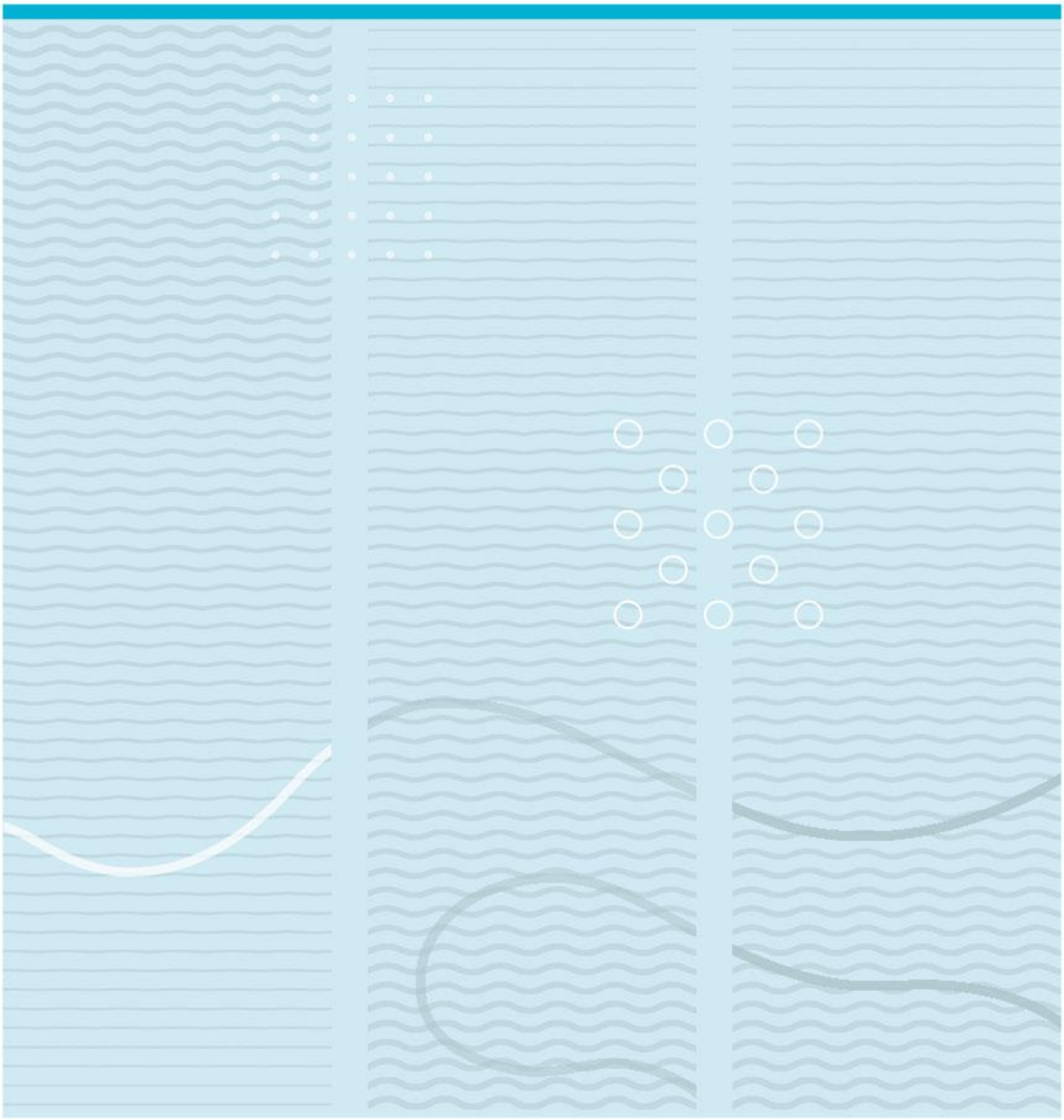
Universitetet i Sørøst-Norge
Fakultet for teknologi, naturvitenskap og maritime fag
–
Mastergradsavhandling
Studieprogram: Lektorutdanning i realfag og teknologi
Vår 2023

Kenneth Dahle

Elliptiske Kurver og Kommuterende *q*-differensialoperatorer



Universitetet i Sørøst-Norge
Fakultet for teknologi, naturvitenskap og maritime fag
Institutt for realfag og industrisystemer
Postboks 235
3603 Kongsberg

http://www.usn.no

Denne avhandlingen representerer 30 studiepoeng

Sammendrag

Burchnall-Chaundyteorien viser at to kommuterende differensialoperatorer gir en algebraisk kurve med en definerende likning. Mer sentralt gir to kommuterende q-differensialoperatorer, av orden to og tre, en algebraisk kurve som er elliptisk i parameter q. I denne avhandlingen konstruerer vi denne og beskriver dens gruppestruktur og supersingulære primtall.

Abstract

The Burchnall-Chaundy theory shows that two commuting differential operators give rise to an algebraic curve with a defining equation. In particular, two commuting q-differential operators, of orders two and three, give rise to an algebraic curve that is elliptic for some q. In this thesis, we construct this curve and describe its structure and supersingular primes.

Til minne om Chrisia

Elliptiske Kurver og Kommuterende q-differensialoperatorer

Kenneth Dahle

Forord

Som snart nyutdannet lektor forsøkte jeg å skrive denne avhandlingen mer eller mindre som en matematisk lærebok. Innholdet krever noe kjennskap til algebra og tallteori. Uansett ønsker jeg leseren en trivelig lesing.

Avhandlingen skrev jeg for kusina mi Chrisia, som brått gikk bort i 2021. Det var ikke ofte at jeg så henne, men hver gang vi pratet, gikk vi aldri lei. Jeg vil takke henne for å ha heiet på meg gjennom hele skrivingen.

Jeg vil også takke nære venner og familie, som villig har hørt på meg bable hodeborrende om elliptiske kurver, og som har gitt meg noe å tygge på mens jeg satt med skrivingen. Ikke minst vil jeg takke veilederen min Daniel, som introduserte meg til både Burchnall-Chaundyteori og elliptiske kurver. Det har vært en verden jeg nå forlater med en bittersøt følelse av stolthet, og litt tomhet. Takk.

Kongsberg, våren 2023
Kenneth Dahle

Innholdsfortegnelse

Kapittel 1

Introduksjon

En elliptisk kurve er en regulær, kubisk kurve utstyrt med et rasjonelt punkt. Dette punktet er et enhetselement som ofte er betegnet med $\mathcal{O}$. En elliptisk kurve lever som regel over kommutative ringer, eller kropper. Hvis den er definert over en endelig kropp, vil mange, interessante områder i matematikk bli gjort tilgjengelig, for eksempel kryptografi.

Likningen til en elliptisk kurve kalles for en Weierstrasslikning, og det er mange former. Den enkleste formen er $\mathbf{y}^2 = \mathbf{x}^3 + b\mathbf{x} + c$, der b og c er koeffisienter i en kropp. En elliptisk kurve må være regulær, som betyr at kurven ikke har doble røtter eller en spiss. Ekvivalent må koeffisientene i likningen være slik at diskriminanten til kurven er ulik null.

En elliptisk kurve over en kropp har en mengde rasjonelle punkter som tilfredsstiller aksiomene til en abelsk gruppe. Geometrisk betyr dette at summen av to punkter på en elliptisk kurve er et eget punkt på den samme kurven. Den enkleste og mest grunnleggende kroppen er de rasjonelle tallene. Her fins resultater som Mordell-Weils teorem [13, 19] og Mazurs teorem [11, 12]. Beviset på Mazurs teorem er kjempelangt og vanskelig å gjennomføre, men teoremet sier at en elliptisk kurve over de rasjonelle tallene har en mengde rasjonelle punkter som er en endelig generert abelsk gruppe. Mordell-Weils teorem var bevist av Louis Mordell over de rasjonelle tallene og mer generelt av André Weil over tallkropper. Over en endelig kropp er punkter på en elliptisk kurve vanskelig å telle, men Hasses teorem [7] er et flott estimat. Dessuten er også Schoofs algoritme [16, 17] en fin metode for å telle punkter over endelige kropper.

En elliptisk kurve er en regulær kubisk kurve over en ring og er en av to typer. Kurven er enten ordinær eller supersingulær. Disse to typene fungerer på forskjellige måter fundamentalt, men forskjellen er enkel. Mer om dette i kapittel 4.

I denne avhandlingen skal vi konstruere elliptiske kurver med Burchnall-Chaundy teori. Teorien handler om forbindelsen mellom par av differensialoperatorer som kommuterer og algebraiske kurver [2]. Den klassiske konstruksjonen sier at hvis

$$P = \sum_{i=0}^{n} p_i \mathrm{D}^i \quad \text{og} \quad Q = \sum_{i=0}^{m} q_i \mathrm{D}^i, \quad \mathrm{D}^i = \frac{d}{d\mathbf{t}}$$

er to differensialoperatorer av henholdsvis orden n og m som kommuterer og der p_i og q_i er polynomer i $\mathbf{t}$ med koeffisienter i en ring R, så fins det en eksplisitt konstruert algebraisk kurve som er definert av en likning $F(\mathbf{x}, \mathbf{y})$ slik at $F(P, Q) = 0$. Kurven kan konstrueres via en resultant, som er det samme som determinanten til en matrise av elementer fra

$$\partial^i(P - \mathbf{x}) \quad \text{for } 0 \leq i \leq m-1 \quad \text{og} \quad \partial^i(Q - \mathbf{y}) \quad \text{for } 0 \leq i \leq n-1.$$

Determinanten gir så et polynom der alle leddene har en variabel $\mathbf{t}$ av lik orden. Variabelen er fjernbar. Som et resultat blir resultanten et polynom i variablene $\mathbf{x}$ og $\mathbf{y}$.

Som et utgangspunkt konstruerer vi den elliptiske kurven i eksempel 5.4 fra [9]. Vi får imidlertid en kurve på formen

$$\xi(\mathbf{x}, \mathbf{y}): \quad \mathbf{y}^2 + \omega_1 \mathbf{y} = \omega_2 \mathbf{x}^3 + \omega_3 \mathbf{x}^2 + \omega_4 \mathbf{x}$$

der ω_i er koeffisienter uttrykket i q og α.

Når vi studerer kurvens gruppestruktur og supersingulære primtall, bruker vi for det meste programmer skrevet i Sage [15]. Alle de sentrale programmene er presenter under Vedlegg.

I kapittel 2 går vi gjennom definisjoner på q-derivasjon og introduserer noen nyttige notasjoner. I tillegg diskuterer vi q-differensialoperatorer og re-

sultanter og hvordan å bruke disse til å konstruere polynomer. Vi går også gjennom noen konkrete eksempler på resultanter som belyser forbindelsen med algebraiske kurver. I kapittel 3 og 4 ser vi på grunnleggende teori på elliptiske kurver. I tillegg går vi gjennom torsjonspunkter og morfismer mellom kurver. I kapittel 5 går vi tilbake til q-differensialoperatorene og det aktuelle eksempelet. Til slutt i kapittel 6 ser vi på eksempler og diskuterer eventuelle observasjoner.

Kapittel 2

Burchnall-Chaundyteori og q-differensialoperatorer

2.1 Burchnall-Chaundyteori

Det fins en sammenheng mellom algebraiske kurver og par av kommuterende differensialoperatorer. Hvis p og q er polynomer i variabel $\mathbf{t}$ og P og Q er to differensialoperatorer på formen

$$P = \sum_{i=0}^{n} p_i \mathrm{D}^i \quad \text{og} \quad Q = \sum_{i=0}^{n} q_i \mathrm{D}^i$$

slik at $[P, Q] = PQ - QP = 0$, så er $F(P, Q)$ en algebraisk kurve definert ved en likning $F(\mathbf{x}, \mathbf{y}) = 0$.

2.2 Derivasjoner og differensialoperatorer

2.2.1 Derivasjoner

La $\mathfrak{R}$ være en ring av funksjoner i en variabel $\mathbf{t}$ og anta at alle funksjoner $f(\mathbf{t}) \in \mathfrak{R}$ er uendelig deriverbare. Da er en derivasjon på $\mathfrak{R}$ en lineær operator D som tilfredsstiller Leibnizregelen,

$$\mathrm{D}(fg) = \mathrm{D}(f)g + f\mathrm{D}(g), \quad f, g \in \mathfrak{R}.$$

Eksempel 2.1. Hvis $f(\mathbf{t}) = \mathbf{t}^n$ og $\mathrm{D} = d/d\mathbf{t}$ så er $\mathrm{D}(f) = n\mathbf{t}^{n-1}$.

Det fins imidlertid andre eksempler på en derivasjon. For eksempel kan en derivasjon være gitt på formen $\mathrm{D} \coloneqq \mathbf{t}d/d\mathbf{t}$. Så hvis $f(t) = \mathbf{t}^n$ så er $\mathrm{D}(f) = n\mathbf{t}^n$.

2.2.2 Differensialoperatorer

En differensialoperator av orden n er en operator på $\mathfrak{R}$ på formen

$$P \coloneqq P(\mathrm{D}) \coloneqq \sum_{j=0}^{n} f_j(\mathbf{t})\mathrm{D}^j, \quad f(\mathbf{t}) \in \mathfrak{R}, \quad \mathrm{D} \coloneqq \frac{d}{d\mathbf{t}}$$

2.3 *q*-derivasjoner og *q*-differensialoperatorer

2.3.1 q-derivasjoner

Den deriverte av en funksjon er gitt ved

$$f'(\mathbf{t}) = \lim_{h \to 0} \frac{f(\mathbf{t}+h) - f(\mathbf{t})}{h}.$$

La R være en ring og $q \in R$ et invertibelt element. Da er en *q-derivasjon* på $\mathfrak{R}$ gitt ved

$$\partial_q f(\mathbf{t}) \coloneqq \frac{f(q\mathbf{t}) - f(\mathbf{t})}{(q-1)\mathbf{t}}.$$

Vi bruker betegnelsen ∂ for enkelhetsskyld.

Merk at en q-derivasjon er en lineær operator, så $\partial(f+g) = \partial(f) + \partial(g)$ for alle deriverbare $f, g \in \mathfrak{R}$. Ofte når q-deriverer, bruker en såkalte q-heltall. Disse er gitt ved

$$\{n\}_q \coloneqq \frac{q^n - 1}{q-1}, \quad n \in \mathbb{Z}_{\geq 0}.$$

Dette er best illustrert i et eksempel. La $f(\mathbf{t}) = \mathbf{t}^n$. Da er $\partial(\mathbf{t}^n) = \{n\}_q \mathbf{t}^{n-1}$. Her kan vi og se at $\{1\}_q = 1$ og $\{0\}_q = 0$.

Lemma 2.2. *Et q-heltall tilfredsstiller*

$$\{n+m\}_q = q^m\{n\}_q + \{m\}_q \quad \text{og} \quad \{n-m\}_q = q^{-m}\{n\}_q - q^{-m}\{m\}_q.$$

Bevis. Det er enkelt å vise den første identiteten:

$$\begin{aligned}\{n+m\}_q &= \frac{q^{n+m}-1}{q-1} \\ &= \frac{q^{n+m}-q^m}{q-1} + \frac{q^m-1}{q-1} \\ &= q^m\{n\}_q + \{m\}_q.\end{aligned}$$

For å vise den andre, merk at

$$\{-n\}_q = \frac{q^{-n}-1}{q-1} = -q^{-n}\frac{q^n-1}{q-1} = -q^{-n}\{n\}_q.$$

Sammen med første identiteten, er

$$\begin{aligned}\{n-m\}_q &= \frac{q^{n-m}-1}{q-1} \\ &= \frac{q^{n-m}-q^{-m}}{q-1} + \frac{q^{-m}-1}{q-1} \\ &= q^{-m}\{n\}_q - q^{-m}\{m\}_q.\end{aligned}$$

Dette fullfører beviset. □

Lemma 2.3. *Leibnizregelen for q-derivasjon er på formen*

$$\partial(f(\mathbf{t})g(\mathbf{t})) = \partial(f(\mathbf{t}))g(\mathbf{t}) + f(q\mathbf{t})\partial(g(\mathbf{t})).$$

Bevis. Beviset følges med uttrykksmanipulasjon:

$$\begin{aligned}\partial(f(\mathbf{t})g(\mathbf{t})) &= \frac{f(q\mathbf{t})g(q\mathbf{t}) - f(\mathbf{t})g(\mathbf{t})}{(q-1)\mathbf{t}} \\ &= \frac{f(q\mathbf{t})g(q\mathbf{t}) - f(\mathbf{t})g(\mathbf{t}) + f(q\mathbf{t})g(\mathbf{t}) - f(q\mathbf{t})g(\mathbf{t})}{(q-1)\mathbf{t}} \\ &= \frac{f(q\mathbf{t})g(\mathbf{t}) - f(\mathbf{t})g(\mathbf{t})}{(q-1)\mathbf{t}} + \frac{f(q\mathbf{t})g(q\mathbf{t}) - f(q\mathbf{t})g(\mathbf{t})}{(q-1)\mathbf{t}} \\ &= \partial(f(\mathbf{t}))g(\mathbf{t}) + f(q\mathbf{t})\partial(g(\mathbf{t})),\end{aligned}$$

og beviset er ferdig. □

Remark 2.4. Merk at $\partial(\alpha\phi) = \partial(\alpha)\phi + \alpha\partial(\phi) = \alpha\partial(\phi)$ for alle $\phi \in \mathfrak{R}$. Så $\partial(\alpha) = \alpha\partial$ for alle $\alpha \in R$.

Eksempel 2.5. Anta at $f(\mathbf{t}) = \mathbf{t}^3 + 5\mathbf{t}^2 - \mathbf{t} + 1$. Da er

$$\partial(f) = \{3\}_q\mathbf{t}^2 + 5\{2\}_q\mathbf{t} - 1 = (1 + q + q^2)\mathbf{t}^2 + (5 + 5q)\mathbf{t} - 1.$$

2.3.2 q-differensialoperatorer

La $\mathfrak{R}\langle\partial\rangle$ være en ring av ikke-kommuterende polynomer i variabel ∂. En *q-differensialoperator* på $\mathfrak{R}$ er gitt ved

$$P \coloneqq P(\partial) \coloneqq \sum_{j=0}^{\deg(P)} p_j\partial^j, \quad p_j \coloneqq f_j(\mathbf{t}) \in \mathfrak{R}.$$

2.4 Resultanter

La P og $Q \in R[\mathbf{t}]$ være to polynomer i variabel $\mathbf{t}$ på formen

$$P = \sum_{j=0}^{n} p_j\mathbf{t}^j \quad \text{og} \quad Q = \sum_{j=0}^{m} q_j\mathbf{t}^j,$$

der p_j og $q_j \in R$ er koeffisienter. Sylvestermatrisen av P og Q er en $(n + m) \times (n + m)$-matrise på formen

$$\mathrm{Syl}(P, Q) \coloneqq \begin{pmatrix} p_0 & p_1 & \cdots & p_n & 0 & \cdots & 0 \\ 0 & p_0 & \cdots & p_{n-1} & p_n & \cdots & 0 \\ \vdots & & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & p_0 & \cdots & p_{n-1} & p_n \\ q_0 & q_1 & \cdots & q_m & 0 & \cdots & 0 \\ 0 & q_0 & \cdots & q_{m-1} & q_m & \cdots & 0 \\ \vdots & & \ddots & & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & q_0 & \cdots & q_{m-1} & q_m \end{pmatrix}.$$

Her består den i-te raden av koeffisientene til

$$\mathbf{t}^i P \quad \text{for } 0 \leq i \leq m-1 \quad \text{og} \quad \mathbf{t}^i Q \quad \text{for } 0 \leq i \leq n-1.$$

Resultanten av P og Q er definert som

$$\mathrm{Res}(P, Q) \coloneqq \det(\mathrm{Syl}(P, Q)).$$

Eksempel 2.6. For å illustrere hvordan å beregne resultanten av polynomer, lar vi $P = p_0 + p_1\mathbf{t} + \mathbf{t}^3$ og $Q = q_0 + \mathbf{t}^2$ være to polynomer med koeffisienter $p_0, p_1, q_0 \in R$. Vi har $\deg(P) = 3$ og $\deg(Q) = 2$. For å beregne $\mathrm{Res}(P, Q)$, bruker vi koeffisientene fra $\mathbf{t}^i P$ for $0 \leq i \leq 1$ og $\mathbf{t}^i Q$ for $0 \leq i \leq 2$. Koeffisientene er altså gitt fra

$$\begin{aligned}
\mathbf{t}^0 P &= p_0 + p_1\mathbf{t} + \mathbf{t}^3 \\
\mathbf{t}^1 P &= p_0\mathbf{t} + p_1\mathbf{t}^2 + \mathbf{t}^4 \\
\mathbf{t}^0 Q &= q_0 + \mathbf{t}^2 \\
\mathbf{t}^1 Q &= q_0\mathbf{t} + \mathbf{t}^3 \\
\mathbf{t}^2 Q &= q_0\mathbf{t}^2 + \mathbf{t}^4
\end{aligned}$$

Derfor er

$$\mathrm{Res}(P, Q) = \begin{vmatrix} p_0 & p_1 & 0 & 1 & 0 \\ 0 & p_0 & p_1 & 0 & 1 \\ q_0 & 0 & 1 & 0 & 0 \\ 0 & q_0 & 0 & 1 & 0 \\ 0 & 0 & q_0 & 0 & 1 \end{vmatrix} = p_0^2 + q_0^3.$$

Vi kan også beregne resultanter av q-differensialoperatorer. Da heter det en differensialresultant. Men matrisen er noenlunde annerledes. Forskjellen er at den i-te raden i matrisen inneholder koeffisientene til $\partial^i P$ for $0 \leq i \leq m-1$ og $\partial^i Q$ for $0 \leq i \leq n-1$, så radene i matrisen er ikke nødvendigvis *forskjøvet*. Dette er best illustrert i følgende eksempel.

Eksempel 2.7. La $P = \mathbf{t}\partial - \alpha$ og $Q = \mathbf{t}^2\partial^2 - \beta$ være to q-differensial-operatorer der $\alpha, \beta \in R$. Først sjekker vi at $[P, Q] = 0$. Vi har

$$\begin{aligned} PQ &= (\mathbf{t}\partial - \alpha)(\mathbf{t}^2\partial^2 - \beta) \\ &= \mathbf{t}\partial(\mathbf{t}^2\partial^2 - \beta) - \alpha(\mathbf{t}^2\partial^2 - \beta) \\ &= q^2\mathbf{t}^3\partial^3 + (\{2\}_q - \alpha)\mathbf{t}^2\partial^2 - \beta\mathbf{t}\partial + \alpha\beta \end{aligned}$$

og likedan,

$$\begin{aligned} QP &= (\mathbf{t}^2\partial^2 - \beta)(\mathbf{t}\partial - \alpha) \\ &= \mathbf{t}^2\partial^2(\mathbf{t}\partial - \alpha) - \beta(\mathbf{t}\partial - \alpha) \\ &= \mathbf{t}^2\partial(\partial + q\mathbf{t}\partial^2 - \alpha\partial) - \beta(\mathbf{t}\partial - \alpha) \\ &= q^2\mathbf{t}^3\partial^3 + (1 + q - \alpha)\mathbf{t}^2\partial^2 - \beta\mathbf{t}\partial + \alpha\beta, \end{aligned}$$

som gir

$$PQ - QP = (\{2\}_q - \alpha)\mathbf{t}^2\partial^2 - (1 + q - \alpha)\mathbf{t}^2\partial^2 = 0,$$

fordi $\{2\}_q = 1 + q$. Koeffisientene til

$$\begin{aligned} \partial^0 P &= \mathbf{t}\partial - \alpha \\ \partial^1 P &= \partial(\mathbf{t}\partial - \alpha) = (1 - \alpha)\partial + q\mathbf{t}\partial^2 \\ \partial^0 Q &= \mathbf{t}^2\partial^2 - \beta \end{aligned}$$

gir

$$\mathrm{Syl}(P, Q) = \begin{pmatrix} -\alpha & \mathbf{t} & 0 \\ 0 & 1 - \alpha & q\mathbf{t} \\ -\beta & 0 & \mathbf{t}^2 \end{pmatrix}$$

og derfor

$$\mathrm{Res}(P, Q) = (\alpha^2 - \alpha - \beta q)\mathbf{t}^2,$$

der $\alpha, \beta \in R$ og $\mathbf{t} \in \mathfrak{R}$.

