \alpha_k H^k\right) = Tr\left(H^*(\tau(\alpha))\right)$$

Teraz potrebujeme dokázať normu. Z definície 1.1.2 vieme že $K = \mathbb{Q}(\theta)$ je konečné rozšírenie telesa $\mathbb{Q}$ stupňa n. Z poznámky 1.1.3 vieme že $\theta_0, \theta_1, \theta_2, \ldots, \theta_{n-1}$ je n rôznych koreňov $m_\theta(x)$. Pre $K = \mathbb{Q}(\theta)$ z vety 1.1.4 vieme že existuje práve n rozdielných $\mathbb{Q}$-homomorfizmov $\sigma_0, \ldots, \sigma_{n-1}$ do $\mathbb{C}$.

Keďže každý prvok $\alpha \in K$ vieme napísať ako $\alpha = \alpha_0 + \alpha_1\theta + \cdots + \alpha_{n-1}\theta^{n-1}$, je potom jednoduché nahliadnuť že pre každý $\mathbb{Q}$-homomorfizmus σ_i platí

$$\sigma_i(\alpha) = \sum_{k=0}^{n-1} \alpha_k \theta_i^k := \alpha(\theta_i), \text{ kde } \theta_0 = \theta \quad a \quad 0 \leq i \leq n-1.$$

Z bodu (4) z lemma 3.5.1 a vety 1.1.12 dostávame

$$N(\alpha) = \prod_{i=0}^{n-1} \sigma_i(\alpha) = \prod_{i=0}^{n-1} \alpha(\theta_i) = \det(H^*(\tau(\alpha))).$$

□

Okrem toho že máme dokázané ako vyzerá stopa a norma pre ľubovoľný prvok $\alpha \in K$, nám izomorfizmus $K \simeq \mathbb{Q}^n \simeq M^*_{\mathbb{Q}}$ hovorí že pre ľubovoľné číselné teleso K a pre ľubovoľné $\alpha \in K$ vieme nájsť maticu $H^*(\tau(\alpha))$. V praxi teda nemáme žiadne obmedzenia a môžeme šifrovať slová ľubovoľnej dĺžky.

4. RSA na mriežkach

4.1 Úvod

V tejto kapitole si dokážeme všetku teóriu a vlastnosti mriežok potrebné k tomu aby sme mohli RSA algoritmus napísať pomocou teórie mriežok.

Pripomeňme že $K = \mathbb{Q}(\theta)$ je číselné teleso, $\mathcal{O}_K$ je okruh celistvých prvkov a že $m_\theta(x)$ je minimalny polynom pre celistvý prvok $\theta \in K$.

4.2 Izomorfizmus $\mathbb{Z}[x]/(m_\theta(x)) \simeq \mathcal{O}_K \simeq \mathbb{Z}^n \simeq M^*_{\mathbb{Z}}$

V kapitole o ideálových maticiach sme si vo vete 3.6.2 dokázali dôležitý izomorfizmus $K \simeq \mathbb{Q}^n \simeq M^*_{\mathbb{Q}}$. Pre dodržanie podstaty RSA si v tejto sekcii dokážeme podobný izomorfizmus nad celými číslami, pretože aj klasické RSA prebieha nad $\mathbb{Z}$.

Veta 4.2.1. *Buď θ celistvý prvok a $m_\theta(x) \in \mathbb{Z}[x]$ jeho minimálny polynóm stupňa n. Buď $\odot$ definované ako v 3.2.4. Nech $\mathcal{O}_K = \mathbb{Z}[\theta]$ je okruh celistvých prvkov. Potom*

$$\mathbb{Z}[x]/(m_\theta(x))(+,\cdot) \simeq \mathcal{O}_K(+,\cdot) \simeq \mathbb{Z}^n(+,\odot) \simeq M^*_{\mathbb{Z}}(+,\cdot).$$

je izomorfizmus okruhov.

Dôkaz. Z vety 3.6.2 vieme že platí $K \simeq \mathbb{Q}^n \simeq M^*_{\mathbb{Q}}$. Pretože $\mathcal{O}_K \subset K$, $\mathbb{Z}^n \subset \mathbb{Q}^n$ a $M^*_{\mathbb{Z}} \subset M^*_{\mathbb{Q}}$ su podokruhy uzavreté na binárne operácie sčítanie a násobenie v príslušných nadokruhoch, takže zobrazenia $\tau\colon K \to \mathbb{Q}^n$ a $H^*\colon \mathbb{Q}^n \to M^*_{\mathbb{Q}}$ zúžené na $\mathbb{Z}$ zachovávajú operácie sčítanie a násobenie v príslušných okruhoch. Z toho potom plynie izomorfizmus $\mathcal{O}_K \simeq \mathbb{Z}^n \simeq M^*_{\mathbb{Z}}$.

