SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Gitter: Från detaljerad teori till kryptering

av

Fredrik Heed Elvegård

2026 - No K17

Gitter: Från detaljerad teori till kryptering

Fredrik Heed Elvegård

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Filip Jonsson Kling

2026

Sammanfattning

I denna uppsats ges detaljerade bevis av grundläggande satser om gitter samt en redogörelse kring olika kryptosystem kopplat till gitter. Avseendet är att läsare på grundnivå i matematik ska snabbt kunna ta till sig bevisen och få en stark förståelse för gitter och hur de appliceras till kryptering. Vi bevisar ett antal gitteregenskaper som tillslut tillåter oss att bevisa Minkowskis sats. Denna sats hjälper oss att visa att vissa mängder som till synes liknar gitter aldrig kan vara gitter och den låter oss även fastställa egenskaper hos den kortaste nollskilda vektorn i ett gitter. Gitterteorin har betydelse för kryptosystemen GGH och NTRU som sedan förklaras i detalj. Slutligen förs en diskussion kring varför den privata nyckleln i NTRU förmodligen är den kortaste nollskillda vektorn i det associerade gittret.

Abstract

In this paper we give detailed proofs of fundamental theorems regarding lattices and discuss various crypto-systems associated with lattices. The aim is to allow undergraduate mathematic students to quickly interpret the proofs and gain a strong understanding of lattices and how they apply to cryptography. We prove a number of lattice properties that eventually allows us to prove Minkowskis theorem. This theorem helps us show that certain sets that may look like lattices can never be lattices and it also lets us determine properties of the shortest non-zero vector in a lattice. The lattice theory has a meaningful role in the crypto-systems GGH and NTRU that are then explained in details. Finally there is a discussion about why the private key in NTRU probably is the shortest nonzero vector in the associated lattice.

Förord

Jag vill tacka min handledare Filip Jonsson Kling som har varit en mycket aktiv handledare och hjälpt till mycket i alla delar av arbetet.

Innehåll

1 Introduktion

Kryptering är en teknik som säkerställer att meddelanden som skickas endast kan läsas av avsändaren och mottagaren. Förenklat finns det en privat och publik nyckel. Den publika nyckeln används av avsändaren för att omforma meddelandet innan det skickas och den privata nyckeln, som bara mottagaren känner till, används för att forma tillbaka meddelandet. Tekniken fungerar när det är tillräckligt matematiskt svårt att forma tillbaka meddelandet endast med de publika parametrarna. Kryptering har funnits länge och användes exempelvis under andra världskriget men kryptosystemen på den tiden slutade fungera när datorerna kunde lösa de matematiska problemen. Sedan dess har säkrare kryptosystem utvecklats, däribland det kända systemet RSA, och dessa kan exempelvis användas för säker elektronisk röstning eller kryptovaluta (Khan m.fl. 2023). Men hotet om det ännu snabbare kvantdatorerna motiverar till fortsatt utveckling av säkrare kryptosystem och i denna uppsats ska vi titta på systemen som är associerade med det som kallas gitter.

Gitterbaserade kryptosysem till skillnad från andra vanliga kryptosystem är mer resistent mot kvantdatorer. Anledningen är att problemen som behöver lösas för att knäcka dessa system kan bli tillräckligt svåra även för kvantdatorer. Detta upptäcktes först 1996 och sedan dess har flera gitterbaserade kryptosystem utvecklats, däribland GGH och NTRU (Pradhan m.fl. 2019). Kryptering baserat på gitter är alltså ett relativt nytt område inom kryptografi som inte är lika välförstådd som tidigare kryptosystem (Hoffstein m.fl. 2008). Denna potential för extra säker kryptering och att det behövs mer förståelse gör detta område särkilt angeläget att studera.

Hur kan vi då börja förstå dessa kryposystem bättre? Både uppbyggnaden av dessa system och de matematiska problemen som utgör säkerheten i systemen är grundat i teori kring det som kallas gitter. Därmed, för att verkligen förstå och kunna bidra till att utveckla dessa kryptosystem, behövs stark förståelse av gitterteori.

Detta arbete ämnar att först ge en stark grund i gitterteori och sedan visa hur det används för att skapa kryptosystem. För att säkerställa full förståelse av gitterteorin kommer fler detaljer att bevisas eller hänvisas till än många andra texter om gitter. De resultat som hänvisas till annan litteratur är oftast huvudresultat inom linjär algebra, analys eller algebra. I övrigt krävs det grundkunskaper i matematik på kandidatnivå för att förstå alla detaljer.

Sedan går vi igenom kryptosystemet GGH som är en naturlig applikation av

gitterteorin. Efter det tas kryptosystemet NTRU upp som enklast förklaras med hjälp av vissa polynomringar. Teorin kring polynomringarna kommer hänvisas till annan litteratur då detta arbete i huvudsak berör gitterteori. Kryptosystemet NTRU kan nämligen också förklaras med hjälp av gitter men där appliceras gitterteorin mest naturligt till de matematiska problemen som utgör säkerheten för systemet. Det finns en del viktiga frågor kring dessa matematiska problem som aldrig formelt har bevisats och denna uppsats avslutas med att föra diskussioner kring detta kopplat till gitterteorin.

2 Gitterteori

Först behöver vi lite definitioner och notationer för att resten av sektionen ska bli läsbar.

Definition 2.1. Låt $v_1, ..., v_n \in \mathbb{R}^m$ vara en mängd linjärt oberoende vektorer, då är

$$L = \left\{ a_1 v_1 + ... + a_n v_n \ : \ a_1, ..., a_n \in \mathbb{Z} \right\}$$

ett *gitter*. Vektorerna $v_1, ..., v_n$ kallas för en bas för L. Antalet basvektorer n, där $n \leq m$, kallas *dimensionen* av gittret. För många sammanhang kommer $n = m$, då sägar man att gittret har *maximal rang*.

Definition 2.2. En mängd $L \subset \mathbb{R}^m$ är en *diskret additiv delgrupp* om den är sluten under addition och det finns ett $\varepsilon > 0$ sådan att för varje $v \in L$ gäller det att

$$L \ \cap \ \left\{ w \in \mathbb{R}^m \ : \ |w - v| < \varepsilon \right\} = \left\{ v \right\}.$$

Mer intuitivt betyder denna definition att L är additativ och att det finns en punkterad omgivning med radie ε kring varje $v \in L$ som inte korsar någon punkt i L. Nedan ska vi visa att Definition 2.1 och Definition 2.2 är ekvivalenta. Givet detta vet vi att det finns en kortaste längd på nollskilda vektorer i L.

Notation. Låt L vara ett gitter. Vi betecknar den kortaste längden på nollskilda vektorer i L som $\lambda_1(L)$.

Definition 2.3. Låt $L \subset \mathbb{R}^m$ vara ett gitter av dimension n med någon bas $v_1, ..., v_n$. Vi definierar *fundamentaldomänen* $\mathcal{F}(v_1, ..., v_n)$ som mängden

$$\left\{ a_1 v_1 + ... + a_n v_n \ : \ 0 \leq a_1, ..., a_n < 1 \right\}.$$

Här är alltså alla $a_i \in \mathbb{R}$. Om det är tydligt vilken bas vi avser skriver vi bara $\mathcal{F}$. Vi definierar även den *slutna fundamentaldomänen* $\bar{\mathcal{F}}(v_1, ..., v_n)$ som mängden

$$\left\{ a_1 v_1 + ... + a_n v_n \ : \ 0 \leq a_1, ..., a_n \leq 1 \right\}.$$

Notation. När vi pratar om en vektor $x \in \mathbb{R}^n$ kommer $x_1, ..., x_n$ vara dess kordinater och x_i är en godtycklig kordinat av x.

2.1 Två ekvivalenta definitioner för ett gitter

Sats 2.4. *En mängd L är ett gitter om och endast om det är en diskret additativ delgrupp.*

Lemma 2.5. *En mängd $L \subset \mathbb{R}^m$ är en diskret additativ delgrupp om och endast om den är sluten under addition och det finns ett $\varepsilon > 0$ sådan att*

$$L \cap \left\{ w \in \mathbb{R}^m : |w| < \varepsilon \right\} = \left\{ 0 \right\}. \tag{1}$$

Bevis. På grund av additiviteten kommer $v = 0$ alltid finnas i en diskret additativ delgrupp och då är egenskapen (1) uppfyllt.

Det återstår att visa att en mängd med egenskap (1) är en diskret addativ delgrupp. Låt $L' \subset \mathbb{R}^m$ vara en mängd med egenskap (1). Ta ett $v \in L'$ och ett $w \in \mathbb{R}^m$ sådan att $|w-v| < \varepsilon$ och $w \neq v$. Om vi visar att $w \notin L'$ uppfylls definitionen av en diskret additativ delgrupp och vi är vi klara. Anta därför att $w \in L'$. På grund av additiviteten hos L' är $w - v \in L'$. Men (1) säger att $w - v \in \mathbb{R}^m$, $w - v \neq 0$ och $|w - v| < \varepsilon$ implikerar att $w - v \notin L'$ vilket blir en motsägelse. Alltså kan inte antagandet att $w \in L'$ stämma. □

Beviset för Sats 2.4 kommer från föreläsningsanteckningar (Vaikuntanathan 2011) men fler detaljer och förklaringar ges i detta bevis.

Bevis av Sats 2.4 del 1: Ett gitter är en diskret additativ delgrupp. Givet ett gitter $L \subset \mathbb{R}^m$ med en bas $v_1, ..., v_n$, låt V vara matrisen med basvektorerna som rader och låt $\tilde{V}$ vara matrisen med basens Gram-smith-orthogonalisering $\tilde{v_1}, ..., \tilde{v_n}$ som rader. Idén är att först visa att $\lambda_1(L) = \varepsilon$ alltid är strikt större än 0 och sedan använda Lemma 2.5.

Låt $x \in \mathbb{Z}^n$ vara en godtyckligt heltalsvektor där $x \neq 0$. Då är xV en godtycklig nollskilld vektor i L. Vi ska först visa att

$$||xV|| \geq \min_{\mathrm{i}=1,\ldots,\mathrm{n}} \|\tilde{v_i}\| > 0. \tag{1}$$

Låt $j \in 1, ..., n$ vara det största indexet sådan att $x_j \neq 0$. Vi ska beräkna $|\langle xV, \tilde{v_j} \rangle|$ på två olika sätt vilket kommer ge oss olikheten (1). Vi har att

$$|\langle xV, \tilde{v_j} \rangle| = |\langle \sum_{i=1}^{n} x_i v_i, \tilde{v_j} \rangle| = |\sum_{i=1}^{n} x_i \langle v_i, \tilde{v_j} \rangle| = |x_j| \langle \tilde{v_j}, \tilde{v_j} \rangle = |x_j| \cdot ||\tilde{v_j}||^2. \tag{2}$$

För de första två likheterna i (2) har vi utvecklad xV samt använt räknelagar för skalärprodukt. För den tredje likheten använder vi följande:

- Om $i < j$ är

$$0 = \langle \tilde{v_i}, \tilde{v_j} \rangle = \langle v_i - \sum_{k=1}^{i-1} \mu_{i,k} \tilde{v_k}, \tilde{v_j} \rangle = \langle v_i, \tilde{v_j} \rangle - \langle \sum_{k=1}^{i-1} \mu_{i,k} \tilde{v_k}, \tilde{v_j} \rangle = \langle v_i, \tilde{v_j} \rangle. \qquad (3)$$

Här har vi först skrivit om $\tilde{v_i}$ enligt Gram-Schmidt ortogonaliseringen. Sedan har vi utnyttjat räknelagar för skalärprodukt och använt att $\tilde{v_k}$ för $1 \leq k < j$ är ortogonala mot $\tilde{v_j}$. Ekvation (3) visar att $\tilde{v_j}$ är ortogonal mot $\text{Span}(v_{j-1}, v_{j-2}, ..., v_1)$.

- Om $i > j$ är alla $x_i = 0$ från hur vi definierade j.

Därmed är den enda nollskilda termen i summan i (2) när $j = i$ och då har vi att

$$\langle \tilde{v_j}, \tilde{v_j} \rangle = \langle v_j - \sum_{k=1}^{j-1} \mu_{j,k} \tilde{v_k}, \tilde{v_j} \rangle = \langle v_j, \tilde{v_j} \rangle. \qquad (4)$$

Här har vi använt samma tekniker som i (3).

Vidare har vi enligt Cauchy-Schwarz olikhet att

$$|\langle xV, \tilde{v_j} \rangle| \leq \|xV\| \cdot \|\tilde{v_j}\|. \qquad (5)$$

Slår vi ihop (2) och (5) får vi att

$$\|xV\| \geq \frac{|\langle xV, \tilde{v_j} \rangle|}{\|\tilde{v_j}\|} = |x_j| \cdot \|\tilde{v_j}\| \geq \|\tilde{v_j}\| \geq \min_{\text{i=1,...,n}} \|\tilde{v_i}\| > 0 \qquad (5)$$

Här försvninner $|x_j|$ för att x_j definierades en nollskild koordinat i en haltalsvektor vilket leder till att $|x_j| \geq 1$. Att näst sista uttrycket är strikt större än noll följer från att alla $\tilde{v_i}$ är linjärt oberoende och därmed nollskilda. Ekvation (5) visar att $\lambda_1(L) > 0$.

