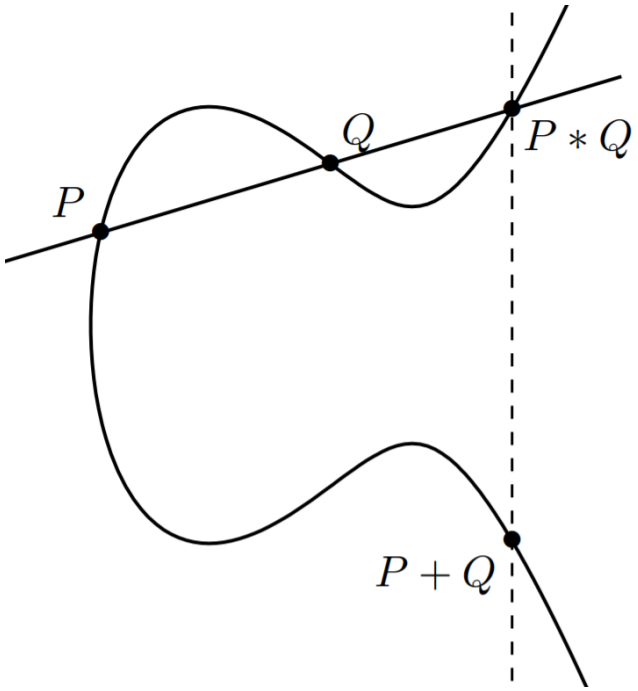
Bacheloroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for matematiske fag

Ole Martin Edstrøm

Elliptiske kurver over de rasjonale tallene

Bacheloroppgave i matematiske fag
Veileder: Petter Andreas Bergh
Mai 2020



NTNU
Kunnskap for en bedre verden

Ole Martin Edstrøm

Elliptiske kurver over de rasjonale tallene

Bacheloroppgave i matematiske fag
Veileder: Petter Andreas Bergh
Mai 2020

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for matematiske fag

NTNU

Kunnskap for en bedre verden

SAMMENDRAG. Formålet med denne oppgaven er å se på elliptiske kurver over de rasjonale tallene, for så å bygge opp en gruppestruktur av de rasjonale punktene på en elliptisk kurve. Videre vil oppgaven ta for seg og bevise to av de mest sentrale teoremene innenfor temaet elliptiske kurver: (1) Nagell-Lutz Teorem, som gir en måte å finne alle punkter av endelig orden på en elliptisk kurve; (2) Mordells Teorem, som sier at gruppen av rasjonale punkter på en elliptisk kurve er endelig generert.

Forord

Denne oppgaven er skrevet fra januar til mai 2020, med veiledning fra Petter Andreas Bergh ved institutt for matematiske fag NTNU. Denne oppgaven markerer slutten på en treårig lang bachelorgrad i matematiske fag.

Jeg har lyst til å takke Bergh for å ha hjulpet med å velge dette temaet til oppgaven, og for hele tiden å ha vært rask til å svare når jeg har lurt på noe. Temaet har vært spendene ved at jeg har måttet sette meg inn i et fagfelt jeg ikke har sett før, for så å bruke det til å vise ting i fagfelt jeg interesserer meg i fra før av.

Til slutt vil jeg gi en stor takk til studievenner og Linjeforeningen Delta for å ha gjort studietiden min i Trondheim til mine 3 beste år så langt.

Innhold

KAPITTEL 1

Innledning

I 1901 kom Henri Poincaré i [**4**] med formodningen om at alle ikkesingulære kubiske likninger av to variabler har en endelig mengde med rasjonale løsninger, som kan brukes for å generere alle de rasjonale løsningene til den samme likningen ved å bruke en geometrisk formel. Det var Louis J. Mordell i [**3**] som beviste denne formodningen i 1922 ved å bruke elliptiske kurver. Vi skall bevise en litt mindre generell versjon av Mordells Teorem, men på samme måte som han gjorde det. I kapittel 2 vil vi introdusere litt projektiv geometri, som vi kommer til å bruke i kapittel 3 for å introdusere elliptiske kurver, og bevise gruppestrukturen av punkter på en elliptisk kurve. I kapittel 4 kommer vi til å gi et bevis for Nagell-Lutz Teorem. I kapittel 5 og 6 kommer vi til å bevise Mordells Teorem for elliptiske kurver med minst ett rasjonalt punkt med orden to.

KAPITTEL 2

Litt projektiv geometri

I dette kapittelet kommer vi til å gi en liten introduksjon i projektiv geometri. Dette kommer til å bli nyttig når vi skal konstruere gruppen av punkter på en elliptisk kurve og for å rettferdigjøre gruppeopperasjonen dens.

1. Det projektive plan

DEFINISJON 2.1. La k være en algebraisk lukket kropp. Vi definerer det n-dimensjonale affine rommet $\mathbb{A}^n$ til å være alle kombinasjoner av n-tupler fra k.

For å definere det projektive rom $\mathbb{P}^n$ trenger vi først en ekvivalensrelasjon $\sim$ på $\mathbb{A}^{n+1}$. Vi sier at $(x_0, x_1, ..., x_n) \sim (y_0, y_1, ..., y_n)$ hvis

$$(y_0, y_1, ..., y_n) = (tx_0, tx_1, ..., tx_n)$$

for en $t \in k\backslash\{0\}$.

Og med denne ekvivalensrelasjonen er vi klare til å definere det projektive rom.