Z vety 3.4.4 vieme že platí izomorfizmus $\mathbb{R}^n \simeq \mathbb{R}[x]/(m_\theta(x))$. Zúžením na racionálne čísla potom platí $K \simeq \mathbb{Q}^n \simeq \mathbb{Q}[x]/(m_\theta(x))$. Opätovným zúžením na celé čísla potom platí $\mathcal{O}_K \simeq \mathbb{Z}^n \simeq \mathbb{Z}[x]/(m_\theta(x)) \Rightarrow \mathcal{O}_K \simeq \mathbb{Z}[x]/(m_\theta(x))$.

Tým je veta dokázaná. □

4.3 Ideálove mriežky

Dôležitým dôsledkom vety 4.2.1 je izomorfizmus $\mathbb{Z}[x]/(m_\theta(x)) \cong \mathbb{Z}^n$ pomocou ktorého môžeme definovať takzvané *Ideálové mriežky*. Pre úplnú definíciu si najprv označme bijektivne zobrazenie Φ_{m_θ}(zobrazenie t z 3.4.1 zúžené na $\mathbb{Z}$) dané predpisom

$$\begin{aligned} \Phi_{m_\theta} &: \mathbb{Z}^n \to \mathbb{Z}[x]/(m_\theta(x)) \\ (v_0, \ldots, v_{n-1}) &\mapsto v_0 + v_1 x + \cdots + v_{n-1}x^{n-1} + m_\theta(x). \end{aligned}$$

Takto definované zobrazenie je bijekcia aj ak uvažujeme faktorokruh $\mathbb{Z}[x]/(q(x))$ kde $q(x)$ je monický polynóm. Potom môžeme *ideálove mriežky* definovať nasledujúcim spôsobom.

Definícia 4.3.1. *Nech $\mathcal{L} \subset \mathbb{Z}^n$ je mriežka. Ak existuje monický polynóm $q(x) \in \mathbb{Z}[x]$ stupňa n, taký že $\Phi_q(\mathcal{L})$ je ideál v $\mathbb{Z}[x]/(q(x))$, potom $\mathcal{L}$ sa nazýva ideálová mriežka.*

Ideálovú mriežku ktorá náleží polynómu $q(x)$ budeme označovať $q(x)$-ideálová mriežka.

Následujúce lemma predstavuje základ celej kapitoly, pretože nám určuje presný popis mriežky $\mathcal{L}$ odvodenej z ideálu $A \leq \mathcal{O}_K$.

Lemma 4.3.2. *Nech K je číselné teleso, $\mathcal{O}_K = \mathbb{Z}[\theta]$ je okruh celistvých prvkov telesa K. Potom existuje bijekcia medzi ideálmi z $\mathcal{O}_K$ a $m_\theta(x)$-ideálovými mriežkami. Navyše ak $\alpha \in \mathcal{O}_K$, potom*

$$\tau(\alpha\mathcal{O}_K) = \mathcal{L}(H^*(\tau(\alpha))).$$

Obecne nech $A < \mathcal{O}_K$ je nenulový ideál, potom existujú dva prvky α a $\beta \in A$ také že

$$\tau(A) = \mathcal{L}(H^*(\tau(\alpha))) + \mathcal{L}(H^*(\tau(\beta))).$$

Dôkaz. Časť o bijekcii plynie z izomorfizmu $\mathbb{Z}[x]/(m_\theta(x)) \simeq \mathcal{O}_K$, špeciálne z izomorfizmu $\mathbb{Z}[x]/(m_\theta(x)) \simeq \mathbb{Z}^n \simeq \mathcal{O}_K$.