Nu kan vi sätta $\varepsilon = \lambda_1(L)$ och det föjer direkt att

$$L \cap \left\{ w \in \mathbb{R}^m \, : \, |w| < \varepsilon \right\} = \left\{ 0 \right\}.$$

Enligt Lemma 2.5 är då L en diskret additativ delgrupp. $\square$

Bevis av Sats 2.4 del 2: En diskret additativ delgrupp är ett gitter. Givet en diskret additativ grupp $L \subset \mathbb{R}^m$ ska vi konstruera en bas $v_1, ..., v_n$ sådan att

$$L = \Big\{a_1v_1 + ... + a_nv_n \ : \ a_1, ..., a_n \in \mathbb{Z}\Big\}$$

vilket visar att L är ett gitter.

Välj ett $y \in L$ sådan att $\Big\{ay \ : \ 0 < a < 1\Big\} \cap L = \emptyset$. Detta är möjligt i och med att avståndet mellan alla vektorer i L är åtminstonde $\varepsilon > 0$ och då måste det finnas ändligt många gittervektorer i ett begränsat linjesegment. I något sådant linjesegment väljer vi det nollskillda $y \in L$ som är närmast 0.

Låt $v_1 = y$ och anta att vi har valt $v_1, ..., v_i$. Då väljer vi v_{i+1} genom att först välja ett $y \in L$ som inte är i $\text{Span}(v_1, ..., v_i)$. Om det inte finns ett sådan y är vi klara och vi sätter $n = i$. Annars tittar vi på mängden

$$A = \bar{\mathcal{F}}(v_1, ..., v_i, y) \setminus \text{Span}(v_1, ..., v_i) \cap L.$$

Då kommer A innehålla åtminstonde y. Eftersom $\bar{\mathcal{F}}(v_1, ..., v_n, y)$ är ett begränsat område i $\mathbb{R}^n$ och att L är diskret finns det ändligt många vektorer i A. Därför kan vi välja v_{i+1} att vara en av ändligt många vektorer i A som ligger närmast $\text{Span}(v_1, ..., v_i)$.

Nu ska vi visa varför $v_1, ..., v_n$ är en bas för ett gitter som är lika med L, alltså att

$$L' = \Big\{a_1v_1 + ... + a_nv_n \ : \ a_1, ..., a_n \in \mathbb{Z}\Big\} = L.$$

Vi säkerställde i konstruktionen att $v_1, ..., v_n$ är i L och på grund av att additiviteten hos L måste då $L' \subset L$.

För att visa att $L \subset L'$ tar vi först en godtycklig vektor $z \in L$. Vi ska visa att z kan skrivas som $a_1v_1 + ... + a_nv_n$ där $a_1, ..., a_n \in \mathbb{Z}$.

Vi säkerställde i konstruktionen att det inte finns vektorer i L utanför $\text{Span}(v_1, ..., v_n)$ och att $v_1, ..., v_n$ är linjärt oberoende. Därför kan z skrivas som $\sum a_iv_i$ där $a_i \in \mathbb{R}$. Vi ska då visa att alla a_i måste vara heltal.

Sätt $z' = \sum \lfloor a_i \rceil v_i$ som också är i L på grund av additiviten. Då har vi att

$$z - z' = \sum (a_i - \lfloor a_i \rceil) v_i = (a_n - \lfloor a_n \rceil) v_n + \sum_{i=1}^{n-1} (a_i - \lfloor a_i \rceil) v_i = (a_n - \lfloor a_n \rceil) \tilde{v_n} + \sum_{i=1}^{n-1} b_i v_i. \tag{1}$$

Här är b_i några tal i $\mathbb{R}$. Att det finns sådana b_i för sista likheten i (1) kan visas på följande sätt. Givet att vi har applicerat Gram Schmidt ortogonalisering på $v_1, ..., v_n$ i den ordningen kommer

$$(a_n - \lfloor a_n \rceil) v_n = (a_n - \lfloor a_n \rceil)(\tilde{v_n} + \sum_{k=1}^{n-1} \mu_{n,k} \tilde{v_k}) = (a_n - \lfloor a_n \rceil) \tilde{v_n} + \sum_{k=1}^{n-1} (a_n - \lfloor a_n \rceil) \mu_{n,k} \tilde{v_k}. \tag{2}$$

I den sista summan i (2) är $(a_n - \lfloor a_n \rceil)\mu_{n,k}$ skalärer och $\tilde{v_k}$ kommer aldrig uttryckas med en vetkor v_n, därför är hela den summan i $\text{Span}(v_1, ..., v_{n-1})$. Även den sista summan i näst sista uttrycket i (1) är i $\text{Span}(v_1, ..., v_{n-1})$ och summan av båda summorna är också i detta Span. Därför kan vi vara säkra på att vi kan skriva $z - z'$ som $(a_n - \lfloor a_n \rceil)\tilde{v_n}$ adderat med någon vektor i $\text{Span}(v_1, ..., v_{n-1})$.

Vi visade i del 1 av satsen att $\tilde{v_n}$ är ortogonal mot $\text{Span}(v_1, ..., v_{n-1})$. Distansen mellan någon vektor $p \in \mathbb{R}^m$ och detta Span är längden på projektionen av p på en vektor som är ortogonal mot detta Span som vi vet att $\tilde{v_n}$ är. Vi har då att

$$dist(z - z', \text{Span}(v_1, ..., v_{n-1})) = \frac{|\langle z - z', \tilde{v_n} \rangle|}{\|\tilde{v_n}\|^2} \|\tilde{v_n}\| = (a_n - \lfloor a_n \rceil) \|\tilde{v_n}\|. \tag{3}$$

För sista likheten i (3) använde vi utvecklingen av $z - z'$ i (1), räknelagar, att $\tilde{v_n}$ är ortogonal mot alla vektorer i $\text{Span}(v_1, ..., v_{n-1})$ och att $0 \leq (a_n - \lfloor a_n \rceil)$ för att få att $|\langle z - z', \tilde{v_n} \rangle| = (a_n - \lfloor a_n \rceil) \langle \tilde{v_n}, \tilde{v_n} \rangle$. På liknande sätt har vi att

$$dist(v_n, \text{Span}(v_1, ..., v_{n-1})) = \frac{|\langle v_n, \tilde{v_n} \rangle|}{\|\tilde{v_n}\|^2} \|\tilde{v_n}\| = \|\tilde{v_n}\|. \tag{4}$$

Här använde vi att $\langle v_n, \tilde{v_n} \rangle = \langle \tilde{v_n}, \tilde{v_n} \rangle$ som vi visade i del 1 av satsen. Eftersom $0 \leq (a_n - \lfloor a_n \rceil) < 1$ har vi nu att

$$dist(z - z', \text{Span}(v_1, ..., v_{n-1})) < dist(v_n, \text{Span}(v_1, ..., v_{n-1})). \tag{5}$$

I och med att v_n valdes till en gittervektor närmast $\text{Span}(v_1, ..., v_{n-1})$ och att $z - z' \in L$ visar (5) att $dist(z - z', \text{Span}(v_1, ..., v_{n-1})) = 0$. Då måste $(a_n - \lfloor a_n \rceil) = 0$ och

alltså är a_n ett heltal. Sedan kan man fortsätta samma process om sätter z till

$$z - a_n v_n, \quad z - a_n v_n - a_{n-1} v_{n-1}, \quad ..., \quad a_1 v_1 + a_2 v_2, \quad a_1 v_1.$$

För $z = a_1 v_1$ finns inget $\text{Span}(v_1, ..., v_{n-1})$ men detta kan ersättas med 0. Detta ger att alla a_i $(1 \leq i \leq n)$ är heltal vilket vi var ute efter. □

Anmärkning 2.6. Att ett gitter måste vara diskret kan också tolkas som att ett gitter $L \subset \mathbb{R}^m$ inte får ha en gränspunkt i L. Anta att det skulle finnas ett $x \in L$ sådan att varje omgivning kring x innehåller punkter $q \in L$ sådan att $q \neq x$. Då får vi omedelbart att för varje $\varepsilon > 0$

$$L \cap \left\{ q \in \mathbb{R}^m \, : \, |x - q| < \varepsilon \right\} \neq \left\{ x \right\}.$$

Detta bryter mot definitionen av att vara diskret och från Sats 2.4 vet vi då att ett gitter L måste sakna gränspunkter i L.

2.2 Relationer mellan baserna för ett gitter

Anmärkning 2.7. **Hur kan vi byta bas för ett gitter?**

Om vi exempelvis har en bas v_1, v_2 för ett gitter $L \subset \mathbb{R}^m$ $(m \geq 2)$ och två andra vektorer w_1, w_2 i L. Då kan vi skriva

$$\begin{aligned} w_1 &= a_{11} v_1 + a_{12} v_2 \\ w_2 &= a_{21} v_1 + a_{22} v_2 \end{aligned} \quad \Leftrightarrow \quad \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \tag{1}$$

Här är alla $a_{i,j}$ heltal. Anta att vi kan invertera matrisen

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \text{ till } A^{-1} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}.$$

Då kan vi få v_1 och v_2 uttryckt i termer och w_1 och w_2 genom att multiplicera A^{-1} från vänster i (1). Anta vidare att A^{-1} också har heltalskoefficienter. Vi ska visa att då är w_1 och w_2 också en bas för L. Vi vill då visa att

$$L' = \left\{ b_1 w_1 + b_2 w_2 \, : \, b_1, b_2 \in \mathbb{Z} \right\} = \left\{ a_1 v_1 + a_2 v_2 \, : \, a_1, a_2 \in \mathbb{Z} \right\} = L.$$

Vi har att

$$L = \left\{a_1 v_1 + a_2 v_2 \,:\, a_1, a_2 \in \mathbb{Z}\right\} = \left\{a_1(b_{11}w_1 + b_{12}w_2) + a_2(b_{21}w_1 + b_{22}w_2) \,:\, a_1, a_2 \in \mathbb{Z}\right\} =$$

$$\left\{(a_1 b_{11} + a_2 b_{21})w_1 + (a_1 b_{12} + a_2 b_{22})w_2 \,:\, a_1, a_2 \in \mathbb{Z}\right\}. \tag{2}$$

I och med att $(a_1 b_{11} + a_2 b_{21})$ och $(a_1 b_{12} + a_2 b_{22})$ bara består av heltal är det tydligt att $L \subset L'$ och det återstår att visa att $L' \subset L$. Givet en godtycklig vektor $b_1 w_1 + b_2 w_2 \in L'$ vi behöver visa att det finns heltal a_1 och a_2 sådan att $b_1 = (a_1 b_{11} + a_2 b_{21})$ och $b_2 = (a_1 b_{12} + a_2 b_{22})$ för enligt (2) är då $b_1 w_1 + b_2 w_2$ också i L. Detta är ekvivalent med att hitta lösningar för a_1 och a_2 i ekvationen

$$\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} b_{11} & b_{21} \\ b_{12} & b_{22} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \;\Leftrightarrow\; \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = (A^{-1})^T \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \;\Leftrightarrow$$

$$A^T \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}.$$

I och med att A^T har heltalskoefficienter har vi hittat de sökta heltalen a_1 och a_2 och därmed är $L' \subset L$.

I denna argumentationen användes 2-dimensionella baser för att presentationen skulle bli tydlig. Det går förstås att föra en liknande argumentation för en bas $v_1, ..., v_n$ och vektorer $w_1, ..., w_n$ i $L \subset \mathbb{R}^m$. På samma sätt om $n \times n$-matrisen A är inverterbar och A^{-1} har heltalskoefficienter kommer $w_1, ..., w_n$ vara en bas för L.

Vi ska nu se att det finns ett förmodligen smidigare sätt att avgöra om vektorerna $w_1, ..., w_n$ utgör en bas eller inte, nämligen om matrisen A har determinant lika med ± 1. Det visas från nästa sats. Först behöver vi några klargöra några definitioner från linjär algebra. För följande två definitioner avser vi A som en $n \times n$-matris.