DEFINISJON 2.2. La $\mathbb{A}^{n+1}$ være det $(n+1)$-dimensjonale affine rom over k og la $\sim$ være ekvivalensrelasjonen definert som over. Da definerer vi det n-dimensjonale projektive rommet som $\mathbb{P}^n = (\mathbb{A}^{n+1}\backslash\{0\})/\sim$.

Vi kommer hovedsaklig til å jobbe med det tillfellet hvor $n = 2$, altså $\mathbb{P}^2$ som er det projektive plan. Vi kommer også til å jobbe med $\mathbb{A}^2$ som kommer til å bli kalt det affine plan.

Vi skal også se på en annen ekvivalent definisjon av det projektive plan, den geometriske tolkningen: $\mathbb{A}^2 \cup \mathbb{P}$. Denne måten å se på det, er det vanlige affine plan, sammen med den projektive linjen som består av alle punkter i uendelig. Hvor med et punkt i uendlig menes det punktet der hvor to paralelle linjer skjærer hverandre.

Disse to tolkningene av det projektive plan er ekvivalente, med det mener vi at det eksisterer en bijeksjon mellom dem. Det er den bijeksjonen som er vist i Figur 2.1.

$\mathbb{P}^2$		$\mathbb{A}^2 \cup \mathbb{P}$
$[a,b,c]$	$\longrightarrow$	$\begin{cases} (\frac{a}{c}, \frac{b}{c}) \in \mathbb{A}^2, \text{hvis } c \neq 0 \\ [a,b] \in \mathbb{P}, \text{hvis } c = 0 \end{cases}$
$[x,y,1]$	$\longleftarrow$	$(x,y) \in \mathbb{A}^2$
$[a,b,0]$	$\longleftarrow$	$[a,b] \in \mathbb{P}$

FIGUR 2.1. En beskrivelse av avbildningen av punkter mellom $\mathbb{P}^2$ og $\mathbb{A}^2 \cup \mathbb{P}$

Videre ønsker vi å studere linjer i det projektive plan, og hvordan disse korresponderer med linjer i $\mathbb{A}^2 \cup \mathbb{P}$. En linje i $\mathbb{P}^2$ vil være alle punkter $[a,b,c] \in \mathbb{P}^2$ som for gitte $\alpha, \beta, \gamma \in k$ tilfredsstiller likningen

$$L: \ \alpha X + \beta Y + \gamma Z = 0.$$

Vi ser også at hvis $X = a, \ Y = b, \ Z = c$ er en løsning på likningen impliserer det at $X = ta, \ Y = tb, \ Z = tc$ også er en løsning. Og dette er akkurat det vi ønsker ettersom $[a,b,c] = [ta,tb,tc]$ i $\mathbb{P}^2$, og vil dermed bli regnet med som samme løsning av likningen. Dette fører til at så lenge $c \neq 0$ så er $[a,b,c] = [\frac{a}{c}, \frac{b}{c}, 1]$, som betyr at for å se på alle unike punkter på en linje, er det nok å se på de der $c = 1$ eller der $c = 0$.

Hvis vi antar at ikke både $\alpha = 0$ og $\beta = 0$, ser vi at hvis vi har et punkt $[a,b,1] \in L$, så vil dette punktet korrespondere med punktet $(a,b) \in \mathbb{A}^2 \cup \mathbb{P}$. Vi kan også se at det vil eksistere én løsning av likningen hvor $Z = 0$. La oss si punktet $[x_0, y_0, 0]$, dette vil korrespondere med punktet $[x_0, y_0] \in \mathbb{A}^2 \cup \mathbb{P}$. Og til slutt kan vi konkludere med at linjen $L: \ \alpha X + \beta Y + \gamma Z = 0$ i $\mathbb{P}^2$ vil korrespondere med linjen bestående av alle punkter $(x,y) \in \mathbb{A}^2$ som er løsninger av likningen $\alpha x + \beta y + \gamma = 0$ sammen med et punkt $[x_0, y_0] \in \mathbb{P}$, som er punktet linjen krysser i uendelig.

Da er det bare en linje vi mangler å studere, nemlig i det tilfelle hvor både $\alpha = 0$ og $\beta = 0$. Som da blir linjen $Z = 0$. Denne vil bestå av alle punkter på formen $[a,b,0]$, så linjen $Z = 0$ vil korrespondere med linjen $\mathbb{P} \subseteq \mathbb{A}^2 \cup \mathbb{P}$. Som er linjen av alle punkter i uendelig.

2. Kurver i det projektive plan

Når vi skal studere kurver i det projektive planet ønsker vi at hvis vi har en kurve $C: \ F(X,Y,Z) = 0$, hvor $[a,b,c]$ er en løsning, så vil vi at $[ta,tb,tc]$ også skal være en løsning. Derfor kommer vi til å studere det som kalles homogene kurver i det projektive planet, som vi definerer på følgende vis.

DEFINISJON 2.3. En homogen kurve av grad $d \geq 1$ i det projektive plan er en kurve $C: \ F(X,Y,Z) = 0$, hvor $F(tX,tY,tZ) = t^d F(X,Y,Z)$ for alle $t \in k \backslash \{0\}$, og det eksisterer minst et punkt $[a,b,c] \in \mathbb{P}^2$ slik at $F(a,b,c) \neq 0$.

Denne definisjonen er ekvivalent med å si at $F(X,Y,Z) = 0$ er en homogen kurve av grad d hvis F kun består av ledd på formen $a_{ij}X^iY^jZ^k$, hvor $i+j+k = d$, $i,j,k \geq 0$, og ikke alle $a_{ij} = 0$.