2.5 Burchnall-Chaundy kurver

La $\mathbf{x}, \mathbf{y} \in R$ være variabler. Da er $P_{\mathbf{x}}$ og $Q_{\mathbf{y}}$ to q-differensialoperatorer på formen

$$P_{\mathbf{x}} \coloneqq \sum_{j=0}^{n} p_j \partial^j - \mathbf{x} \quad \text{og} \quad Q_{\mathbf{y}} \coloneqq \sum_{j=0}^{m} q_j \partial^j - \mathbf{y}, \quad p_j, q_j \in \mathfrak{R}.$$

Anta at $[P, Q] = 0$. Sylvestermatrisen beregnes på samme måte: Den i-te raden finner vi fra

$$\partial^i P_{\mathbf{x}} = \partial^i \Big(\sum_{j=0}^{n} p_j \partial^j \Big) - \mathbf{x} \partial^i, \quad \text{for} \quad 0 \leq i \leq m$$

og

$$\partial^i Q_{\mathbf{y}} = \partial^i \Big(\sum_{j=0}^{m} q_j \partial^j \Big) - \mathbf{y} \partial^i, \quad \text{for} \quad 0 \leq i \leq n-1.$$

Resultanten beregnes også på samme måte. Vi introduserer notasjonen

$$\Xi(\mathbf{x}, \mathbf{y}) \coloneqq \mathrm{Res}(P_{\mathbf{x}}, Q_{\mathbf{y}}).$$

Remark 2.8. Merk at $\mathrm{Res}(P_{\mathbf{x}}, Q_{\mathbf{y}}) = \det(\mathrm{Syl}(P_{\mathbf{x}}, Q_{\mathbf{y}}))$ gir polynomer uttrykt med $\mathbf{x}$ og $\mathbf{y}$. Med andre ord, $\Xi(\mathbf{x}, \mathbf{y}) = \mathrm{Res}(P_{\mathbf{x}}, Q_{\mathbf{y}})$ definerer algebraiske kurver i $\mathfrak{R}^2$.

Definisjon 2.9. Anta at $[P_{\mathbf{x}}, Q_{\mathbf{y}}] = 0$. Kurven $\Xi \subset \mathfrak{R}^2$ definert av

$$\Xi(\mathbf{x}, \mathbf{y}) \coloneqq \mathrm{Res}(P_{\mathbf{x}}, Q_{\mathbf{y}}) = 0,$$

kalles for *Burchnall-Chaundy kurven av $P_{\mathbf{x}}$ og $Q_{\mathbf{y}}$*. Hvis koeffisientene i Ξ er uavhengig av $\mathbf{t}$ så er kurven en undermengde av R^2.

Eksempel 2.10. La $P_{\mathbf{x}} = P - \mathbf{x}$ og $Q_{\mathbf{x}} = Q - \mathbf{y}$, der P og Q er operatorene gitt i eksempel 2.7.

Først, $P_{\mathbf{x}}$ og $Q_{\mathbf{y}}$ kommuterer, siden

$$\begin{aligned}
P_{\mathbf{x}}Q_{\mathbf{y}} &= (\mathbf{t}\partial - \alpha - \mathbf{x})(\mathbf{t}^2\partial^2 - \beta - \mathbf{y}) \\
&= \mathbf{t}\partial(\mathbf{t}^2\partial^2 - \beta - \mathbf{y}) - \alpha(\mathbf{t}^2\partial^2 - \beta - \mathbf{y}) - \mathbf{x}(\mathbf{t}^2\partial^2 - \beta - \mathbf{y}) \\
&= \mathbf{t}(\{2\}_q\mathbf{t}\partial^2 + q^2\mathbf{t}^2\partial^3 - \beta\partial - \mathbf{y}\partial) - \alpha(\mathbf{t}^2\partial^2 - \beta - \mathbf{y}) \\
&\quad - \mathbf{x}(\mathbf{t}^2\partial^2 - \beta - \mathbf{y}) \\
&= q^2\mathbf{t}^3\partial^3 + (\{2\}_q - \alpha - \mathbf{x})\mathbf{t}^2\partial^2 - (\beta + \mathbf{y})\mathbf{t}\partial + \alpha\mathbf{y} + \beta\mathbf{x} + \mathbf{x}\mathbf{y} + \alpha\beta
\end{aligned}$$

og

$$\begin{aligned}
Q_{\mathbf{y}}P_{\mathbf{x}} &= (\mathbf{t}^2\partial^2 - \beta - \mathbf{y})(\mathbf{t}\partial - \alpha - \mathbf{x}) \\
&= \mathbf{t}^2\partial^2(\mathbf{t}\partial - \alpha - \mathbf{x}) - \beta(\mathbf{t}\partial - \alpha - \mathbf{x}) - \mathbf{y}(\mathbf{t}\partial - \alpha - \mathbf{x}) \\
&= \mathbf{t}^2\partial(\partial + q\mathbf{t}\partial^2 - \alpha\partial - \mathbf{x}\partial) - \beta(\mathbf{t}\partial - \alpha - \mathbf{x}) - \mathbf{y}(\mathbf{t}\partial - \alpha - \mathbf{x}) \\
&= \mathbf{t}^2(\partial^2 + q\partial^2 + q^2\mathbf{t}\partial^3 - \alpha\partial^2 - \mathbf{x}\partial^2) - \beta(\mathbf{t}\partial - \alpha - \mathbf{x}) \\
&\quad - \mathbf{y}(\mathbf{t}\partial - \alpha - \mathbf{x}) \\
&= q^2\mathbf{t}^3\partial^3 + (1 + q - \alpha - \mathbf{x})\mathbf{t}^2\partial^2 - (\beta + \mathbf{y})\mathbf{t}\partial + \alpha\mathbf{y} + \beta\mathbf{x} + \mathbf{x}\mathbf{y} + \alpha\beta
\end{aligned}$$

gir

$$P_{\mathbf{x}}Q_{\mathbf{y}} - Q_{\mathbf{y}}P_{\mathbf{x}} = (\{2\}_q - \alpha - \mathbf{x})\mathbf{t}^2\partial^2 - (1 + q - \alpha - \mathbf{x})\mathbf{t}^2\partial^2 = 0.$$

Koeffisientene fra

$$\begin{aligned}
\partial^0 P_{\mathbf{x}} &= \mathbf{t}\partial - \alpha - \mathbf{x} \\
\partial^1 P_{\mathbf{x}} &= \partial(\mathbf{t}\partial - \alpha - \mathbf{x}) = q\mathbf{t}\partial^2 - (\alpha + \mathbf{x} - 1)\partial \\
\partial^0 Q_{\mathbf{y}} &= \mathbf{t}^2\partial^2 - \beta - \mathbf{y}
\end{aligned}$$

gir

$$\mathrm{Syl}(P_{\mathbf{x}}, Q_{\mathbf{y}}) = \begin{pmatrix} -(\alpha + \mathbf{x}) & \mathbf{t} & 0 \\ 0 & -(\alpha + \mathbf{x} - 1) & q\mathbf{t} \\ -(\beta + \mathbf{y}) & 0 & \mathbf{t}^2 \end{pmatrix},$$

og derfor

$$\begin{aligned}\mathrm{Res}(P_{\mathbf{x}}, Q_{\mathbf{y}}) &= (\alpha + \mathbf{x})(\alpha + \mathbf{x} - 1)\mathbf{t}^2 - q\mathbf{t}^2(\beta + \mathbf{y}) \\ &= \left(\mathbf{x}^2 + (2\alpha - 1)\mathbf{x} + (\alpha^2 - \alpha - q\beta) - q\mathbf{y}\right)\mathbf{t}^2,\end{aligned}$$

der $\alpha, \beta \in R$ og $\mathbf{t} \in \mathfrak{R}$.

Remark 2.11. Merk at koeffisientene til $\mathrm{Res}(P_{\mathbf{x}}, Q_{\mathbf{y}})$ er uavhengig av $\mathbf{t} \in \mathfrak{R}$, så $\mathbf{t}^2$ er kansellerbar. Dette etterlater koeffisienter i R. La Ξ være en kurve definert ved $\Xi(\mathbf{x}, \mathbf{y}) = \mathbf{x}^2 + (2\alpha - 1)\mathbf{x} + (\alpha^2 - \alpha - q\beta) - q\mathbf{y}$. Når vi har kansellert $\mathbf{t}^2$, er Ξ en kurve i R^2.

Som vi ser, har eksempel 2.10 og remark 2.11 har vist at to kommuterende q-differensialoperatorer av orden en og to gir en parabel med likning

$$q\mathbf{y} = \mathbf{x}^2 + (2\alpha - 1)\mathbf{x} + (\alpha^2 - \alpha - q\beta).$$

Senere skal vi hvordan to q-differensialoperatorer av orden to og tre gir en elliptisk kurve.

Kapittel 3

Elliptiske kurver

3.1 Weierstrassform og diskriminanten

3.1.1 Weierstrassform

Vi begynner med en definisjon for $\mathrm{char}(R)$. Siden $\mathbb{Z}$ er en PID er hvert ideal (p) prinsipalt og generert av p.

Definisjon 3.1. La R være en kommutativ ring og $g : \mathbb{Z} \to R$ en homomorfisme med $g(n) = n \cdot 1_R$. Da er *karakteristikken av* R som er betegnet $\mathrm{char}(R)$, et positivt heltall p slik at $\ker(g) = (p)$.

Definisjon 3.2. En *kubisk kurve* $\mathscr{C}$ som er definert over R, er en kurve definert ved polynomet

$$\mathbf{y}^2 + a_1\mathbf{xy} + a_3\mathbf{y} = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6, \quad a_i \in R.$$

Dette er en likning som kalles for den *utvidede Weierstrassformen*. Hvis $\mathrm{char}(R) \neq 2, 3$, så kan den skrives på formen

$$\mathbf{y}^2 = \mathbf{x}^3 + b\mathbf{x} + c, \quad b, c \in R,$$

som kalles for den *korte Weierstrassformen*.

For å vise at den utvidede formen kan skrives på den korte, antar vi at $\mathrm{char}(R) \neq 2$ og skriver $\mathbf{y}^2 + (a_1\mathbf{x} + a_3)\mathbf{y} - g(\mathbf{x}) = 0$ der $g(\mathbf{x}) = \mathbf{x}^3 +$

$a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6$. Så velger vi $\mathbf{y}' = \mathbf{y} - (a_1\mathbf{x} + a_3)/2$. Det gir

$$\begin{aligned} g(\mathbf{x}) &= \left(\mathbf{y} - \frac{1}{2}(a_1\mathbf{x} + a_3)\right)^2 + (a_1\mathbf{x} + a_3)\left(\mathbf{y} - \frac{1}{2}(a_1\mathbf{x} + a_3)\right) \\ &= \mathbf{y}^2 - \mathbf{y}(a_1\mathbf{x} + a_3) + \frac{1}{4}(a_1\mathbf{x} + a_3)^2 + \mathbf{y}(a_1\mathbf{x} + a_3) - \frac{1}{2}(a_1\mathbf{x} + a_3)^2 \\ &= \mathbf{y}^2 - \frac{1}{4}(a_1\mathbf{x} + a_3)^2 \\ &= \mathbf{y}^2 - \frac{a_1^2}{4}\mathbf{x}^2 + \frac{a_1a_3}{2}\mathbf{x} + \frac{a_3^2}{4}. \end{aligned}$$

Med $g(\mathbf{x}) = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6$ har vi

$$\begin{aligned} \mathbf{y}^2 - \frac{a_1^2}{4}\mathbf{x}^2 + \frac{a_1a_3}{2}\mathbf{x} + \frac{a_3^2}{4} &= \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6 \\ \mathbf{y}^2 &= \mathbf{x}^3 + \left(a_2 + \frac{a_1^2}{4}\right)\mathbf{x}^2 + \left(a_4 - \frac{a_1a_3}{2}\right)\mathbf{x} + a_6 - \frac{a_3^2}{4} \\ &= \mathbf{x}^3 + a\mathbf{x}^2 + b\mathbf{x} + c. \end{aligned}$$

Hvis vi antar at $\mathrm{char}(R) \neq 2, 3$, så kan dette skrives som

$$\mathbf{y}^2 = \mathbf{x}^3 + b\mathbf{x} + c,$$

der $\mathbf{x}' = \mathbf{x} - a/3$.

Remark 3.3. Når $\mathrm{char}(R) \neq 2$, så kan den utvidede Weierstrassformen skrives som den *normale Weierstrassformen* $\mathbf{y}^2 = \mathbf{x}^3 + a\mathbf{x}^2 + b\mathbf{x} + c$, der $a, b, c \in R$. Merk at $a_2, a_4, a_6 \in R$ ikke nødvendigvis er det samme som $a, b, c \in R$. Merk også at a ikke er det samme som null, siden $a, b, c \in R$ når $\mathrm{char}(R) \neq 2$ og $b, c \in R$ når $\mathrm{char}(R) \neq 2, 3$.

Hvis vi ønsker å spesifisere at $a_i \in R$, bruker vi notasjonen $\mathscr{C}/R$ og sier at $\mathscr{C}$ er definert over R.

3.1.2 Diskriminanten

La $\mathscr{C}$ være en kubisk kurve definert ved

$$\mathbf{y}^2 + a_1\mathbf{x}\mathbf{y} + a_3\mathbf{y} = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6.$$

Sett

$$\begin{aligned} b_2 &\coloneqq a_1^2 + 4a_2 \\ b_4 &\coloneqq 2a_4 + a_1a_3 \\ b_6 &\coloneqq a_3^2 + 4a_6 \\ b_8 &\coloneqq a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Da er *diskriminanten* til $\mathscr{C}$ en verdi gitt ved

$$\Delta \coloneqq -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Hvis $\mathrm{char}(R) \neq 2, 3$, så er diskriminanten til $\mathscr{C}$ gitt ved

$$\Delta \coloneqq -16(4b^3 + 27c^2).$$

Hvis $\Delta = 0$, så sier man at $\mathscr{C}$ er en ikke-glatt (singulær) kurve. Med andre ord, det fins punkter der en tangentlinje ikke er veldefinert. La for eksempel S være en mengde med løsninger til polynomet $f(\mathbf{x}_1, \ldots, \mathbf{x}_n) = 0$. Da er $\mathbf{p} \in S$ et singulært punkt hvis

$$\frac{\partial f}{\partial \mathbf{x}_1}(\mathbf{p}) = \cdots = \frac{\partial f}{\partial \mathbf{x}_n}(\mathbf{p}) = 0.$$

Ellers er $\mathbf{p}$ ikke-singulær (regulær) og $\mathscr{C}$ en glatt (regulær) kurve.

Proposisjon 3.4. *Hvis* $\mathrm{char}(R) \neq 2$ *og* $\mathscr{C}$ *er definert ved* $\mathbf{y}^2 = \mathbf{x}^3 + a\mathbf{x}^2 + b\mathbf{x} + c$*, da er diskriminanten til* $\mathscr{C}$ *gitt ved*

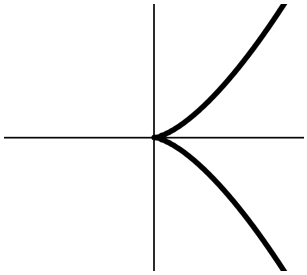
$$\Delta(\mathscr{C}) \coloneqq -4a^3c + a^2b^2 - 4b^3 - 27c^2 + 18abc.$$

Bevis. Med de definerte koeffisientene over, finner vi

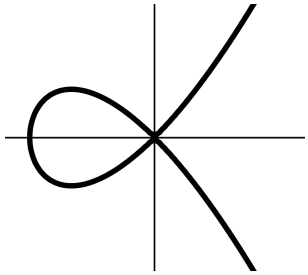
$$\begin{aligned} \Delta(\mathscr{C}) &= -16a^2(4ac - b^2) - 64b^3 - 27(16c^2) + 9(32abc) \\ &= -4a^3c + a^2b^2 - 4b^3 - 27c^2 + 18abc, \end{aligned}$$

der vi har multiplisert med 16^{-1}. □

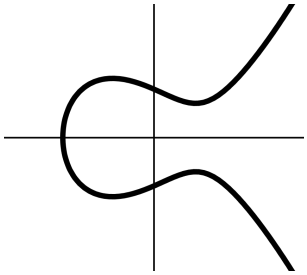
3.1.3 Eksempler på kubiske kurver



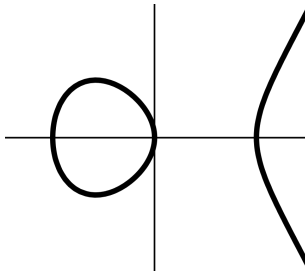
Figur 3.1: $y^2 = x^3$.



Figur 3.2: $y^2 = x^3 + 3x^2$.



Figur 3.3: $y^2 = x^3 - 3x + 4$.



Figur 3.4: $y^2 = x^3 - 6x$.

Figurene over er eksempler på forskjellige kubiske kurver. Alle kurvene er på Weierstrassform, men diskriminantene er ulike. Figur 3.1 og 3.2 er eksempler på singulære kubiske kurver, siden $\Delta = 0$. Figur 3.3 og 3.4 har $\Delta \neq 0$. Disse er regulære kurver.

3.1.4 *j*-invarianten

La $\mathscr{C}$ være en kubisk kurve. En *j-invariant* er en verdi definert ved

$$j \coloneqq \frac{(b_2^2 - 24b_4)^3}{\Delta(\mathscr{C})}, \quad \Delta(\mathscr{C}) \neq 0.$$

Hvis $\mathscr{C}$ er på den korte Weierstrassformen, er

$$j \coloneqq \frac{1728(4a)^3}{\Delta(\mathscr{C})}, \quad \Delta(\mathscr{C}) = -16(4b^3 + 27c^2) \neq 0.$$

Merk at hvis $\Delta = 0$, så er $j = \infty$.

3.2 Elliptiske kurver

3.2.1 Definisjon

Definisjon 3.5. En kubisk kurve $\mathscr{C}$ på Weierstrassform er en *elliptisk kurve* hvis $\Delta \neq 0$ og det er gitt et punkt $\mathcal{O} \in \mathbb{P}$ som er rasjonell over R. Vi betegner en elliptisk kurve med $\mathscr{E}$.

Den første betingelsen er at $\mathscr{E}$ må være regulær. For å vise dette, la f være et polynom på, for eksempel, kort Weierstrassform med $\mathrm{char}(R) \neq 2, 3$ og beregn $\partial f/\partial \mathbf{x}$ og $\partial f/\partial \mathbf{y}$ for alle $\mathbf{x}, \mathbf{y} \in R$. Å gjøre det gir

$$f_{\mathbf{x}} = \frac{\partial f}{\partial \mathbf{x}}(\mathbf{x}, \mathbf{y}) = 3\mathbf{x}^2 + b \quad \text{og} \quad f_{\mathbf{y}} = \frac{\partial f}{\partial \mathbf{y}}(\mathbf{x}, \mathbf{y}) = -2\mathbf{y}.$$

For en regulær kubisk kurve, må enten $f_{\mathbf{x}}$ eller $f_{\mathbf{y}}$ være ulik null. På samme måte må $\mathbf{x}^3 + b\mathbf{x} + c \neq 3\mathbf{x}^2 + b$. Det kan vises med $\mathbf{x}^2 = -b/3$ at

$$\frac{2b\mathbf{x}}{3} + c \neq 0,$$

som er ekvivalent med $4b^3 + 27c^2 = \Delta \neq 0$.

Den andre betingelsen er at det fins et punkt $\mathcal{O}$ som er rasjonell over R. Merk at $\mathcal{O} \coloneqq (0 : 1 : 0)$ ikke er i R^2, men tenkes på som et punkt som ligger langt oppe eller langt nede på $\mathbf{y}$-aksen.

Lemma 3.6. *Punktet $\mathcal{O} \in \mathbb{P}$ er et regulært punkt.*

Bevis. Siden $\mathcal{O} \in \mathbb{P}$, så må vi se den korte Weierstrassformen som

$$F(X : Y : Z) = Y^2Z - (X^3 + bXZ^2 + cZ^3).$$

De partiellderiverte er

$$\begin{aligned} F_X &= \frac{\partial F}{\partial X}(X : Y : Z) = -(3X^2 + bZ^2), \\ F_Y &= \frac{\partial F}{\partial Y}(X : Y : Z) = 2YZ, \\ F_Z &= \frac{\partial F}{\partial Z}(X : Y : Z) = Y^2 - (2bXZ + 3cZ^2). \end{aligned}$$

Anta nå at $\mathcal{O}$ er singulær. Da må $F_X = F_Y = F_Z = 0$. Når vi evaluerer de partiellderiverte ved $\mathcal{O}$, finner vi at

$$\frac{\partial F}{\partial X}(\mathcal{O}) = \frac{\partial F}{\partial Y}(\mathcal{O}) = 0 \neq \frac{\partial F}{\partial Z}(\mathcal{O}) = 1.$$

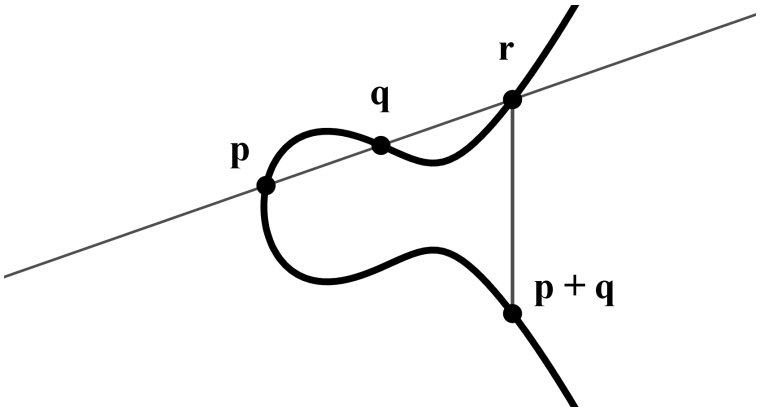
Dette viser at $\mathcal{O}$ er regulær. □

Definisjon 3.7. La R være en ring og $\mathscr{E}$ en elliptisk kurve. Da er $\mathscr{E}$ over R definert som en mengde

$$\mathscr{E}(R) \coloneqq \big\{(\mathbf{x} : \mathbf{y}) \in R^2 \mid \mathbf{y}^2 + a_1\mathbf{x}\mathbf{y} + a_3\mathbf{y} = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6\big\},$$

og kalles de *R-rasjonelle punktene på $\mathscr{E}$*.

3.2.2 Gruppeloven



Figur 3.5: Addisjon på en elliptisk kurve.

Definisjon 3.8. La $\mathscr{E}$ være en elliptisk kurve og $\mathbf{p}$ og $\mathbf{q}$ to rasjonale punkter. En linje gjennom $\mathbf{p}$ og $\mathbf{q}$ skjærer et tredje punkt $\mathbf{r}$. Refleksjonen til $\mathbf{r}$ om $\mathbf{x}$-aksen er definert som $\mathbf{p} + \mathbf{q}$.