Nech $\alpha \neq 0 \in \mathcal{O}_K$ a $\alpha\mathcal{O}_K$, potom $\alpha\mathcal{O}_K = \{\alpha x \mid x \in \mathcal{O}_K\}$. Podľa lemma 3.3.4 máme

$$\tau(\alpha x) = \sum_{k=0}^{n-1} \alpha_k \tau(\theta^k x) = \sum_{k=0}^{n-1} \alpha_k H^k(\tau(x)) = H^*(\tau(\alpha))\tau(x).$$

Potom pre celý ideál $\alpha\mathcal{O}_K$ dostávame

$$\tau(\alpha\mathcal{O}_K) = \{H^*(\tau(\alpha))\tau(x) \mid \tau(x) \in \mathbb{Z}^n\} \overset{1.2.2}{=} \mathcal{L}(H^*(\tau(\alpha))).$$

Teraz si dokážeme poslednú časť. Existencia α a $\beta \in A$ plynie z vety 1.1.14. ideál A si potom vieme napísať ako $A = \alpha\mathcal{O}_K + \beta\mathcal{O}_K$. Z platnosti $\tau(\alpha\mathcal{O}_K) = \mathcal{L}(H^*(\tau(\alpha)))$ potom dostávame

$$\tau(A) = \tau(\alpha\mathcal{O}_K) + \tau(\beta\mathcal{O}_K) = \mathcal{L}(H^*(\tau(\alpha))) + \mathcal{L}(H^*(\tau(\beta))).$$

□

Jednoduchým dôsledkom tohto lemmatu je prípad kedy $A = \alpha\beta\mathcal{O}_K$.

Dôsledok 4.3.3. *Nech $A = \alpha\beta\mathcal{O}_K \neq 0$ je ideál v $\mathcal{O}_K = \mathbb{Z}[\theta]$ kde $\alpha, \beta \in \mathcal{O}_K$ sú dva odlišné prvočinitele a zobrazenie τ je definované ako v 2.4.1. Potom platí*

$$\tau(A) = \mathcal{L}(H^*(\tau(\alpha) \odot \tau(\beta))).$$

Dôkaz. Vieme že $A = \alpha\beta\mathcal{O}_K$ je hlavný ideál. Označme si $\gamma = \alpha\beta$. Potom platí

$$\tau(A) = \tau(\gamma\mathcal{O}_K) \overset{4.3.2}{=} \mathcal{L}(H^*(\tau(\gamma))) = \mathcal{L}(H^*(\tau(\alpha) \odot \tau(\beta))).$$

Pričom posledná rovnosť plynie z lema 3.3.4 pretože $\tau(\gamma) = \tau(\alpha\beta) = \tau(\alpha) \odot \tau(\beta)$. □

4.4 Množina reprezentantov S

V sekcii 2.3 sme si rozobrali množiny reprezentantov pre faktorokruhy $\mathcal{O}_K/A$. V tejto sekcii naopak ukážeme že pre ľubovolný faktorokruh $\mathbb{Z}^n/\mathcal{L}$ existuje jednotná množina reprezentantov, navyše to bude množina reprezentantov aj pre ľubovoľné $\mathcal{O}_K/A$.

Z vety 1.2.10 vieme že dve rozdielne bázy B, C nám popisujú rovnakú mriežku $\mathcal{L}$ práve vtedy ak existuje matica $U \in GL_n(\mathbb{Z})$ taká že $B = CU$. Zároveň z vety 1.2.11 vieme že každú štvorcovú regulárnu maticu M vieme napísať ako maticu B v HNF pre ktorú platí $B = MU$ kde $U \in GL_n(\mathbb{Z})$. Z toho teda plynie že pre ľubovoľnú bázu C s plnou hodnosťou existuje báza B s plnou hodnosťou ktorá popisuje tú istú mriežku.

Práve možnosť vyjadriť ľubovoľnú bázu v HNF je hlavný dôvod prečo vieme nájsť jednotnú množinu reprezentantov pre ľubovoľné $\mathbb{Z}^n/\mathcal{L}$. Báza v HNF je v horná trojuholníkova matica, takže z nej dokážeme jednoducho spočítať determinant mriežky $\mathcal{L}$ a rovnako z nej jednoducho spočítame všetky vektory množiny reprezentantov.

Najprv si ale dokážeme jedno pomocné lema.

Lemma 4.4.1. *Nech $\mathcal{L} = \mathcal{L}(B) \subset \mathbb{Z}^n$ je mriežka, B = HNF($\mathcal{L}$) = $[b_1, \ldots, b_n]$ je báza plnej hodnosti v HNF. Potom pre ortogonálnu bázu $B^* = [b_1^*, \ldots, b_n^*]$ platí*

$$B^* = diag\{b_{11}, \ldots, b_{nn}\}$$

kde b_{ii} je i-ty koeficient vektoru $b_i \in \mathbb{Z}^n$. Navyše $\det(\mathcal{L}) = \prod_{i=1}^n b_{ii}$.

Dôkaz. Lema dokážeme indukciou podľa $k \in \{1, \ldots, n\}$ pomocou vzorca z definície 1.2.3. Pre $k = 1$ platí $b_1^* = b_1$.