Vi ønsker også en måte å kunne se på homogene kurver i det projektive plan i det affine plan i tillegg. Fra definisjonen på en homogen kurve får vi

$$F(a,b,c) = c^d F\left(\frac{a}{c}, \frac{b}{c}, 1\right), \text{hvis } c \neq 0.$$

Dette impliserer at hvis vi ser på kurven $K: \ f(x,y) = F(x,y,1) = 0$ i $\mathbb{A}^2$, så vil alle punktene på K svare til alle punktene C hvor $Z \neq 0$. Punktene på formen $[a,b,0]$, som er en løsning av likningen $F(X,Y,0) = 0$ blir sendt til de punktene der K skjærer linjen av punkter i uendelig.

Hvis vi har en kurve i $\mathbb{A}^2 \cup \mathbb{P}$ av grad $d \geq 1$ gitt ved

$$K: \ f(x,y) = \sum_{i=0}^{d} \sum_{j=0}^{d-i} a_{ij}x^iy^j = 0,$$

så vil denne kurven bli sendt til kurven i $\mathbb{P}^2$ gitt ved likningen

$$F(X,Y,Z) = \sum_{i=0}^{d} \sum_{j=0}^{d-i} a_{ij}X^iY^jZ^{d-i-j} = 0.$$

Det man fort legger merke til er at disse to måtene å sende kurver mellom $\mathbb{P}^2$ og $\mathbb{A}^2 \cup \mathbb{P}$ er inverser til hverandre.

Da er det bare ett spørsmål vi mangler å svare på før vi kan starte å se på elliptiske kurver: hvor mange ganger skjærer to kurver av grad d_1 og d_2 hverandre? Dette besvares i Bezouts Teorem som han viste i [**1**]. Dette teoremet er et av de mest fundamentale teoremene innenfor projektiv geometri. Vi kommer til å nevne dette teoremet uten bevis.

THEOREM 2.4 (Bezouts Teorem). *La C_1 og C_2 være to kurver i det projektive plan av grad d_1 og d_2, som ikke har noen felles komponenter. Da vil man få følgende likhet*

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = d_1 d_2,$$

hvor $I(C_1 \cap C_2, P)$ er multiplisiteten til skjæringspunktet mellom C_1 og C_2 i P.

KAPITTEL 3

Elliptiske kurver

I dette kapittelet skal vi først vise at det holder å se på kubiske likninger på en spesiell form for å bevise Mordells Teorem. Deretter kommer vi til å bygge opp en binæroperasjon mellom punktene på denne kurven, for å så vise at disse danner en abelsk gruppe.

1. Weierstrass normal form

I kapittel 2 så vi at hvis vi har en kurve av grad tre i $\mathbb{A}^2 \cup \mathbb{P}$, så har vi en måte å finne en korresponderende kurve i $\mathbb{P}^2$, nemlig,

$$C : 0 = F(X,Y,Z) = a_1Y^3 + a_2Y^2X + a_3Y^2Z + a_4YX^2 + a_5YXZ \\ + a_6YZ^2 + a_7X^3 + a_8X^2Z + a_9XZ^2 + a_{10}Z^3.$$

Vi ønsker å vise at hvis vi har en rasjonal kurve av grad tre som ikke har en linje som komponent, sammen med et rasjonalt punkt $\mathcal{O}$ på kurven, så kan vi gjøre et bytte av koordinater slik at vi får kurven på en penere form. Denne måten å skrive kurven på er det som kalles Wierstrass normal form. Derfor noterer vi oss først at en rasjonal kurve av grad tre er en kurve på samme form som over, hvor $a_i \in \mathbb{Q}$ for $i = 1, 2, ..., 10$, og ikke alle $a_i = 0$.

Vi kommer til å dele det opp i to tilfeller; det hvor $\mathcal{O}$ er et vendepunkt på kurven, og det hvor $\mathcal{O}$ ikke er det.

Først ser vi på tilfellet der $\mathcal{O}$ er et vendepunkt, dette vil si at tangenten til C i $\mathcal{O}$ har skjæringspunkt med multiplisitet 3. I dette tilfelle velger vi akser slik at $\mathcal{O} = [0,1,0]$ og at det er linjen $Z = 0$ som tangerer C i $\mathcal{O}$. Vi velger $X = 0$ som hvilken som helst linje som skjærer C i $\mathcal{O}$, men som ikke er $Z = 0$, og vi lar $Y = 0$ være en linje som ikke skjærer C i $\mathcal{O}$.
Hvis vi da setter in $Z = 0$ i uttrykket for C, får vi

$$F(X,Y,0) = a_1Y^3 + a_2Y^2X + a_4YX^2 + a_7x^3.$$

Ettersom dette uttrykket skal ha et nullpunkt av multiplisitet 3 i $[0,1,0]$ får vi at $a_1 = a_2 = a_4 = 0$. Da står vi igjen med et uttrykk for kurven på formen

$$a_1Y^2Z + a_2YXZ + a_3YZ^2 + a_4X^3 + a_5X^2Z + a_6XZ^2 + a_7Z^3 = 0.$$

Vidre mulipliserer vi begge sider med $1/a_1$, og får kurven på formen

$$Y^2Z + a_1YXZ + a_2YZ^2 + a_3X^3 + a_4X^2Z + a_5XZ^2 + a_6Z^3 = 0.$$

Deretter flytter vi kurven til det affine plan, hvor vi også flytter alle leddene med kun x som variabel over på høyre side av likhetstegnet slik at vi får en kurve på formen

$$y^2 + a_1xy + a_2y = a_3x^3 + a_4x^2 + a_5x + a_6.$$

Og til slutt substituerer vi y med $y - \frac{a_1}{2}x - \frac{a_2}{2}$ uten tap av punkter på kurven og får kurven til å være på formen

$$y^2 - \left(\frac{a_1}{2}x\right)^2 - \frac{a_1a_2}{2}x + \frac{b^2}{4} = a_3x^3 + a_4x^2 + a_5x + a_6.$$