Definisjonen lar oss geometrisk summere to punkter på en elliptisk kurve. Ved å tegne ℓ gjennom to valgte punkter $\mathbf{p}$ og $\mathbf{q}$, finner vi skjæringspunktet $\mathbf{r}$, som er refleksjonen til summen av $\mathbf{p}$ og $\mathbf{q}$. Det dette forteller oss, er at siden siden $\mathscr{E}(R)$ er en mengde med R-rasjonale punkter og $+$ en operasjon, så er $\mathscr{E}(R)$ en abelsk gruppe.

Teorem 3.9. *En mengde $\mathscr{E}(R)$ sammen med addisjon $+$ er en abelsk gruppe som tilfredsstiller følgende fire krav:*

(i) *For hvert $\mathbf{p} \in \mathscr{E}(R)$ fins det et enhetselement $\mathcal{O} \in \mathscr{E}(R)$ slik at*

$$\mathbf{p} + \mathcal{O} = \mathcal{O} + \mathbf{p},$$

(ii) *for hvert $\mathbf{p} \in \mathscr{E}(R)$ fins det et inverselement $-\mathbf{p}$ slik at*

$$\mathbf{p} + (-\mathbf{p}) = (-\mathbf{p}) + \mathbf{p} = \mathcal{O},$$

(iii) *hvis $\mathbf{p}, \mathbf{q} \in \mathscr{E}(R)$,*

$$\mathbf{p} + \mathbf{q} = \mathbf{q} + \mathbf{p},$$

(iv) *og hvis $\mathbf{p}, \mathbf{q}, \mathbf{r} \in \mathbf{p}$,*

$$(\mathbf{p} + \mathbf{q}) + \mathbf{r} = \mathbf{p} + (\mathbf{q} + \mathbf{r}).$$

Bevis. La $\mathbf{p} = (\mathbf{x}_0, \mathbf{y}_0) \in \mathscr{E}(R)$ være et punkt med $\mathbf{y}_0 \neq 0$. For å vise (i), anta at ℓ er en linje gjennom $\mathbf{p}$ og $\mathcal{O}$. Per definisjon vil ℓ gå gjennom $-\mathbf{p}$, som er refleksjonen til $\mathbf{p} + \mathcal{O}$ om $\mathbf{x}$-aksen. Da er $\mathcal{O}$ et enhetselement, siden $\mathbf{p} + \mathcal{O} = \mathcal{O} + \mathbf{p} = \mathbf{p}$.

For å vise (ii), la $\mathbf{q} \in \mathscr{E}(R)$ være punkt. Anta at ℓ er en vertikal linje gjennom $\mathbf{q}$ og $-\mathbf{q}$ og så $\mathcal{O}$, som er refleksjonen til $\mathcal{O}$. Da er $-\mathbf{q}$ inversen til $\mathbf{q}$, siden $\mathbf{q} + (-\mathbf{q}) = (-\mathbf{q}) + \mathbf{q} = \mathcal{O}$.

(iii) er opplagt. Anta at ℓ er en linje gjennom $\mathbf{p}$ og $\mathbf{q}$ og så $\mathbf{r}$, som er refleksjonen til $\mathbf{p} + \mathbf{q}$. Anta nå at ℓ' er en annen linje som går gjennom de samme punktene $\mathbf{q}$ og $\mathbf{p}$ og så $\mathbf{r}$. Denne gangen er $\mathbf{r}$ refleksjonen til $\mathbf{q} + \mathbf{p}$, siden ℓ' går gjennom $\mathbf{q}$ og så $\mathbf{p}$. Men siden ℓ og ℓ' er essensielt samme linje, så er $\mathbf{p} + \mathbf{q} = \mathbf{q} + \mathbf{p}$.

(iv) er notorisk for å være vanskelig å bevise. Vi referer til Friedl [4] og Fujii [5] for et elementært og et algebraisk bevis. □

3.3 Eksplisitte formler og eksempler

Først trenger vi noen notasjoner. Hvis $\mathbf{x}_1 \neq \mathbf{x}_2$,

$$\lambda = \frac{\mathbf{y}_2 - \mathbf{y}_1}{\mathbf{x}_2 - \mathbf{x}_1}.$$

Hvis $\mathbf{x}_1 = \mathbf{x}_2$,

$$\lambda = \frac{3\mathbf{x}_1^2 + 2a_1\mathbf{x}_1 + a_4 - a_1\mathbf{y}_1}{2\mathbf{y}_1 + a_1\mathbf{x}_1 + a_3}.$$

3.3.1 Ulike punkter

Proposisjon 3.10. *La $\mathscr{E}$ være en elliptisk kurve på formen $\mathbf{y}^2 + a_1\mathbf{x}\mathbf{y} + a_3\mathbf{y} = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6$, $a_i \in R$. La også $\mathbf{p} = (\mathbf{x}_1, \mathbf{y}_2)$ og $\mathbf{q} = (\mathbf{x}_2, \mathbf{y}_2)$ være to punkter på $\mathscr{E}$. Da er $\mathbf{p} + \mathbf{q} \coloneqq (\mathbf{x}_3, \mathbf{y}_3)$ der*

$$\begin{aligned}\mathbf{x}_3 &= \lambda^2 + a_1\lambda - a_2 - \mathbf{x}_1 - \mathbf{x}_2\\ \mathbf{y}_3 &= -\lambda(\mathbf{x}_3 - \mathbf{x}_1) - \mathbf{y}_1 - (a_1\mathbf{x}_1 + a_3),\end{aligned}$$

hvis $\mathbf{x}_1 \neq \mathbf{x}_2$.

Bevis. La $\mathbf{y} = \lambda(\mathbf{x} - \mathbf{x}_1) + \mathbf{y}_1$ definere en linje gjennom to ulike punkter $\mathbf{p}$ og $\mathbf{q}$ på $\mathscr{E}$. Innsetting og omskriving i utvidet Weierstrassform gir

$$\mathbf{x}^3 - (\lambda^2 + \lambda a_1 - a_2)\mathbf{x}^2 + [\text{ resten av polynomet }] = 0.$$

Dette er et polynom i $\mathbf{x}$ i tredje orden med løsninger $\mathbf{x}_1$, $\mathbf{x}_2$ og $\mathbf{x}_3$ til $(\mathbf{x} - \mathbf{x}_1)(\mathbf{x} - \mathbf{x}_2)(\mathbf{x} - \mathbf{x}_3) = 0$. Når vi sammenlikner koeffisienten til $\mathbf{x}^2$, finner vi $\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 = \lambda^2 + \lambda a_1 - a_2$, som er ekvivalent med

$$\mathbf{x}_3 = \lambda^2 + \lambda a_1 - a_2 - \mathbf{x}_1 - \mathbf{x}_2.$$

For å finne $\mathbf{y}_3$, setter vi inn $\mathbf{x}_3$ i likningen til linjen:

$$\mathbf{y}_3 = -\lambda(\mathbf{x}_3 - x_1) - \mathbf{y}_1 - (a_1\mathbf{x}_1 + a_3).$$

Beviset er ferdig. □

Remark 3.11. Hvis en elliptisk kurve er definert ved den normale Weierstrassformen, så blir formlene i proposisjon ?? forenklet. For eksempel, hvis $\mathrm{char}(R) \neq 2$, da er $a_1, a_3 \mapsto 0$, $a_4, a_6 \mapsto b, c$. Da er

$$\mathbf{x}_3 = \lambda^2 - a_2 - \mathbf{x}_1 - \mathbf{x}_2 \quad \text{og} \quad \mathbf{y}_3 = -\lambda(\mathbf{x}_3 - \mathbf{x}_1) - \mathbf{y}_1,$$

hvis $\mathrm{char}(R) \neq 2, 3$. Likedan, hvis en elliptisk kurve er definert ved den korte Weierstrassformen, så blir $a_2 \mapsto 0$ og

$$\mathbf{x}_3 = \lambda^2 - \mathbf{x}_1 - \mathbf{x}_2 \quad \text{og} \quad \mathbf{y}_3 = -\lambda(\mathbf{x}_3 - \mathbf{x}_1) - \mathbf{y}_1,$$

hvis $\mathrm{char}(R) \neq 2, 3$.

Eksempel 3.12. For å illustrere, ser vi på kurven $\mathscr{E}$ gitt ved

$$\mathbf{y}^2 = \mathbf{x}^3 + \mathbf{x}^2 - \mathbf{x}.$$

Kurven er elliptisk og likningen er på normal Weierstrassform. Så koeffisientene er $a = 1$, $b = 1$ og $c = -1$. Kurven har fem $\mathbb{Z}$-rasjonale punkter,

$$\mathscr{E}(\mathbb{Z}) = \big\{(-1 : \pm 1), (0 : 0), (1 : \pm 1)\big\}.$$

Vi bruker betegnelsene $\mathbf{p}_1 = (-1 : -1)$, $\mathbf{p}_2 = (0 : 0)$ og $\mathbf{p}_1 + \mathbf{p}_2 = (1 : -1)$. Vi vil nå vise at $(-1 : 1) + (0 : 0) = (1 : -1)$.

Siden likningen til kurven er på normal Weierstrassform, bruker vi de eksplisitte likningene

$$\mathbf{x}_3 = \lambda^2 - a_2 - \mathbf{x}_1 - \mathbf{x}_2 \quad \text{og} \quad \mathbf{y}_3 = -\lambda(\mathbf{x}_3 - \mathbf{x}_1) - \mathbf{y}_1$$

Først finner vi λ^2:

$$\lambda^2 = \left(\frac{\mathbf{y}_2 - \mathbf{y}_1}{\mathbf{x}_2 - \mathbf{x}_1}\right)^2 = \left(\frac{1}{1}\right)^2 = 1.$$

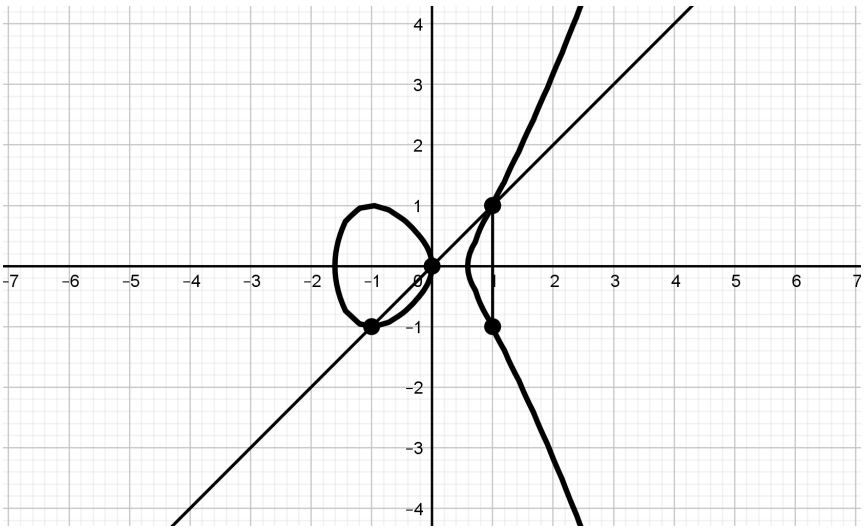
Dette gir

$$\mathbf{x}_3 = 1 - a_2 - \mathbf{x}_1 - \mathbf{x}_2 = 1 - 1 + 1 = 1.$$

Så finner vi $\mathbf{y}_3$:

$$\mathbf{y}_3 = -1(1+1) + 1 = -1.$$

I alt ser vi at $(-1 : -1) + (0 : 0) = (1 : -1)$. Merk at denne algebraiske beregningen samsvarer med figur 3.6



Figur 3.6: Figuren viser den geometriske konstruksjonen av addisjon på kurven $\mathscr{E}$ definert ved likningen $\mathbf{y}^2 = \mathbf{x}^3 + \mathbf{x}^2 - \mathbf{x}$. Her er $\mathbf{p}_1 = (-1 : -1)$, $\mathbf{p}_2 = (0 : 0)$ og $\mathbf{p}_1 + \mathbf{p}_2 = (1 : -1)$.

3.3.2 Like punkter

Proposisjon 3.13. *La $\mathscr{E}$ være en elliptisk kurve definert ved utvidet Weierstrassform $\mathbf{y}^2 + a_1\mathbf{x}\mathbf{y} + a_3\mathbf{y} = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6$. Hvis $\mathbf{p} = (\mathbf{x}_1, \mathbf{y}_1)$ og $2\mathbf{p} = (\mathbf{x}_2, \mathbf{y}_2)$, så er*

$$\mathbf{x}_2 = \left(\frac{g'(\mathbf{x}_1) - a_1\mathbf{y}_1}{2\mathbf{y}_1 + a_1\mathbf{x}_1 + a_3}\right)\left(\frac{g'(\mathbf{x}_1) - a_1\mathbf{y}_1}{2\mathbf{y}_1 + a_1\mathbf{x}_1 + a_3} + a_1\right) - a_2 - 2\mathbf{x}_1,$$

og

$$\mathbf{y}_2 = -\left(\frac{g'(\mathbf{x}_1) - a_1\mathbf{y}_1}{2\mathbf{y}_1 + a_1\mathbf{x}_1 + a_3}\right)(\mathbf{x}_2 - \mathbf{x}_1) - \mathbf{y}_1 - (a_1\mathbf{x}_1 + a_3).$$

Disse kalles for duplikasjonsformler.

Bevis. La $\mathbf{p} = (\mathbf{x}_1, \mathbf{y}_1)$ og anta at det fins en tangentlinje ℓ ved $\mathbf{p}$ på $\mathscr{E}$ med likningen

$$\mathbf{y} = \mathbf{y}_1'(\mathbf{x} - \mathbf{x}_1) + \mathbf{y}_1, \quad \mathbf{y}_1' = \frac{d\mathbf{y}}{d\mathbf{x}}.$$

Per definisjon vil tangentlinjen ℓ skjære refleksjonen til $2\mathbf{p} = (\mathbf{x}_2, \mathbf{y}_2)$. Nå, la $g(x) = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6$. For å finne $2\mathbf{p}$, deriverer vi den utvidede Weierstrassformen med hensyn på $\mathbf{x}$. Åpenbart er

$$\frac{d}{d\mathbf{x}}\left(\mathbf{y}^2 + a_1\mathbf{x}\mathbf{y} + a_3\mathbf{y} - g(\mathbf{x})\right) = 2\mathbf{y}\mathbf{y}' + a_1\mathbf{y} + a_1\mathbf{x}\mathbf{y}' + a_3\mathbf{y}' - g'(\mathbf{x}),$$

og derfor,

$$\mathbf{y}' = \frac{g'(\mathbf{x}) - a_1\mathbf{y}}{2\mathbf{y} + a_1\mathbf{x} + a_3}.$$

Merk at dette og likningen til ℓ har samme punkt $\mathbf{p}$ på $\mathscr{E}$ med stigningstall $\mathbf{y}' = \mathbf{y}_1'$. La $\lambda \coloneqq \mathbf{y}_1'$. Når vi setter dette inn i de eksplisitte formlene, får vi

$$\begin{aligned}\mathbf{x}_2 &= \lambda(\lambda + a_1) - a_2 - 2\mathbf{x}_1 \\ &= \left(\frac{g'(\mathbf{x}_1) - a_1\mathbf{y}_1}{2\mathbf{y}_1 + a_1\mathbf{x}_1 + a_3}\right)\left(\frac{g'(\mathbf{x}_1) - a_1\mathbf{y}_1}{2\mathbf{y}_1 + a_1\mathbf{x}_1 + a_3} + a_1\right) - a_2 - 2\mathbf{x}_1,\end{aligned}$$

og

$$\begin{aligned}\mathbf{y}_2 &= -\lambda(\mathbf{x}_2 - \mathbf{x}_1) - \mathbf{y}_1 - (a_1\mathbf{x}_1 + a_3) \\ &= -\left(\frac{g'(\mathbf{x}_1) - a_1\mathbf{y}_1}{2\mathbf{y}_1 + a_1\mathbf{x}_1 + a_3}\right)(\mathbf{x}_2 - \mathbf{x}_1) - \mathbf{y}_1 - (a_1\mathbf{x}_1 + a_3),\end{aligned}$$

og beviset er ferdig. □

Remark 3.14. I likhet med remark 3.11 hvis en elliptisk kurve er definert ved den normale Weierstrassformen, så er

$$\mathbf{x}_2 = \left(\frac{g'(\mathbf{x}_1)}{2\mathbf{y}_1}\right)^2 - a_2 - 2\mathbf{x}_1 \quad \text{og} \quad \mathbf{y}_2 = -\left(\frac{g'(\mathbf{x}_1)}{2\mathbf{y}_1}\right)(\mathbf{x}_2 - \mathbf{x}_1) - \mathbf{y}_1,$$

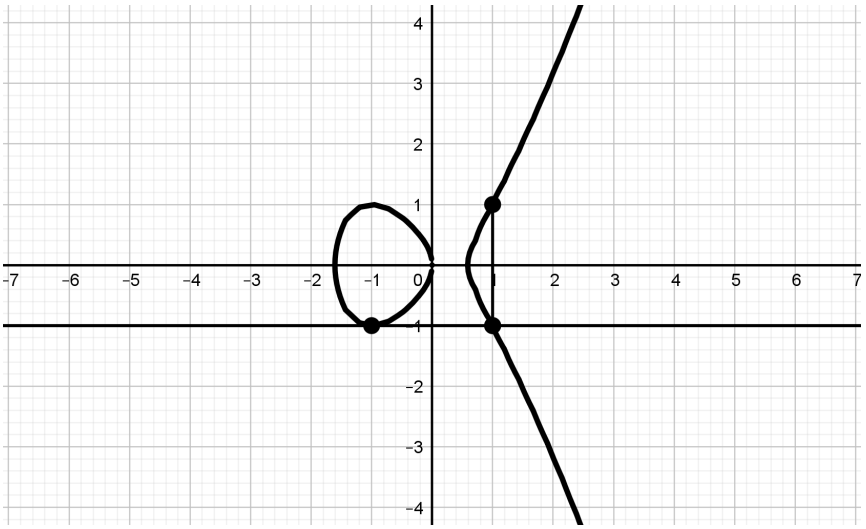
hvis $\mathrm{char}(R) \neq 2$. Hvis den elliptiske kurven er definert ved den korte Weier-

strassformen, så er $a_2 \mapsto 0$ og

$$\mathbf{x}_2 = \left(\frac{g'(\mathbf{x}_1)}{2\mathbf{y}_1}\right)^2 - 2\mathbf{x}_1 \quad \text{og} \quad \mathbf{y}_2 = -\left(\frac{g'(\mathbf{x}_1)}{2\mathbf{y}_1}\right)(\mathbf{x}_2 - \mathbf{x}_1) - \mathbf{y}_1,$$

hvis $\mathrm{char}(R) \neq 2, 3$.

Eksempel 3.15. Vi fortsetter å bruke kurven fra eksempel 3.12. Denne gangen ønsker vi å vise at $2(-1 : -1) = (1 : 1)$. Den geometriske konstruksjonen er vist i figuren:



Figur 3.7: Figuren viser den geometriske konstruksjonen av addisjon på kurven $\mathscr{E}$ definert ved likningen $\mathbf{y}^2 = \mathbf{x}^3 + \mathbf{x}^2 - \mathbf{x}$. Her er $\mathbf{p} = (-1 : -1)$ og $2\mathbf{p} = (1 : 1)$.

Nok en gang ser vi at likningen til kurven er på normal Weierstrassform, så vi bruker

$$\mathbf{x}_2 = \left(\frac{g'(\mathbf{x}_1)}{2\mathbf{y}_1}\right)^2 - a_2 - 2\mathbf{x}_1 \quad \text{og} \quad \mathbf{y}_2 = -\left(\frac{g'(\mathbf{x}_1)}{2\mathbf{y}_1}\right)(\mathbf{x}_2 - \mathbf{x}_1) - \mathbf{y}_1.$$

I tillegg bruker vi betegnelsene $\mathbf{p} = (-1 : -1)$ og $2\mathbf{p} = (1 : 1)$. Vi begynner beregningene ved å først finne $g'(\mathbf{x}_1)$:

$$g'(\mathbf{x}_1) = \frac{d}{d\mathbf{x}_1}\left(\mathbf{x}_1^3 + \mathbf{x}_1^2 - \mathbf{x}_1\right) = 3\mathbf{x}_1^2 + 2\mathbf{x}_1 - 1.$$

Når $\mathbf{x}_1 = -1$ får vi

$$g'(-1) = 3 - 2 - 1 = 0.$$

Da kan vi finne $\mathbf{x}_2$:

$$\mathbf{x}_2 = \left(\frac{0}{2\mathbf{y}_1}\right)^2 - a_2 - 2\mathbf{x}_1 = -1 + 2 = 1.$$

Med dette finner vi $\mathbf{y}_2$:

$$\mathbf{y}_2 = \left(\frac{0}{2\mathbf{y}_1}\right)^2 (\mathbf{x}_2 - \mathbf{x}_1) - \mathbf{y}_1 = 1.$$

Som vi ser er $2(-1 : -1) = (1 : 1)$.

3.3.3 Den assosiative loven, notat

En kan bruke de eksplisitte formlene til å bevise den assosiative loven for elliptiske kurver. Loven sier at for punkter $\mathbf{p}$, $\mathbf{q}$ og $\mathbf{r}$ på $\mathscr{E}$, så er $(\mathbf{p}+\mathbf{q})+\mathbf{r} = \mathbf{p} + (\mathbf{q} + \mathbf{r})$. Altså kan vi velge punkter på kurven og vise at denne likheten stemmer. For eksempel, la $\mathbf{p} = (-1 : -1)$, $\mathbf{q} = (0 : 0)$ og $\mathbf{r} = (-1 : 1)$. Disse er punkter på kurven i eksempel 3.12 og 3.15. Med de eksplisitte formlene kan vi sjekke at begge sider av loven er like. Venstre side gir

$$(\mathbf{p} + \mathbf{q}) + \mathbf{r} = (1 : -1) + (-1 : 1) = (0 : 0).$$

Høyre side gir

$$\begin{aligned}\mathbf{p} + (\mathbf{q} + \mathbf{r}) &= (-1 : -1) + ((0 : 0) + (-1 : 1)) \\ &= (-1 : -1) + (1 : 1) = (0 : 0).\end{aligned}$$

Som vi ser, så er begge sidene like. Problemet er at dette gjelder kun for disse punktene og for den elliptiske kurven med likning $\mathbf{y}^2 = \mathbf{x}^3 + \mathbf{x}^2 - \mathbf{x}$. Med andre ord er det mye mer å gjøre for å grundig bevise denne loven.

Kapittel 4

Strukturen av elliptiske kurver

Kapittel 3 viste at en elliptisk kurve som er definert over en kommutative ring R er en mengde R-rasjonelle punkter med en abelsk gruppestruktur. Det naturlige spørsmålet er hvordan en sånn gruppe ser ut. Et annet er hvor mange R-rasjonelle punkter fins det? Og hva med når R er en endelig kropp? Vi begynner med det grunnleggende.