Definition 2.8. Vi definierar $\tilde{A_{ij}}$ av A som $(n-1) \times (n-1)$-matrisen när man tar bort rad i och kollon j och vi definierar *kofaktorn* C_{ij} som

$$C_{ij} = (-1)^{i+j} \det(\tilde{A_{ij}})$$

Definition 2.9. Vi definierar *adjunkten* av A som matrisen

$$adj(A) = \begin{pmatrix} C_{11} & ... & C_{n1} \\ \vdots & \ddots & \vdots \\ C_{1n} & ... & C_{nn} \end{pmatrix}.$$

Sats 2.10. *En $n \times n$-matris A har en invers A^{-1} med heltalskoefficienter om och endast om* $\det(A) = \pm 1$

Lemma 2.11 (Cramers regel)**.** *Låt x vara lösningen till ekvationen $Ax = b$ där A är en inverterbar $n \times n$-matris och $b \in \mathbb{R}^n$. Låt A_i vara matrisen som fås genom att ersätta i:te kolumnen av A med vektorn b. Då är i:te kordinaten av x*

$$x_i = \frac{\det(A_i)}{\det(A)}.$$

Bevis: Se Friedberg m.fl. (2014, sida 224). □

Lemma 2.12. *Låt A vara en inverterbar $n \times n$-matris. Då är*

$$A^{-1} = \frac{adj(A)}{\det(A)}.$$

Bevis. Vi vet att A^{-1} existerar och beteckna kolumn j av A^{-1} som x_j. Betrakta ekvationerna $Ax_j = e_j$, $(1 \leq j \leq n)$, där e_j är standardvektorn med kordinat j lika med 1. Enligt Cramers regel är då kordinat i av x_j lika med

$$(x_j)_i = \frac{\det(A_i)}{\det(A)}.$$

I matrisen A_i har vi alltså bytt ut kolumn i med vektorn e_j i A. Om vi expanderar kofaktorerna längs den kolumnen för att beräkna determinanten av A_i kommer därför alla nollor i e_j ta bort allt utom kofaktorn C_{ji}. Alltså är $\det(A_i) = C_{ji}$. Därför är

$$x_j = \frac{1}{\det(A)}(C_{j1}, C_{j2}, ..., C_{jn}).$$

Från hur vi definierade x_j är då

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} C_{11} & ... & C_{n1} \\ \vdots & \ddots & \vdots \\ C_{1n} & ... & C_{nn} \end{pmatrix} = \frac{1}{\det(A)} adj(A).$$

□

Bevis for Sats 2.10. Anta att A har en invers A^{-1} med heltalskoefficienter. Enligt räknelagar för determinanter är

$$1 = \det(I_n) = \det(AA^{-1}) = \det(A)\det(A^{-1}). \tag{1}$$

Då är $\det(A) \neq 0$ för annars får vi $1 = 0$ i (1). Anta att $\det(A) = a$ där $a \neq 1$, $a \neq -1$ och $a \neq 0$. Då är

$$\frac{1}{a} = \det(A^{-1})$$

där $\frac{1}{a}$ inte är ett heltal. Vi antog att A^{-1} har heltalskoefficienter och om vi tittar på definitionen av determinanter kommer då $\det(A^{-1})$ vara summor och produkter av heltal vilket blir ett heltal. Alltså får vi en motsägelse och $\det(A)$ måste vara lika med 1 eller -1.

Anta nu att $\det(A) = \pm 1$. Eftersom $\det(A) \neq 0$ är A inverterbar och utifrån Lemma 2.12 har vi då att

$$A^{-1} = \frac{adj(A)}{\det(A)} \quad \Leftrightarrow \quad A^{-1} = \pm adj(A). \tag{2}$$

Som vi etablerade tidigare måste determinanten av en heltalsmatris vara ett heltal och eftersom A var en heltalsmatris måste $\tilde{A_{ji}}$ också vara det. Då måste alla koefficienter i $adj(A)$ vara heltal från hur adjunkten definieras och (2) visar då att A^{-1} är en heltalsmatris. □

Anmärkning 2.13. Givet en bas $v_1, ..., v_n \in L$ och ett antal vektorer $w_1, ..., w_n \in L$ vet vi från definitionen av gitter att det finns en heltalsmatris A sådan att

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = A \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

Från Sats 2.10 och argumenationen innan Sats 2.10 vet vi nu att det räcker att kolla om $\det(A) = \pm 1$ för att avgöra om $w_1, ..., w_n$ också är en bas för L.

2.3 Mer om fundamentaldomänerna för ett gitter

Sats 2.14. *Låt $L \subset \mathbb{R}^n$ vara ett gitter av dimension n och låt $\mathcal{F}$ vara ett fundamentaldomän för L. Då kan varje vektor $w \in \mathbb{R}^n$ bli skriven på formen*

$$w = t + l \text{ för ett unikt } t \in \mathcal{F} \text{ och ett unikt } l \in L.$$

Bevis. Låt $v_1, ..., v_n$ vara en bas för L som bildar fundamentaldomänen $\mathcal{F}$. Eftersom $v_1, ..., v_n$ spänner upp $\mathbb{R}^n$ kan w uttryckas som $w = a_1v_1 + ... + a_nv_n$ där $a_1, ..., a_n \in \mathbb{R}$. För varje a_i är $a_i = a_i - \lfloor a_i \rfloor + \lfloor a_i \rfloor$. Därmed är

$$w = \overbrace{(a_1 - \lfloor a_1 \rfloor)v_1 + ... + (a_n - \lfloor a_n \rfloor)v_n}^{t \in \mathcal{F}} \quad + \quad \overbrace{\lfloor a_1 \rfloor v_1 + ... + \lfloor a_n \rfloor v_n}^{l \in L}. \tag{1}$$

I och med att $0 \leq (a_i - \lfloor a_i \rfloor) < 1$ är vektorn t i $\mathcal{F}$ och eftersom $\lfloor a_i \rfloor$ är heltal är vektorn l i L. Nu återstår det att visa att t och l måste vara som i (1).

Anta w har två godtyckliga representationer med $w = t + l = t' + l'$. Här är $t = t_1v_1 + ... + t_nv_n$ och $t' = t'_1v_1 + ... + t'_nv_n$ där $0 \leq t_i, t'_i < 1$. Dessutom är $l = l_1v_1 + ... + l_nv_n$ och $l' = l'_1v_1 + ... + l'_nv_n$ där alla $l_i, l'_i \in \mathbb{Z}$. Vi ska visa att $t = t'$ och $l = l'$. Vi har att

$$t + l = (t_1 + l_1)v_1 + ... + (t_n + l_n)v_n = (t'_1 + l'_1)v_1 + ... + (t'_n + l'_n)v_n = t' + l' \quad \Leftrightarrow$$

$$(t_1 + l_1 - (t'_1 + l'_1))v_1 + ... + (t_1 + l_1 - (t'_1 + l'_1))v_n = 0 \tag{2}$$

Eftersom $v_1, ..., v_n$ är linjärt oberoende har den sista ekvationen i (2) den enda lösningen att alla koefficienter framför v_i är 0. Därför är $t_i + l_i = t'_i + l'_i$ för alla $1 \leq i \leq n$ och då är $(t_i - t'_i = l'_i - l_i)$ vilka är ett heltal eftersom alla l'_i och l_i är heltal. Återkalla att $0 \leq t_i, t'_i < 1$. Vi har då att

$$-1 < -t'_i \leq t_i - t'_i < 1 - t'_i \overset{t'_i \neq 0}{<} 1 \overset{t'_i \neq 0}{\Rightarrow} -1 < t_i - t'_i < 1. \tag{3}$$

Alltså om $t'_i \neq 0$ är $-1 < t_i - t'_i < 1$. Vi visade tidigare att $t_i - t'_i$ var heltal och då visar (3) att $t_i = t'_i$ om $t'_i \neq 0$. Om $t'_i = 0$ har vi att

$$0 \leq t_i < 1 \quad \Leftrightarrow \quad 0 \leq t_i - t'_i < 1$$

vilket leder till samma slutsats att $t_i = t_i'$ för alla $1 \leq i \leq n$. Alltså är $t = t'$ och från antagandet att $t + l = t' + l'$ får vi direkt då att $l = l'$. Alltså om w har två sådana representationer måste de vara samma och därmed är representationen unik.

□

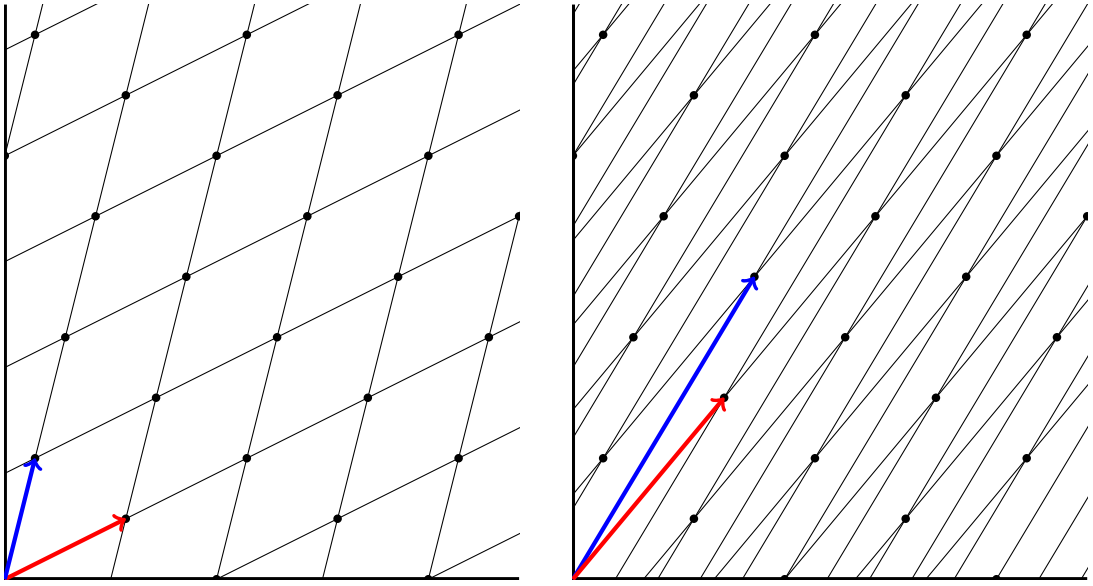
Anmärkning 2.15. Sats 2.14 innebär att mängden

$$\bigcup_{l \in L} \mathcal{F} + l$$

exakt täcker $\mathbb{R}^n$. Detta innebär att alla $\mathcal{F} + l$ är parvis disjunkta. Mer specifikt innebär det att för varje par av l och l' i L sådan att $l \neq l$ är

$$(\mathcal{F} + l) \cap (\mathcal{F} + l') = \emptyset. \tag{1}$$

Egenskapen (1) illustreras i Figur 1 nedan.



(a) Bas: v_1 =(2,1) och v_2 =(0.5,2)

(b) Bas: v_1 =(3,5) och v_2 =(2.5,3)

Figur 1: Figuren visar samma gitter med två olika baser. På båda bilderna ser man att alla parallelogram $\mathcal{F}+l$ ligger perfekt separerade, alltså att de är parvis disjunkta och täcker hela $\mathbb{R}^2$.

Egenskapen (1) gäller alltså för alla gitter oavsett fundamentaldomän $\mathcal{F}$. Den egenskapen behövs för att bevisa den viktiga Minkonwski sats. Följdsatsen till nästa sats behövs också i beviset av Minkowskis sats.

Sats 2.16. *Låt $L \subset \mathbb{R}^n$ vara ett gitter av dimension n med $v_1, ..., v_n$ som bas. Sätt basvektorerna som rader i matrisen V. Då är volymen av $\mathcal{F}$ givet av formeln*

$$Vol(\mathcal{F}) = |\det(V)|.$$

Bevis. Vi vet från flervariabelanalysen att volymen av $\mathcal{F}$ kan beräknas av integralen

$$\int_{\mathcal{F}} 1 \, dx_1 \, dx_2 ... dx_n = \int_{\bar{\mathcal{F}}} 1 \, dx_1 \, dx_2 ... dx_n.$$

Vi behöver att $\bar{\mathcal{F}}$ måste vara jordan-mätbar för att integralen ska vara definierad och detta får vi exempelivs från proposition 10.7.1 (Lebl, 2025, sida 134). För att beräkna integralen kan vi göra ett variabelbyte som tillåter oss att integrera över enhetskuben istället för över $\bar{\mathcal{F}}$. Vi ser kordinaterna till basvektorerna som $v_1 = (v_{11}, ...v_{1n}),\ v_2 = (v_{21}, ..., v_{2n}),\ ..., v_n = (v_{n1}, ..., v_{nn})$. Gör då variabelbytet från $x_1, ..., x_n$ till $t_1, ..., t_n$ med

$$\begin{cases} x_1 = t_1 v_{11} + t_2 v_{21} + ... + t_n v_{n1} \\ x_2 = t_1 v_{12} + t_2 v_{22} + ... + t_n v_{n2} \\ \vdots \\ x_n = t_1 v_{1n} + t_2 v_{2n} + ... + t_n v_{nn} \end{cases} . \tag{1}$$

Anledningen till detta variabelbyte är sambandet med området $\bar{\mathcal{F}}$ att vi får att

$$\bar{\mathcal{F}} = \left\{ t_1 v_1 + ... t_n v_n \ : \ 0 \leq t_1, ..., t_n \leq 1 \right\} = \left\{ (x_1, ..., x_n) \ : \ 0 \leq t_1, ..., t_n \leq 1 \right\}.$$