Ettersom y^2 er det eneste leddet som ikke kun har x som variabel kan vi flytte over og får kurven på formen vi ønsker, som er

$$C: \ y^2 = a_3x^3 + a_2x^2 + a_1x + a_0.$$

Deretter ser vi på det tilfellet hvor $\mathcal{O}$ ikke er et vendepunkt, dette vil si at tangenten i $\mathcal{O}$ skjærer C med en multiplisitet på 2. I dette tilfelle velger vi koordinater slik at $\mathcal{O} = [1, 0, 0]$ og at tangenten til C i $\mathcal{O}$ er linjen $Z = 0$. Fra Teorem 2.4 får vi at linjen $Z = 0$ vil skjære C i et punkt til, og ettersom C og $Z = 0$ er to rasjonale kurver med et rasjonalt skjæringspunkt av multiplistet 2, så vil det siste skjæringspunktet også være et rasjonalt punkt. Derfor kan vi videre velge akser slik at $Z = 0$ har sitt andre skjæringspunkt i $P = [0, 1, 0]$, og slik at linjen $X = 0$ tangerer C i P. Til slutt velger vi linjen $Y = 0$ til å være hvilken som helst linje som går igjennom $\mathcal{O}$ og som ikke er $Z = 0$.
I likhet med forrige tilfelle, setter vi $Z = 0$ inn i uttrykket for C, og får

$$F(X, Y, 0) = a_1Y^3 + a_2Y^2X + a_4YX^2 + a_7x^3.$$

Ettersom $F(X, Y, 0)$ skal ha et nullpunkt med multiplisitet 2 i $\mathcal{O}$, får vi at

$$a_4 = a_7 = 0.$$

Hvis vi deretter setter inn $X = 0$ i utrykket for C får vi at

$$F(0, Y, Z) = a_1Y^3 + a_3Y^2Z + a_6YZ^2 + a_{10}Z^3,$$

som skal ha et nullpunkt med multiplisitet ≥ 2 i punktet $P = [0, 1, 0]$. Fra dette får vi at $a_1 = a_3 = 0$. Da har vi et uttrykk for kurven C på formen

$$a_1Y^2X + a_2YXZ + a_3YZ^2 + a_4X^2Z + a_5xZ^2 + a_6Z^3 = 0.$$

I likhet med når $\mathcal{O}$ var et vendepunkt, mulipliserer vi begge sider med $1/a_1$, flytter kurven til det affine plan og flytter alle ledd som ikke avhenger av y over på høyre side av likhetstegnet og får et utrykk på formen

$$y^2x + (a_1x + a_2)y = a_3x^2 + a_4x + a_5.$$

Deretter multipliserer vi begge sider med x og setter $y = yx$, og får et uttrykk på formen

$$y^2 + (a_1x + a_2)y = a_3x^3 + a_4x^2 + a_5x.$$

Til slutt gjør vi en substitusjon av y med $y - \frac{1}{2}(a_1x + a_2)$ og ganger ut, så får vi

$$y^2 - \frac{1}{4}(a_1x + a_2)^2 = a_3x^3 + a_4x^2 + a_5x.$$

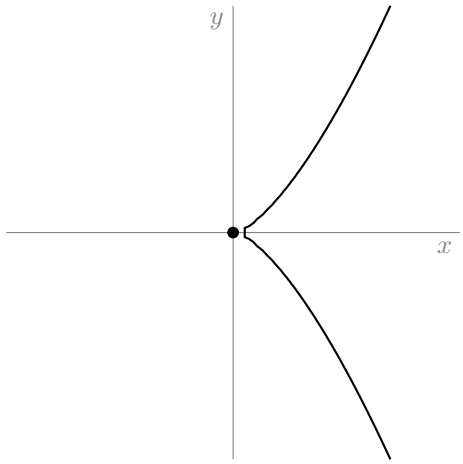
Og igjen har vi fått kurven slik vi ønsker, med y^2 som eneste ledd avhengig av y. Så da kan vi igjen flytte over og få C på formen

$$C: \ y^2 = a_3x^3 + a_2x^2 + a_1x + a_0.$$

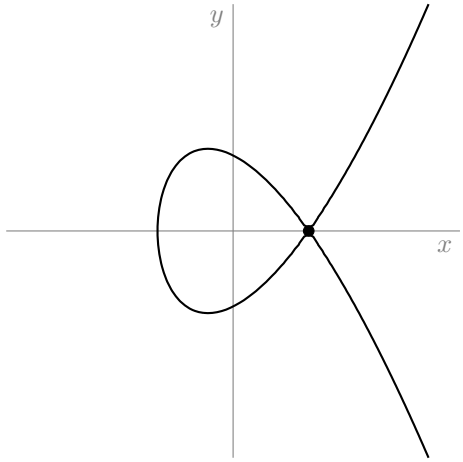
For å bli kvitt a_3 kan vi gjøre et variabelskifte til, hvor vi setter $x = \frac{x}{a_3}$ og $y = \frac{y}{a_3}$, så multipliserer vi begge sider med a_3^2 og får kurven på Weierstrass normal form