4.1 Torsjonspunkter

Definisjon 4.1. La $\mathscr{E}(R)$ være en mengde med R-rasjonelle punkter på en elliptisk kurve $\mathscr{E}$. Et *N-torsjonspunkt* er da et punkt $\mathbf{p} \in \mathscr{E}(R)$ som er slik at

$$[N]\mathbf{p} = \mathbf{p} + \mathbf{p} + \cdots + \mathbf{p} = \mathcal{O}, \quad N \in \mathbb{Z}_{\geq 1}.$$

Hvis $\mathscr{E}$ er definert over R, så er

$$\mathscr{E}(R)[N] \coloneqq \big\{\mathbf{p} \in \mathscr{E}(R) \mid [N]\mathbf{p} = \mathcal{O}\big\}$$

en *N-torsjonsundermengde* av $\mathscr{E}(R)$. Undermengden av alle torsjonspunkter er betegnet $\mathscr{E}(R)_{\text{tor}}$

Merk at $\mathscr{E}(R)[N]$ er en abelsk gruppe. La $\mathbf{p}, \mathbf{q} \in \mathscr{E}(R)[N]$ være torsjonspunkter av orden N. Da er $\mathbf{p} + \mathbf{q}$ element i $\mathscr{E}(R)[N]$ siden $[N](\mathbf{p} + \mathbf{q}) = [N]\mathbf{p} + [N]\mathbf{q} = \mathcal{O}$. Dermed er $\mathcal{O}$ et N-torsjonspunkt for alle N. Dette kalles for det trivielle torsjonspunktet.

4.1.1 Torsjonspunkter av små orden

Koordinatene til torsjonspunkter av små orden er relativt enkelt å beregne. La $\mathbf{p} = (\mathbf{x}, \mathbf{y})$ være et torsjonspunkt av orden to. Da er $[2]\mathbf{p} = \mathcal{O}$ og derfor $\mathbf{p} = -\mathbf{p}$. Geometrisk betyr det at det er en vertikal tangentlinje i $\mathbf{p} = (\mathbf{x}, \mathbf{y})$. Her er $\mathbf{y} = 0$ og $\mathbf{x}$ er løsningene til likningen $\mathbf{x}^3 + a\mathbf{x}^2 + b\mathbf{x} + c = 0$. Merk at det er enten null, ett eller tre torsjonspunkter av orden to på kurven avhengig av hvor mange løsninger det er for $\mathbf{x}^3 + a\mathbf{x}^2 + b\mathbf{x} + c = 0$.

Anta at $\mathscr{E}$ er en elliptisk kurve over en kropp R der $\mathrm{char}(R) \neq 2, 3$, og anta at $\mathbf{p}_1$, $\mathbf{p}_2$ og $\mathbf{p}_3$ er torsjonspunkter av orden to på $\mathscr{E}/R$. Da er Da er 2-torsjonspundermengden gitt ved

$$\mathscr{E}(R)[2] = \{\mathcal{O}, \mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3\}.$$

Merk at $\mathcal{O}$ har orden 1 og $\mathbf{p}_i$ orden 2. Det betyr at torsjonsundermengden er isomorf med et produkt av to undermengder av orden to:

$$\mathscr{E}(R)[2] \simeq \mathbb{Z}/2 \times \mathbb{Z}/2.$$

En elliptisk kurve har enten null, et eller tre 2-torsjonspunkter, så en 2-torsjonsundermengde er isomorf med enten den trivielle undermengden $\{\mathcal{O}\}$, den sykliske $\mathbb{Z}/2$ eller den abelske $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Et 3-torsjonspunkt tilfredsstiller $2\mathbf{p} = -\mathbf{p}$, så koordinatene finner vi ved å bruke duplikasjonsformelen

$$\left(\frac{g'(\mathbf{x})}{2\mathbf{y}}\right)^2 - 2\mathbf{x} = \mathbf{x}.$$

En omskriving gir

$$\psi_3 = 3\mathbf{x}^4 + 6b\mathbf{x}^2 + 12c\mathbf{x} - b^2.$$

Dette er et polynom av orden fire, så det er enten null, en, to eller fire løsninger, der hver verdi for $\mathbf{x}$ korresponderer til enten null eller to verdier for $\mathbf{y}$, siden $\mathbf{y} \neq 0$. Hvis $\mathbf{y} = 0$, så er punktet et torsjonspunkt av orden to. Hvis $\mathbf{p}$ er et torsjonspunkt av orden tre, så er dets invers det også. Dermed kan det

være opp til åtte torsjonspunkter av orden tre på en elliptisk kurve. Anta at

$$\mathscr{E}(R)[3] = \big\{\mathcal{O}, (\mathbf{x}_1 : \pm\mathbf{y}_1), (\mathbf{x}_2 : \pm\mathbf{y}_2), (\mathbf{x}_3 : \pm\mathbf{y}_3), (\mathbf{x}_4 : \pm\mathbf{y}_4)\big\}$$

er en 3-torsjonsundermengde. Da er

$$\mathscr{E}(R)[3] \simeq \mathbb{Z}/3 \times \mathbb{Z}/3.$$

Men generelt er en 3-torsjonsundermengde isomorf med enten $\{\mathcal{O}\}$, $\mathbb{Z}/3$ eller $\mathbb{Z}/3 \times \mathbb{Z}/3$.

Eksempel 4.2. La $R = \mathbb{Q}$ og $\mathscr{E}/\mathbb{Q}$ være en elliptisk kurve som er definert ved $\mathbf{y}^2 = \mathbf{x}^3 + \mathbf{x}^2 - 2\mathbf{x}$. Kurven har tre 2-torsjonspunkter til sammen, og vi kan finne dem ved å løse likningen $\mathbf{x}^3 + \mathbf{x}^2 - 2\mathbf{x} = 0$. Åpenbart er $\mathbf{x} = 0$ en løsning, så neste er å løse $\mathbf{x}^2 + \mathbf{x} - 2 = 0$. Her er løsningene $\mathbf{x} = -2$ og $\mathbf{x} = 1$, så 2-torsjonspunktene er $(-2 : 0)$, $(0 : 0)$ og $(1 : 0)$ og

$$\mathscr{E}(\mathbb{Q})[2] \simeq \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Dette er en abelsk gruppe som lett kan sjekkes med de eksplisitte formlene. Det er ingen andre torsjonspunkter. Derfor er $\mathscr{E}(\mathbb{Q})[2] = \mathscr{E}(\mathbb{Q})_{\text{tor}}$ og $\mathscr{E}(\mathbb{Q})_{\text{tor}} \simeq \mathbb{Z}/2 \times \mathbb{Z}/2$.

Den ovenforliggende diskusjonen og det illustrerende eksempelet, har så langt handlet om å bestemme torsjonsgruppen til en gitt elliptisk kurve. Det teoremet som viser hva en torsjonsgruppe er isomorf med, er teoremet av Mazur. Vi kun nevner dette her. Beviset er langt og utenfor avhandlingens rekkevidde å gjennomføre.

Teorem 4.3 (Mazur [11, 12])**.** *La $\mathscr{E}/\mathbb{Q}$ være en elliptisk kurve over de rasjonelle tallene. Da er*

$$\mathscr{E}(\mathbb{Q})_{\text{tor}} \simeq \begin{cases} \mathbb{Z}/n & 1 \leq n \leq 10, \quad n = 12, \quad \text{eller} \\ \mathbb{Z}/n \times \mathbb{Z}/2, & n = 2, 4, 6, 8, \end{cases}$$

og alle tilfeller oppstår.

4.2 Elliptiske kurver over endelige kropper

La $\mathbb{F}_p$ betegne en endelig kropp. Dette er kroppen av heltallene modulo p. Nå er det ikke lenger lett å visualisere kurvene. Men vi kan fortsatt studere løsningene til $F(\mathbf{x}, \mathbf{y}) = 0$ med koeffisienter i $\mathbb{F}_p$. En sånn løsning er et $\mathbb{F}_p$-rasjonalt punkt på $\mathscr{E}$. Siden $\mathbb{F}_p$ er en *endelig* kropp, så er antallet punkter i $\mathscr{E}(\mathbb{F}_p)$ endelig. Dette antallet estimert ved følgende:

Teorem 4.4 (Hasse)**.**

$$|\#\mathscr{E}(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}.$$

Her betegner $\#\mathscr{E}(\mathbb{F}_p)$ antallet punkter i $\mathscr{E}(\mathbb{F}_p)$.

Også kjent som *Hasses begrensning* er Hasses teorem analog med Riemannhypotesen for elliptiske kurver. Resultatet var først formodet av Emil Artin [1] i 1924 og senere bevist av Helmut Hasse [7] i 1936.

4.2.1 Rasjonelle punkter over endelige kropper

Det er relativt enkelt å finne punkter i $\mathscr{E}(\mathbb{F}_p)$. Anta nå at vi vil finne alle de $\mathbb{F}_5$-rasjonelle punktene på den elliptiske kurven $\mathscr{E}$ med likningen $y^2 = \mathbf{x}^3 + \mathbf{x} + 1$. For hver $\mathbf{x}_i \in \mathbb{F}_5$ sjekker vi om $\mathbf{y}_i^2 = \mathbf{x}_i^3 + \mathbf{x}_i + 1$ har løsninger modulo 5 med kvadratisk resiprositet. Hvis en løsning eksisterer, så er $(\mathbf{x}_i, \mathbf{y}_i)$ et punkt på $\mathscr{E}/\mathbb{F}_5$. Det kan vises at løsningsmengden er

$$\mathscr{E}(\mathbb{F}_5) = \big\{\mathcal{O}, (0 : \pm 1), (2 : \pm 1), (3 : \pm 1), (4 : \pm 2)\big\}.$$

Siden $\mathscr{E}(\mathbb{F}_5)$ inneholder ni punkter, så er den enten isomorf med en abelsk gruppe $\mathbb{Z}/9$ eller med et produkt av sykliske grupper $\mathbb{Z}/3 \times \mathbb{Z}/3$. For å bestemme hvilken mulighet som er riktig, sjekker vi om $3\mathbf{p} = \mathcal{O}$ eller ikke for alle $\mathbf{p} \in \mathscr{E}(\mathbb{F}_5)$. For $\mathbf{p} = (0 : 1)$, så er $3\mathbf{p} = (2 : 1)$. Dette viser at $\mathscr{E}(\mathbb{F}_5) \simeq \mathbb{Z}/9$.

Remark 4.5. Siden alle punkter på en elliptisk kurve er en gruppe og det er endelige mange punkter på en elliptisk kurve over en endelig kropp, er gruppen endelig, og hvert punkt i $\mathscr{E}(\mathbb{F}_p)$ er et torsjonspunkt.

4.2.2 Kropputvidelse

Som vi har sett er er det enkleste eksempelet på en endelig kropp $\mathbb{F}_p$. Et mer interessant eksempel er $\mathbb{F}_q$ der $q = p^n$ for noe n. Dette er en kropputvidelse av $\mathbb{F}_p$ som er endelig. Hvis $q = p^n$ så er

$$\mathbb{F}_q \simeq \mathbb{F}_p[\mathbf{t}]/(f(\mathbf{t})),$$

der $f \in \mathbb{F}_p[\mathbf{t}]$ er et irredusibelt polynom av grad n i variabel $\mathbf{t}$, en kropputvidelse av grad n. Hvis $R = \mathbb{F}_q$ så sier vi at R har karakteristikk p. Det betyr at $p\mathbf{x} = 0$ for alle $\mathbf{x} \in R$.

4.2.3 Reduksjoner

Definisjon 4.6. La $\mathbf{y}^2 = \mathbf{x}^3 + b\mathbf{x} + c$ definere en kubisk kurve $\mathscr{C}$. Da er $\mathbf{x}^2 = \mathbf{x}^3 + b'\mathbf{x} + c'$ som definerer $\mathscr{C}'$ definert som *reduksjonen modulo* p av $\mathscr{C}$ hvis $b \equiv b' \pmod{p}$ og $c \equiv c' \pmod{p}$. Vi betegner reduksjoner med $\mathscr{E}_{/p}$.

Merk at en reduksjon av en elliptisk kurve ikke nødvendigvis er elliptisk. For eksempel er reduksjonen til den elliptisk kurven gitt ved $\mathbf{y}^2 = \mathbf{x}^3 + 47$ en kurve på formen $\mathbf{y}^2 = \mathbf{x}^3$, som ikke er elliptisk fordi $\Delta = 0$.

Definisjon 4.7. En elliptisk kurve $\mathscr{E}$ har enten en *god reduksjon* hvis $\Delta(\mathscr{E}') \neq 0$ eller en *dårlig reduksjon* hvis $\Delta(\mathscr{E}') = 0$

Teorem 4.8. *La $\mathscr{E}$ være en elliptisk kurve over $\mathbb{Z}$, og p et primtall. Da har $\mathscr{E}/\mathbb{Z}$ en dårlig reduksjon ved p hvis og bare hvis p deler $\Delta(\mathscr{E})$.*

Bevis. Først viser vi høyre implikasjon. Husk at

$$p \mid \Delta(\mathscr{E}) \iff \Delta(\mathscr{E}) \equiv 0 \pmod{p}.$$

La $\mathscr{E}$ være en elliptisk kurve med diskriminant $\Delta(\mathscr{E})$, og la $\rho(\Delta) = p_1 p_2 \cdots$ være primtallfaktoriseringen til $\Delta(\mathscr{E})$. Hvis vi reduserer $\mathscr{E}$ modulo p og p er et primtall i $\rho(\Delta)$, så vil $p \mid \Delta(\mathscr{E}) \iff \Delta(\mathscr{E}) \equiv 0 \pmod{p} \iff \Delta(\mathscr{E}) = 0$.

Venstre implikasjon er nå opplagt. Hvis $\mathscr{E}$ har en dårlig reduksjon, så er $\Delta(\mathscr{E}) = 0$. Dette er samme som at $\Delta(\mathscr{E}) \equiv 0 \pmod{p} \iff p \mid \Delta(\mathscr{E})$. $\square$

Remark 4.9. Hvis en elliptisk kurve har en dårlig reduksjon, så gjelder dette et endelig antall p, nemlig de som deler Δ. Sagt på en annen måte, en elliptisk kurve har dårlig reduksjon kun ved alle p som deler Δ.

4.2.4 Supersingulære kurver

Definisjon 4.10. La $\mathscr{E}$ være en elliptisk kurve over den endelige kroppen $\mathbb{F}_p$ av karakteristikk p og la $\mathscr{E}(\mathbb{F}_p)[p] \subset \mathscr{E}(\mathbb{F}_p)$ være en undermengde av p-torsjonspunkter på $\mathscr{E}/\mathbb{F}_p$. Da er

$$\mathscr{E}(\mathbb{F}_p)[p] \simeq \begin{cases} \mathcal{O} & \text{eller} \\ \mathbb{Z}/p \end{cases}$$

og p kalles for et *supersingulært primtall*. I det første tilfellet kalles $\mathscr{E}$ for *supersingulær*, og det andre for *ordinær*.

Eksempel 4.11. La $\mathscr{E}$ være en elliptisk kurve som er definert ved

$$\mathbf{y}^2 = \mathbf{x}^3 + \mathbf{x}^2 - 2\mathbf{x}.$$

Over den endelige kroppen $\mathbb{F}_{23}$ er $\mathscr{E}$ definert ved $\mathbf{y}^2 = \mathbf{x}^3 + \mathbf{x}^2 + 21\mathbf{x}$. Den har tjuefire $\mathbb{F}_{23}$-rasjonelle punkter, så $\#\mathscr{E}(\mathbb{F}_{23}) = 24$ og $\mathscr{E}(\mathbb{F}_{23}) \simeq \mathbb{Z}/12 \times \mathbb{Z}/2$. Det eneste punktet som er 23-torsjon det trivielle torsjonspunktet $\mathcal{O}$. Så $\mathscr{E}(\mathbb{F}_{23})[23] \simeq \mathcal{O}$. Dette betyr følgelig at $\mathscr{E}$ er supersingulær elliptisk kurve over $\mathbb{F}_{23}$.

Eksempel 4.12. La $\mathscr{E}/R$ være en elliptisk kurve på formen

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 - \mathbf{x}.$$

Merk at likningen er på utvidet Weierstrassform, så karakteristikken til R kan være 2. Faktisk er $p = 2$ et supersingulært primtall for denne kurven. Reduksjonen, som vi betegner med $\mathscr{E}_{/2}$, har tre rasjonelle punkter i den endelige kroppen $\mathbb{F}_2$. Punktene der er 3-torsjon. Siden $\mathcal{O}$ er det eneste punktet som er 2-torsjon, $\mathscr{E}(\mathbb{F}_2)[2] \simeq \{\mathcal{O}\}$, så er reduksjonen, $\xi_{/2}$, en supersingulær elliptisk kurve.

4.3 Avbildninger mellom elliptiske kurver

Nå som vi har sett på gruppestrukturen til $\mathscr{E}(R)$, er det naturlig å se etter avbildninger mellom elliptiske kurver. Vi har allerede sett noen eksempler, nemlig $[N]$-isogenien (multiplikasjon av punkter, torsjonspunkter) og representasjonen av likninger over $\mathbb{F}_p$.

4.3.1 Isogenier

Definisjon 4.13. En *isogeni* av elliptiske kurver som er definert over R er en morfisme $f : \mathscr{E} \to \mathscr{E}'$ slik at $f(\mathbf{p}+\mathbf{q}) = f(\mathbf{p}) +' f(\mathbf{q})$ for alle $\mathbf{p}, \mathbf{q} \in \mathscr{E}(R)$. Hvis det fins en isogeni som er ulik null mellom $\mathscr{E}$ og $\mathscr{E}'$ sier vi at $\mathscr{E}$ og $\mathscr{E}'$ er *isogene* kurver over R.

Merk at hvis $\mathscr{E}$ og $\mathscr{E}'$ er to elliptiske kurver og $f : \mathscr{E} \to \mathscr{E}'$ er en isogeni, følger det fra definisjonen at $f(\mathcal{O}) = \mathcal{O}'$.

Definisjon 4.14. En mengde av isogenier f mellom elliptiske kurver $\mathscr{E}$ og $\mathscr{E}'$ som er definert over R er betegnet med

$$\mathrm{Hom}_R(\mathscr{E}) \coloneqq \big\{ f : \mathscr{E} \to \mathscr{E}' \mid f \text{ er en isogeni over } R \big\}.$$

Hvis $\mathscr{E} = \mathscr{E}'$ over R så er isogenien f en endomorfisme over R. Vi betegner dette med

$$\mathrm{End}_R(\mathscr{E}) \coloneqq \big\{ f \mid f \text{ er en endomorfisme} \big\}.$$

Mengden av invertible elementer i $\mathrm{End}_R(\mathscr{E})$ er betegnet med $\mathrm{Aut}_R(\mathscr{E})$.

Eksempel 4.15. Det første og enkleste eksempelet på en isogeni kommer fra multiplikasjonen av et heltall. La $\mathscr{E}$ være en elliptisk kurve over R og $N \in \mathbb{Z}$ et heltall. Da er $[N] : \mathscr{E} \to \mathscr{E}$ en isogeni slik at for alle $\mathbf{p} \in \mathscr{E}(R)$

$$[N](\mathbf{p}) = \mathbf{p} + \mathbf{p} + \cdots + \mathbf{p} \quad N > 0.$$

Hvis $N < 0$ så er

$$[N](\mathbf{p}) = (-\mathbf{p}) + (-\mathbf{p}) + \cdots + (-\mathbf{p}).$$

Og hvis $N = 0$ så er

$$[N](\mathbf{p}) = \mathcal{O}.$$

Merk at hvis $[N](\mathbf{p}) = \mathcal{O}$ for noe $N > 0$, så er $\mathbf{p} \in \mathscr{E}(R)$ et torsjonspunkt av orden N.

4.3.2 Isomorfier

Definisjon 4.16. To elliptiske kurver $\mathscr{E}$ og $\mathscr{E}'$ som er definert over R sier vi er *isomorfe* hvis det fins en isogeni $\phi : \mathscr{E} \to \mathscr{E}'$ som er bijektiv. Hvis $\mathscr{E}$ og $\mathscr{E}'$ er definert på Weierstrassform, så er isomorfien $\phi : \mathscr{E} \to \mathscr{E}$ en Weierstrassisomorfi.

Definisjon 4.17 (LMFDB [10])**.** La $\mathscr{E}$ og $\mathscr{E}'$ være elliptisk kurver over R som er definert på Weierstrassform

$$\begin{aligned}\mathbf{y}^2 + a_1\mathbf{xy} + a_3\mathbf{y} &= \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6,\\ \mathbf{y}^2 + a_1'\mathbf{xy} + a_3'\mathbf{y} &= \mathbf{x}^3 + a_2'\mathbf{x}^2 + a_4'\mathbf{x} + a_6',\end{aligned}$$

og la R^* være en restkropp. Da er $\mathscr{E} \simeq \mathscr{E}'$ over R hvis det fins $u \in R^*$ og $r, s, t \in R$ slik at

$$\begin{aligned}ua_1' &= a_1 + 2s,\\ u^2a_2' &= a_2 - sa_1 + 3r - s^2,\\ u^3a_3' &= a_3 + ra_1 + 2t,\\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,\\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1.\end{aligned}$$

For isomorfe elliptiske kurver er diskriminantene $\Delta(\mathscr{E})$ og $\Delta(\mathscr{E}')$ relaterte ved $u^{12}\Delta(\mathscr{E}') = \Delta(\mathscr{E})$. Og $\phi(\mathcal{O}) = \mathcal{O}'$.

Husk at en elliptisk kurve som er definert ved utvidet Weierstrassform $\mathscr{E}$ kan (nesten) alltid skrives på kort Weierstrassform $\mathscr{E}_W$, se kapittel 3. Hvis det fins en substitusjon mellom $\mathscr{E}$ og $\mathscr{E}_W$, så er dette det samme som at $\mathscr{E}$ er isomorf med $\mathscr{E}_W$.

Proposisjon 4.18. *Anta at* $\mathrm{char}(R) \neq 2, 3$ *og la* $\mathscr{E}$ *være en elliptisk kurve over* R *som er gitt på kort Weierstrassform. Da er den eneste substitusjonen som ivaretar formen gitt ved*

$$\mathbf{x}' = u^2\mathbf{x} \quad \text{og} \quad \mathbf{y}' = u^3\mathbf{y},$$

for noe $u \in R^*$.

Bevis. La $u \in R^*$. Med substitusjonene får vi

$$\begin{aligned}(u^3\mathbf{y})^2 &= (u^2\mathbf{x})^3 + b(u^2\mathbf{x}) + c \\ \mathbf{y}^2 &= \mathbf{x}^3 + b'\mathbf{x} + c', \quad b' = \frac{b}{u^4}, \quad c' = \frac{c}{u^6}.\end{aligned}$$

Fra dette ser vi at $u^{12}\Delta(\mathscr{E}) = \Delta(\mathscr{E})$. □

Merk at $b' = b/u^4$ og $c' = c/u^6$ tilfredsstiller formene gitt i definisjonen. Strengt tatt er $b' \neq a_4'$ og $c' \neq a_6'$, siden $b', c' \in R$ der $\mathrm{char}(R) \neq 2, 3$ og $a_4', a_6' \in R$ der $\mathrm{char}(R) \geq 2$. Men siden substitusjonen mellom elliptiske kurver på kort Weierstrassform ikke involverer r, s, t (de kan settes til *null*), ser vi at $b' = b/u^4$ og $c' = c/u^6$ er gyldige substitusjoner.

Proposisjon 4.19. *De to elliptiske kurvene* $\mathscr{E}$ *og* $\mathscr{E}'$ *definert over* R *med* $\phi(\mathcal{O}) = \mathcal{O}'$ *er isomorfe med substitusjonen*

$$\mathbf{x}' = u^2\mathbf{x} + r \quad \text{og} \quad \mathbf{y}' = u^3\mathbf{y} + u^2 s\mathbf{x} + t,$$

for noe $r, s, t \in R$ *og* $u \in R^*$.

Bevis. Beviset er ganske likt det andre. Resultatet her er at uttrykkene for a_i' tilsvarer de som er gitt i definisjonen. □

Proposisjon 4.20. *To elliptiske kurver* $\mathscr{E}$ *og* $\mathscr{E}'$ *som er isomorfe over* $R = \mathbb{Q}$ *har samme* j*-invariant. Med andre ord,*

$$\mathscr{E} \simeq \mathscr{E}' \implies j(\mathscr{E}) = j(\mathscr{E}').$$

Remark 4.21. Implikasjonen i proposisjonen går begge veier hvis $R = \mathbb{C}$.