Teraz to chceme dokázať pre obecné k. Predpokladajme že pre $k-1$ to platí. Podľa indukčného predpokladu potom pre vektory $b_1^*, \ldots, b_{k-1}^*$ platí $b_i^* = (0, \ldots, b_{ii}, \ldots, 0)^T$ kde $b_{ii} \neq 0$. Z definície 1.2.3 vypočítame vektor b_k^* podľa vzorca

$$b_k^* = b_k - \sum_{j<k} \mu_{kj} b_j^* \; kde \; \mu_{ij} = \langle b_k, b_j^* \rangle / \langle b_j^*, b_j^* \rangle.$$

Potom obecne platí $\langle b_k, b_j^* \rangle = b_{kj} \cdot b_{jj}$, $\langle b_j^*, b_j^* \rangle = b_{jj}^2 \Rightarrow \langle b_k, b_j^* \rangle / \langle b_j^*, b_j^* \rangle = b_{kj}/b_{jj}$. Potom pre j-tu zložku vektoru b_k^* platí

$$b_{kj}^* = b_{kj} - (b_{kj}/b_{jj}) \cdot b_{jj}.$$

Z toho je jednoduché vidieť že $b_{kj}^* = 0$ pre všetky $j \in \{1, \ldots, k-1\}$. Keďže B je v HNF $\Rightarrow b_{ij} = 0$, $j > i$, $\forall\ 1 \leq i, j \leq n \Rightarrow b_{kj} = 0$, $j > k$, $\forall\ 1 \leq j \leq n \Rightarrow b_{kj}^* = 0$, $j > k$. Tak e $b_k^* = (0, \ldots, b_{kk}, \ldots, 0)^T$.

Časť o determinante sa už ukáže jednoducho. Z definície 1.2.6 platí $det(\mathcal{L}) = \prod_{i=1}^n ||b_i^*||$, kde $||b_i^*|| = \sqrt{b_{ii}^2} = b_{ii} \Rightarrow \det(\mathcal{L}) = \prod_{i=1}^n b_{ii}$. □

Veta 4.4.2. *Nech $\mathcal{L} = \mathcal{L}(B) \subset \mathbb{Z}^n$ je mriežka, B = HNF($\mathcal{L}$) = $[b_1, \ldots, b_n]$ je báza plnej hodnosti v HNF, $B^* = [b_1^*, \ldots, b_n^*]$ je ortogonálna báza vytvorená z B a $\mathcal{P}(B^*)$ je rovnobežnosten. Nech*

$$S = \mathcal{P}(B^*) \cap \mathbb{Z}^n = \{x = (x_1, \ldots, x_n) \mid x_i \in \mathbb{Z}, 0 \leq x_i < b_{ii}\}$$

kde b_{ii} je i-ty koeficient vektoru $b_i \in \mathbb{Z}^n$. Potom S je množina reprezentantov pre $\mathbb{Z}^n/\mathcal{L}$.

Dôkaz. Vieme že B je HNF báza pre mriežku $\mathcal{L}(B)$. To znamená že pre každý vektor b_i platí že koeficienty $b_{ii} \neq 0$ a $b_{ij} = 0$, $j > i$, $\forall\ 1 \leq i,j \leq n$, takže $b_{11}, \ldots, b_{nn} \in \mathbb{Z}$ sú diagonálne prvky.

Z lema 2.4.3 a vety 4.2.1 platí

$$\mathbb{Z}^n/\mathcal{L} \simeq \mathcal{O}_K/A.$$

Keďže $\mathcal{O}_K/A$ kde $A \leq \mathcal{O}_K$ je ideál, je konečný faktorokruh $\Rightarrow \mathbb{Z}^n/\mathcal{L}$ je konečný a keďže $|\mathcal{O}_K/A| = N(A) \Rightarrow |\mathbb{Z}^n/\mathcal{L}| = \det(\mathcal{L})$.