$$y^2 = x^3 + ax^2 + bx + c, \quad \text{hvor } a, b, c \in \mathbb{Q}.$$

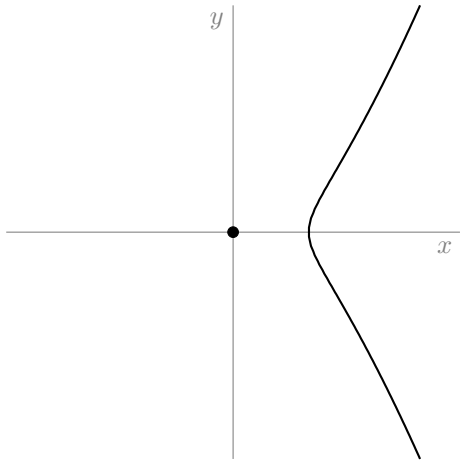
I Figur 3.1, 3.2 og 3.3 ser vi tre eksempler på det som kalles singulære kurver. Vi sier at en kurve $K: \ f(x, y) = 0$ er singulær hvis $f(y, x)$ deler et nullpunkt med begge sine prtiellderiverte. Når kurven K er på Weierstrass normal form vil dette være når $f(x)$ og $f'(x)$ har en felles rot, eller ekvivalent sagt hvis $f(x)$ har en rot av orden større eller lik 2.



FIGUR 3.1. Singulær kurve med rot av orden tre: $y^2 = x^3$



FIGUR 3.2. Singulær kurve som krysser seg selv: $y^2 = (x-1)^2(x+1)$

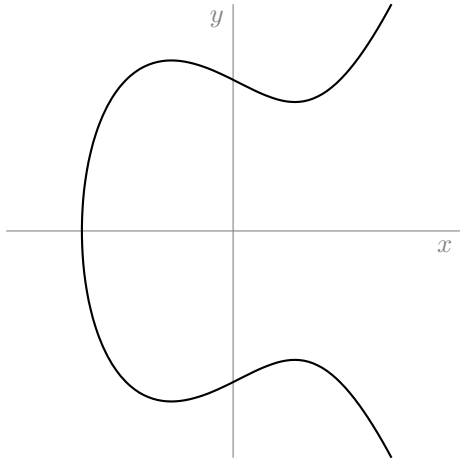


FIGUR 3.3. Singulær kurve med eksternt punkt fra kurven med rot av orden tre: $y^2 = x^2(x-1)$

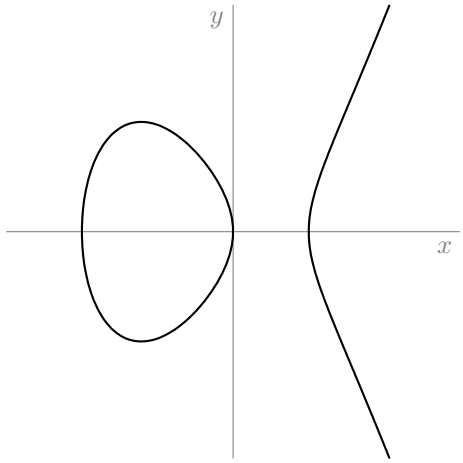
Vi kommer ikke til å studere singulære kurver, vi kommer til å studere det som kalles elliptiske kurver, som vi definerer på følgende måte.

DEFINISJON 3.1. Vi kaller en kurve $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ av grad tre på Weierstrass normal form for en elliptisk kurve over de rasjonale tallene, hvis a, b og c er rasjonale tall og $f(x)$ har tre distinkte komplekse røtter.

I Figur 3.4 og 3.5 ser vi to vanlige eksempler på rasjonale elliptiske kurver.



FIGUR 3.4. Elliptisk kurve med én rasjonal rot: $y^2 = x^3 - 2x + 4$



FIGUR 3.5. Elliptisk kurve med tre rasjonale røtter: $y^2 = x^3 + x^2 - 2x$

Legg merke til at hvis vi har en elliptisk kurve $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ over de rasjonale tallene, kan vi gjøre et bytte av koordinater ved å sette $y = d^3y$ og $x = d^2x$, hvor d er produktet av nevnerne i de rasjonale tallene a, b og c, så får vi

$$y^2 = x^3 + d^2ax^2 + d^4bx + d^6c.$$

Fra dette ser vi at hvis vi har en elliptisk kurve over de rasjonale tallene, så kan vi gjøre den om på formen

$$E : \ y^2 = x^3 + ax^2 + bx + c, \quad \text{hvor } a, b, c \in \mathbb{Z}.$$

Dettte viser at det kommer alltid til å være greit å anta at en elliptisk kurve over de rasjonale tallene har heltalls koeffisienter.