Bevis på Proposisjon 4.20. Å vise at isomorfe elliptiske kurver har lik j-invariant over $R \subset \mathbb{C}$, er ganske enkelt. Anta at $\mathscr{E} \simeq \mathscr{E}'$. I dette beviset lar vi $\mathscr{E}$ og $\mathscr{E}'$ være på utvidet Weierstrassform. Det er for å gi et sterkere bevis. j-invarianten til $\mathscr{E}'$ er

$$j(\mathscr{E}') = \frac{1728(b_2'^2 - 24b_4')^3}{\Delta(\mathscr{E}')}, \quad b_2' = a_1'^2 + 4a_2', \quad b_4' = 2a_4' + a_1'a_3'.$$

Målet er å skrive om på $b_2'^2$ og b_4' med definisjonen. Siden $\mathscr{E} \simeq \mathscr{E}'$, får vi

$$\begin{aligned} b_2'^2 &= \frac{a_1^4 + 8a_1^2a_2 + 24ra_1^2 + 16a_2^2 + 96ra_2 + 144r^2}{u^4} \\ b_4' &= \frac{2a_4 + 4ra_2 + 6r^2 + a_1a_3 + ra_1^2}{u^4}, \quad u \in k, \quad r, s \in R, \end{aligned}$$

og derfor er

$$\begin{aligned} b_2'^2 - 24b_4' &= \frac{a_1^4 + 8a_1^2a_2 + 16a_2^2 - 48a_4 - 24a_1a_3}{u^4} \\ &= \frac{(a_1^2 + 4a_2)^2}{u^4} - 24\frac{2a_4 + a_1a_3}{u^4}. \end{aligned}$$

Merk nå at $a_1^2 + 4a_2 \coloneqq b_2$ og $2a_4 + a_1a_3 \coloneqq b_4$ fra kapittel 3, så

$$b_2'^2 - 24b_4' = \frac{b_2^2 - 24b_4}{u^4}.$$

Når vi setter dette inn i telleren og bruker $\Delta(\mathscr{E}') = \Delta(\mathscr{E})/u^{12}$, så har vi

$$j(\mathscr{E}') = \frac{(b_2^2/u^4 - 24b_4/u^4)^3}{\Delta(\mathscr{E})/u^{12}} = \frac{(b_2^2 - 24b_4)^3/u^{12}}{\Delta(\mathscr{E})/u^{12}} = j(\mathscr{E}),$$

som beviser proposisjonen. □

Eksempel 4.22. For å illustrere er den elliptiske kurven $\mathscr{E}$ som er gitt ved $\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3$ isomorf med den elliptiske kurven $\mathscr{E}_W$ gitt ved $\mathbf{y}^2 = \mathbf{x}^3 + 16$ via substitusjonen

$$\mathbf{x} = 4\mathbf{x}_W \quad \text{og} \quad \mathbf{y} = 8\mathbf{y}_W - 4.$$

Her er $u = 1/2$ og $t = 1/2$.

4.3.3 Frobeniusmorfismen

Hvis vi ønsker å avbilde elementer i en endelig kropp $\mathbb{F}_p$ til dets p-te potens, bruker vi Frobeniusmorfismen $\pi : \mathbb{F}_p \to \mathbb{F}_p$.

Forbeniusmorfismen er en multiplikativ morfisme: $\pi(\mathbf{xy}) = (x\mathbf{y})^p = \mathbf{x}^p\mathbf{y}^p = \pi(\mathbf{x})\pi(\mathbf{y})$ for alle $\mathbf{x}, \mathbf{y} \in \mathbb{F}_p$. Den er også additiv: $\pi(\mathbf{x} + \mathbf{y}) = (\mathbf{x} + \mathbf{y})^p = \mathbf{x}^p + \mathbf{y}^p = \pi(\mathbf{x}) + \pi(\mathbf{y})$. For å vise at Frobeniusmorfismen er additiv, bruker vi en utvidelse av binomialteoremet:

$$\begin{aligned}(\mathbf{x} + \mathbf{y})^p &= \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} x^{p-k}\mathbf{y}^k \\ &= \mathbf{x}^p + p\mathbf{x}^{p-1}\mathbf{y} + \frac{p(p-1)}{2}\mathbf{x}^{p-2}\mathbf{y}^2 + \cdots + \mathbf{y}^p.\end{aligned}$$

Siden $p \equiv 0 \pmod{p}$ vil alle ledd untatt $\mathbf{x}^p$ og $\mathbf{y}^p$ forsvinne.

Kapittel 5

Elliptiske kurver og q-differensialoperatorer

Kapittel 2 viste at det fins en forbindelse mellom par av kommuterende differensialoperatorer og algebraiske kurver. Vi så at to q-differensialoperatorer av orden en og to som kommuterer, ga en parabel som er definert over R. Målet i dette kapitlet er å rekonstruere et eksempel i [9], som handler om operatorer av orden to og tre som gir elliptiske kurver.

5.1 q-differensialoperatorer og eigenproblemer

5.1.1 q-differensialoperatorer

Først går vi gjennom nyttige fakta, som vil hjelpe oss når vi gjennomgår eksempelet. Husk at q-derivasjonen på en funksjonsring $\mathfrak{R}$, er gitt som

$$\partial(f) \coloneqq \partial_q(f) = \frac{f(q\mathbf{t}) - f(t)}{(q-1)\mathbf{t}}, \quad f \in \mathfrak{R}.$$

Vi antar at $f \in \mathfrak{R}$ er uendelig deriverbar på $\mathfrak{R}$.

Lemma 5.1. *La P og Q være to q-differensialoperatorer på formen*

$$P = \mathbf{t}^n\partial^n - \alpha \quad \text{og} \quad Q = \mathbf{t}^m\partial^m - \beta, \quad \alpha, \beta \in R. \tag{5.1}$$

Da kommuterer P og Q for alle n og $m = 1, 2, 3$.

Bevis. Vi skriver ut derivasjonene eksplisitt. Deretter sjekker vi for n og m om operatorene kommuterer. Det er tilstrekkelig å sjekke at likningen $PQ = QP$ holder for n og $m = 1, 2, 3$. Først har vi

$$\begin{aligned} PQ &= (\mathbf{t}^n\partial^n - \alpha)(\mathbf{t}^m\partial^m - \beta) \\ &= \mathbf{t}^n\partial^n(\mathbf{t}^m\partial^m) - \mathbf{t}^n\partial^n(\beta) - \alpha\mathbf{t}^m\partial^m + \alpha\beta \\ &= \mathbf{t}^n\partial^n(\mathbf{t}^m\partial^m) - \beta\mathbf{t}^n\partial^n - \alpha\mathbf{t}^m\partial^m + \alpha\beta, \end{aligned}$$

og, for QP,

$$QP = \mathbf{t}^m\partial^m(\mathbf{t}^n\partial^n) - \alpha\mathbf{t}^m\partial^m - \beta\mathbf{t}^n\partial^n + \alpha\beta.$$

Nå kan vi sammenlikne PQ og QP og teste for hvilke n og m de er like. Åpenbart er $PQ = QP$ når $n = m$, så vi sjekker når $n \neq m$. Det er også tydelig at for alle n og m, er

$$-\beta\mathbf{t}^n\partial^n - \alpha\mathbf{t}^m\partial^m + \alpha\beta = -\alpha\mathbf{t}^m\partial^m - \beta\mathbf{t}^n\partial^n + \alpha\beta,$$

så vi trenger kun å sjekke $\mathbf{t}^n\partial^n(\mathbf{t}^m\partial^m) = \mathbf{t}^m\partial^m(\mathbf{t}^n\partial^n)$ for $n, m = 1, 2, 3$. Det er i alt tre tilfeller: $n = 1$ og $m = 2, 3$ og $n = 2$ og $m = 3$. Når $n = 1$ og $m = 2$, får vi

$$\begin{aligned} \mathbf{t}\partial(\mathbf{t}^2\partial^2) &= \mathbf{t}(\{2\}_q\mathbf{t}\partial^2 + q^2\mathbf{t}^2\partial^3) \\ &= \mathbf{t}^2\partial^2 + q\mathbf{t}^2\partial^2 + q^2\mathbf{t}^3\partial^3 \end{aligned}$$

og

$$\begin{aligned} \mathbf{t}^2\partial^2(\mathbf{t}\partial) &= \mathbf{t}^2\partial(\partial + q\mathbf{t}\partial^2) \\ &= \mathbf{t}^2(\partial^2 + q\partial^2 + q^2\mathbf{t}\partial^3) \\ &= \mathbf{t}^2\partial^2 + q\mathbf{t}^2\partial^2 + q^2\mathbf{t}^3\partial^3 \end{aligned}$$

Her er $PQ = QP$ når $n = 1$ og $m = 2$. Når $n = 1$ og $m = 3$, får vi

$$\begin{aligned} \mathbf{t}\partial(\mathbf{t}^3\partial^3) &= \mathbf{t}(\{3\}_q\mathbf{t}^2\partial^3 + q^3\mathbf{t}^3\partial^4) \\ &= \mathbf{t}^3\partial^3 + q\mathbf{t}^3\partial^3 + q^2\mathbf{t}^3\partial^3 + q^3\mathbf{t}^4\partial^4 \end{aligned}$$

og

$$\begin{aligned}\mathbf{t}^3\partial^3(\mathbf{t}\partial) &= \mathbf{t}^3\partial^2(\partial + q\mathbf{t}\partial^2)\\ &= \mathbf{t}^3\partial(\partial^2 + q\partial^2 + q^2\mathbf{t}\partial^3)\\ &= \mathbf{t}^3(\partial^3 + q\partial^3 + q^2\partial^3 + q^3\mathbf{t}\partial^4)\\ &= \mathbf{t}^3\partial^3 + q\mathbf{t}^3\partial^3 + q^2\mathbf{t}^3\partial^3 + q^3\mathbf{t}^4\partial^4,\end{aligned}$$

som er det samme. Til slutt når $n = 2$ og $m = 3$, får vi

$$\begin{aligned}\mathbf{t}^2\partial^2(\mathbf{t}^3\partial^3) &= \mathbf{t}^2\partial(\{3\}_q\mathbf{t}^2\partial^3 + q^3\mathbf{t}^3\partial^4)\\ &= \mathbf{t}^2(\{3\}_q\{2\}_q\mathbf{t}\partial^3 + \{3\}_q q^2\mathbf{t}^2\partial^4 + \{3\}_q q^3\mathbf{t}^2\partial^4 + q^6\mathbf{t}^3\partial^5)\\ &= \{3\}_q\{2\}_q\mathbf{t}^3\partial^3 + \{3\}_q\{2\}_q q^2\mathbf{t}^4\partial^4 + q^6\mathbf{t}^5\partial^5\end{aligned}$$

og

$$\begin{aligned}\mathbf{t}^3\partial^3(\mathbf{t}^2\partial^2) &= \mathbf{t}^3\partial^2(\{2\}_q\mathbf{t}\partial^2 + q^2\mathbf{t}^2\partial^3)\\ &= \mathbf{t}^3\partial(\{2\}_q\partial^2 + \{2\}_q q\mathbf{t}\partial^3 + \{2\}_q q^2\mathbf{t}\partial^3 + q^4\mathbf{t}^2\partial^4)\\ &= \mathbf{t}^3(\{2\}_q\partial^3 + \{2\}_q q\partial^3 + \{2\}_q q^2\mathbf{t}\partial^4 + \{2\}_q q^2\partial^3 + \{2\}_q q^3\mathbf{t}\partial^4\\ &\quad + \{2\}_q q^4\mathbf{t}\partial^4 + q^6\mathbf{t}^2\partial^5)\\ &= \{3\}_q\{2\}_q\mathbf{t}^3\partial^3 + \{3\}_q\{2\}_q q^2\mathbf{t}^4\partial^4 + q^6\mathbf{t}^5\partial^5,\end{aligned}$$

som er det samme. Dermed er $PQ = QP$. □

Remark 5.2. Lemma 5.1 kan bevises i det generelle for alle n og $m \geq 1$. Som vi ser er det å bevise dette eksplisitt ganske krevende for store n og m. Antakelig er et generelt bevis best gjennomførbart med andre matematiske verktøy, men vi skal kun se på operatorer av orden to og tre primært, så vi utelar bevis på dette.

5.1.2 Eigenproblemer, notat

Merk at likningen $P_{\mathbf{x}}\phi = 0$ er det samme som å si at ϕ er en eigenvektor til P en q-differensialoperator med eigenverdi $\mathbf{x}$. I denne delseksjonen diskuterer vi følgende teorem:

Teorem 5.3. *La P og Q være to q-differensialoperatorer som kommuterer. Da fins det en eigenvektor $\phi \in \mathfrak{R}$ slik at*

$$P\phi = a\phi \quad \text{og} \quad Q\phi = b\phi,$$

der a og b er eigenverdier fra ξ, hvis og bare hvis $\xi(a, b) = 0$. Hvis k er en algebraisk lukket ring der $k \coloneqq \ker(\partial : \mathfrak{R} \to \mathfrak{R})$, så er kurven ξ definert over underringen $\mathfrak{o} \subset k$ av trancendensgrad null over R. Dessuten inneholder ringen $\mathfrak{o}$ tallet q og dets invers.

Bevis. Se [9]. □

I denne avhanglingen om elliptiske kurver, er en kropp algebraisk lukket hvis hvert polynom i variabel $\mathbf{t}$ i $R[\mathbf{t}]$ har en løsning i R. Det kan være intuitivt å tenke at de reelle tallene er algebraisk lukket, men det er de ikke, fordi likningen $\mathbf{x}^2 + 1 = 0$ har ingen reelle løsninger. Det samme kan sies om underkropper av de reelle tallene; ingen av dem er algebraisk lukket. Heller ingen endelige kropper er algebraisk lukket. For eksempel hvis a_i er elementer i en endelig kropp, da har ikke polynomet $(\mathbf{x}-a_1)(\mathbf{x}-a_2)\cdots(\mathbf{x}-a_i)$ en løsning i kroppen. Men unionen av alle endelige kropper av en gitt p et primtall er en algebraisk lukket kropp. Denne kalles for den algebraiske tillukkingen av kroppen $\mathbb{F}_p$.

I kontekst av algebraisk lukkede kropper, fins det en såkalt *syklotomisk utvidelse*. Hvis R er en algebraisk lukket kropp, da inneholder R alle n-te enhetsrøtter som er løsningene til polynomet $\mathbf{x}^n - 1$. En syklotomisk utvidelse er da en kropputvidelse som er inneholdt i en utvidelse generert av enhetsrøttene. En utvidelse av en kropp generert av enhetsrøtter kalles for dens syklotomiske tillukning. Så algebraiske lukkede kropper er syklotomisk lukket. Merk, fra kapittel 2, at $\{n\}_{\zeta_N}$ er et syklotomisk heltall.

På en annen side, at $R \subseteq \mathfrak{o}$ er av transcendens null betyr at koeffisientene til en kurves likning involverer ikke variabelen $\mathbf{t}$. Sagt med andre ord: kurven *kan* være definert ved en likning som ikke involverer $\mathbf{t}$. (Vi skal se dette i praksis i neste delseksjon). Det som vil skje er at hvert ledd i likningen vil ha en $\mathbf{t}$ med samme potens, så den kan fjernes.

5.2 Hovedeksempelet

5.2.1 Konstruksjon

Vi reproduserer nå eksempelet fra [9], som handler om kommuterende q-differensialoperatorer av orden to og tre. La $\partial(f) = (f(q\mathbf{t}) - f(\mathbf{t}))/((q-1)\mathbf{t})$ være den q-deriverte av f. Anta at

$$P = \mathbf{t}\partial(\mathbf{t}\partial - \alpha) \quad \text{og} \quad Q = (\mathbf{t}\partial)^3.$$

Først og fremst ser vi at P og Q kommuterer. Det neste er å beregne resultanten, $\mathrm{Res}(P_{\mathbf{x}}, Q_{\mathbf{y}})$, der $P_{\mathbf{x}}$ og $Q_{\mathbf{y}}$ er på formen

$$P_{\mathbf{x}} = \mathbf{t}\partial(\mathbf{t}\partial - \alpha) - \mathbf{x} \quad \text{og} \quad Q_{\mathbf{y}} = (\mathbf{t}\partial)^3 - \mathbf{y}.$$

Vi beregner resultanten på den klassiske måten. Sylvestermatrisen av $P_{\mathbf{x}}$ og $Q_{\mathbf{y}}$ er en 5×5-matrise der den i-te raden inneholder koeffisientene til $\partial^i(P_{\mathbf{x}})$ for $0 \le i \le 2$ og $\partial^i(Q_{\mathbf{y}})$ for $0 \le i \le 1$. Koeffisientene finner vi fra

$$\begin{aligned}
P_{\mathbf{x}} &= (1-\alpha)\mathbf{t}\partial + q\mathbf{t}^2\partial^2 - \mathbf{x} \\
\partial(P_{\mathbf{x}}) &= (1-\alpha-\mathbf{x})\partial + (2-\alpha+q)q\mathbf{t}\partial^2 + q^3\mathbf{t}^2\partial^3 \\
\partial^2(P_{\mathbf{x}}) &= (\{2\}_q^2 - \{2\}_q\alpha - \mathbf{x})\partial^2 + (\{2\}_q^2 + 1 - \alpha)q^2\mathbf{t}\partial^3 + q^5\mathbf{t}^2\partial^4 \\
Q_{\mathbf{y}} &= \mathbf{t}\partial + q(2+q)\mathbf{t}^2\partial^2 + q^3\mathbf{t}^3\partial^3 - \mathbf{y} \\
\partial(Q_{\mathbf{y}}) &= (1-\mathbf{y})\partial + (\{2\}_q^2 + \{2\}_q + 1)q\mathbf{t}\partial^2 + (\{3\}_q + \{2\}_q + 1)q^3\mathbf{t}^2\partial^3 \\
&\quad + q^6\mathbf{t}^3\partial^4
\end{aligned}$$

Vi finner resultanten ved å beregne følgende determinant,

$$\begin{vmatrix}
-\mathbf{x} & (1-\alpha)\mathbf{t} & q\mathbf{t}^2 & 0 & 0 \\
0 & 1-\alpha-\mathbf{x} & (2-\alpha+q)q\mathbf{t} & q^3\mathbf{t}^2 & 0 \\
0 & 0 & \{2\}_q^2 - \{2\}_q\alpha - \mathbf{x} & (\{2\}_q^2 + 1 - \alpha)q^2\mathbf{t} & q^5\mathbf{t}^2 \\
-\mathbf{y} & \mathbf{t} & (2q+q^2)\mathbf{t}^2 & q^3\mathbf{t}^3 & 0 \\
0 & 1-\mathbf{y} & (\{2\}_q^2 + \{2\}_q + 1)q\mathbf{t} & (\{3\}_q + \{2\}_q + 1)q^3\mathbf{t}^2 & q^6\mathbf{t}^3
\end{vmatrix}.$$

Den gir

$$\begin{aligned}\mathrm{Res}(\mathbf{x},\mathbf{y}) = \mathbf{y}^2 - \mathbf{y} - \mathbf{x}^3 + (\{2\}_q^2 - \{2\}_q\alpha + 1 - \alpha)\mathbf{x}^2 \\ - (1-\alpha)(\{2\}_q^2 - \{2\}_q\alpha)\mathbf{x} = 0.\end{aligned}$$

Merk det faktum at alle potensene av $\mathbf{t}$ (og q) i alle ledd er den samme, så $\mathbf{t}$ kan fjernes fra hele uttrykket. Uttrykket er ekvivalent med

$$\xi(\mathbf{x},\mathbf{y}): \quad \mathbf{y}^2 + \omega_1\mathbf{y} = \omega_2\mathbf{x}^3 + \omega_3\mathbf{x}^2 + \omega_4\mathbf{x}.$$

Koeffisientene er etter en liten omskriving, gitt ved

$$\begin{aligned}\omega_1 &= -1,\\ \omega_2 &= 1,\\ \omega_3 &= \alpha(2+q) - (2+q)q - 2,\\ \omega_4 &= (1-\alpha)(1+q)(1+q-\alpha), \quad \omega_i \in R.\end{aligned}$$

At koeffisientene er fra R er fordi α og q er fra R.

Vi ser at at $\xi(\mathbf{x},\mathbf{y})$ er en kubisk kurve over R på utvidet Weierstrassform. Den mangler konstantleddet og $\mathbf{xy}$-leddet, men oppfyller å være likningen til en kubisk kurve. Generelt definerer den en elliptisk kurve hvis diskriminanten er ulik null.

5.2.2 Diskriminanten

Diskriminanten til en kubisk kurve forteller oss om den har et singulært punkt eller ikke. Et singulært punkt er i denne konteksten et punkt der tangenten er ikke veldefinert. Som vi så i kapittel 3 er et punkt $\mathbf{p}$ singulært hvis alle de partiellderiverte av kurvefunksjonen i $\mathbf{p}$ er null. Da er diskriminanten *lik* null. Hvis diskriminanten er *ulik* null, så er kurven elliptisk.

Proposisjon 5.4. *Diskriminanten til $\xi(\mathbf{x},\mathbf{y})$ er gitt ved*

$$\Delta(\xi) \coloneqq -16\omega_3^2(\omega_3 - \omega_4^2) - 64\omega_4^3 + 72\omega_3\omega_4 - 27,$$

$\omega_i \in R$.

Bevis. Husk fra kapittel 3 at hvis en kubisk kurve er på utvidet Weierstrass-form, så er diskriminanten gitt ved

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b6^2 + 9b_2 b_4 b_6.$$

Koeffisientene gitt ved

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1 a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2. \end{aligned}$$

Merk at a_i er koeffisientene i utvidet Weierstrassform. En enkel sammenlikning med $\xi(\mathbf{x}, \mathbf{y})$ gir

$$\begin{aligned} \Delta(\xi) &= -(4\omega_3)^2(\omega_3\omega_1^2 - \omega_4^2) - 8(2\omega_4)^3 + 72\omega_1^2\omega_3\omega_4 - 27\omega_1^4 \\ &= -16\omega_3^2(\omega_3 - \omega_4^2) - 64\omega_4^3 + 72\omega_3\omega_4 - 27 \end{aligned}$$

Beviset er fullført. □

Som nevnt er diskriminanten til en elliptisk kurve ulik null. Men vi merker oss følgende:

Remark 5.5. Uttrykket for $\Delta(\xi)$ er avhengig av parametrene q og $\alpha \in R$. Så ξ er en singulær kurve hvis $\Delta(\xi)(q, \alpha) = 0$. Hvis en fikserer q, så er likningen til $\Delta(\xi)(\alpha)$ et polynom i variabel α av orden seks. Derfor, hvis en fikserer q, er det på det meste seks kurver som ikke er elliptisk.

Kapittel 6

Eksempler og observasjoner

Det er ett hovedtema i dette kapitlet. Som det står i kapitlets tittel, handler det altså om å konstruere eksempler på den kubiske kurven $\xi(\mathbf{x}, \mathbf{y})$ og observere dens egenskaper. Den etablerte teorien fra de forrige kapitlene blir både implisitt og eksplisitt brukt for å støtte den diskusjonen vi gjør rundt observasjonene.