Z definície 1.2.6 a vety 4.4.1 môžme veľkosť $\mathbb{Z}^n/\mathcal{L}$ vyjadriť ako

$$|\mathbb{Z}^n/\mathcal{L}| = \det(\mathcal{L}) = \prod_{i=1}^{n} ||b_i^*|| = \prod_{i=1}^{n} b_{ii}.$$

Z definície S je hneď vidieť že $|S| = \prod_{i=1}^{n} b_{ii}$, takže S a $\mathbb{Z}^n/\mathcal{L}$ majú rovnakú veľkosť. Majme zobrazenie

$$\begin{aligned} \psi : S &\to \mathbb{Z}^n/\mathcal{L} \\ v &\mapsto v + \mathcal{L}. \end{aligned}$$

Chceme ukázať že ψ je bijekcia. Vďaka poznámke 1.2.5 vieme, že pre každý vektor $x \in \mathbb{Z}^n$ platí $x \in u + \mathcal{P}(B^*)$ kde $u \in \mathcal{L}$. Každý vektor $x \in \mathbb{Z}^n$ teda môžeme vyjadriť ako $x = u + v$ kde $u \in \mathcal{L}$ a $v \in \mathcal{P}(B^*)$. Zároveň je hneď vidieť že $v \in \mathbb{Z}^n$ pretože $x \in \mathbb{Z}^n$ a aj $u \in \mathcal{L} \subset \mathbb{Z}^n$.

Potom platí

$$x = u + v \equiv v \pmod{\mathcal{L}}.$$

Takže pre každé $x \in \mathbb{Z}^n$ platí $x \in v + \mathcal{L} = \psi(v)$, pričom $v \in (\mathcal{P}(B^*) \cap \mathbb{Z}^n) = S \Rightarrow$ ψ je surjektivné zobrazenie medzi rovnako veľkými konečnými množinami, takže ψ je bijekcia.

Teraz potrebujeme určiť ako vyzerá $\mathcal{P}(B^*) \cap \mathbb{Z}^n$. Vezmime $y \neq 0 \in (\mathcal{P}(B^*) \cap \mathbb{Z}^n)$. Z definície 1.2.4 vidíme že $y \notin \mathcal{L}(B)$ a zároveň $y = \sum_{i=1}^{n} z_i b_i^*$ kde $0 \leq z_i < 1$ pre všetky $i \in \{1, \ldots, n\}$. Pre i-tú zložku vektoru y potom platí $y_i = z_i b_{ii} \in \mathbb{Z}$ pretože z vety 4.4.1 platí $b_i^* = b_{ii} \neq 0$ a ostatné koeficienty v i-tom riadku sú rovné 0. $\Rightarrow z_i = y_i/b_{ii}$. Keďže $0 \leq z_i < 1 \Rightarrow 0 \leq y_i/b_{ii} < 1 \Rightarrow 0 \leq y_i < b_{ii}$ pre všetky $i \in \{1, \ldots, n\}$.

Takže $(\mathcal{P}(B^*) \cap \mathbb{Z}^n) \subset \{x = (x_1, \ldots, x_n) \mid x_i \in \mathbb{Z}, 0 \leq x_i < b_{ii}\}$. Opačná inklúzia platí okamžite takže $(\mathcal{P}(B^*) \cap \mathbb{Z}^n) = \{x = (x_1, \ldots, x_n) \mid x_i \in \mathbb{Z}, 0 \leq x_i < b_{ii}\}$ a tým je dôkaz hotový. □

Vďaka vete 4.4.2 a dôsledku 4.3.3 si môžeme definovať nasledujúce pojmy.

Definícia 4.4.3. *Pre $\alpha, \beta \in \mathcal{O}_K$ definujeme mriežku $\mathcal{L}_{\alpha,\beta}$ ako*

$$\mathcal{L}_{\alpha,\beta} = \mathcal{L}(H^*(\tau(\alpha) \odot \tau(\beta))).$$

HNF bázu $\mathcal{L}_{\alpha,\beta}$ budeme označovať $B_{\alpha,\beta}$ a príslušnú ortogonálnu bázu budeme označovať

$$B^*_{\alpha,\beta} = diag\{b_{11}, \ldots, b_{nn}\}$$

$b_{11}, \ldots, b_{nn} \in \mathbb{Z}$ *a* $b_{ii} > 0$. *Množinu reprezentantov budeme označovať* $S_{\alpha,\beta}$ *a budeme rozumieť množinu*

$$S_{\alpha,\beta} = \{(x_1, \cdots, x_n) \in \mathbb{Z}^n \mid x_i \in \mathbb{Z}, 0 \leq x_i < b_{ii}\}.$$

Priamym dôsledkom vety 4.4.2 je nasledujúce lemma.

Lemma 4.4.4. *Nech* $\alpha, \beta \in \mathcal{O}_K$ *sú dva odlišné prvočinitele a* $A = \alpha\beta\mathcal{O}_K \leq \mathcal{O}_K = \mathbb{Z}[\theta]$. *Potom* $S_{\alpha,\beta}$ *je množina reprezentantov pre faktorokruhu* $\mathcal{O}_K/A$.