Hvis vi nå har en elliptisk kurve E og flytter den til det projektive plan, da får vi

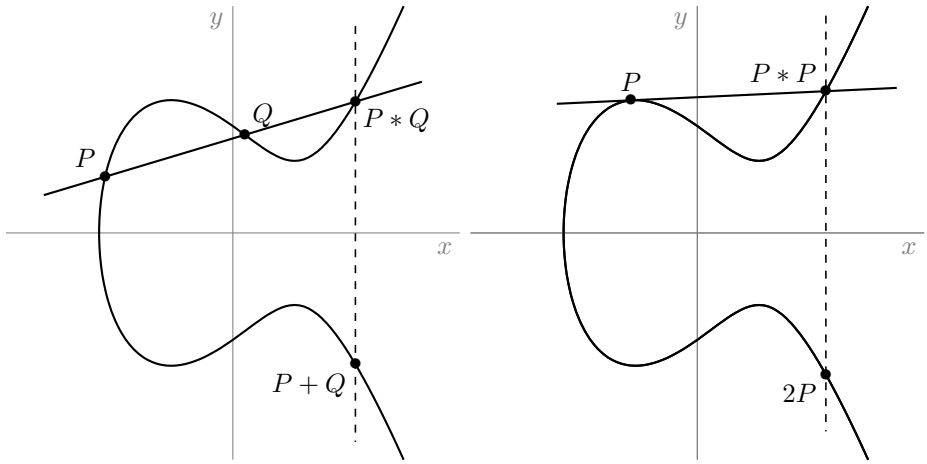
$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

Hvis vi plotter in $Z = 0$ for å se hvor kurven vår skjærer linjen av punkter i undelig får vi $X^3 = 0$. Dette vil si at E kun skjærer et punkt i uendelig, nemlig $\mathcal{O} = [0, 1, 0]$ og dette er også et vendepunkt på kurven, siden det har multiplisitet 3.

2. Addisjon av punkter

DEFINISJON 3.2. La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve over de rasjonale tallene, og la $\mathcal{O}$ være punket på kurven i uendelig. La deretter P og Q være to punkter på E. Vi definerer punktet $P * Q$ til å være det tredje skjeringspunktet mellom E og linjen som går igjennom P og Q. $P * P$ er definert som det siste punktet på linjen som tangerer E i P. Vi definerer deretter bineroperasjonen + ved at $P + Q = \mathcal{O} * (P * Q)$.

Vi ser en visualisering av hvordan punkter adderes på en elliptisk kurve i Figur 3.6 og 3.7.



FIGUR 3.6. Addisjon av punkter på en elliptisk kurve

Vi starter med å se på uttrykket $\mathcal{O} + \mathcal{O} = \mathcal{O} * (\mathcal{O} * \mathcal{O})$. Vi så at $\mathcal{O}$ er et vendepunkt på den elliptiske kurven, så vil tangenten i $\mathcal{O}$ kun skjære kurven i $\mathcal{O}$, som impliserer at $\mathcal{O} * \mathcal{O} = \mathcal{O}$, som betyr at $\mathcal{O} + \mathcal{O} = \mathcal{O}$.

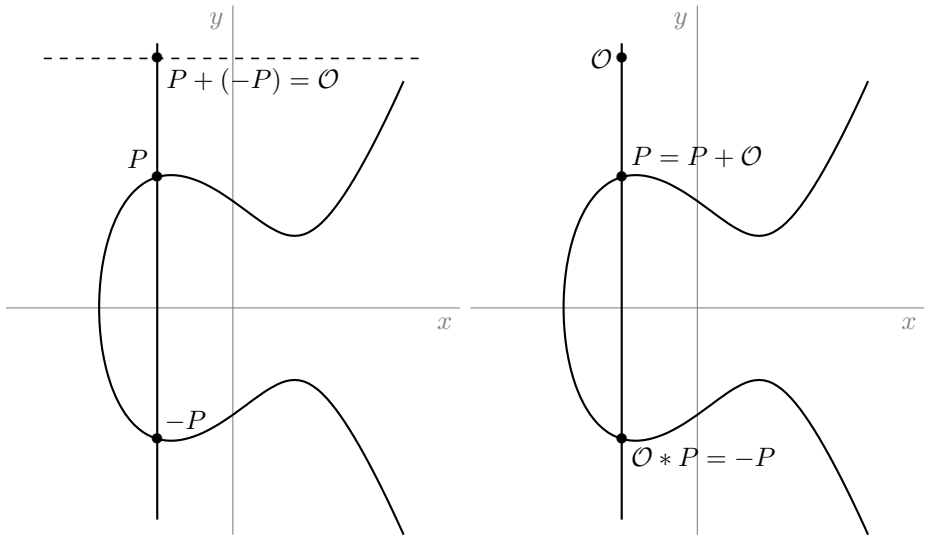
La nå $P = (x_1, y_1)$ være et punkt på E som er ulik $\mathcal{O}$. Da ser vi at punktet $(x_1, -y_1)$ også vil ligge på E, la oss kalle det for $-P$. Hvis vi nå ser på linjen $x = x_1$ så ser vi at denne går igjennom både P og $-P$, og hvis vi flytter linjen til $\mathbb{P}^2$ får

vi linjen $X = x_1 Z$, som også skjærer igjennom punktet $\mathcal{O} = [0, 1, 0]$, fra dette kan vi regne ut de to uttrykkene

$$P + (-P) = \mathcal{O} * (P * (-P)) = \mathcal{O} * \mathcal{O} = \mathcal{O},$$

og

$$\mathcal{O} + P = \mathcal{O} * (\mathcal{O} * P) = \mathcal{O} * (-P) = P.$$



FIGUR 3.7. Ilustrasjon av $P + (-P) = (x, y) + (x, -y) = \mathcal{O}$ og $P + \mathcal{O} = P$ på en elliptisk kurve