I forrige kapittel beregnet vi determinanten til en matrise som besto av koeffisientene til $\partial^i P_{\mathbf{x}} = \partial^i(\mathbf{t}\partial(\mathbf{t}\partial - \alpha) - \mathbf{x})$ og $\partial^i Q_{\mathbf{y}} = \partial^i((\mathbf{t}\partial)^3 - \mathbf{y})$, og konstruerte en kubisk kurve på formen

$$\xi(\mathbf{x}, \mathbf{y}): \quad \mathbf{y}^2 + \omega_1 \mathbf{y} = \omega_2 \mathbf{x}^3 + \omega_3 \mathbf{x}^2 + \omega_4 \mathbf{x}, \tag{6.1}$$

der koeffisientene er gitt ved

$$\begin{aligned}
\omega_1 &= -1, \\
\omega_2 &= 1, \\
\omega_3 &= (2+q)(\alpha - q) - 2, \\
\omega_4 &= (1-\alpha)(1+q)(1+q-\alpha), \quad \omega_i \in R.
\end{aligned}$$

Denne kurven er elliptisk hvis diskriminanten som er gitt ved

$$\Delta(\xi) \coloneqq -16\omega_3^2(\omega_3 - \omega_4^2) - 64\omega_4^3 + 72\omega_3\omega_4 - 27,$$

er ulik null.

6.1 Valg av koeffisienter

Siden koeffisientene til likningen $\xi(\mathbf{x}, \mathbf{y})$ er kompliserte og nær umenneskelig å jobbe med, er det naturlig å velge verdier for α og q som forenkler dem. Det er fire naturlige valg:

$$\alpha = 0, \quad \alpha = 1, \quad \alpha = q, \quad \alpha = 1 + q.$$

Her er q enten -1 eller 1. Men i noen eksempler tillater vi q å være en fri parameter $q \in \mathbb{Z}$. Det er for å konstruere flere elliptiske kurve som vi vil undersøke. Neste seksjonen lar vi $q = \zeta_N$. Mer om dette senere.

De fire valgene for α gir oss fire likninger for den kubiske kurven:

$$\begin{aligned}
\alpha = 0 : &\qquad \mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - (q^2 + 2q + 2)\mathbf{x}^2 + (1 + q)^2\mathbf{x}; \\
\alpha = 1 : &\qquad \mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - (q^2 + q)\mathbf{x}^2; \\
\alpha = q : &\qquad \mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 + (1 - q^2)\mathbf{x}; \\
\alpha = 1 + q : &\quad \mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + q\mathbf{x}^2.
\end{aligned}$$

Disse likningene er på utvidet Weierstrassform, så det betyr at vi kan tillate $\mathrm{char}(R) = 2, 3, \ldots$ og dermed definere elliptiske kurver over R. For eksempel kan vi kan definere elliptiske kurver over $\mathbb{F}_2$ og $\mathbb{F}_3$ uten at reduksjonen er dårlig. Hvis likningene derimot var på kort Weierstrassform, ville kurvene ikke være elliptisk over R fordi $\mathrm{char}(R) \neq 2, 3$. Dessuten ville kurver på kort Weierstrassform ha en diskriminant der 2 og 3 er en faktor, og reduksjonen ville vært dårlig ved $p = 2, 3$.

6.1.1 Heltallspunkter og torsjonspunkter

Eksempel 6.1. Sett $\alpha = 0$ og $q = 1$. Med disse valgene får vi den elliptiske kurven ξ som er definert ved

$$\xi(\mathbf{x}, \mathbf{y}) : \quad \mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 5\mathbf{x}^2 + 4\mathbf{x}$$

Kurven er elliptisk fordi diskriminanten er 2837. Definert over $\mathbb{Z}$ har kurven fjorten heltallspunkter:

$$\begin{aligned}\xi(\mathbb{Z}) = \big\{&(0:1),(0:0),(1:1),(1:0),(4:1),(4:0),\\ &(5:5),(5:-4),(12:33),(12:-32),\\ &(21:85),(21:-84),(141:1645),(141:-1644)\big\},\end{aligned}$$

så $\#\xi(\mathbb{Z}) = 14$.

Bortsett fra det trivielle, har kurven ingen torsjonspunkter over $\mathbb{Z}$. Vi kan se på likningen til kurven at den har en horisontal symmetrilinje ved $\mathbf{y} = 1/2$. Dette ser vi fra likningen $\mathbf{y}^2 - \mathbf{y} = (\mathbf{y}-1)\mathbf{y} = 0$. Løsningene er $\mathbf{y} = 1$ og 0, så symmetrilinjen er $\mathbf{y} = 1/2$. Dette impliserer påfølgende at det ikke fins 2-torsjonspunkter på kurven, siden dette krever at $\mathbf{y} = 0$. Det eneste torsjonspunktet er $\mathcal{O}$, så torsjonsundermengden $\xi(\mathbb{Z})_{\text{tor}}$ er isomorf med den trivielle gruppen $\{\mathcal{O}\}$.

Likningen til den elliptiske kurven kan skrives på kort Weierstrassform. La ξ_W betegne den formen. Likningen er gitt ved

$$\xi_W(\mathbf{x},\mathbf{y}) = \mathbf{y}^2 = \mathbf{x}^3 - 5616\mathbf{x} - 109296.$$

Faktisk er $\xi \simeq \xi_W$. Altså er det en isomorfi $\phi : \xi \to \xi_W$ som her gir $\phi(\mathbf{x},\mathbf{y}) = (36\mathbf{x} - 60, 216\mathbf{y} - 108)$. Og siden $\xi \simeq \xi_W$, så er $j(\xi) = j(\xi_W) = 2^{12}\cdot 13^3 \cdot 2837^{-1}$. Det følger proposisjon ??.

Til sammen har ξ_W seksten heltallspunkter:

$$\begin{aligned}\xi_W(\mathbb{Z}) = \big\{&(-60:\pm 108),(-56:\pm 172),(-24:\pm 108),\\ &(84:\pm 108),(120:\pm 972),(372:\pm 7020),\\ &(696:\pm 18252),(5016:\pm 355212)\big\},\end{aligned}$$

så $\#\xi_W(\mathbb{Z}) = 16$, noe som er interessant. Den har en symmetrilinje som er lik $\mathbf{x}$ aksen. Dermed er det intuitivt å tenke at kurven har torsjonspunkter, men det har den ikke. Faktisk har ξ_W bare det trivielle torsjonspunktet. Derfor er $\xi_W(\mathbb{Z})_{\text{tor}} \simeq \{\mathcal{O}\}$.

Remark 6.2. Før vi går over til neste eksempel, føler vi det er viktig å gjøre en bemerkning på hvorfor antallet heltallspunkter på ξ og ξ_W er forskjellig. Det er tross alt en interessant bemerkning.

Som vi har sett er $\#\xi(\mathbb{Z}) = 14$ og $\#\xi_W(\mathbb{Z}) = 16$ så $\#\xi(\mathbb{Z}) \neq \#\xi_W(\mathbb{Z})$. Årsaken ligger i isomorfien $\phi : \xi \to \xi_W$. Husk fra kapittel 3 at en kubisk kurve på formen

$$\mathbf{y}^2 + a_1\mathbf{x}\mathbf{y} + a_3\mathbf{y} = \mathbf{x}^3 + a_2\mathbf{x}^2 + a_4\mathbf{x} + a_6, \quad a_i \in R,$$

kan (nesten) alltid skrives på normal og deretter på kort Weierstrassform med transformasjonen $\mathbf{y} \mapsto \mathbf{y} - (a_1\mathbf{x} + a_3)/2$ og etterpå $\mathbf{x} \mapsto \mathbf{x} - (a_2 + a_1^2/4)/3$. Merk nå at koeffisientene vi får er fra $\mathbb{Q}$, så selv om en kurve er definert over $\mathbb{Z}$, så er ikke koeffisientene i den normale eller korte Weierstrassformen fra $\mathbb{Z}$ generelt. Sagt med andre ord, punkter som er $\mathbb{Z}$-rasjonale i den ene formen, kan bli $\mathbb{Q}$-rasjonale i den andre.

Eksempel 6.3. La $q = 1$ og $\alpha = 1$. Da får vi den elliptiske kurven

$$\xi(\mathbf{x}, \mathbf{y}) : \quad \mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2$$

Den er elliptisk fordi diskriminanten er 101. Sammenliknet med det forrige eksempelet har denne bare seks heltallspunkter:

$$\xi(\mathbb{Z}) = \big\{(0:1), (0:0), (2:1), (2:0), (14:49), (14:-48)\big\}.$$

Den har også bare et torsjonspunkt, altså $\mathcal{O}$, så $\xi(\mathbb{Z})_{\text{tor}} \simeq \{\mathcal{O}\}$. Kurven ξ_W, som er ξ på kort Weierstrassform

$$\mathbf{y}^2 = \mathbf{x}^3 - 1728\mathbf{x} - 15984,$$

er elliptisk med diskriminant $2^{12} \cdot 3^{12} \cdot 101$. Kurven er isomorf med ξ med $\phi(\mathbf{x}, \mathbf{y}) = (36\mathbf{x} - 24, 216\mathbf{y} - 108)$. Over $\mathbb{Z}$ har den åtte heltallspunkter:

$$\xi_W(\mathbb{Z}) = \big\{(-24 : \pm 108), (-15 : \pm 81), (48 : \pm 108), (480 : \pm 10476)\big\}.$$

Men bare $\mathcal{O}$ er et torsjonspunkt på ξ_W. Så $\xi_W(\mathbb{Z}) \simeq \{\mathcal{O}\}$.

Eksempel 6.4. Sett $\alpha = q$ der $q \in \mathbb{Z}_{\geq 0}$ er en fri parameter. Da får vi

$$\xi(\mathbf{x}, \mathbf{y}): \quad \mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 + (1 - q^2)\mathbf{x}. \tag{6.2}$$

Diskriminanten er gitt ved

$$\Delta(\xi) = 64q^6 - 128q^4 - 208q^2 - 43.$$

Dette er et polynom i sjette orden. Det betyr at $\xi(\mathbf{x}, \mathbf{y})$ har opp til seks kurver som ikke er elliptisk. Sagt på en annen måte, det er veldig få singulære kurver og veldig mange elliptiske kurver.

q	ξ_q	$\Delta(\xi_q)$	$\#\xi_q(\mathbb{Z})$	$\#\xi_q(\mathbb{Z})_{\text{tor}}$
0	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 + \mathbf{x}$	$-1 \cdot 43$	10	1
1	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2$	101	6	1
2	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 - 3\mathbf{x}$	2837	14	1
3	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 - 8\mathbf{x}$	$47 \cdot 811$	16	1
4	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 - 15\mathbf{x}$	$11 \cdot 13 \cdot 1627$	20	1
5	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 - 24\mathbf{x}$	$17 \cdot 54421$	12	1
6	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 - 35\mathbf{x}$	$31 \cdot 197 \cdot 463$	12	1
7	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 - 48\mathbf{x}$	$11 \cdot 337 \cdot 1951$	12	1
8	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 - 63\mathbf{x}$	$139 \cdot 117023$	34	1
9	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 - 80\mathbf{x}$	$13 \cdot 2553017$	12	1

Table 6.1: Tabellen viser ulike elliptiske kurver ξ_q for $q \in \{0, 1, \ldots, 9\}$. Tredje kolonne viser diskriminanten faktorisert i primtall. Fjerde viser antallet heltallspunkter på ξ_q, og femte viser antall torsjonspunkter på ξ_q.

Som vi ser er kurvene ingen ikke-trivielle torsjonspunkter. Faktisk viser det seg at for alle q har *ingen* av kurvene flere enn et torsjonspunkt. Vi har skrevet et program som skriver ut hvilke kurver på formen 6.2 som har en torsjonsorden større enn en. Resultatet viser at for $q \in \{0, 1, \ldots, 9999\}$ er ingen av kurvene en kurve med torsjonsorden større enn en. Programmet vi har skrevet her, og mange andre, er presentert under Vedlegg.

Eksempel 6.5. Sett $\alpha = 1 + q$ og la $q \in \mathbb{Z}$ være en fri parameter. Da får vi den kubiske kurven

$$\xi_q(\mathbf{x}, \mathbf{y}): \quad \mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + q\mathbf{x}^2$$

med diskriminant

$$\Delta(\xi) = -16q^3 - 27.$$

Merk at det er på det meste tre kurver som ikke er elliptisk. For å være presis ser vi at ξ er elliptisk for alle q over $\mathbb{Z}$, siden likningen $q^3 = -27/16$ ikke har løsninger over $\mathbb{Z}$.

Denne kurven har torsjonspunkter når $q = -1$ og 0. Den elliptiske kurven ξ_{-1} gitt ved

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - \mathbf{x}^2$$

har fem torsjonspunkter. Torsjonsundermengden er

$$\xi_{-1}(\mathbb{Z})_{\text{tor}} = \big\{\mathcal{O}, (0:0), (0:1), (1:0), (1:1)\big\}.$$

Siden det er fem torsjonspunkter på ξ_{-1} og $\xi_{-1}(\mathbb{Z})_{\text{tor}}$ er en abelsk gruppe, er $\xi_{-1}(\mathbb{Z})_{\text{tor}} \simeq \mathbb{Z}/5$.

Den elliptiske kurven ξ_0 er gitt ved

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3$$

og har tre torsjonspunkter. Torsjonsundermengden er

$$\xi_0(\mathbb{Z})_{\text{tor}} = \big\{\mathcal{O}, (0:0), (0:1)\big\}.$$

Siden det er tre torsjonspunkter, så ser vi at $\xi_0(\mathbb{Z})_{\text{tor}} \simeq \mathbb{Z}/5$. Med programmet vi brukte i forrige eksempel, ser vi for alle andre q, at kurvene kun har det trivielle torsjonspunktet.

6.1.2 Supersingulære reduksjoner

Eksempel 6.6. La $q = 1$ og $\alpha \in \mathbb{Z}$. Med disse valgene får vi en elliptisk kurve som er gitt ved

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + (3\alpha - 5)\mathbf{x}^2 + 2(1-\alpha)(2-\alpha)\mathbf{x}.$$

I dette eksempelet velger vi $p = 7$.

α	ξ_α	$\Delta(\xi_\alpha)$	Supersingulær
-5	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 20\mathbf{x}^2 + 84\mathbf{x}$	$11 \cdot 337 \cdot 1951$	Ja
-4	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 17\mathbf{x}^2 + 60\mathbf{x}$	$31 \cdot 197 \cdot 463$	Nei
-3	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 14\mathbf{x}^2 + 40\mathbf{x}$	$17 \cdot 54421$	Nei
-2	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 11\mathbf{x}^2 + 24\mathbf{x}$	$11 \cdot 13 \cdot 1627$	Nei
-1	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 8\mathbf{x}^2 + 12\mathbf{x}$	$47 \cdot 811$	Nei
0	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 5\mathbf{x}^2 + 4\mathbf{x}$	2837	Nei
1	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2$	101	Nei
2	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + \mathbf{x}^2$	$-1 \cdot 43$	Ja
3	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + 4\mathbf{x}^2 + 4\mathbf{x}$	101	Nei
4	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + 7\mathbf{x}^2 + 12\mathbf{x}$	2837	Nei
5	$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + 10\mathbf{x}^2 + 24\mathbf{x}$	$47 \cdot 811$	Nei

Table 6.2: Tabellen viser ulike elliptiske kurver for $\alpha \in \{-5, \ldots, 5\}$. Tredje kolonne viser diskriminanten (ikke redusert). Den fjerde viser om kurven er supersingulær modulo 7.

Som vi ser har ξ_{-5} og ξ_2 supersingulær reduksjon ved $p = 7$. De andre kurvene har ikke det i tabellen. Hvis vi definerer ξ_{-5} over $\mathbb{F}_7$, får vi en elliptisk kurve med åtte $\mathbb{F}_7$-rasjonale punkter og $\xi_{-5}(\mathbb{F}_7)_{\text{tor}} \simeq \mathbb{Z}/8$. Hvert punkt $\mathbf{p} \in \xi_{-5}(\mathbb{F}_7)$ er et torsjonspunkt av orden henholdsvis to, fire og åtte. Det eneste punktet av orden syv er $\mathcal{O}$, så $\xi_{-5}(\mathbb{F}_7)[7] \simeq \{\mathcal{O}\}$. Dette er det samme som at ξ_{-5} er supersingulær over $\mathbb{F}_7$. Den elliptiske kurven ξ_2 er også supersingulær over $\mathbb{F}_7$. Hvert punkt er et torsjonspunkt, men bare $\mathcal{O}$ har orden syv, så $\xi_2(\mathbb{F}_7)[7] \simeq \{\mathcal{O}\}$.

Hvis vi ser på kurver for andre verdier α, ser vi at det dukker opp et visst mønster. Faktisk er det et mønster i diskriminantene til de forskjellige kurvene, men det er også et mønster på når en kurve er supersingulær. Vi kan se at den syvende neste kurven er en supersingulær kurve. Så $\xi_{\alpha\pm7}$ er supersingulær over $\mathbb{F}_7$ hvis ξ_α er det. Det betyr at ξ_9, ξ_{16}, ξ_{23}, og så videre, er alle supersingulære kurver. Det er ξ_{-12}, ξ_{-19}, og så videre, også.

Men hvis vi sjekker for $p = 11$, får vi et annet mønster. Hvis ξ_α er supersingulær, så er enten $\xi_{\alpha\pm4}$ eller $\xi_{\alpha\pm7}$ supersingulær. Nærmere observasjon viser at ξ_α er supersingulær for alle

$$\alpha \in \{\ldots, -11, -7, 0, 4, 11, 15, 22, 26, 33, 37, 44, 48, 55, 59, \ldots\}.$$

Det er tydelig et alternerende og gjentakende mønster. Fra null og oppover, gir den fjerde neste α en supersingulær kurve, etterpå ser vi at den syvende neste α som gir en supersingulær kurve. Dette er et distribusjonsmønster som vi betegner med $4, 7$.

Distribusjonsmønsteret er forskjellig for andre primtall. For eksempel så vi at for $p = 7$ er mønsteret $7, 7, 7$, og så videre, mens mønsteret for $p = 11$ er $4, 7, 4, 7$, og så videre. Når $p = 2$, er mønsteret veldig enkelt, det er $1, 1, 1$. Dette betyr følgende at ξ_α er supersingulær over $\mathbb{F}_2$ for alle $\alpha \in \mathbb{Z}$. For eksempel når $\alpha = 0$ er kurven, som er gitt ved

$$\mathbf{y}^2 + \mathbf{y} = \mathbf{x}^3 + \mathbf{x}^2,$$

en supersingulær kurve. Når $\alpha = 1$ er kurven, som er gitt ved

$$\mathbf{y}^2 + \mathbf{y} = \mathbf{x}^3,$$

en supersingulær kurve. For $p = 29$ er distribusjonsmønsteret $1, 4, 6, 4, 1, 13$ og noen av verdiene for α som gir supersingulære kurver over $\mathbb{F}_{29}$ er -6, -5, -1, 5, 9, 10 og 2.

En litt *merkelig* observasjon er at summen av hvert tall i distribusjonsmønsteret er lik det supersingulære primtallet (bortsett fra $p = 2$). For eksempel når $p = 11$, så ser vi at mønsteret er $4, 7$, og summen er 11.

p	α	Mønster
2	$\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots$	1
3		
5		
7	$\ldots, -26, -19, -12, -5, 2, 9, 16, 23, 30, 37, 44, \ldots$	7
11	$\ldots, -22, -18, -11, -7, 0, 4, 11, 15, 22, 26, 33, \ldots$	$4, 7$
13		
17		
19	$\ldots, -30, -23, -11, -4, 8, 15, 27, 34, 46, 53, 65, \ldots$	$7, 12$
23	$\ldots, -46, -42, -23, -19, 0, 4, 23, 27, 46, 50, 69, \ldots$	$4, 19$
29	$\ldots, -19, -6, -5, -1, 5, 9, 10, 23, 24, 28, 34, 38, \ldots$	$1, 4, 6, 4, 1, 13$
31	$\ldots, -20, -14, -13, -7, 11, 17, 18, 24, 42, 48, \ldots$	$1, 6, 18, 6$
37	$\ldots, -109, -72, -35, 2, 39, 76, 113, 150, 187, \ldots$	37
41		
43	$\ldots, -30, -29, -10, -9, 13, 14, 33, 34, 56, 57, \ldots$	$1, 19, 1, 22$
47	$\ldots, -39, -32, -11, -4, 8, 15, 36, 43, 55, 62, 83, \ldots$	$7, 12, 7, 21$
53	$\ldots, -97, -58, -44, -5, 9, 48, 62, 101, 115, 154, \ldots$	$14, 39$
59	$\ldots, -29, -26, -18, -10, 14, 22, 30, 33, 41, 49, \ldots$	$8, 8, 3, 8, 8, 24$
61	$\ldots, -117, -62, -56, -1, 5, 60, 66, 121, 127, \ldots$	$6, 55$
67		

Table 6.3: Tabellen viser for p primtall, hvilke α som gir en supersingulær kurve.

Eksempel 6.7. Distribusjonsmønsteret dukker også opp når $q = -1$, det vil si for kurver på formen

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + (\alpha - 1)\mathbf{x}^2.$$

Resultatet er vist i tabellen.

p	α	Mønster
2	$\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \ldots$	1
3		
5	$\ldots, -19, -14, -9, -4, 1, 6, 11, 16, 21, 26, 31, 36, 41, \ldots$	5
7	$\ldots, -9, -5, -4, -2, 2, 3, 5, 9, 10, 12, 16, 17, 19, 23, \ldots$	1, 2, 4
11	$\ldots, -21, -17, -10, -6, 1, 5, 12, 16, 23, 27, 34, 38, 45, \ldots$	4, 7
13		
17	$\ldots, -67, -50, -33, -16, 1, 18, 35, 52, 69, 86, 103, \ldots$	17
19	$\ldots, -25, -19, -10, -6, 0, 9, 13, 19, 28, 32, 38, 47, 51, \ldots$	4, 6, 9

Table 6.4: Tabellen viser for p primtall, hvilke α som gir en supersingulær kurve. Merk at summen av tallene i mønsteret for p er lik p.

Eksempel 6.8. La oss se på kurvene for $p = 5$ og $q = -1$. Den elliptiske kurven som er definert ved likningen i forrige eksempel, er supersingulær når α er lik verdiene listet i tabell ??. Vi betegner disse α-verdiene med A. Siden kurven er supersingulær for hver femte α er spørsmålet hvordan gruppestrukturen ser ut.

La oss se på når $\alpha = 1$ først. Det gir en elliptisk kurve ξ_1 definert ved $\mathbf{y}^2 - \mathbf{y} = \mathbf{x^3}$ som er supersingulær over $\mathbb{F}_5$. Den reduserte likningen er $\mathbf{y}^2 + 4\mathbf{y} = \mathbf{x}^3$. Kurven har totalt seks $\mathbb{F}_5$-rasjonelle punkter, så $\#\xi_1(\mathbb{F}_5) = 6$. Det følger at $\xi(\mathbb{F}_5) \simeq \mathbb{Z}/6$. Dessuten ser vi at $\xi_1(\mathbb{F}_5)[5] \simeq \{\mathcal{O}\}$, så kurven er supersingulær. Når $\alpha = 6$ får vi en elliptisk kurve ξ_6 som er definert ved $\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + 5\mathbf{x}^2$ og ved den reduserte formen $\mathbf{y}^2 + 4\mathbf{y} = \mathbf{x}^3$. Umiddelbart ser vi at den reduserte formen er lik den for $\alpha = 1$. Dermed er det åpenbart at kurven har like mange $\mathbb{F}_5$-rasjonelle punkter.

Det er derfor åpenbart at de neste verdiene for α gir en supersingulær kurve over $\mathbb{F}_5$. Dessuten ser vi at $5 \mid (\alpha - 1)$ for alle $\alpha \in A$ og kurven er alltid på formen $\mathbf{y}^2 + 4\mathbf{y} = \mathbf{x}^3$, som er supersingulær over $\mathbb{F}_5$.