Dôkaz. Z vety 4.4.2 a bodu (2) z lematu 3.5.1 plati

$$\begin{aligned} |S_{\alpha,\beta}| = \prod_{i=1}^{n} &= |\det(H^*(\tau(\alpha) \odot \tau(\beta)))| \\ &= |\det(H^*(\tau(\alpha)))| \cdot |\det(H^*(\tau(\beta)))| = \det(\mathcal{L}_{\alpha,\beta}). \end{aligned}$$

Z vety 3.6.2 plati

$$\begin{aligned} N(A) &= |N(\alpha \cdot \beta)| = |N(\alpha)| \cdot |N(\beta)| \\ &= |det(H^*(\tau(\alpha)))| \cdot |det(H^*(\tau(\beta)))| = \det(\mathcal{L}_{\alpha,\beta}). \end{aligned}$$

Takže $N(A) = |S_{\alpha,\beta}|$. Keďže $\mathcal{O}_K = \mathbb{Z}[\theta]$, potom pre každé $\alpha \in K$ platí $\tau(\alpha) \in \mathbb{Z}^n$, takže

$$\alpha \equiv \beta \pmod{A} \Leftrightarrow \tau(\alpha) \equiv \tau(\beta) \pmod{\mathcal{L}_{\alpha,\beta}}.$$

Potom lema plynie okamžite vďaka vete 4.4.2. □

4.5 Eulerova veta pre mriežky

V tejto sekcii si dokážeme platnosť Eulerovej vety aj pre mriežky.

Veta 4.5.1. *Nech* $K = \mathbb{Q}(\theta)$ *je číselné teleso stupňa* n, $\mathcal{O}_K = \mathbb{Z}[\theta]$ *je okruh celistvých prvkov telesa* K, $\alpha, \beta \in \mathcal{O}_K$ *dva odlišné prvočinitele,* $A = \alpha\beta\mathcal{O}_K$ *ideál a* $\mathcal{L}_{\alpha,\beta}$ *mriežka daná ideálom* A. *Potom pre každé* $\tau(a) \in \mathbb{Z}^n$, $k \in \mathbb{Z}$, $k \geq 0$ *platí*

$$\tau(a)^{\odot(k\varphi(\alpha,\beta)+1)} \equiv \tau(a) \pmod{\mathcal{L}_{\alpha,\beta}}.$$

Dôkaz. Z vety 2.2.1 vieme že platí

$$a^{k\varphi(A)+1} \equiv a \pmod{A}.$$

Následne si $\varphi(A)$ môžme vyjadriť ako

$$\begin{aligned} \varphi(A) = \varphi(\alpha\beta\mathcal{O}_K) &= \varphi(\alpha\mathcal{O}_K) \cdot \varphi(\beta\mathcal{O}_K) \\ &= (N(\alpha\mathcal{O}_K) - 1) \cdot (N(\alpha\mathcal{O}_K) - 1) \\ &= (|\det(H^*(\alpha))| - 1) \cdot (|\det(H^*(\beta))| - 1) \\ &= \varphi(\alpha,\beta). \end{aligned}$$

Po aplikácii zobrazenia τ na $a^{k\varphi(\alpha,\beta)+1}$ a A dostávame

$$\tau(A) = \mathcal{L}_{\alpha,\beta} \quad a \quad \tau(a^{k\varphi(\alpha,\beta)+1}) = \underbrace{\tau(a) \cdot \cdots \cdot \tau(a)}_{(k\varphi(\alpha,\beta)+1)-krát} = \tau(a)^{\odot(k\varphi(\alpha,\beta)+1)}$$

čím je veta dokázaná. □

Teraz už máme dokázané všetko potrebné na to aby sme mohli RSA algoritmus vyjadriť pomocou mriežok a číselných telies.

5. Algoritmus RSA

V tejto kapitole si predstavíme algoritmus RSA napísaný pomocou mriežok a číselných telies. Rovnako predvedieme tento algoritmus na príklade.