Hvis vi sier at $-\mathcal{O} = \mathcal{O}$, $-(x, y) = (x, -y)$ og lar Q være et punkt på E så kan vi se at

$$P + Q = \mathcal{O} * (P * Q) = -(P * Q).$$

Og nå gjenstår det bare å finne et uttrykk for $P + Q$ når $P \neq \mathcal{O}$, $Q \neq \mathcal{O}$, og $Q \neq -P$. Vi uttrykker linjen som går igjennom punktene $P = (x_1, y_1)$, $Q = (x_2, y_2)$ og $P * Q = (x_3, y_3)$ med likningen

$$y = \lambda x + \nu. \tag{1}$$

Dermed får vi at linjen og E skjærer hverandre når

$$(\lambda x + \nu)^2 = x^3 + ax^2 + bx + c,$$

som vi ganger ut og flytter alt over på høyre side og får

$$0 = x^3 + (a - \lambda^2)x^2 + (b + 2\lambda\nu)x + (c - \nu^2).$$

Dette tredjegradspolynomet vil ha sine tre røtter i x_1, x_2 og x_3, som vil si at

$$\begin{aligned} & x^3 + (a - \lambda^2)x^2 + (b + 2\lambda\nu)x + (c - \nu^2) \\ = \quad & (x - x_1)(x - x_2)(x - x_3) \\ = \quad & x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned}$$

Hvis vi ser på koeffisientene forran andregradsleddene får vi at

$$(a - \lambda^2) = -(x_1 + x_2 + x_3),$$

som impliserer at

$$x_3 = \lambda^2 - x_1 - x_2 - a.$$

Ved å sette x_1 og y_1 inn i utrykk (1) for linjen gjennom P og Q får vi at $y_1 = \lambda x_1 + \nu$, som impliserer at

$$\nu = y_1 - \lambda x_1.$$

Videre ved å sette in x_3 og y_3 i uttrykk (1) for linjen ser vi at

$$y_3 = \lambda x_3 + \nu,$$

som impliserer at

$$y_3 = \lambda(x_3 - x_1) + y_1.$$

Nå har vi funnet et uttrykk for både x_3 og y_3, hvor det er verdt å legge merke til at dette fungerer både når $P = Q$ og $P \neq Q$. Så nå er det eneste som mangler å finne et uttrykk for stigningstallet λ. Men når vi skal gjøre dette må vi dele det opp i de to tilfellene hvor $P \neq Q$ som impliserer at $x_1 \neq x_2$, og $P = Q$ som betyr at $x_1 = x_2$.

Vi ser på tilfellet hvor $P \neq Q$. Da får vi at

$$y_1 = \lambda x_1 + \nu \quad \text{og} \quad y_2 = \lambda x_2 + \nu,$$

hvor vi tar differansen mellom uttrykkene og får

$$y_2 - y_1 = \lambda(x_2 - x_1),$$

deretter deler vi på $(x_2 - x_1)$ på begge sider og får til slutt

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

I tilfellet hvor $P = Q$ kan vi se at dette argumentet ikke vil fungere ettersom man ender opp med å dele på 0. Derfor trenger vi å bruke derivasjon for å kunne regne ut stigningstallet til tangenten i punktet P. Så hvis vi tar vår elliptiske kurve $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ og deriverer med hensyn på x på begge sider får vi

$$\begin{aligned} \frac{d}{dx}y^2 &= \frac{d}{dx}(x^3 + ax^2 + bx + c) \\ 2y\frac{dy}{dx} &= 3x^2 + 2ax + b \end{aligned}$$

Hvis vi så evaluerer i $P = (x_1, y_1)$ får vi følgende uttrykk for λ

$$\lambda = \frac{3x_1^2 + 2ax_1 + b}{2y_1}$$

Dermed har vi funnet ut hvordan vi adderer to punkter på en elliptisk kurve i alle mulige tilfeller, som kan oppsumeres i disse tre punktene:

(1) $\mathcal{O} + P = P$ for alle $P \in E$
(2) $P + (-P) = (x, y) + (x, -y) = \mathcal{O}$ for alle $P = (x, y) \in E$
(3) For $P = (x_1, y_1)$ og $Q = (x_2, y_2)$ hvor $Q \neq (x_1, -y_1)$ så er $P+Q = (x_3, y_3)$ hvor

$$x_3 = \lambda^2 - x_1 - x_2 - a,$$
$$y_3 = \lambda(x_1 - x_3) - y_1,$$
$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \frac{3x_1^2 + 2ax_1 + b}{2y_1}, & x_1 = x_2 \end{cases}$$

3. Gruppen av punkter på en elliptiske kurve

I denne seksjonen skal vi vise at mengden av rasjonale punkter på en elliptisk kurve danner en abelsk gruppe. Men før vi gjør dette trenger vi et Lemma.

LEMMA 3.3 (Cayley-Bacharach for kurver av grad tre). *La C_1, C_2 og C være tre curver i $\mathbb{P}^2$ av grad tre. La C_1 og C_2 skjære hverandre i de ni punktene $A_1, ..., A_9$, og la C skjære C_1 og C_2 i $A_1, ..., A_8$. Da vil C gå igjennom A_9.*