La oss sjekke for andre primtall som gir et mer *fargerikt* mønster. Ta for eksempel $p = 19$. Da er den elliptiske kurven supersingulær når α er lik dem i tabellen. Vi betegner denne mengden med B. Vi begynner med $\alpha = 0$. Det gir en elliptisk kurve ξ_0 som er definert ved den reduserte formen

$\mathbf{y}^2 + 18\mathbf{y} = \mathbf{x}^3 + 18\mathbf{x}^2$ over $\mathbb{F}_{19}$. Kurven har totalt 20 rasjonelle punkter over $\mathbb{F}_{19}$, så $\#\xi_0(\mathbb{F}_{19}) = 20$ og $\xi_0(\mathbb{F}_{19}) \simeq \mathbb{Z}/20$. I tillegg er $\xi_0(\mathbb{F}_{19})[19] \simeq \{\mathcal{O}\}$, som viser at det er en supersingulær kurve over $\mathbb{F}_{19}$. Når $\alpha = 9$ får vi en elliptisk kurve som er definert ved $\mathbf{y}^2 + 18\mathbf{y} = \mathbf{x}^3 + 8\mathbf{x}$. På samme måte har kurven totalt 20 rasjonelle punkter over $\mathbb{F}_{19}$, men det er andre punkter. Uansett ser vi også for kurven ξ_9 at $\xi_9(\mathbb{F}_{19})[19] \simeq \{\mathcal{O}\}$, som viser at ξ_9 er en supersingulær kurve over $\mathbb{F}_{19}$

6.2 Kvadratiske og syklotomiske kropper

6.2.1 Kvadratiske kropper

La $\mathfrak{o} = \mathbb{Z}[\sqrt{d}] \subset \mathbb{Q}(\sqrt{d})$ med et kvadratfritt tall d være en ring av heltall i en kvadratisk kropp. Som vanlig er alle $a \in \mathfrak{o}$ faktoriserbar og gir irredusible elementer. For eksempel er $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ i heltallsringen $\mathbb{Z}[\sqrt{-5}]$. Kurven ξ over $\mathfrak{o}$ er en kubisk kurve gitt ved

$$\mathbf{y}^2 + \omega_1\mathbf{y} = \omega_2\mathbf{x}^3 + \omega_3\mathbf{x}^2 + \omega_4\mathbf{x},$$

der koeffisientene $\omega_i \in \mathfrak{o}$ er

$$\begin{aligned}
\omega_1 &= -1, \\
\omega_2 &= 1, \\
\omega_3 &= (2 + \sqrt{d})(\alpha - \sqrt{d}) - 2, \\
\omega_4 &= (1 - \alpha)(1 + \sqrt{d})(1 + \sqrt{d})(1 + \sqrt{d} - \alpha).
\end{aligned}$$

Denne er en elliptisk kurve hvis diskriminanten

$$\Delta(\xi) = -16\omega_3^2(\omega_3 - \omega_4^2) - 64\omega_4^3 + 72\omega_3\omega_4 - 27$$

er ulik null.

I denne delseksjonen skal vi for enkelhetsskyld undersøke kurver over heltallsringene $\mathbb{Z}[\sqrt{2}]$ og $\mathbb{Z}[\sqrt{3}]$ og den komplekse heltallsringen $\mathbb{Z}[\sqrt{-1}]$. Primært diskuterer vi gruppestrukturen og hvor mange torsjonspunkter en kurve har. Vi skal også undersøke supersingulære primtall.

Torsjonspunkter

For enkelhetsskyld lar vi A og B betegne koeffisientene ω_3 og ω_4.

Eksempel 6.9. Vi begynner med $\alpha = 0$ og $\mathfrak{o}_2 = \mathbb{Z}[\sqrt{2}]$. Da har vi den elliptiske kurven $\xi/\mathfrak{o}_2$ som er gitt ved likningen

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - (2\sqrt{2}+4)\mathbf{x}^2 + (2\sqrt{2}+3)\mathbf{x}.$$

Denne definerer en elliptisk kurve fordi diskriminanten er $\Delta(\xi) = (-12\sqrt{2}-17)(-340\sqrt{2}+43)$. Dette betyr følgende at ξ har en dårlig reduksjon ved $(-340\sqrt{2}+43)$. Denne faktoren er et primideal i $\mathfrak{o}_2$. Den andre er ikke det. Kurven har kun det trivielle torsjonspunktet. Dermed er $\xi(\mathfrak{o}_2)_{\text{tor}} \simeq \{\mathcal{O}\}$. Og det samme skjer over de andre heltallsringene:

$\mathfrak{o}_N$	A	B	$\#\xi(\mathfrak{o}_N)_{\text{tor}}$	$\simeq$
$\mathfrak{o}_{-1}$	$(-2\sqrt{-1}-1)$	$2\sqrt{-1}$	1	$\{\mathcal{O}\}$
$\mathfrak{o}_2$	$(-2\sqrt{2}-4)$	$(2\sqrt{2}+3)$	1	$\{\mathcal{O}\}$
$\mathfrak{o}_3$	$(-2\sqrt{3}-5)$	$(2\sqrt{3}+4)$	1	$\{\mathcal{O}\}$

Table 6.5: Tabellen viser koeffisientene A og B for ξ over $\mathfrak{o}_p$.

Eksempel 6.10. Med $\alpha = 1$ er kurven $\xi/\mathfrak{o}_{-1}$ gitt ved

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - (\sqrt{-1}-1)\mathbf{x}^2.$$

en elliptisk kurve med $\Delta(\xi) = (-\sqrt{-1})(5\sqrt{-1}-32)$. På samme måte ser vi at ξ har en dårlig reduksjon ved $(5\sqrt{-1}-32)$, siden dette er et primideal i $\mathfrak{o}_{-1}$. Kurven har kun torsjonspunktet $\mathcal{O}$, så $\xi(\mathfrak{o}_{-1})_{\text{tor}} \simeq \{\mathcal{O}\}$. Det samme ser vi også for kurvene $\xi/\mathfrak{o}_2$ og $\xi/\mathfrak{o}_3$.

$\mathfrak{o}_N$	A	B	$\#\xi(\mathfrak{o}_N)_{\text{tor}}$	$\simeq$
$\mathfrak{o}_{-1}$	$(-\sqrt{-1}+1)$	0	1	$\{\mathcal{O}\}$
$\mathfrak{o}_2$	$(-\sqrt{2}-2)$	0	1	$\{\mathcal{O}\}$
$\mathfrak{o}_3$	$(-\sqrt{3}-3)$	0	1	$\{\mathcal{O}\}$

Eksempel 6.11. La $\alpha = \sqrt{d} \in \mathfrak{o}_d = \mathbb{Z}[\sqrt{d}]$ der d er et kvadratfritt heltall som vanlig. Sett $d = 3$. Da er $\xi/\mathfrak{o}_3$ en elliptisk kurve på formen

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 - 2\mathbf{x}.$$

Dette er en elliptisk kurve over heltallsringen $\mathfrak{o}_3$ med der diskriminanten er $\Delta(\xi) = (-1)(\sqrt{3}-4)(\sqrt{3}+4) \cdot 89$. Med diskriminanten ser vi at kurven har en dårlig reduksjon henholdsvis ved $(\sqrt{3}-4)$, $(\sqrt{3}+4)$ og 89. For å illustrere er reduksjonen, $\xi_{/89}$, en singulær kurve på formen

$$\mathbf{y}^2 + 88\mathbf{x} = \mathbf{x}^3 - 87\mathbf{x}^2 - 87\mathbf{x}$$

over restkroppen $\mathfrak{o}_3'$. Det kan likevel se ut som at kurven er elliptisk over, for eksempel, $\mathbb{Q}$, og det er den. Men den er ikke elliptisk over $\mathfrak{o}_3'$ fordi vi ser at $p = 89$ deler $\Delta(\xi_{/89}')$. Se kapittel 4 teorem ??.

Tilbake til $\xi/\mathfrak{o}_3$ ser vi at kurven ikke har noen torsjonspunkter. Den har kun det trivielle torsjonspunktet $\mathcal{O}$. Dermed ser vi at $\xi(\mathfrak{o}_3)_{\text{tor}} \simeq \{\mathcal{O}\}$. Og det samme ser vi over de andre heltallsringene:

$\mathfrak{o}_d$	A	B	$\#\xi(\mathfrak{o}_d)_{\text{tor}}$	$\simeq$
$\mathfrak{o}_{-1}$	-2	2	1	$\{\mathcal{O}\}$
$\mathfrak{o}_2$	-2	-1	1	$\{\mathcal{O}\}$
$\mathfrak{o}_3$	-2	-2	1	$\{\mathcal{O}\}$

Eksempel 6.12. Med $\alpha = 1+\sqrt{2}$ og $\mathfrak{o}_2 = \mathbb{Z}[\sqrt{2}]$ får vi den elliptiske kurven $\xi/\mathfrak{o}_2$ som er gitt ved

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + \sqrt{2}\mathbf{x}^2.$$

Denne likningen definerer en elliptisk kurve over $\mathfrak{o}_2$ siden diskriminanten er $\Delta(\xi) = (\sqrt{2}+1)(5\sqrt{2}-37)$. Siden $(5\sqrt{2}-37)$ er et primideal i $\mathfrak{o}_2$, ser vi at $\xi/\mathfrak{o}_2$ har en dårlig reduksjon ved $(5\sqrt{2}-37)$.

Denne kurven og kurvene $\xi/\mathfrak{o}_{-1}$ og $\xi/\mathfrak{o}_3$ har kun ett torsjonspunkt, nemlig $\mathcal{O}$. Dermed ser vi at de respektive torsjonsundermengdene, $\xi(\mathfrak{o}_{-1})_{\text{tor}}$, $\xi(\mathfrak{o}_2)_{\text{tor}}$ og $\xi(\mathfrak{o}_3)_{\text{tor}}$, alle er isomorf med den trivielle gruppen.

Supersingulære reduksjoner

Eksempel 6.13. La $\alpha = 0$. Da er den elliptiske kurven ξ over heltallsringen $\mathfrak{o}_2 = \mathbb{Z}[\sqrt{2}]$ gitt ved likningen

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - (2\sqrt{2} + 4)\mathbf{x}^2 + (2\sqrt{2} + 3)\mathbf{x}.$$

Med vårt Sage-program ser vi at kurven kun har ett supersingulært primtall under 10^4. Dette primtallet er $p = 5$, og reduksjonen $\xi'_{/5}$ som er definert over en restkropp $\mathfrak{o}'_2$, er en elliptisk kurve på formen

$$\mathbf{y}^2 + 4\mathbf{y} = \mathbf{x}^3 + (3\sqrt{2}' + 1)\mathbf{x}^2 + (2\sqrt{2}' + 3)\mathbf{x}.$$

Her er $(3\sqrt{2}' + 1)$ og $(2\sqrt{2}' + 3)$ er koeffisienter i $\mathfrak{o}'_2$. Nå, denne reduksjonen har totalt 21 $\mathfrak{o}'_2$-rasjonelle punkter, og alle punktene er 21-torsjon. Dermed er $\xi'_{/5}(\mathfrak{o}'_2)[21] = \xi'_{/5}(\mathfrak{o}'_2) \simeq \mathbb{Z}/21$. Følgelig er $\xi'_{/5}(\mathfrak{o}'_2)[5] \simeq \{\mathcal{O}\}$, siden $\xi'_{/5}$ er supersingulær.

Den elliptiske kurven over $\mathfrak{o}_{-1} = \mathbb{Z}[\sqrt{-1}]$ har ingen supersingulære primtall $p < 10^4$, og dermed ingen supersingulære reduksjoner. Det samme ser vi for kurven over $\mathfrak{o}_3$.

Fortsatt for $p < 10^4$ ser vi at de elliptiske kurvene $\xi/\mathfrak{o}_5$ og $\xi/\mathfrak{o}_7$ har en supersingulær reduksjon ved $p = 2$ og $p = 5$, respektivt. Reduksjonen $\xi_{/2}$ over restkroppen $\mathfrak{o}'_5$ har totalt fem $\mathfrak{o}'_5$-rasjonelle punkter, og alle punktene er 5-torsjon, så $\xi_{/2}(\mathfrak{o}'_5) \simeq \mathbb{Z}/5$. Den andre reduksjonen, $\xi_{/5}/\mathfrak{o}'_7$ har 21 rasjonelle punkter, og $\xi_{/5}(\mathfrak{o}'_7) \simeq \mathbb{Z}/21$.

Eksempel 6.14. Med $\alpha = 1$ er den elliptiske kurven $\xi/\mathfrak{o}_3$ gitt ved

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - (\sqrt{3} + 3)\mathbf{x}^2.$$

Denne kurven har ingen supersingulære primtall $p < 10^4$. Faktisk ser vi med Sage-programmet at kurven har ingen supersingulære primtall $p < 3 \cdot 10^4$. Det er sannsynlig at denne kurven ikke har noen supersingulære primtall i det hele tatt. Det samme kan vi se for kurven over heltallsringene $\mathfrak{o}_2$ og $\mathfrak{o}_{-1}$, for også her har kurven ingen supersingulære primtall $p < 3 \cdot 10^4$. Men dette kan selvsagt bekreftes (eller avkreftes) med Sage programmet.

Den første kurven vi fant som har et supersingulært primtall for $p < 10^4$, var ξ over heltallsringen $\mathfrak{o}_5$. Denne er en elliptisk kurve på formen

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - (\sqrt{5} + 5)\mathbf{x}^2,$$

og det supersingulære primtallet er $p = 2$. Reduksjonen $\xi_{/2}/\mathfrak{o}_5'$ er en supersingulær elliptisk kurve på formen

$$\mathbf{y}^2 + \mathbf{y} = \mathbf{x}^3.$$

Interessant nok ser vi at $-(\sqrt{5} + 5) \equiv 0 \pmod 2$. I tillegg ser vi at $\Delta(\xi) = (\sqrt{5} + 2)(3/2\sqrt{5} + 1/2)(-41/2\sqrt{5} + 831/2)$, noe som betyr at faktorene er inneholdt i den kvadratiske kroppen $\mathbb{Q}(\sqrt{5})$. Når det kommer til gruppestrukturen har $\xi_{/2}$ totalt ni $\mathfrak{o}_5'$-rasjonelle punkter, og alle er 3-torsjon, så $\xi_{/2}(\mathfrak{o}_5') \simeq \mathbb{Z}/3 \times \mathbb{Z}/3$.

Av ren nysgjerrighet sjekket vi kurver over flere heltallsringer, som i tillegg til de over er vist i følgende tabell:

$\mathfrak{o}_d$	P	%
$\mathfrak{o}_{-2}$	-	-
$\mathfrak{o}_{-1}$	-	-
$\mathfrak{o}_2$	-	-
$\mathfrak{o}_3$	-	-
$\mathfrak{o}_5$	2	0.002
$\mathfrak{o}_6$	-	-
$\mathfrak{o}_7$	-	-
$\mathfrak{o}_8$	-	-

Table 6.6: En tabell over supersingulære primtall for $\xi/\mathfrak{o}_d$ med prosentandel av 1229 primtall.

Som vi ser er det ikke mange heltallsringer der ξ har supersingulære primtall. Nå stresser vi så klart at det er *hypotetisk* svært få heltallringer med supersingulære primtall for ξ.

Eksempel 6.15. La nå $\alpha = \sqrt{d}$ der d er et kvadratfritt tall som vanlig. Først vil vi diskutere den elliptiske kurven ξ over heltallringen $\mathfrak{o}_2 = \mathbb{Z}[\sqrt{2}]$. Likningen til denne kurven er

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 - \mathbf{x},$$

og diskriminanten er $\Delta(\xi) = 373$. Dette betyr følgelig at $\xi/\mathfrak{o}_2$ har en dårlig reduksjon ved $p = 373$. Når det gjelder supersingulære primall $p < 10^4$, så har denne kurven så mange som fem:

$$\big\{563, 811, 941, 6299, 9221\big\}.$$

For å ta et eksempel, diskuterer vi $p = 941$. Den supersingulære reduksjon $\xi_{/941}$ er er definert over restkroppen $\mathfrak{o}_2'$, og har en likning på formen

$$\mathbf{y}^2 + 940\mathbf{y} = \mathbf{x}^3 + 939\mathbf{x}^2 + 940\mathbf{x}.$$

Denne reduksjonen har 887364 $\mathfrak{o}_2'$-rasjonelle punkter, og den abelske gruppen $\xi_{/941}(\mathfrak{o}_2') \simeq \mathbb{Z}/942 \times \mathbb{Z}/942$.

Det viser seg at det er mange heltallringer der den elliptiske kurven ξ har supersingulære primtall. Følgende tabell viser noen av disse.

$\mathfrak{o}_d$	P	%
$\mathfrak{o}_{-3}$	$2, 251, 677, 1061, 1571, 2411, 3719, 8147$	0.007
$\mathfrak{o}_{-2}$	$5, 101, 599, 647, 3671, 4133, 6263, 8831$	0.007
$\mathfrak{o}_{-1}$	$107, 1979, 2351, 2851, 3559, 4567, 7583$	0.006
$\mathfrak{o}_2$	$563, 811, 941, 6299, 9221$	0.004
$\mathfrak{o}_3$	$5, 389, 607, 1663, 5393, 7841, 9283, 9391, 9871$	0.007
$\mathfrak{o}_5$	$2, 263, 367, 2903, 8423$	0.004
$\mathfrak{o}_6$	$83, 1619, 2393, 8291$	0.003
$\mathfrak{o}_7$	$11, 67, 191, 593, 5669$	0.004

Table 6.7: En tabell over supersingulære primtall for $\xi/\mathfrak{o}_d$ med prosentandel av 1229 primtall.

Det er verdt å merke seg at den elliptiske kurven $\xi/\mathfrak{o}_d$ er en kurve som kan defineres over de rasjonelle tallene $\mathbb{Q}$. Årsaken er at kurven, der $\alpha = \sqrt{d}$, alltid har en definerende likning med koeffisienter i $\mathbb{Q}$. Likevel er det viktig at den elliptiske kurven over $\mathbb{Q}$ ikke nødvendigvis har de samme egenskapene eller de samme supersingulære primtallene som kurven over $\mathfrak{o}_d$. Dessuten er $\mathfrak{o}_d \subset \mathbb{Q}(\sqrt{d})$ en utvidelse av $\mathbb{Z} \subset \mathbb{Q}$. Det er med andre ord mye mer interessant å se kurver over $\mathfrak{o}_d$. For eksempel ser vi at $\xi/\mathfrak{o}_7$ har fem supersingulære reduksjoner, mens $\xi/\mathbb{Q}$ har tolv. Det naturlige spørsmålet er hvorfor, og svaret er ganske enkelt. Som nevnt i de tidligere eksemplene fins det primtall i $\mathfrak{o}_d$ som er faktoriserbare idealer. I den konteksten er det syv supersingulære primtall for $\xi/\mathbb{Q}$ som er faktoriserbar i $\mathfrak{o}_d$.

6.2.2 Syklotomiske kropper

La $\mathfrak{o} = \mathbb{Z}[\zeta_N]$ være ringen av heltallene i en syklotomisk kropp, og la $\xi/\mathfrak{o}$ være en kubisk kurve gitt ved

$$\mathbf{y}^2 + \omega_1\mathbf{y} = \omega_2\mathbf{x}^3 + \omega_3\mathbf{x}^2 + \omega_4\mathbf{x},$$

der $\omega_i \in \mathfrak{o}$ er gitt ved

$$\begin{aligned}
\omega_1 &= -1,\\
\omega_2 &= 1,\\
\omega_3 &= (2+\zeta_N)(\alpha-\zeta_N) - 2,\\
\omega_4 &= (1-\alpha)(1+\zeta_N)(1+\zeta_N)(1+\zeta_N-\alpha),
\end{aligned}$$

og diskriminanten er gitt ved

$$\Delta(\xi) = -16\omega_3^2(\omega_3 - \omega_4^2) - 64\omega_4^3 + 72\omega_3\omega_4 - 27.$$

Hvis $\Delta(\xi) \neq 0$ så er ξ en elliptisk kurve over $\mathfrak{o}$.

I denne delseksjonen undersøker vi gruppestrukturen til $\xi/\mathfrak{o}$ for ulike verdier N i en heltallsring $\mathfrak{o} = \mathbb{Z}[\zeta_N]$. Vi skal også diskutere hvor mange og hvilke supersingulære primtall den elliptiske kurven $\xi/\mathfrak{o}$ har. Vi begynner med torsjonspunkter.

Torsjonspunkter

Eksempel 6.16. Vi begynner med $\alpha = 0$ og $\mathfrak{o}_2 = \mathbb{Z}[\zeta_2]$. Da har vi den kubiske kurven $\xi/\mathfrak{o}_2$ gitt ved

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - \mathbf{x}^2.$$

Denne er en elliptisk kurve siden $\Delta(\xi) = -11$. Diskriminanten impliserer at kurven har en dårlig reduksjon ved $p = 11$.

Kurven har totalt fem torsjonspunkter: $\mathcal{O}, (1:1), (0:1), (0:0), (1:0)$. Alle punktene inkludert $\mathcal{O}$ er 5-torsjon. Det kan vi lett sjekke ved at punktene tilfredsstiller $[5]\mathbf{p} = \mathcal{O}$. For eksempel ser vi for $(1:1)$ at $2(1:1) = (0:1)$, $3(1:1) = (0:0)$, $4(1:1) = (1:0)$ og $5(1:1) = \mathcal{O}$. Dette gjelder også for de andre torsjonspunktene. Siden det er fem torsjonspunkter og alle er 5-torsjon, så er $\xi(\mathfrak{o})_{\text{tor}} \simeq \mathbb{Z}/5$.

Over $\mathfrak{o}_3 = \mathbb{Z}[\zeta_3]$ definerer $\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - (\zeta_3 + 1)\mathbf{x}^2 + \zeta_3\mathbf{x}$ en elliptisk kurve med $\Delta(\xi) = -19$, som betyr at kurven har en dårlig reduksjon ved $p = 19$. Denne kurven har totalt tre torsjonspunkter og alle er 3-torsjon. Dermed er $\xi(\mathfrak{o}_3)_{\text{tor}} \simeq \mathbb{Z}/3$.

Over $\mathfrak{o}_5 = \mathbb{Z}[\zeta_5]$ får vi en elliptisk kurve med likningen $\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - (\zeta_5^2 + 2\zeta_5 + 2)\mathbf{x}^2 + (\zeta_5^2 + 2\zeta_5 + 1)\mathbf{x}$ og $\Delta(\xi) = (-3\zeta_5^3 + 5\zeta_5 + 5)(-25\zeta_5^3 - 81\zeta_5^2 - 41\zeta_5 - 72)$. Denne kurven har kun det trivielle torsjonspunktet, så $\xi(\mathfrak{o})_{\text{tor}} \simeq \{\mathcal{O}\}$. Det samme ser vi for andre $\mathfrak{o}_p$.

$\mathfrak{o}_p$	A	B	$\#\xi(\mathfrak{o}_p)_{\text{tor}}$	$\simeq$
$\mathfrak{o}_2$	-1	0	5	$\mathbb{Z}/5$
$\mathfrak{o}_3$	$-(\zeta_3 + 1)$	ζ_3	3	$\mathbb{Z}/3$
$\mathfrak{o}_5$	$-(\zeta_5^2 + 2\zeta_5 + 2)$	$(\zeta_5^2 + 2\zeta_5 + 1)$	1	$\{\mathcal{O}\}$
$\mathfrak{o}_7$	$-(\zeta_7^2 + 2\zeta_7 + 2)$	$(\zeta_7^2 + 2\zeta_7 + 1)$	1	$\{\mathcal{O}\}$
$\mathfrak{o}_{11}$	$-(\zeta_{11}^2 + 2\zeta_{11} + 2)$	$(\zeta_{11}^2 + 2\zeta_{11} + 1)$	1	$\{\mathcal{O}\}$
$\mathfrak{o}_{13}$	$-(\zeta_{13}^2 + 2\zeta_{13} + 2)$	$(\zeta_{13}^2 + 2\zeta_{13} + 1)$	1	$\{\mathcal{O}\}$

Table 6.8: Tabellen viser koeffisientene A og B for ξ over $\mathfrak{o}_p$, antall torsjonspunkter og hva torsjonsundermengden er isomorf med.