Avbildningen (1) täcker alltså hela områden $\bar{\mathcal{F}}$ när definitionsmängden är enhetskuben $C_n = \left\{ (t_1, ..., t_n) \ : \ 0 \leq t_1, ..., t_n \leq 1 \right\}$. Ett variablebyte kräver att avbildningen (1) är en bijektiv C^1-avbildning över ett kompakt jordan-mätbart område och att funktionaldeterminanten är skild från 0 (Lebl, 2025, sida 134, 2025). Vi har redan visat att (1) är surjektiv och eftersom avbildningen är synligt linjär innebär det också att den är injektiv från en känd sats från analysen. Vidare är alla partiella derivator konstanter, alltså kontiunerliga, och därmed är avbidlningen C^1. Funktionalmatrisen R definieras i detta fall som

$$R = \begin{pmatrix} \frac{\partial x_1}{\partial t_1} & ... & \frac{\partial x_1}{\partial t_1} \\ \vdots & & \vdots \\ \frac{\partial x_n}{\partial t_1} & ... & \frac{\partial x_n}{\partial t_n} \end{pmatrix} = \begin{pmatrix} v_{11} & ... & v_{n_1} \\ \vdots & & \vdots \\ v_{1n} & ... & v_{nn} \end{pmatrix}.$$

I och med att kollonvektorerna i R är basen för L är kollonerna linjärt oberoende vilket är ekvivalent med att $\det(R) \neq 0$. Vidare är enhetskuben jordan-mätbar från proposition 10.7.1 (Lebl, 2025, sida 134) och kompakt. Alltså får vi göra variabelbytet och vi får att

$$Vol(\mathcal{F}) = \int_{\bar{\mathcal{F}}} 1 \, dx_1 \, dx_2 ... dx_n = \int_{C_n} 1 \cdot |\det(R)| \, dt_1 \, dt_2 ... dt_n =$$

$$= |\det(R)| = |\det(R^T)| = |\det(V)|.$$

□

Följdsats 2.17. *Låt $L \subset \mathbb{R}^n$ vara ett gitter av dimension n. Då har varje fundamental domän $\mathcal{F}$, oberoende av bas, samma volym.*

Bevis. Låt $v_1, ..., v_n$ och $w_1, ..., w_n$ vara två godtyckliga baser för L. Låt $V(v_1, ..., v_n)$ och $V(w_1, ..., w_n)$ vara matriserna med $v_1, ..., v_n$ som radvektorer respektive $w_1, ..., w_n$ som radvektorer. Vi vet från *Anmärkning 2* att det finns en heltalsmatris A med $\det(A) = \pm 1$ sådan att

$$V(v_1, ..., v_n) = AV(w_1, ..., w_n). \tag{1}$$

Nu har vi att

$$Vol(\mathcal{F}(v_1, ..., v_n)) = |\det(V(v_1, ..., v_n))| = |\det(AV(w_1, ..., w_n))| =$$

$$|\det(A)||\det(V(w_1, ..., w_n))| = |\det(V(w_1, ..., w_n))| = Vol(\mathcal{F}(w_1, ..., w_n)).$$

Här har vi använt Sats 2.16, ekvation (1), att $|\det(A)| = 1$ och räknelagar för determinanter och absolutbelopp. Eftersom $v_1, ..., v_n$ och $w_1, ..., w_n$ var godtyckliga är volymen av fundamentaldomänerna samma oavsett bas. □

2.4 Minkowskis sats och applikationer

Definition 2.18. Vi definierar determinanten $\det(L)$ av ett gitter $L \subset \mathbb{R}^m$ som volymen av fundamentaldomänen $\mathcal{F}$ från någon bas $v_1, ..., v_n$. Från Följdsats 2.17 är detta nu väldefinierat eftrsom det endast finns ett värde på volymen av $\mathcal{F}$ oavset bas och därmed endast ett värde på $\det(L)$.

Sats 2.19 (Minkowskis sats)**.** *Låt $L \subset \mathbb{R}^n$ vara ett gitter av dimension n och låt $S \subset \mathbb{R}^n$ vara en begränsad, symetrisk och konvex mängd vars volym uppfyller*

$$Vol(S) > 2^n \det(L).$$

Då innehåller S en vektor $l \in L$ sådan att $l \neq 0$. Om S dessutom är sluten gäller samma result om

$$Vol(S) \geq 2^n \det(L).$$

Lemma 2.20. *Låt $S \subset \mathbb{R}^n$ vara en begränsad, symetrisk och konvex mängd och låt $p \in \mathbb{R}$. Då är*

$$Vol(pS) = p^n Vol(S).$$

Här är mängen $pS = \Big\{ps \,:\, s \in S\Big\}$.

Bevis. Vi kommer använda att en begränsad konvex mängd är jordan-mätbar (Lebl, 2025, sida 127), alltså att S är jordan-mätbar. Om man tittar på definitionen av konvexitet är det tydligt att pS också är konvex och begränsad, alltså jordan-mätbar. Då kan vi räkna volymen av pS som

$$Vol(pS) = \int_{pS} 1 \, dx_1 ... dx_n \, .$$

Sedan gör vi variabelbytet

$$\begin{cases} x_1 = pt_1 \\ x_2 = pt_2 \\ \vdots \\ x_n = pt_n \end{cases} . \tag{1}$$

Alla $(t_1, ..., t_n)$ i S kommer då ge pS i $x_1 ... x_n$-rummet. Avbildningen (1) är då surjektiv och linjäriteten gör den bijektiv. Den är även C^1 för att alla partiella derivator är konstanter. Funktionaldeterminanten R är

$$R = pI_n.$$

Från variabelbytet har vi då att

$$Vol(pS) = \int_{pS} 1 \, dx_1 ... dx_n \, = \int_S |\det(pI_n)| \, dt_1 ... dt_n \, = p^n Vol(S).$$

Här har vi använt en känd räknelag för determinanter att $\det(pA) = p^n \det(A)$ för en $n \times n$-matris A. Vi kan anta att vi integrerar över S och pS med sina gränspunkter vilket gör mängderna kompakta. Därmed är vi säkra på att variabelbytet blir korrekt från sats 10.7.2 (Lebl, 2025, sida 134).

□

Följande första del av beviset av Minkowskis sats är delvis inspirerat av Kumar (2023). Den första delen av beviset är även delvis illustrerat i Figur 2.

Bevis för Sats 2.19 (Minkowskis sats). Låt $\mathcal{F}$ vara något fundamentaldomän av L och betrakta mängden

$$\frac{1}{2}S = \left\{ \tfrac{1}{2}s \,:\, s \in S \right\}.$$

Från Lemma 2.20 och antagandet i satsen vet vi att

$$Vol\left(\frac{1}{2}S\right) = \frac{1}{2^n} Vol(S) > \frac{1}{2^n} \cdot 2^n \det(L) = \det(L). \tag{1}$$

Från Anmärkning 2.15 har vi att $\mathbb{R}^n$ kan täckas med en union av disjunkta translationer $\mathcal{F} + l$ där $l \in L$. Därmed kan vi täcka delmängden $\frac{1}{2}S \subset \mathbb{R}^n$ med sådana disjunkta translationer och därmed har vi att

$$\frac{1}{2}S = \bigcup_{l \in L} \left(\left(\frac{1}{2}S \right) \cap (\mathcal{F} + l) \right). \tag{2}$$

I och med att alla $\mathcal{F} + l$ i (2) är parvis disjunkta måste även alla $(\frac{1}{2}S \cap (\mathcal{F} + l))$ vara det. Därför kan vi summera alla sådana mängder när vi räknar volymen av $\frac{1}{2}S$. Vi har då att

$$Vol\left(\frac{1}{2}S\right) = \sum_{l \in L} Vol\left(\left(\frac{1}{2}S \right) \cap (\mathcal{F} + l) \right) = \sum_{l \in L} Vol\left(\left(\frac{1}{2}S - l \right) \cap \mathcal{F} \right). \tag{3}$$

Den sista likheten i (3) följer av att om vi flyttar mängderna $\frac{1}{2}S$ och $(\mathcal{F} + l)$ med samma translationen $-l$ har vi bara flyttat hela mängden $\left(\left(\frac{1}{2}S \right) \cap (\mathcal{F} + l) \right)$ med vektorn $-l$ och därmed bevaras volymen av den mängden. Denna idé illustreras i Figur 2.

Anta nu för en motsägelse att för varje par av l och l' i L, där $l \neq l'$, är

$$\left(\frac{1}{2}S - l \right) \cap \left(\frac{1}{2}S - l' \right) = \emptyset \quad \text{vilket skulle innebära att}$$

$$\left(\left(\frac{1}{2}S - l\right) \cap F\right) \cap \left(\left(\frac{1}{2}S - l'\right) \cap F\right) = \emptyset.$$

Då kan vi byta ut summmorna av volymerna i sista uttrycket i (3) på följande sätt:

$$Vol\left(\frac{1}{2}S\right) = Vol\left(\bigcup_{l\in L}\left(\left(\frac{1}{2}S - l\right) \cap \mathcal{F}\right)\right) = Vol\left(\mathcal{F} \cap \bigcup_{l\in L}\left(\frac{1}{2}S - l\right)\right) \leq Vol(\mathcal{F}) = \det(L). \tag{4}$$

Här använde vi räknelagar för snitt och unioner och vi fick en motsägelse mot (1) med olikheten i (4). Alltså måste det finnas ett $l \in L$ och ett $l' \in L$, där $l \neq l'$, sådan att

$$\left(\frac{1}{2}S - l\right) \cap \left(\frac{1}{2}S - l'\right) \neq \emptyset.$$

Därför måste det finnas ett $s_1 \in S$ och ett $s_2 \in S$ sådan att

$$\frac{1}{2}s_1 - l = \frac{1}{2}s_1 - l' \;\Leftrightarrow\; \frac{1}{2}s_1 - \frac{1}{2}s_2 = l - l' \neq 0. \tag{5}$$

Det är tydligt att $\frac{1}{2}s_1 - \frac{1}{2}s_2$ är i L eftersom $l - l'$ är det från additiviteten. Det återstår och visa att $\frac{1}{2}s_1 - \frac{1}{2}s_2$ är i S. Eftersom S är symetrisk är $-s_1$ i S och från definitionen av konvexitet är då $\frac{1}{2}s_1 + \frac{1}{2}(-s_2)$ också i S. Därmed är

$$0 \neq l - l' \in S \cap L$$

vilket visar första delen av satsen när vi antar att $Vol(S) > 2^n \det(L)$.

Anta nu att S är sluten och att $Vol(S) = 2^n \det(L)$. Ta hänsyn till följden av mängder

$$(1 + \frac{1}{k})S,\ k = 1, 2, 3, ... \quad \text{med volymerna } (1 + \frac{1}{k})^n Vol(S) > Vol(S). \tag{6}$$

Mängderna i följden (6) bibehåller naturligt egenskaperna för S och eftersom volymerna är strikt större än $2^n \det(L)$ kan vi använda första delen av satsen för att få en följd av vektorer v_k sådan att

$$0 \neq v_k \in \left(\left(1 + \frac{1}{k}\right) S \cap L\right),\ k = 1, 2, 3, ... \tag{7}$$

Från symetrin och konvexiteten av S har vi att $aS \subset bS$ om $a \leq b$. Därför är

$$(1 + \frac{1}{k})S \subset 2S \text{ för alla } k = 1, 2, 3, ...$$

Alltså är följden (7) i den begränsade mängden $2S$ och eftersom alla v_k också är i den diskreta mängden L måste det finnas ett ändligt antal v_k i $2S$. Följden (7) innehåller alltså ett ändligt antal vektorer v_k och då måste minst en vektor x förekomma i följden oändligt antal gånger och alltså finnas i $(1 + \frac{1}{k})S$ för oändligt många k. I och med att $(1 + \frac{1}{k_2})S \subset (1 + \frac{1}{k_1})S$ om $k_1 \leq k_2$ måste vi då ha att

$$x \in \bigcap_{k=1}^{\infty} (1 + \frac{1}{k})S. \tag{8}$$

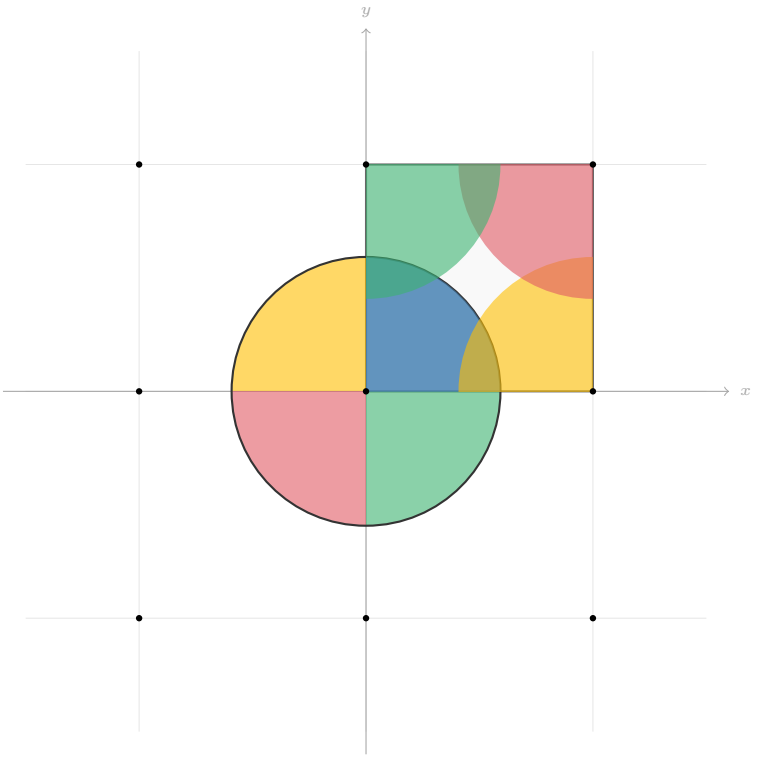
Nu återstår det att visa att x är i S för då är x den nollksilda vektorn i $L \cap S$. Från (8) har vi att för varje $k \geq 1$ finns det ett $s_k \in S$ sådan att

$$x = (1 + \frac{1}{k})s_k \quad \Leftrightarrow \quad s_k = \frac{k}{k+1}x. \tag{9}$$