5.1 Algoritmus

$n \geq 1$, $K/\mathbb{Q}$ je číselné teleso stupňa n, $\mathcal{O}_K = \mathbb{Z}[\theta] \subset K$ je okruh celistvých prvkov telesa K, $\alpha, \beta \in K$ sú dva rozdielne prvočinitele telesa K, $A = \alpha\beta\mathcal{O}_K$ je hlavný ideál, $H^*(\tau(\alpha)\odot\tau(\beta))$ je ideálova matica pre ideál A, $\mathcal{L}_{\alpha,\beta} = \mathcal{L}(H^*(\tau(\alpha)\odot\tau(\beta)))$ je mriežka generovaná maticou $H^*(\tau(\alpha)\odot\tau(\beta))$, $B_{\alpha,\beta} = \mathrm{HNF}(\mathcal{L}_{\alpha,\beta})$ je báza mriežky $\mathcal{L}_{\alpha,\beta}$ v HNF, $B^*_{\alpha,\beta} = diag\{b_{11}, \ldots, b_{nn}\}$ je príslušná ortogonálna báza.

- Parametre: $\varphi(\alpha,\beta) = (|\det(H^*(\tau(\alpha)))| - 1)(|\det(H^*(\tau(\beta)))| - 1)$, $S_{\alpha,\beta} = \{x = (x_1, \ldots, x_n) \in \mathbb{Z}^n \mid 0 \leq x_i < b_{ii}\}$, $1 \leq e \leq \varphi(\alpha,\beta)$ a $1 \leq d \leq \varphi(\alpha,\beta)$ sú čísla také že $ed \equiv 1 \pmod{\varphi(\alpha,\beta)}$.
- Verejné kľúče: Matica H, mriežka $\mathcal{L}(B_{\alpha,\beta}) = \mathcal{L}_{\alpha,\beta}$ a prirodzené číslo e.
- Súkromné kľúče: Ideálové matice $H^*(\tau(\alpha))$, $H^*(\tau(\beta))$, báza $H^*(\tau(\alpha)\odot\tau(\beta))$ mriežky $\mathcal{L}_{\alpha,\beta}$ a prirodzené číslo d.
- Šifrovanie: Pre ľubovoľnú správu $\tau(a) \in S_{\alpha,\beta}$ získame šifrovanú správu $\tau(c)$ ako $\tau(c) \equiv \tau(a)^{\odot e} \pmod{\mathcal{L}_{\alpha,\beta}}$.
- Dešifrovanie: $\tau(c)^{\odot d} \equiv \tau(a)^{\odot de} \equiv \tau(a)^{\odot(k\varphi(\alpha,\beta)+1)} \equiv \tau(a) \pmod{\mathcal{L}_{\alpha,\beta}}$.

5.2 Príklad

Predpokládajme že chceme zašífrovať správu AHOJ. Správa má 4 písmená takže si potrebujeme zvoliť číselné teleso ktorého stupeň rozšírenia bude 4. Voľme napríklad teleso $K = \mathbb{Q}(\zeta_5)$ kde $\zeta_5 = e^{(2i\pi)/5}$ je primitívna piata odmocnina z jednej. Celistvá báza $\mathbb{Q}(\zeta_5)$ je potom $\{1,\zeta_5,\zeta_5^2,\zeta_5^3\}$, $\mathcal{O}_K = \mathbb{Z}[\zeta_5]$ a minimálny polynóm čísla ζ_5 je polynóm $m_{\zeta_5}(x) = x^4 + x^3 + x^2 + x + 1$. Ďalej si zvolíme dva rôzne prvočinitele. V tomto prípade to môžu byť prvočísla 7 a 13. Potom $A = 91\mathcal{O}_K$ a uvažujme faktorokruh $\mathcal{O}_K/A$.

Podľa ASCII tabuľky si môžme jednotlivé písmená napísať ako čísla $A = 65$, $H = 72$, $O = 79$, $J = 74$. Následne si môžme vziať $\alpha \in \mathbb{Z}[\zeta_5]$ také že $\alpha = 65 + 72\zeta_5 + 79\zeta_5^2 + 74\zeta_5^3$. Teraz si $\alpha, p\ a\ q$ prevedieme na vektory

$$\tau(\alpha) = \begin{pmatrix} 65 \\ 72 \\ 79 \\ 74 \end{pmatrix}, \quad \tau(p) = \begin{pmatrix} 7 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \tau(q) = \begin{pmatrix} 13 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Následne si spočítame matice $H^*(\tau(7)), H^*(\tau(13))$ *a* $H^*(\tau(7) \odot \tau(13))$ pre ktoré platí

$$H^*(\tau(i)) = \begin{pmatrix} j & 0 & 0 & 0 \\ 0 & j & 0 & 0 \\ 0 & 0 & j & 0 \\ 0 & 0 & 0 & j \end{pmatrix},\ j = 7{,}13 \quad a \quad H^*(\tau(7) \odot \tau(13)) = \begin{pmatrix} 91 & 0 & 0 & 0 \\ 0 & 91 & 0 & 0 \\ 0 & 0 & 91 & 0 \\ 0 & 0 & 0 & 91 \end{pmatrix}.$$