Men vi kan selvfølgelig undersøke den elliptiske kurven over $\mathfrak{o}_N$ der N er ikke-prim (et sammensatt tall). Derimot ser vi, når vi sjekker for $\mathfrak{o}_N$, $N < 20$, at kurvene over disse heltallringene likevel har kun ett torsjonspunkt, og de respektive torsjonsundermengdene er derfor isomorf med den trivielle gruppen.

Eksempel 6.17. La $\alpha = 1$. Den elliptisk kurven ξ over $\mathfrak{o}_2$ er gitt ved

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3.$$

Denne likningen har $\Delta(\xi) = -1 \cdot 3^3$, så $\xi/\mathfrak{o}_2$ har en dårlig reduksjon ved $p = 3$. Kurven har i alt tre torsjonspunkter, og alle er 3-torsjon. Dermed er $\xi(\mathfrak{o}_2)_{\text{tor}} \simeq \mathbb{Z}/3$.

Over $\mathfrak{o}_3$ er den elliptiske kurven gitt ved $\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + \mathbf{x}^2$. Diskriminanten er $\Delta(\xi) = -43$, så $\xi/\mathfrak{o}$ har en dårlig reduksjon ved $p = 43$. Imidlertid ser vi at -43 er faktoriserbar over $\mathfrak{o}_3$. Diskriminanten kan derfor skrives som $-43 = (\zeta_3 - 6)(\zeta_3 + 7)$. Det betyr at idealet $I = (43)$ ikke er prim i $\mathfrak{o}_3$. Det er bare ett torsjonspunkt på $\xi/\mathfrak{o}_3$, så $\xi(\mathfrak{o}_3)_{\text{tor}} \simeq \{\mathcal{O}\}$. Det samme ser vi for den neste heltallsringene.

Eksempel 6.18. La nå $\alpha = 1 + \zeta_N$. Over heltallsringen $\mathfrak{o}_3$ er den elliptiske kurven ξ gitt ved likningen

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + \zeta_3\mathbf{x}^2.$$

Diskriminanten er $\Delta(\xi) = -43$, så kurven har en dårlig reduksjon ved $p = 43$. Igjen ser vi at -43 er faktoriserbar over $\mathfrak{o}_3$. Kurven har bare ett torsjonspunkt, så $\xi(\mathfrak{o})_{\text{tor}} \simeq \{\mathcal{O}\}$.

Det kan virke som at alle kurvene over de neste heltallsringene kun har ett torsjonspunkt hver, men det er først over heltallsringen $\mathfrak{o}_6$ at torsjonsundermengden til kurven har flere enn ett torsjonspunkt. Over $\mathfrak{o}_6$ har nemlig den elliptiske kurven ξ totalt fem torsjonspunkter:

$$\big\{\mathcal{O}, (-\zeta_6 : 0), (-\zeta_6 : 1), (0 : 0), (0 : 1)\big\}.$$

Alle punktene er 5-torsjon. Dermed er $\xi(\mathfrak{o}_6)_{\text{tor}} \simeq \mathbb{Z}/5$.

Supersingulære reduksjoner

Eksempel 6.19. La oss gå tilbake til kurvene i eksempel 6.16 der $\alpha = 0$. For å begynne med det enkle, så har den elliptiske kurven $\xi/\mathfrak{o}_2$ som er gitt ved

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - \mathbf{x}^2,$$

en supersingulær reduksjon først ved $p = 2$. Reduksjonen modulo 2 er en elliptisk kurve $\xi'_{/2}$, som er definert over restkroppen $\mathfrak{o}'_2$ med likningen

$$\mathbf{y}^2 + \mathbf{y} = \mathbf{x}^3 + \mathbf{x}^2.$$

Reduksjonen har fem $\mathfrak{o}'_2$-rasjonelle punkter i en abelsk gruppe isomorf med $\mathbb{Z}/5$. Disse punktene er

$$\big\{\mathcal{O}, (0:0), (0:1), (1:0), (1:1)\big\}.$$

Det eneste punktet som er 2-torsjon, er det trivielle punktet $\mathcal{O}$, så

$$\xi'(\mathfrak{o}'_2)[2] \simeq \{\mathcal{O}\}.$$

Dette betyr at reduksjonen $\xi'_{/2}$ er en supersingulær kurve og at 2 er et supersingulært primtall for den elliptiske kurven $\xi/\mathfrak{o}_2$.

Men det er flere supersingulære primtall for $\xi/\mathfrak{o}_2$. Ved å bruke Sage-programmet vårt, kan vi enkelt finne hvilke $p \in \mathrm{Spec}(\mathbb{Z})$ som er supersingulær. For $p < 1000$ så er det totalt seks supersingulære primtall:

$$\big\{2, 19, 29, 199, 569, 809\big\}.$$

Det tilsvarer 0.03 % av alle primtallene under tusen. Når det kommer til gruppestrukturen, så har reduksjonen modulo 19 (av ξ), $\xi'_{/19}$, totalt tjue torsjonspunkter. Mer presist har $\xi'_{/19}$ en abelsk gruppe av $\mathfrak{o}'_2$-rasjonelle punkter som er isomorf med $\mathbb{Z}/20$. Det som her er interessant, er at $\xi'_{/19}$ har de samme fem $\mathfrak{o}'_2$-rasjonelle punktene som $\xi'_{/2}$. Disse er også 5-torsjon, men de femten andre er 20-torsjon. Dette er et interessant fenomen som også dukker opp for $\xi'_{/29}$, $\xi'_{/199}$ og så videre.

Eksempel 6.20. Vi fortsetter der eksempel 6.19 sluttet og ser på kurver over de andre heltallsringene (fortsatt $\alpha = 0$). Over $\mathfrak{o}_3$ har den elliptiske kurven, som er gitt ved likningen

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - (\zeta_3 + 1)\mathbf{x}^2 + \zeta_3\mathbf{x},$$

en supersingulær reduksjon først ved $p = 2$. Reduksjonen ξ_2' er en elliptisk kurve over restkroppen $\mathfrak{o}_3'$ med likningen

$$\mathbf{y}^2 + \mathbf{y} = \mathbf{x}^3 + (\zeta_3' + 1)\mathbf{x}^2 + \zeta_3'\mathbf{x}.$$

Denne kurven har en mengde med ni $\mathfrak{o}_3'$-rasjonelle punkter som er en abelsk gruppe isomorf med $\mathbb{Z}/3 \times \mathbb{Z}/3$.

$\mathfrak{o}_p$	P	%
$\mathfrak{o}_2$	$2, 19, 29, 199, 569, 809$	0.03
$\mathfrak{o}_3$	$2, 23, 257, 449, 509, 521, 641$	0.04
$\mathfrak{o}_5$	2	0.01
$\mathfrak{o}_7$	-	-
$\mathfrak{o}_{11}$	2	0.01
$\mathfrak{o}_{13}$	2	0.01

Table 6.9: En tabell over supersingulære primtall for $\xi/\mathfrak{o}_p$ med prosentandel.

Tabellen viser de supersingulære primtallene $p < 1000$ for $\xi/\mathfrak{o}_p$ og hvor mange prosent disse tilsvarer av totalt 168 primtall. Som vi ser har de elliptiske kurvene $\xi/\mathfrak{o}_2$ og $\xi/\mathfrak{o}_3$ mer enn ett supersingulært primtall. Kurvene $\xi/\mathfrak{o}_5$, $\xi/\mathfrak{o}_{11}$ og $\xi/\mathfrak{o}_{13}$ har kun ett supersingulært primtall. Reduksjonen $\xi_{/2}'$ har sytten $\mathfrak{o}_5'$-rasjonelle punkter, så $\#\xi_{/2}'(\mathfrak{o}_5') = 17$ og $\xi_{/2}'(\mathfrak{o}_5') \simeq \mathbb{Z}/17$. Reduksjonen $\xi_{/2}'$ over $\mathfrak{o}_{11}'$ og $\mathfrak{o}_{11}'$ respektivt har henholdsvis 1089 og 4097 punkter. Påfølgende er $\xi_{/2}'(\mathfrak{o}_{11}') \simeq \mathbb{Z}/33 \times \mathbb{Z}/33$ og $\xi_{/2}'(\mathfrak{o}_{13}') \simeq \mathbb{Z}/4097$. Kurven $\xi/\mathfrak{o}_7$ har ingen supersingulære primtall. Hvis $\mathfrak{o}_N = \mathbb{Z}[\zeta_N]$ der N er et sammensatt tall, ser vi at over $\mathfrak{o}_6$ har ξ har en supersingulær reduksjon kun ved $p = 2$. Den har også en supersingulær reduksjon ved $p = 2$ over $\mathfrak{o}_9$ og $\mathfrak{o}_{10}$, men ingen over $\mathfrak{o}_4$, $\mathfrak{o}_8$ og $\mathfrak{o}_{12}$.

Eksempel 6.21. La $\alpha = 1$. Da er $\xi/\mathfrak{o}_N$ en kubisk kurve på formen

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + \omega\mathbf{x}^2, \quad \omega = -\zeta_N^2 - \zeta_N$$

Denne er en elliptisk kurve hvis diskriminanten

$$\Delta(\xi) = -16\omega^3 - 27$$

er ulik null. Over $\mathfrak{o}_3$ er $\omega = 1$ siden

$$-\zeta_3^2 - \zeta_3 = -\left(\frac{-1+\sqrt{-3}}{2}\right)^2 - \frac{-1+\sqrt{-3}}{2} = 1,$$

og $\xi/\mathfrak{o}_3$ er en elliptisk kurve på formen

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 + \mathbf{x}^2.$$

Diskrimininanten er -43, så ξ har en dårlig reduksjon ved $p = 43$. Husk at ξ er den samme som i eksempel ??, og (43) er ikke et primideal i $\mathfrak{o}_3$. Kurven har en supersingulær reduksjon først ved $p = 2$. Reduksjonen $\xi'_{/2}$ har fem $\mathfrak{o}'_3$-rasjonelle punkter og mengden er en abelsk gruppe isomorf med $\mathbb{Z}/5$. For $p < 10^4$ er det i alt ti supersingulære primtall:

$$\{2, 1109, 1361, 2069, 2543, 3011, 5351, 6569, 7211, 9923\}$$

Dette tilsvarer 0.008 % av alle primtallene under ti tusen.

Den elliptiske kurven ξ over heltallsringen $\mathfrak{o}_5$ har diskriminant $-32\zeta_5^3 - 48\zeta_5^2 - 32\zeta_5 - 27$. Mer preist er

$$\Delta(\xi) = (-\zeta_5^3 - \zeta_5^2 - \zeta_5 - 1)(-\zeta_5^2 - \zeta_5 + 1)(-3\zeta_5^3 + 15\zeta_5^2 + 10\zeta_5 + 17).$$

Det er bare tallene $(-\zeta_5^2 - \zeta_5 + 1)$ og $(-3\zeta_5^3 + 15\zeta_5^2 + 10\zeta_5 + 17)$ som er prim i $\mathfrak{o}_5$, og ved begge disse har ξ en dårlig reduksjon. Når det kommer til supersingulære primtall, har $\xi/\mathfrak{o}_5$ en supersingulær reduksjon kun ved $p = 2$ for $p < 10^4$. Reduksjonen $\xi_{/2}/\mathfrak{o}'_5$ har totalt sytten $\mathfrak{o}'_5$-rasjonelle punkter, og denne mengden er en abelsk gruppe isomorf med $\mathbb{Z}/17$. Supersingulære primtall over andre heltallsringer er vist i følgende tabell.

$\mathfrak{o}_N$	P	%
$\mathfrak{o}_2$	$2, 5, 11, 17, 23, 29, 41, 47, 53, 59, 71, 83, 89, 101, 107, \ldots$	0.502
$\mathfrak{o}_3$	$2, 1109, 1361, 2069, 2543, 3011, 5351, 6569, 7211, 9923$	0.008
$\mathfrak{o}_4$	-	-
$\mathfrak{o}_5$	2	0.001
$\mathfrak{o}_6$	2	0.001
$\mathfrak{o}_7$	-	-
$\mathfrak{o}_8$	-	-

Table 6.10: Tabell over supersingulære primtall $p < 10^4$ for $\xi/\mathfrak{o}_N$ med prosentandel.

Eksempel 6.22. Den elliptiske kurven $\xi/\mathfrak{o}_3$ med $\alpha = \zeta_3$ er gitt ved

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 + (\zeta_3 + 2)\mathbf{x}.$$

Den har en supersingulær reduksjon først ved $p = 2$, og reduksjonen $\xi'_{/2}$ har en abelsk gruppe med fem $\mathfrak{o}'_3$-rasjonelle punkter som er isomorf med $\mathbb{Z}/5$. Kurven har også en supersingulær reduksjon ved $p = 503$, og $\xi'_{/503}$ har så mange som 254016 $\mathfrak{o}'_3$-rasjonelle punkter i en abelsk gruppe som er isomorf med $\mathbb{Z}/504 \times \mathbb{Z}/504$. Primtallene 2 og 503 er de eneste under ti tusen som er supersingulær for $\xi/\mathfrak{o}_3$. Det tilsvarer 0.002 %.

Det viser seg å være mange flere supersingulære primtall hvis ξ er definert over $\mathfrak{o}_4$. Årsaken kan være at koeffisientene ikke lenger er i $\mathfrak{o}_4$. Forøvrig er den elliptiske kurven ξ definert over $\mathbb{Z} \subset \mathbb{Q}$ med likningen

$$\mathbf{y}^2 - \mathbf{y} = \mathbf{x}^3 - 2\mathbf{x}^2 + 2\mathbf{x}.$$

Diskriminanten er -443, så kurven har en dårlig reduksjon ved $p = 443$. Nå, den elliptiske kurven ξ har ikke en supersingulær reduksjon ved $p = 2$. Over $\mathfrak{o}_4$ er (2) dessuten ikke et primideal, siden det kan skrives som $(\zeta_4 + 1)^2$. For $p < 10^3$ er det i alt syv supersingulære primtall og det første er $p = 107$. Reduksjonen $\xi'_{/107}$ over restkroppen $\mathfrak{o}'_4$ har 11664 rasjonelle punkter i en abelsk gruppe som er isomorf med $\mathbb{Z}/108 \times \mathbb{Z}/108$.

Referanser

[1] Artin, E. (1924). Quadratische Körper im Gebiete der höheren Kongruenzen. I. Arithmetischer Teil. *Mathematische Zeitschrift*, *19*(1), 153-206.

[2] Burchnall, J. L., & Chaundy, T. W. (1928). Commutative ordinary differential operators. *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, *118*(780), 557-583.

[3] Festi, D. (2018). *Notes on elliptic curves*.

[4] Friedl, S. (2017). An elementary proof of the group law for elliptic curves. *Groups Complexity Cryptology*, *9*(2), 117-123.

[5] Fujii, K., & Oike, H. (2017). An algebraic proof of the associative law of elliptic curves. *Advances in Pure Mathematics*, *7*(12), 649-659.

[6] Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge University Press. (s. 165-200).

[7] Hasse, H. (1936). Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung.

[8] Kline, D. (2016). *Elliptic Curves and Cryptography*.

[9] Larsson, D. (2014). Burchnall-Chaundy theory, Ore extensions and σ-differential operators. *Journal of Algebra and Its Applications*, *13*(07), 1450049.

[10] The LMFDB Collaboration. (2023). *Isomorphism between Weierstrass models (reviewed)*, `https://www.lmfdb.org/knowledge/show/ec.weierstrass_isomorphism`, [Online; accessed 10 May 2023]

[11] Mazur, B. (1977). Modular curves and the Eisenstein ideal. *Publications Mathématiques de l'IHÉS, 47*, 33-186.

[12] Mazur, B., & Goldfeld, D. (1978). Rational isogenies of prime degree. *Inventiones mathematicae, 44*, 129-162.

[13] Mordell, L. J. (1922). On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. London Math. Soc.*, 21, 179–192.

[14] Nguyen, N. P. (2019). A Note on Cyclotomic Integers. *The American Mathematical Monthly*, *126*(2), 168-172.

[15] SageMath, the Sage Mathematics Software System (Version 9.7), The Sage Developers, 2023, `https://www.sagemath.org`.

[16] Schoof, R. (1985). Elliptic curves over finite fields and the computation of square roots mod *p*. *Mathematics of computation*, *44*(170), 483-494.

[17] Schoof, R. (1995). Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, *7*(1), 219-254.

[18] Silverman, J. H., & Tate, J. T. (1994). *Rational Points on Elliptic Curves*. Springer Science & Business Media.

[19] Weil, A. (1928). *L'arithmétique sur les courbes algébriques.* Acta Math. 52, 281-315.

Vedlegg

Alle de sentrale Sage-programmene presentert her, ble brukt til å studere de elliptiske kurvene i kapittel 6.

Antakelig det mest interessante er hvordan vi beregnet en stor mengde med supersingulære primtall for en gitt kurve, så vi begynner der. Programmet bruker en *for*-løkke som for hvert primtall i en mengde sjekker hvilket som er gir en god reduksjon. Deretter sjekker det om primtallet er supersingulær. Hvis det er et supersingulært primtall, legges dette i en liste som til slutt skrives ut. Hvis primtallet ikke er supersingulært (eller gir en god reduksjon), blir neste primtall sjekket i stedet.

```
E = EllipticCurve([0,-19,-1,83,0])

def supersing_red():
    lst = []
    for p in prime_range(100):
        if E.has_good_reduction(p) == True:
            if E.reduction(p).is_supersingular() == True:
                lst.append(p)
            else:
                pass
        else:
            pass
    return lst

print(supersing_red())
```

```
[2, 47]
```

Figur 6.1: Supersingulære reduksjoner (primtall).

Programmet som beregner supersingulære primtall over syklotomiske og kvadratiske kropper er formmessig det samme. Eneste og viktigste forskjell er at programmet må sørge for at primtallet p er et primideal. Hvis ikke er det ikke mulig å redusere kurven ved p.

```
Q.<q> = CyclotomicField(3)
a = q
E = EllipticCurve(Q, [0,(2 + q)*(a - q) - 2,-1,(1 - a)*(1 + q)*(1 + q -
a),0])

def cyclo():
    lst = []
    for p in prime_range(10000):
        if Q.ideal(p).is_prime() == True:
            if E.has_good_reduction(p):
                if E.reduction(p).is_supersingular():
                    lst.append(p)
                else:
                    pass
            else:
                pass
        else:
            pass
    return len(lst), lst

print(cyclo(), E)
```

```
(2, [2, 503]) Elliptic Curve defined by y^2 + (-1)*y = x^3 + (-2)*x^2 +
(q+2)*x over Cyclotomic Field of order 3 and degree 2
```

Figur 6.2: Supersingulære reduksjoner (primtall) over heltallsringen $\mathbb{Z}[\zeta_3]$.

```
Q.<q> = QuadraticField(7)
a = q
E = EllipticCurve(Q, [0,(2 + q)*(a - q) - 2,-1,(1 - a)*(1 + q)*(1 + q -
a),0])

def cyclo():
    lst = []
    for p in prime_range(10000):
        if Q.ideal(p).is_prime() == True:
            if E.has_good_reduction(p):
                if E.reduction(p).is_supersingular():
                    lst.append(p)
                else:
                    pass
            else:
                pass
        else:
            pass
    return len(lst), lst

print(cyclo(), E)
```

```
(5, [11, 67, 191, 593, 5669]) Elliptic Curve defined by y^2 + (-1)*y =
x^3 + (-2)*x^2 + (-6)*x over Number Field in q with defining polynomial
x^2 - 7 with q = 2.645751311064591?
```

Figur 6.3: Supersingulære reduksjoner (primtall) over heltallsringen $\mathbb{Z}[\sqrt{7}]$.

På liknende måte sjekker følgende program hvilke kurver som har en torsjonsorden større enn én. Dette programmet ble blant annet brukt i eksempel 6.4 og 6.5.

```
def torsion():
    lsttor = []
    for q in range(-1000,1000):
        E = EllipticCurve([0,-2,-1,1 - q^2, 0])
        if E.torsion_order() != 1:
            lsttor.append(q)
        else:
            pass
    return lsttor
print(torsion())
```

```
[]
```

Figur 6.4: Torsjonsorden.

I eksempel 6.6 og 6.7 brukte vi følgende program til skrive ut *supersingulære* α.

```
def a():
    lsta = []
    for a in range(-1000,1000):
        p = 5
        Ea = EllipticCurve([0,a - 1,-1,0,0])
        if Ea.has_good_reduction(p) == True:
            if Ea.reduction(p).is_supersingular() == True:
                lsta.append(a)
            else:
                pass
        else:
            pass
    return lsta

print(a())
```

Vi brukte også mindre program til å kontrollere forskjellige resultat. De fleste er allerede godt innebygd i Sage. For å finne den korte Weierstrassformen av en elliptisk kurve brukte vi

```
E = EllipticCurve([0,-19,-1,83,0])
Ew = E.short_weierstrass_model(); Ew
```

```
Elliptic Curve defined by y^2 = x^3 - 48384*x + 832464 over Rational
Field
```

For å sjekke at to elliptiske kurver er isomorfe, brukte vi

```
Q3.<i> = CyclotomicField(3)
a = i
E3 = EllipticCurve(Q3, [0,(2 + i)*(a - i) - 2,-1,(1 - a)*(1 + i)*(1 + i
- a),0]); print(E3)

Q6.<j> = CyclotomicField(6)
a = j
E6 = EllipticCurve(Q6, [0,(2 + j)*(a - j) - 2,-1,(1 - a)*(1 + j)*(1 + j
- a),0]); print(E6)

E3.is_isomorphic(E6)
```

```
Elliptic Curve defined by y^2 + (-1)*y = x^3 + (-2)*x^2 + (i+2)*x over
Cyclotomic Field of order 3 and degree 2
Elliptic Curve defined by y^2 + (-1)*y = x^3 + (-2)*x^2 + (-j+2)*x over
Cyclotomic Field of order 6 and degree 2

False
```

Når to elliptiske kurver er isomorfe, vil vi ofte finne isomorfien ϕ. Her er isomorfien mellom en kurve ξ og den korte Weierstrassformen ξ_W gitt ved

```
Q.<q> = CyclotomicField(3)
a = q
E = EllipticCurve(Q, [0,(2 + q)*(a - q) - 2,-1,(1 - a)*(1 + q)*(1 + q -
a),0])

Ew = E.short_weierstrass_model()

iso = E.isomorphism_to(Ew); iso
```

```
Elliptic-curve morphism:
  From: Elliptic Curve defined by y^2 + (-1)*y = x^3 + (-2)*x^2 + (q+2)*x
over Cyclotomic Field of order 3 and degree 2
  To:   Elliptic Curve defined by y^2 = x^3 + (1296*q+864)*x +
(31104*q+46224) over Cyclotomic Field of order 3 and degree 2
  Via:  (u,r,s,t) = (1/6, 2/3, 0, 1/2)
```

og den rasjonelle substitusjonen er gitt ved

```
iso.rational_maps()
```

```
(36*x - 24, 216*y - 108)
```