Alla s_k bildar alltså en följd i S. Vi ser att följden $\frac{k}{k+1}$ konvergerar till 1 i $\mathbb{R}$ och att den konstanta följden x konvergerar till x i $\mathbb{R}^n$. Enligt sats 3.4 (Rudin, 1976, sida 50) kovergerar då s_k till $1 \cdot x = x$. Enligt definitionen av konvergens kan vi då för varje $\varepsilon > 0$ hitta $s_k \in S$ sådan att

$$|s_k - x| < \varepsilon. \tag{10}$$

Om $s_k \neq x$ för alla $k \geq 1$ visar (10) att x är en gränspunkt till S och eftersom S är sluten måste då x tillhöra S. Om $x = s_k$ för något $k \geq 1$ är x också i S. Därmed är x i S och då har vi att x är en nollskild vektor som är i $S \cap L$ vilket visar sista delen av satsen. □



Figur 2: I figuren är skivan $\frac{1}{2}S$ precis större än volymen av fundamentaldomänen $\mathcal{F}(e_1, e_2)$ av $\mathbb{Z}^2$. Vi flyttar in alla delar av skivan i $\mathcal{F}$ och visar att skivans delar måste överlappa någonstans efter denna förflyttning.

Anmärkning 2.21. Det finns olika applikationer från Minkowskis sats. En fråga som kan ställas är exempelvis varför mängden $A = \left\{\sqrt{2}a + \sqrt{3}b \,:\, a, b \in \mathbb{Z}\right\}$ inte får vara ett gitter? Hur bevisar man att A innehåller en gränspunkt och därmed bryter mot kravet att ett gitter måste vara diskret? Med Minkowskis sats kan vi nu visa ett Lemma som hjälper till att bevisa just detta.

Sats 2.22. *Låt $\alpha, \beta \in \mathbb{R}$ vara två nollskilda reella tal sådana att $\frac{\alpha}{\beta}$ är irrationelt. Då är*

$$A = \left\{a\alpha + b\beta \,:\, a, b \in \mathbb{Z}\right\}$$

inte ett gitter.

Lemma 2.23 (Dirichlets approximationssats)**.** *Låt α och N vara reella tal där $0 < N$. Då existerar det heltal p och q där $(p, q) \neq (0, 0)$ sådana att*

$$|q\alpha - p| \leq \frac{1}{N}.$$

Bevis. Låt S vara mängden

$$S = \left\{(x, y) \in \mathbb{R}^2 \,:\, -N \leq x \leq N,\ \ |x\alpha - y| \leq \tfrac{1}{N}\right\}.$$

Vi ska visa att S för ett godtyckligt $N > 0$ uppfyller kraven för Minkowskis sats. Vi börjar med att räkna volymen av S. Vi ser att S begränsas av linjerna $x = N$, $x = -N$, $y = \alpha x + \frac{1}{N}$ och $y = \alpha x - \frac{1}{N}$. Allt innanför ingår i S och därmed behöver vi beräkna arean av detta parallelogrammet som S utgör. Vi kan då skapa två vektorer ut av kanterna och beräkna beloppet av determinanten av dessa vektorer. Vi kan se de ickevertikala randlinjerna som alla punkter

$$(x, \alpha x - \frac{1}{N}) \text{ och } (x, \alpha x + \frac{1}{N}) \text{ där } -N \leq x \leq N.$$

Därmed får vi vektorerna som spänner upp parellelogrammet som

$$v_1 = (N, \alpha N + \tfrac{1}{N}) - (N, \alpha N - \tfrac{1}{N}) = (0, \tfrac{2}{N}) \text{ och}$$

$$v_2 = (N, \alpha N + \tfrac{1}{N}) - (-N, \alpha(-N) + \tfrac{1}{N}) = (2N, 2\alpha N).$$

Om nu V är matrisen med v_1 och v_2 som kollonvektorer är

$$Vol(S) = |\det(V)| = \left|0 - \frac{2}{N} \cdot 2N\right| = 4 = 2^2 \det(\mathbb{Z}^2). \tag{1}$$

Här är $\mathbb{Z}^2$ gittret L i Minkowskis sats. Det räcker med likheten till sista uttrycket i (1) eftersom S är tydligt sluten. Det återstår att visa att S är symetrisk och konvex. Vi ser att om (x, y) är i S kommer $(-x, -y)$ uppfylla kraven för S. Vi har då att $|-x| = |x| \leq N$ och $|-x\alpha - (-y)| = |y - x\alpha| = |x\alpha - y| \leq \frac{1}{N}$. Alltså är S symetrisk. För att visa konvexiteten kan vi, givet två punkter (x_1, y_1) och (x_2, y_2) i S, titta på linjesegmentet mellan punkterna:

$$\left\{(x_1 + (x_2 - x_1)t,\ y_1 + (y_2 - y_1)t) \,:\, 0 \leq t \leq 1\right\}.$$

För en godtycklig förstakordinat $(x_1 + (x_2 - x_1)t_1)\,(0 \leq t_1 \leq 1)$ i linjesegmentet har vi då att

$$|x_1 + (x_2 - x_1)t_1| = |(1 - t_1)x_1 + tx_2| \leq (1 - t_1)|x_1| + t_1|x_2| \leq (1 - t_1)N + t_1 N = N. \tag{2}$$

Här använde vi triangelolikheten och uttnyttjade att t_1 och $(1-t_1)$ är större eller lika med 0. Detta visar att hela linjnen uppfyller första kravet i S. Vidare har vi att

$$|((1-t_1)x_1+t_1x_2)\alpha-((1-t_1)y_1+t_1y_2)| = |(1-t_1)x_1\alpha-(1-t_1)y_1+t_1x_1\alpha-t_1y_2| \leq$$

$$(1-t_1)|x_1\alpha-y_1|+t_1|x_2\alpha-y_2| \leq \tfrac{1}{N}. \tag{3}$$

Här har vi använt liknande tekniker som i (2). Då hela linjen uppfyller kravet för S visar det att S är konvex. Då kan vi applicera Minkowskis sats på S och $L=\mathbb{Z}^2$ som visar att det finns en nollskilld vektor $(p,q)\in S\cap\mathbb{Z}^2$. Från hur S och $\mathbb{Z}^2$ är definierade är p och q heltal som uppfyller att $|p\alpha-q|\leq\frac{1}{N}$ för detta $N>0$. □

Bevis för Sats 2.22. Om vi använder $\frac{\alpha}{\beta}$ från Sats 2.22 istället för α i Dirichlets approximationssats får vi att för varje $N>0$ finns det en nollskild heltalsvektor (p,q) sådan att

$$\left|p\frac{\alpha}{\beta}-q\right| \leq \frac{1}{N} \quad\Leftrightarrow\quad |p\alpha-q\beta| \leq \frac{|\beta|}{N}. \tag{1}$$

I och med att p och $-q$ är heltal måste vektorn $p\alpha-q\beta$ alltid finnas i A. Vidare måste $p\alpha-q\beta$ vara nollskilld, för

$$\frac{\beta}{\alpha}=\frac{p}{q} \overset{q\neq0}{\Leftrightarrow} p\alpha-q\beta=0 \overset{p\neq0}{\Leftrightarrow} \frac{\alpha}{\beta}=\frac{q}{p}. \tag{2}$$

I och med att antingen p eller q är nollskillt och att $\frac{q}{p}$ eller $\frac{p}{q}$ är rationella i respektive fall medan $\frac{\alpha}{\beta}$ och $\frac{\beta}{\alpha}$ är irrationella visar (2) att $p\alpha-q\beta$ i (1) alltid är nollskillt.

Från (1) och (2) vet vi att vi kan skapa en följd $\left\{v_n\right\}=v_1,v_2,v_3,...$ i A sådan att alla v_i är nollskilda och

$$|v_i| \leq \frac{|\beta|}{i}.$$

Vi ska visa att denna följd kovergerar mot (0,0). För varje $\varepsilon>0$ finns talet $\frac{|\beta|+1}{\varepsilon}$ sådan att

$$n \geq \frac{|\beta|+1}{\varepsilon} \quad\Rightarrow\quad \varepsilon \geq \frac{|\beta|+1}{n} > \frac{|\beta|}{n} \geq |v_n|.$$

Enligt definitionen av konvergens av följder konvergerar då $\left\{v_n\right\}$ mot (0,0). En annan känd sats i analysen säger då att varje omgivning kring $(0,0)$ måste innehålla v_n för oändligt många n. I och med att alla v_i är skilda från $(0,0)$ och att alla v_i tillhör A

är då $(0,0)$ per definition en gränspunkt till A. Punkten $(0,0)$ tillhör också A. Från Anmärkning 2.6 vet vi att eftersom A har en gränspunkt som tillhör A kan inte A vara ett gitter. □

Anmärkning 2.24. En annan applikation av Minkowski sats kopplat till gitter är Hermites sats som säger att den kortaste vektorn i alla gitter av maximal rang har en viss övre begränsning.

Sats 2.25 (Hermites sats)**.** *Låt $L \subset \mathbb{R}^n$ av dimension n, då är*

$$\lambda_1(L) \leq \sqrt{n}\det(L)^{1/n}.$$

Bevis. Låt $L \subset \mathbb{R}^n$ vara ett godtyckligt gitter av dimension n och låt S vara kuben

$$S = \left\{(x_1, ..., x_n) \in \mathbb{R}^n \,:\, -B \leq x_1, ..., x_n \leq B\right\} \text{ där } B = \det(L)^{1/n}.$$

Då är S tydligt symetrisk, begränsad, konvex och sluten. Kubens sidor har längd $2B$, därför är volymen

$$(2B)^n = 2^n \det(L).$$

Alltså uppfyller S Minkowskis sats och då finns det en vektor v sådan att

$$0 \neq v \in L \cap S.$$

Den längsta vektorn inom kuben S är den som går till ett av hörnen av S som därför har längd

$$|(B, ..., B)| = \sqrt{B^2 + ... + B^2} = \sqrt{nB^2} = \sqrt{n}B = \sqrt{n}\det(L)^{1/n}.$$

Då v är inom S är $\lambda_1(L) \leq \|v\| \leq \sqrt{n}\det(L)^{1/n}$.

□

Anmärkning 2.26. Problemet att hitta den kortaste gittervektorn och även den närmaste gittervektorn till en vektor är det som utgör säkerheten hos kryptosystemen. Som vi pratade om i introduktionen är det dessa problem som kan bli tillräckligt svåra för att kvantdatorer ska ha svårt att lösa dem (Pradhan m.fl. 2019). Vi kommer använda följande förkortningar för dessa problem och sedan kan vi börja prata om kryptosystem.

Notation. Vi betecknar problemet att hitta den kortaste vektorn i ett gitter som *kortaste vektor-problemet* (KVP).

Notation. Vi betecknar problemet att hitta den närmaste gittervektorn till en vektor som *närmaste vektor-problemet* (NVP).

3 GGH kryptosystem

Innan vi förklarar GGH kryptosystemet behöver vi algoritmer för att mäta ortogonaliteten i en bas och för att lösa NVP i ett gitter.

3.1 Hadamards kvot

Sats 3.1 (Hadamards olikhet)**.** *Låt $v_1, ..., v_n$ vara linjärt oberoende vektorer och låt V vara matrisen med dessa som kollonvektorer. Då är*

$$|\det(V)| \leq \|v_1\|\|v_2\|...\|v_n\|.$$

Likhet uppstår om och endast om $v_1, ..., v_n$ är alla ortogonala mot varandra.

För bevis av Hadamards olikhet och vidare diskussion se exempelvis Holland (2007). Detta motiverar till en definition för att mäta hur ortogonal en bas är:

Definition 3.2. Låt $v_1, ..., v_n$ vara en bas för ett gitter $L \subset \mathbb{R}^m$ och låt V vara matrisen med basvektorerna som rader. Vi definierar *Hadamards kvot* som

$$\mathcal{H}(V) = \left(\frac{\det(L)}{\|v_1\|...\|v_n\|}\right)^{1/n}.$$

Från Hadamards olikhet vet vi att $0 \leq \mathcal{H}(V) \leq 1$ och ortogonaliteten bestäms av hur nära $\mathcal{H}(V)$ är 1.