Vidíme že matica $H^*(\tau(7) \odot \tau(13))$ je zároveň v HNF, takže môžme stľpcové vektorý tejto matice vziat ako bázu a vytvoriť mriežku $\mathcal{L}_{7,13} = \mathcal{L}(H^*(\tau(7) \odot \tau(13)))$. Následne $\varphi(7{,}13) = (7^4 - 1) \cdot (13^4 - 1) = 68544000$ a z definície 4.4.3 je množina reprezentantov pre $\mathcal{L}_{7,13} = \mathcal{L}(H^*(\tau(7) \odot \tau(13)))$ množina vektorov

$$S_{7,13} = \{x = (x_1, x_2, x_3, x_4) \mid 0 \leq x_i < 91, 1 \leq i \leq 4\}.$$

V ďalšom kroku by sme si zvolili čísla e, d také že $1 \leq e$,$d \leq \varphi(7{,}13)$ kde $ed \equiv 1 \pmod{\varphi(7{,}13)}$. Pre tento prípad platí $e = 11$ a $d = 24925091$.

Keďže $\tau(\alpha) \in S_{7,13}$, sifrovaním dostaneme správu $\tau(c) \equiv \tau(\alpha)^{\odot 11} \pmod{\mathcal{L}_{7,13}}$. a dešifrovaním $\tau(c)^{\odot 24925091}$ dostaneme našu pôvodnú správu $\tau(\alpha)$.

Závěr

Cieľom tejto práce bolo matematicky popísať a ukázať chod RSA algoritmu na číselných telesách a na mriežkach. Tento cieľ sa nám podarilo splniť za predpokladu že $\mathcal{O}_K = \mathbb{Z}[\theta]$ je okruh celistvých prvkov číselného telesa $K = \mathbb{Q}(\theta)$ a že ideál $A \leq \mathcal{O}_K$ berieme ako $A = \alpha\beta\mathcal{O}_K$ kde α,$\beta \in \mathcal{O}_K$ sú dva odlišné prvočinitele.

Možné návrhy na zlepšenie tejto práce z hľadiska teórie čísel sú dokázať kapitolu 4 pre obecné $\mathcal{O}_K$ a vytvoriť RSA algoritmus aj pre obecné ideály $A \leq \mathcal{O}_K$, čím by sme dostali RSA v obecnej podobe. Z kryptografického hľadiska by bolo zaujímavé napísať prácu o možných útokoch na tento algoritmus a bezpečnosti. Samostatnú prácu by napríklad šlo vypracovať o útoku za predpokladu znalosti faktorizácie v $\mathbb{Z}$.

Seznam použité literatury

Cohen, H. (1996). *A course in computational algebraic number theory*, volume 138 of *Third edition*. Springer Science & Business Media. ISBN 3-540-55640-0. URL https://link.springer.com/book/10.1007/978-3-662-02945-9.

Kala, V. (2022). Úvod do komutativní algebry. URL http://karlin.mff.cuni.cz/~kala/files/UKA22.pdf.

Micciancio, D. (2001). 1: Introduction to lattices. URL https://cseweb.ucsd.edu/classes/wi10/cse206a/lec1.pdf.

Micciancio, D. (2010). Improving lattice based cryptosystem using the hermite normal form. URL https://cseweb.ucsd.edu/~daniele/papers/HNFcrypt.pdf.

Milne, J. S. (2020). *Algebraic number theory*. 3.08. JS Milne. URL https://www.jmilne.org/math/CourseNotes/ANT.pdf.

Narkiewicz, W. (1974). *Elementary and analytic theory of algebraic numbers*, volume 57 of *Third edition*. Springer. ISBN 978-3-662-07001-7. URL https://archive.org/details/ElementaryAndAnalyticTheoryOfAlgebraicNumbers3rdEdition/page/n13/mode/1up?view=theater.

Stewart, I. a Tall, D. (2002). *Algebraic number theory and Fermat's last theorem*. Third edition. CRC Press. ISBN 1-56881-119-5.

Zheng, Z. a Liu, F. (2022). On the high dimensional rsa algorithm–a public key cryptosystem based on lattice and algebraic number theory. *arXiv preprint arXiv:2202.02675*. URL https://arxiv.org/pdf/2202.02675.pdf.