3.2 Babais algoritm för att lösa NVP

Låt $L \subset \mathbb{R}^n$ vara ett gitter av dimension n. Det finns en algoritm för att hitta den närmaste gittervektorn till en given vektor $w \in \mathbb{R}^n$ om basen för L är tillräckligt ortogonal. Som vi poängterade i anmärkning 2.15 ligger w i en mängd $\mathcal{F} + l$ för ett unikt $l \in L$. Vi kom även fram till att mängderna i $\left\{\mathcal{F} + v \,:\, v \in L\right\}$ är parvis disjunkta. Det betyder att det inte finns någon annan gitterpunkt än l i $\mathcal{F} + l$ eller om man tittar på $\bar{\mathcal{F}} + l$ innehåller den endast hörnen av det parellogrammet. Därmed om basen för ett gitter är tillräckligt ortogonal kommer den närmaste gitterpunkten till w vara det närmaste hörnet i paralellogrammet $\mathcal{F} + l$.

Det är denna idé som Babais algoritm utgår från när man ska hitta den närmaste gittervektorn till w. Mer specifikt vet vi att $w = a_1v_1 + ... + a_nv_n$ där alla $a_i \in \mathbb{R}$.

Vidare är

$$w = \overbrace{\lfloor a_1 \rfloor v_1 + ... + \lfloor a_n \rfloor v_n}^{l} + \overbrace{(a_1 - \lfloor a_1 \rfloor)v_1 + ... + (a_n - \lfloor a_n \rfloor)v_n}^{t \in \mathcal{F}}.$$

För att hittade det närmaste hörnet av $l + \mathcal{F}$ till w sätter vi då alla $a_i - \lfloor a_i \rfloor$ i t till 0 om $a_i - \lfloor a_i \rfloor < \frac{1}{2}$ och annars till 1. Om $v_1, ..., v_n$ är tillräckligt ortogonala är detta inte bara det närmaste hörnet men också den närmaste gittervektorn till w.

Om däremot $v_1, ..., v_n$ är långt ifrån ortogonala finns det en risk att det närmaste hörnet inte är den närmaste gittervektorn. Exempelvis kan vi använda Anmärkning 2.13 för att se att $v_1 = (10, 1)$ och $v_2 = (9, 1)$ är en bas för $\mathbb{Z}^2$ som är längt ifrån ortogonal. Betrakta mängden

$$\mathcal{F} + 0 = \left\{ t_1(10, 1) + t_2(9, 1) \ : \ 0 \leq t_1, t_2 < 1 \right\}.$$

Sätt då $w = 0.5(10, 1) + 0(9, 1) = (5, 0.5)$ som är i $\mathcal{F} + 0$. Babais algoritm ger det närmaste hörnet av $\mathcal{F} + 0$ till w som $(9, 1)$. Men w är närmare till gittervektorerna $(5, 0)$ och $(5, 1)$ än till $(9, 1)$.

3.3 GGH kryptosystem

Alice väljer en mängd linjärt oberoende heltalsvektorer $v_1, ..., v_n \in \mathbb{Z}^n$. Dessa behöver vara tillräckligt ortogonala för att Babais algoritm ska fungera väl. För att säkerställa detta kan man använda Hadamards kvot. Då formar $v_1, ..., v_n$ en bas för ett gitter $L \subset \mathbb{R}^n$ och denna bas är Alices privata nyckel. Som publik nyckel vill Alice välja en ny bas som inte är särskilt ortogonal. Från Anmärkning 2.13 vet vi att om vi hittar en heltalsmatris U där $\det(U) = \pm 1$ kan vi få fram en ny bas för L.

Hur kan man då gererera olika U? En egenskap för determinanter är att elementära matriser där man bytt ut två rader i I_n eller adderat en multipel av en rad av I_n har determinant ± 1 (Friedberg, Incel och Spence, 2014, sida 223). Om vi sätter U till mulitplikationen av ett antal sådana elementära matriser $E_1, E_2, ..., E_k$ får vi att

$$\det(U) = \det(E_1 ... E_k) = \det(E_1) \det(E_2) ... \det(E_k) = \pm 1.$$

Alltså kan vi få nya baser till L genom att slumpmässigt välja $E_1, E_2, ..., E_k$ för något slumpmässigt antal k. Då får vi $W = UV$ där V är matrisen med $v_1, ..., v_n$

som rader. Raderna $w_1, ..., w_n$ till W är den nya basen och återigen kan vi använda Hadamards kvot för säkerställa att dessa är långt ifrån ortogonala. Basen $w_1, ..., w_n$ är då Alice publika nyckel.

Bob ska skicka meddelandet m som är en n-dimensionell heltalsvektor. Bob väljer även en liten n-dimesnionell vektor r där alla kordinater av r är i segmentet $(-\delta, \delta)$ där δ är ett tillräckligt litet reellt tal. Det krypterade meddelandet är då

$$e = mW + r.$$

Vi vet att mW är i L för att m har heltalskoefficienter och om r är tillräckligt litet kommer e garanterat inte vara i L och mW kommer vara den närmaste gittervektorn till e. Därmed kan Alice dekryptera e genom att använda den mer ortogonala basen $v_1, ..., v_1$ i Babais algoritm för att hitta den närmaste gittervektorn mW till e. Sedan kan Alice lösa ut m från mW med hjälp av W^{-1}.

Säkerheten i systemet lutar sig alltså mot ett NVP vilket vi konsterade kan bli ett mycket svårt problem.

Exempel 3.3. Vi tar ett mindre exempel i dimension 3 och utför beräkningarna i programmet Mathematica (Bilaga 1). Alice väljer tre större vektorer $v_1 = (68, 4, 0)$, $v_2 = (-4, 73, 8)$ och $v_3 = (2, -12, 76)$ och sätter V till matrisen med dessa som rader. Vi säkerställer att V är en bas för ett gitter genom att kolla att $\det(V) \neq 0$. Vi beräknar sedan Hadamards kvot $\mathcal{H}(V) = 0.999553$ vilket förmodligen är mer än tillräckligt nära 1 för att Babais algoritm ska fungera väl. Sedan skapar vi några elementära matriser som har determinant ± 1. I programmet gjordes exempelvis funktionen

$$RandomE(n) = \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

för att frå fram flera slumpartade sådana matriser. Efter att ha satt U till produkten av dessa elementära matriser blev den nya basen

$$W = UV = \begin{pmatrix} 15 & 12736 & 0 \\ 1 & 849 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{med} \quad \mathcal{H}(W) = 0.00440613.$$

Alltså är W en usel bas för Babais algoritm. Alice publicerar W som publik nyckel.

Bob ska då skicka ett meddelande $m = (34, 21, 36)$ och väljer $r = (3, -6, 3)$. Bob skickar då det krypterade meddelandet $e = mW + r$ till Alice.

Vi gjorde sedan en funktion $Babai(A, w)$ i Mathematica som utför Babais algoritm på en vektor w med hjälp av en basmatris A. Anta att Eve skulle få tag i meddelandet e som Bob skickade och sedan försökte få ut m genom att beräkna

$$Babai(W, e)W^{-1} = (1, 509, 36) \neq m.$$

Babais algoritm hittade alltså inte den närmaste gittervektorn mW till e då basen W var för dålig och därmed gav inte beräkning m som Eve hade önskat. Däremot har Alice sin bas V som sin hemliga privata nyckel och när hon utför samma beräkning får hon

$$Babai(V, e)W^{-1} = (34, 21, 36) = m.$$

4 NTRU Kryptosystem

Logiken för detta system förklaras naturligt genom teorin kring polynomringar. Då detta arbete främst rör gitterteori kommer en del resultat kring polynomringar hänvisas till Hoffstein m.fl (2008). Senare ska vi se hur NTRU kopplas till gitterteorin.

4.1 Faltningspolynom-ringar förenklat

Vi betecknar faltningspolynom-ringarna R, R_q och R_p som

$$R = \frac{\mathbb{Z}[x]}{(x^N - 1)}, \quad R_q = \frac{\mathbb{Z}q\mathbb{Z}[x]}{(x^N - 1)}, \quad R_p = \frac{\mathbb{Z}p\mathbb{Z}[x]}{(x^N - 1)}.$$

Simpelt förklarat, för att få ett polynom $f(x)$ i R reducerar man det moduli $x^N - 1$ vilket innebär att man byter ut alla x^N mot 1 (Hoffstein m.fl, 2008). Då kan alla polynom $f(x)$ i R reduceras till $f_0 + f_1x + ... + f_{N-1}x^{N-1}$. För att få $f(x)$ i R_q reducerar man det ytterligare moduli q. Additionen och multiplikationen $\star$ i R och R_q är den vanliga för polynom men att man reducerar summan/produkten enligt ovan. Multiplikationen med reduktionen är inte lätt att se direkt från godtyckliga polynom men Hoffstein m.fl (2008) visade att om $f(x)$ och $h(x)$ är polynom i R har produkten $c(x) = f(x) \star h(x)$ ett mönster. De visade att koeffecienterna c_k, $(0 \leq k \leq N-1)$, av $c(x)$ är

$$c_k = \sum_{i,j} f_i h_j.$$

Här är summan tagen över alla i, j sådan att $0 \leq i, j \leq N-1$ och $i + j \equiv k \bmod N$. Ett annat sätt att visualisera alla c_k är titta på alla i från 0 till $N-1$ och se att j måste vara $k - i \bmod N$. Därmed får vi att att

$$c_k = f_0h_k + f_1h_{(k-1 \bmod N)} + f_2h_{(k-2 \bmod N)} + ... + f_{N-1}h_{(k+1 \bmod N)}.$$

Definition 4.1. Vi definierar en *centrerad lyftning* $f^q(x)$ av polynomet $f(x) \in \mathbb{Z}[x]$ med q som polynomet med heltalskoefficienter f_i^q $(0 \leq i \leq N-1)$ sådana att $-\frac{1}{2}q < f_i^q \leq \frac{1}{2}q$ och $f(x) \equiv f^q(x) \bmod q$.

Anmärkning 4.2. Från definition 4.1 kan vi dra följande slutsats som behövs för dekrypteringen i NTRU. Om vi har en centrerad lyftning $f^q(x)$ och $g(x) = f^q(x) \bmod q$, då är $g^q(x) = f^q(x)$. Vi kan se detta eftersom vi får $g(x) = f^q(x) \bmod q$ genom att addera alla negativa koefficienter i $f^q(x)$ med q.

Definition 4.3. Vi definierar mängden $\mathcal{T}(d_1, d_2)$ som alla $a(x) \in R$ sådan att $a(x)$ har d_1 koefficienter lika med 1, d_2 koefficienter lika med -1 och resten av koefficienterna är lika med 0. Sådana polynom kallas *ternära polynom.*

4.2 NTRU kryptosystem

Alice börjar med välja parametrar N, p, q och d. Här är N ett primtal, d är något positivt heltal och p, q är heltal sådana att $sgd(N, q) = sgd(p, q) = 1$ och $q > (6d + 1)p$.

Alice privata nyckel är två slumpvis valda polynom

$$f(x) \in \mathcal{T}(d + 1, d) \quad \text{och} \quad g(x) \in \mathcal{T}(d, d)$$

sådan att $f(x)$ är inverterbar i R_q och R_p. Inversen av $f(x)$ i R_q och R_p betecknar vi som $F_q(x)$ respektive $F_p(x)$. Inversen definieras av att $F_q(x) \star f(x) \bmod q = 1$. Den publika nyckeln är polynomet

$$h(x) = F_q(x) \star g(x) \bmod q.$$

Nu när vi har nycklarna, hur går krypteringen och dekrypteringen till? Bob ska skicka ett meddelanden $m^p(x)$ som är en centrerad lyftning av något polynom $m(x) \in \mathbb{Z}[x]$ med p. Han väljer sedan ett slumpvist polynom $r(x) \in \mathcal{T}(d, d)$ och skickar det krypterade meddelandet

$$e(x) = ph(x) \star r(x) + m^p(x) \bmod q.$$

För att dekryptera $e(x)$ använder Alice sin privata nyckel $f(x)$ och beräknar först

$$a(x) = f(x) \star e(x) \bmod q.$$

Sedan beräknar hon

$$b(x) = F_p(x) \star a^q(x) \bmod p.$$

Enligt proposition 6.48 (Hoffstein m.fl. 2008, sida 394) är $b(x) = m^p(x) \bmod p$ från att vi valde q sådan $q > (6d + 1)p$. Från anmärkning 4.2 vet vi då att Alice får ut

det ursprungliga meddelandet $m^p(x)$ genom att beräkna

$$m^p(x) = b^p(x).$$

Exempel 4.4. Vi illustrerar med ett mindre exempel där vi använder Mathematica för de flesta beräkningarna (Bilaga 2). Alice väljer parametrarna $(N, p, q, d) = (5, 3, 41, 2)$. Vi ser att $41 = q > (6d+1)p = 39$ och eftersom alla parametrar är skilda primtal är $sgd(N, q) = sgd(p, q) = 1$. Då är kraven för parametrarna uppfyllda och hon väljer då de privata nycklarna

$$f(x) = -x^4 + x^3 + x^2 - x + 1 \in \mathcal{T}(3, 2) \quad \text{och} \quad g(x) = x^4 + x^3 - x^2 - x \in \mathcal{T}(2, 2).$$

Vi tar sedan fram

$$F_{41}(x) = 21x^3 + 21x^2 \quad \text{och} \quad F_3(x) = 2x^3 + 2x^2.$$

För detaljer kring hur man tar fram sådana inverser se Hoffstein m.fl (2008). Vi kontrollerar i Mathematica att dessa är korrekta inverser genom att kolla att $F_{41}(x) \star f(x) \bmod 41 = 1$ och $F_3(x) \star f(x) \bmod 3 = 1$. Alice publicerar sen den publika nyckeln

$$h(x) = 40x^4 + 20x^3 + 21x^2 + x.$$

När Bob ska skicka meddelandet $m^3(x) = x^3 + x^2 - 1$ väljer han ett $r(x) = -x^4 + x^3 + x^2 - 1 \in \mathcal{T}(2, 2)$ och skickar istället

$$e(x) = 28x^4 + 29x^3 + 39x^2 + 32x + 37.$$

Nu kan Alice använda sin privata nyckel $f(x)$ för att beräkna

$$a(x) = 33x^4 + 31x^3 + 2x^2 + 13x + 4.$$

Den centrerade lyftning av $a(x)$ med 41 kan räknas för hand till $a^{41}(x) = -8x^4 - 10x^3 + 2x^2 + 13x + 4$. Sedan beräknar hon

$$b(x) = x^3 + x^2 + 2 \quad \text{och} \quad m^3(x) = b^3(x) = x^3 + x^2 - 1.$$

4.3 NTRU som ett gitter

Vi vet nu från nycklarna till NTRU att en del av säkerheten lutar sig mot problemet att hitta de privata nycklarna $f(x)$ och $g(x)$ från den publika nyckeln $h(x)$. Vi ska nu se att detta problem kan likställas med problemet att hitta den kortaste nollskilda vektorn i ett gitter. Först behövs följande definition:

Definition 4.5. Den *cirkulära matrisen* $\mathcal{A}(f)$ av ett faltningspolynom $f(x) \in R$ är

$$\mathcal{A}(f) = \begin{pmatrix} f_0 & f_1 & ... & f_{N-1} \\ f_{N-1} & f_0 & ... & f_{N-2} \\ \vdots & \vdots & \ddots & \vdots \\ f_1 & f_2 & ... & f_0 \end{pmatrix}.$$

Nu kan vi definiera NTRU-gittret $L_h^{NTRU} \subset \mathbb{Z}^{2N}$, associerat till den publika nyckeln $h(x)$, som det gitter som spänns up av radvektorerna i matrisen

$$M_h^{NTRU} = \begin{pmatrix} I_N & \mathcal{A}(h) \\ 0 & qI_N \end{pmatrix}.$$

Faltningspolynomen $f(x)$ och $g(x)$ kan representeras som vektorer (f, g)
$= (f_0, ..., f_{N-1}, g_0, ..., g_{N-1}) \in \mathbb{Z}^{2N}$ vilket passar till detta gitter. Till en början måste vi säkerställa att de privata nycklarna $f(x)$ och $g(x)$ är i gittret och då måste vi först etablera en relation mellan den publika och de privata nycklarna. Från hur nycklarna definierades kan vi se att

$$f(x) \star h(x) \equiv f(x) \star (F_q(x) \star g(x)) = (f(x) \star F_q(x)) \star g(x) \equiv g(x) \bmod q. \qquad (1)$$

Här följer associativiteten från att R är en ring. Säkerheten i NTRU lutar sig alltså mot svårigheten att hitta $f(x)$ och $g(x)$ sådan att $f(x) \star h(x) \equiv g(x) \bmod q$. Denna relation uppfylls även om $f(x) = p(x) \star f(x)$ och $g(x) = p(x) \star g(x)$ för något polynom $p(x)$ med heltalskoefficienter. Däremot kommer bara $p(x) \star f(x)$ och $p(x) \star g(x)$ vara nycklar till NTRU om $p(x)$ har tillräckligt små koefficienter. Detta har med den centrerade lyftningen som görs under dekrypteringen och vi kan se om vi tittar nogrant att $p(x)$ därför måste ha koefficienter mellan $-\frac{1}{2}p$ och $\frac{1}{2}p$. Om $p(x) = x^k$ kallas $p(x) \star f(x)$ rotationen av $f(x)$ eftersom koefficienterna roteras k steg.

Att $f(x) \star h(x) \equiv g(x) \bmod q$ betyder per definition av kongruensrelationen att

det finns ett polynom $u(x)$ med heltalskoefficienter sådan att $f(x) \star h(x) = g(x) + qu(x)$. Detta hjälper oss att förstå nästa sats som visar att de privata nycklarna och dess rotationer är i L_h^{NTRU}.

Sats 4.6. *Anta att $f(x) \star h(x) \equiv g(x) \bmod q$ och låt $u(x)$ vara polynomet sådan att $f(x) \star h(x) = g(x) + qu(x)$. Då är*

$$(f, -u)M_h^{NTRU} = (f, g). \tag{1}$$

Vektorn (f, g) är då i L_h^{NTRU}.

Bevis. Det är tydligt att de första N kordinaterna av produkten (1) är f eftersom för varje kordinat i, $(1 \leq i \leq N)$, $(f, -u)$ multipliceras med vektorerna $(e_i, 0)$ där alla e_i är standardvektorerna i $\mathbb{R}^N$. För kordinaterna $N + 1$ till $2N$ kan vi först observera att alla kollonvektorer i $\mathcal{A}(h)$ är

$$(h_k, h_{(k-1 \bmod N)}, h_{(k-2 \bmod N)}, ..., h_{(k+1 \bmod N)}) \quad \text{för} \quad 0 \leq k \leq N - 1.$$

Därmed blir det tydligt att kordinat $N + k + 1$, $(0 \leq k \leq N - 1)$, i (1) blir

$$f_0 h_k + f_1 h_{(k-1 \bmod N)} + ... + f_{N-1} h_{(k+1 \bmod N)} - qu_k. \tag{2}$$

Från hur vi omformulerade produkten av faltningspolynom i avsnitt 4.1 ser vi att (2) är koefficient k i $f(x) \star h(x) - qu(x) = g(x)$. Därmed har vi visat att kordinat $N + 1$ till $2N$ är g. Produkten (1) blir alltså (f, g) och eftersom $(f, -u)$ är en heltalsvektor blir (1) en heltalslinjärkombination av basvektorerna i L_h^{NTRU} och därmed är (f, g) i L_h^{NTRU}. □

Anmärkning 4.7. Nu vet vi att de privata nycklarna som inkluderar rotationerna är i NTRU gittret. Vi vill också veta $\det(L_h^{NTRU})$ och längden på nycklarna som vektorer i gittret.

Sats 4.8. *Om vi för enkelhetens skull väljer parametrarna (N, p, q, d) för NTRU sådana att $d \approx N/3$ och $q \approx 6d \approx 2N$ som då bildar ett NTRU-gitter L_h^{NTRU} med den associerade privata nyckeln (f, g). Då är*

$$\det(L_h^{NTRU}) = q^N \quad \textit{och} \tag{1}$$

$$\|(f, g)\| \approx \sqrt{4d} \approx \sqrt{4N/3} \approx 1.155\sqrt{N}. \tag{2}$$

Lemma 4.9. *Om en $n \times n$-matris A är övre triangulär är determinanten av A lika med produkten av alla diagonalkoefficienter.*

Bevis. Låt $x_1, ..., x_n$ vara diagonalkoefficienterna till A. Vi kan expandera kofaktorerna av A längs kollon 1 och den enda termen i summan som blir kvar då är $x_1 C_{11}$ och alltså är $\det(A) = x_1 C_{11} = x_1 \det(\tilde{A_{11}})$. Men $\tilde{A_{11}}$ är i sin tur en övre triangulär matris med diagonalkoefficienter $x_2, ..., x_n$. Alltså kan vi fortsätta expandera kofaktorer längs kollon 1 av $\tilde{A_{11}}$ och får att $\det(A) = x_1 x_2 \tilde{\tilde{A_{11}}}$. Då blir det tydligt att vi tillslut får att $\det(A) = x_1 x_2 x_3 ... x_n$. □

Bevis av Sats 4.8. Vi vet från Följdsats 2.17 att $\det(L)$ kan beräknas från volymen av ett valfritt fundamentaldomän av L_h^{NTRU}. Vi har ett fundamentaldomän $\mathcal{F}$ från basvektorerna i raderna av matrisen M_h^{NTRU} och från Sats 2.16 vet vi då att $\det(L) = Vol(\mathcal{F}) = \det(M_h^{NTRU})$. Eftersom M_h^{NTRU} är en övre triangulärmatris kan vi använda Lemma 4.9 och få att $\det(L) = q^N$ vilket visar (1).

I och med att $f(x) \in \mathcal{T}(d, d+1)$ och $g(x) \in \mathcal{T}(d, d)$ har både f och g ungefär d kordinater lika med 1, ungefär d kordinater lika med -1 och resten lika med 0. Då följer normen (2) omedelbart. □

Anmärkning 4.10. Vi ska nu resonera varför de privata nycklarna (f, g) och dess rotationer är med stor sannolikhet de kortaste nollskillda gittervektorerna och att säkerheten i NTRU därmed förlitar sig på ett KVP. Innan vi påbörjar ett argument för varför de privata nycklarna bör ha längden $\lambda_1(L_h^{NTRU})$ behöver vi den Gausiska Heuristiken som gör en uppskattning av $\lambda_1(L)$ för slumpmässiga gitter L. Det är inte självklart när eller varför denna uppskattning fungerar och därför för vi först ett resonomang kring detta.

4.4 Gausiska Heuristiken

För följande resonomang behöver vi volymen av en n-dimesnionell boll centrerad i origo i högre dimensioner som är ungefär

$$Vol(B_r(0)) \approx \left(\frac{2\pi e}{n}\right)^{n/2} r^n \text{ (Hoffstein m.fl, 2008, sida 376).} \quad (1)$$

Även fast det inte går att beräkna $\lambda_1(L)$ för alla slumpmässiga gitter L finns det ett sätt att approximera den. Låt $L \subset \mathbb{R}^n$ vara ett n-dimesnionellt gitter. Den

Gausiska Heuristiken är idén att antalet gitterpunkter i bollen $B_r(0) \subset \mathbb{R}^n$ är ungefär lika med

$$\frac{Vol(B_r(0))}{\det(L)}. \tag{2}$$

Om man då räknar ut radien r för vilket uttrycket (2) är lika med 1 får man bollen $B_r(0)$ som innehåller endast en gitterpunkt. Enligt denna idé är då r den förväntade värdet på $\lambda_1(L)$. Mer specifikt om vi löser ut r när ekvationen (2) är lika med 1 och använder formeln (1) för $Vol(B_r(0))$ får vi att $\lambda_1(L)$ är ungefär

$$\lambda_1(L) \approx \sigma(L) = \sqrt{\frac{n}{2\pi e}} \det(L)^{1/n}. \tag{3}$$

Anmärkning 4.11. Ett problem med denna estimering är den fungerar olika bra för olika gitter och olika dimensioner.

Exempel 4.12. Om L har en nära ortogonal bas där basvektorerna är ungefär lika långa, med längder ungefär lika med a, säger (3) att

$$\lambda_1(L) \approx \sigma(L) = \sqrt{\frac{n}{2\pi e}} a.$$

Men vi vet att ett sådant gitter har den kortaste vektorlängden ungefär lika med a och alltså fungerar inte (3) när n inte är nära $2\pi e$. När n fortsätter växa blir det större och större error.

Exempel 4.13. Även ett gitter där alla $\mathcal{F}$ är avlånga rektanglar kan estimeringen misslyckas. Ta exempelvis ett gitter $L_\varepsilon \subset \mathbb{R}^2$ där

$$L_\varepsilon = \left\{ (\varepsilon, 0)a_1 + (0, \tfrac{\pi}{\varepsilon})a_2 \ : \ a_1, a_2 \right\}$$

Då är $\det(L_\varepsilon) = \pi$ för alla $\varepsilon > 0$ och den Gausistika Heuristiken säger då att antalet gitterunkter i enhetskivan är ungefär 1. Om vi sätter $a_2 = 0$ i L_ε kan vi tydligt se att alla gitterpunkter $(a_1\varepsilon, 0)$ sådan att $-1 \leq a_1\varepsilon \leq 1$ finns i enhetskivan. Med andra ord när ε går mot 0 går antalet gitterpunkter i enhetskivan mot oändligheten trots att denna princip säger att det bara finns ungefär 1 sådan gitterpunkt.

Frågan är då när estimering (3) faktiskt fungerar eller varför den ska fungera okej för slumpartade gitter (Hoffstein m.fl. 2008). För att troligöra estimeringen mer kan vi konstatera att exemplen vi tog upp inte är slumpartade gitter. I exempel 4.12

blir estimeringen fram för allt sämre när n blir större. Samtidigt kan man tänka sig att chansen att ett slumpartat gitter har en fullt ortgonal bas bör minska när n blir större eftersom antalet par av vektorer som måste vara ortogonala i en bas är $\binom{n}{2}$ som ökar snabbt i takt med n. Därmed bör inte Exempel 4.12 representera ett slumpartat gitter när n blir större och därmed motbevisar inte det estimeringen (3).

Vi kan också konstatera att värdet $\det(L)^{1/n}$ i $\sigma(L)$ kan minska när n ökar om ortogonaliteten försämras. Ta exempelvis kollonvektorerna i matrisen aI_n som basen för ett gitter $L_n \subset \mathbb{R}^n$ där $a \in \mathbb{R}^+$. Där är alla basvektorer ortogonala och $\det(L_n) = a^n$. Om vi ökar dimensionen ett steg genom att lägga till basvektorn $v_{n+1} = (0, ..., 0, \sqrt{a^2 - \varepsilon^2}, \varepsilon) \in \mathbb{R}^{n+1}$ kan vi få ett gitter $L_{n+1} \subset \mathbb{R}^{n+1}$ där basen är kollonvektorerna i $(n+1) \times (n+1)$-matrisen

$$\begin{pmatrix} a & 0 & ... & 0 & 0 \\ 0 & a & ... & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & a & \sqrt{a^2 - \varepsilon^2} \\ 0 & 0 & ... & 0 & \varepsilon \end{pmatrix}.$$

Då har v_{n+1} samma längd som alla övriga basvektorer oavsett värdet på $\varepsilon\,(0 < \varepsilon \leq a)$. Vi har att för alla $\varepsilon\,(0 < \varepsilon \leq a)$ att

$$\det(L_n)^{1/n} = a \geq a^{n/(n+1)}\varepsilon^{1/(n+1)} = \det(L_{n+1})^{1/(n+1)} \quad \Leftrightarrow \quad a^{n+1} \geq a^n\varepsilon. \tag{4}$$

Här har vi använt Lemma 4.9 för determinanten. Skalärprodukten av v_{n+1} och näst sista kollonvektorn v_n är $\langle v_n, v_{n+1} \rangle = a\sqrt{a^2 - \varepsilon^2}$. Om $\varepsilon = a$ är hela basen ortogonal och $\det(L_{n+1})^{1/n+1} = \det(L_n)^{1/n} = a$. Men när ε närmar sig 0 närmar sig v_n och v_{n+1} att bli parallella och vi ser samtidigt att olikheten (4) blir större eftersom $\det(L_{n+1})^{1/n+1}$ närmar sig 0.

Då kan man tänka sig att en minskning av uttrycket $\det(L)^{1/n}$ i $\sigma(L)$, för något gitter L, kan balansera ökningen av uttrycket $\sqrt{\frac{n}{2\pi e}}$ när n ökar. Alltså om vi har en viss längd $\lambda_1(L)$ på den kortaste nollskillda vektorn i ett gitter L och sedan ökar dimensionen på gittret med slumpartade vektorer kan vi nu se att $\sigma(L)$ fortfarande skulle kunna bibehålla den korta och rätta längden trots att n blir stort.

Att formelt bevisa att $\sigma(L)$ fungerar för slumpartade gitter är bortom ramen för

denna uppsats men med detta resonomang kan vi åtminstonde föreställa oss varför den fungerar.

Nu kan vi återgå till frågan om (f, g) och dess rotationer faktiskt är de kortaste nollskillda gittervektorerna. För enkelhetens skull använder vi samma parametrar på (N, p, q, d) som i Sats 4.8, alltså att $d \approx N/3$ och $q \approx 2N$. Återkalla att $\|(f, g)\| \approx 1.155\sqrt{N}$ i detta fall och $\det(L_h^{NTRU}) = q^N$. Den Gausiska heurestiken säger att

$$\lambda_1(L_h^{NTRU}) \approx \sigma(L_h^{NTRU}) = \sqrt{\frac{2N}{2\pi e}}(q^N)^{1/2N} = \sqrt{\frac{Nq}{\pi e}} \approx \sqrt{\frac{2N^2}{\pi e}} = \sqrt{\frac{2}{\pi e}}N \approx 0.484N.$$

Hur säkra kan vi då vara på att $\lambda_1(L_h^{NTRU}) = \|(f, g)\|$? I högre dimensioner blir $\|(f, g)\|$ mycket mindre än estimeringen $\sigma(L_h^{NTRU})$ vilket är ett positivt tecken men vi har sett i exempel 4.12 att den Gausiska Heuristiken kan gissa för högt i högre dimensioner. Samtidigt vet vi att L_h^{NTRU} inte kan ha en liknande bas som i exempel 4.12 för då skulle $\lambda_1(L_h^{NTRU})$ vara ungefär $\sqrt{q} \approx \sqrt{2}\sqrt{N} \approx 1.414\sqrt{N}$ som är större än $\|(f, g)\|$. Detta är också ett positivt tecken för att $\|(f, g)\| = \lambda_1(L_h^{NTRU})$. Vi kan också verifiera att (f, g) uppfyller kravet på $\lambda_1(L_h^{NTRU})$ från Hermats sats, nämligen att

$$\|(f, g)\| \approx 1.155\sqrt{N} \leq \sqrt{2N}(q^N)^{1/2N} = 2N \quad \text{för alla} \quad N \geq 1.$$

Trots dessa argument har vi fortfarande inte övertygat oss helt om att $\|(f, g)\| = \lambda_1(L_h^{NTRU})$ men det verkar mer troligt. Det går att skapa starka övertygelser om detta med annan teori som faller utanför ramen för denna uppsats. Däremot finns inga formella bevis för detta ännu (Bi och Cheng 2014). Därmed kan vi inte vara fullt säkra på att alla skapelser av NTRU-system kan översättas till ett KVP i ett gitter.

5 Framtida projekt

Tiden var knapp på detta kandidatarbete och på grund av fokuset på gitterteorin har säkerhetsaspekterna kring kryptosystemen inte diskuterats. Detta hade såklart varit intressant att undersöka om tiden hade funnits.

Det hade också varit önskvärt att göra ett mer rigoröst argument för varför (f, g) är den kortaste nollskilda vektorn i NTRU-gittret. Som tidigare nämnts finns det annan teori som ger ett argument (Bi och Cheng 2014) men detta är inte heller ett formelt bevis. Det hade varit intressant att undersöka mer kring exakt hur icke-ortogonal den kortaste basen för NTRU är och utifrån detta se om det går att ge ett bättre argument gällande den kortaste nollskilda vektorn. Att kunna ge sådana argument är positivt för utvecklandet av nya gitterbaserade kryptosystem som vill förlita sig på ett KVP.

Referenser

Bi, Jingguo, och Qi Cheng. 2014. ”Lower Bounds of Shortest Vector Lengths in Random NTRU Lattices”. Theoretical Computer Science 560 (december): 121–30. https://doi.org/10.1016/j.tcs.2014.10.011.

Friedberg, Stephen, Arnold Insel, och Lawrence Spence. 2014. Linear Algebra. Fjärde upplagan.

Hoffstein, Jeffrey, Jill Catherine Pipher, och Joseph H. Silverman. 2008. An Introduction to Mathematical Cryptography. Undergraduate Texts in Mathematics. Springer.

Holland, Finbarr. 2007. ”Another Proof of Hadamard’s Determinantal Inequality”.

Khan, Mohammad Rafeek, Kamal Upreti, Mohammad Imran Alam, m.fl. 2023. ”Analysis of Elliptic Curve Cryptography & RSA”. Journal of ICT Standardization, advance online publication, november 18. https://doi.org/10.13052/jicts2245-800X.1142.

Kumar, Abhiram. 2023. ”Minkowski’s theorem and applications”. April 17.

Lebl, Jiri. 2025. Introduction to Real Anlysis, Volume 2.

Pradhan, Pawan Kumar, Sayan Rakshit, och Sujoy Datta. 2019. ”Lattice Based Cryptography: Its Applications, Areas of Interest & Future Scope”. 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), mars, 988–93. https://doi.org/10.1109/ICCMC.2019.8819706.

Rudin, Walter. 1976. Principles of Mathematical Analysis. Third ed. International Series in Pure and Applied Mathematics. McGraw-Hill.

Vaikuntanathan, Vinod. 2011. ”CSC 2414 Lattices in Computer Science, Lecture 1 and 2”. September 13.

6 Bilagor

6.1 Bilaga 1: Mathematica-kod för exemplet för GGH kryptosystem

```
    Clear[v1, v2, v3, V, Orth, HadamardTest, E1, E2, RandomE,  RandomE2,
  U, W, r, m, e, s, a, Babai, WInverse];
v1 = {68, 4, 0};
v2 = {-4, 73, 8};
v3 = {2, -12, 76};
V = {v1, v2, v3};
V // MatrixForm
Det[F];
Orth[A_] := Norm[A[[1]]]*Norm[A[[2]]]*Norm[A[[3]]];
HadamardTest[A_] := N[(Abs[Det[A]]/Orth[A])^(1/3)];

E1 = {{0, 1, 0}, {1, 0, 0}, {0, 0, 1}};
E2 = {{0, 0, 1}, {0, 1, 0}, {1, 0, 0}};
RandomE[n_] := {{1, n, 0}, {0, 1, 0}, {0, 0, 1}};
RandomE2[n_] := {{1, 0, 0}, {0, 1, n}, {0, 0, 1}};

s[A_, w_] :=
 NSolve[w == t1*A[[1]] + t2*A[[2]] + t3*A[[3]], {t1, t2, t3}]

Babai[A_, w_] :=
  Round[s[A, w][[1, 1, 2]]]*A[[1]] +
   Round[s[A, w][[1, 2, 2]]]*A[[2]] + Round[s[A, w][[1, 3, 2]]]*A[[3]];

U = RandomE[15] . E2 . E1 . E1 . RandomE2[13] . RandomE2[4] . E2 .
   E1 . RandomE[832];
U // MatrixForm
W = U . V;
WInverse = Inverse[W];

HadamardTest[V]
HadamardTest[W]
```

```
r = {3, -6, 3};
m = {34, 21, 36};
e = m . W + r;

m "m"
m . W "m.W"
Labeled[Babai[W, e] . WInverse , "Babai dålig bas"]
Labeled[Babai[V, e] . WInverse , "Babai bra bas"]
```

6.2 Bilaga 2: Mathematica-kod för exemplet för NTRU kryptosystem

```
ClearAll[R_q, f, f41Inverse, f3Inverse, a, aLift, b, m];


f[x_] := -x^4 + x^3 + x^2 - x + 1
g[x_] := x^4 + x^3 - x^2 - x


f41Inverse[x_] := 21 x^3 + 21 x^2

f3Inverse[x_] := 2 x^3 + 2 x^2


PolynomialMod[PolynomialMod[f[x]*f41Inverse[x], x^5 - 1], 41]
PolynomialMod[PolynomialMod[f[x]*f3Inverse[x], x^5 - 1], 3]

h[x_] :=
 PolynomialMod[PolynomialMod[f41Inverse[x]*g[x], x^5 - 1], 41]
Labeled["h[x]", h[x]]

m[x_] := x^3 + x^2 - 1

Labeled[ "m[x]", m[x]]
```

```
Labeled["m[x] mod 3", PolynomialMod[m[x], 3]]

r[x_] := -x^4 + x^3 + x^2 - 1

e[x_] :=
 PolynomialMod[PolynomialMod[3 h[x]*r[x] + m[x], x^5 - 1], 41]
Labeled["e[x]", e[x]]

a[x_] := PolynomialMod[PolynomialMod[f[x]*e[x], x^5 - 1], 41]
Labeled["a[x]", a[x]]

aLift[x_] := 4 + 13 x + 2 x^2 - 10 x^3 - 8 x^4
Labeled["aLift", aLift[x]]

b[x_] :=
 PolynomialMod[PolynomialMod[f3Inverse[x]*aLift[x], x^5 - 1], 3]
Labeled["b[x]", b[x]]
```

Fel i C-uppsats

Fredrik Heed Elvegård

31 Maj 2026

- Ett förtydligande om varför det finns en kortaste längd för nollskilda gittervektorer hade varit bra - genom att förklara diskretheten av gitter mer noggrant.

- I beviset av Sats 2.4 del 1 skrev jag att vi ska visa att $\lambda(L)$ är strikt större än 0 med det är den ju per definition och $\lambda(L)$ går inte att använda i just detta sammanhang. Jag borde sagt att vi ska visa att alla nollskilda gittervektorer har en längd som är strikt större än 0 och utelämnat definitionen av $\lambda(L)$ från beviset.

- Det var lite felstavning här och där och framför allt på det viktiga namnet Gauss där jag istället skrev "Gaus". Jag visste inte att overleaf hade stavkontrollering och jag borde inte varit så naiv och tro att jag var okej på att stava, det var ett dumt misstag.

- I exemplet för GGH kryptosystem råkade jag printa ut matrisen U istället för $W = UV$ som var tänkt.