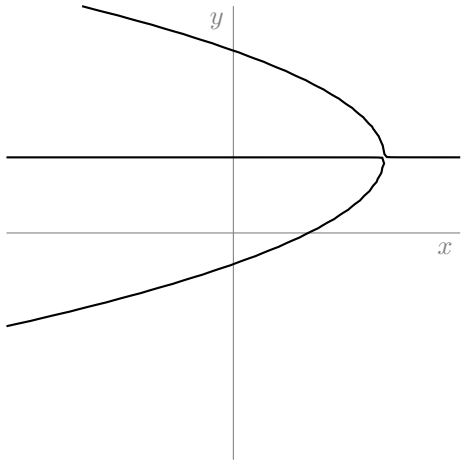
BEVIS. Først lar vi kurvene være gitt ved likningene

$$C_1 : \ F_1(X, Y, Z) = 0,$$
$$C_2 : \ F_2(X, Y, Z) = 0,$$
$$C \ : \ F\ (X, Y, Z) = 0.$$

Vi antar videre at F ikke er en lineærkombinasjon av F_1 og F_2. Vi noterer oss fra Teorem 2.4 at en linje ikke kan skjære en kurve av grad tre i mer enn tre punkter med mindre kurven er en union av den linjen og en kurve av grad to, slik som vi ser i Figur 3.8. I tillegg noterer vi oss at hvis vi har fem punkter, så kan vi alltid lage en kurve av grad to som går igjennom disse punktene. Hvis disse punktene er skjæringspunktene mellom kurven av grad to og en kurve av grad tre, vil denne kurven av grad to, fra Teorem 2.4 være unik, med mindre fire av dem ligger på samme linje.

La oss anta at tre av punktene $A_1, ...A_8$ ligger på samme linje, si A_1, A_2 og A_3 ligger på linjen ℓ. Og la σ være kurven av grad to som skjærer C_1, C_2 og C i $A_4, ..., A_8$. Vi lar også B_1 være et punkt på ℓ som er ulik $A_1, ..., A_8$, og la B_2 være et punkt som ikke ligger på ℓ eller σ. Ettersom F ikke er en lineærkombinasjon av F_1 og F_2 så kan vi finne en ikketriviell løsning på likningssettet

$$aF_1(B_1) + bF_2(B_1) + cF(B_1) = 0$$
$$aF_1(B_2) + bF_2(B_2) + cF(B_2) = 0.$$



FIGUR 3.8. En kurve av grad tre som består av unionen av en linje og en kurve av grad to: $0 = (y-1)^3 + (x-2)(y-1)$

La nå kurven C' av grad tre være gitt ved

$$C' : \ aF_1(X,Y,Z) + bF_2(X,Y,Z) + cF(X,Y,Z) = 0.$$

Da kan vi se at kurven C' og linjen ℓ vil skjære hverandre i de fire punktene A_1, A_2, A_3 og B_1. Da får vi fra Teorem 2.4 at C' må være unionen av ℓ og en kurve av grad to. Siden C' skjærer C_1, C_2 og C i $A_4, ..., A_8$ så vil C' være unionen av ℓ og σ, men vi valgte B_2 til å verken ligge på ℓ eller σ så vi får en motsigelse. Dermed er det ingen tre av $A_1, ..., A_8$ som kan ligge på samme linje.

Vi antar nå at en kurve σ av grad to skjærer C_1, C_2 og C i seks av punktene $A_1, ..., A_8$, la oss si $A_1, ..., A_6$, og la ℓ være linjen som skjærer C_1, C_2 og C i A_7 og A_8. Vi velger punktet B_1 til å være et punkt som ligger på σ, som er ulik $A_1, ..., A_8$, og vi velger B_2 til å være et punkt som ikke ligger på σ eller ℓ. Vi kan igjen finne en ikketriviell løsning på

$$aF_1(B_1) + bF_2(B_1) + cF(B_1) = 0$$
$$aF_1(B_2) + bF_2(B_2) + cF(B_2) = 0,$$

og vi velger C' til å være kurven av grad tre gitt ved

$$C' : \ aF_1(X,Y,Z) + bF_2(X,Y,Z) + cF(X,Y,Z) = 0.$$

Ettersom vi ser at C' da skjærer σ i syv punkter, får vi fra Teorem 2.4 at C' må være unionen av σ og en linje. Siden C' går igjennom A_7 og A_8, må C' være unionen av σ og ℓ. Igjen får vi en motsigelse siden B_2 ikke ligger på σ eller ℓ, men ligger på C'. Dermed går det ikke at en kurve av grad to som skjærer C_1, C_2 og C i seks av punktene $A_1, ..., A_8$.

Nå lar vi ℓ være linjen som skjærer C_1, C_2 og C i A_1 og A_2 og vi lar σ være kurven av grad to som skjærer C_1, C_2 og C i $A_3, .., A_7$. Vi lar også B_1 og B_2 være to ulike punkter som ligger på ℓ, men ikke lik noen av $A_1, ..., A_8$. Vi finner igjen en ikketriviell løsning på likningssettet

$$aF_1(B_1) + bF_2(B_1) + cF(B_1) = 0$$
$$aF_1(B_2) + bF_2(B_2) + cF(B_2) = 0,$$

og vi lar C' være kurven av grad tre gitt ved

$$C' : \ aF_1(X, Y, Z) + bF_2(X, Y, Z) + cF(X, Y, Z) = 0.$$

Da vil C' skjære ℓ i de fire punktene A_1, A_2, B_1, B_2, og vi får igjen fra Teorem 2.4 at C' må være unionen av ℓ og σ. Vi ser fra uttrykket for C', at A_8 ligger på C', men vi så over at A_8 hverken kan ligge på ℓ eller σ, og vi får igen en selvmotsigelse.

Så da kan vi si at F må være en lineærkombinasjon av F_1 og F_2. Dermed kan vi skrive C på følgende måte

$$C : \ \lambda_1 F_1(X, Y, Z) + \lambda_2 F_2(X, Y, Z) = 0.$$

Fra dette uttrykket ser vi at C vil skjære C_1 og C_2 i A_9.

□

Og med dette er vi klar til å vise at punktene på en elliptisk kurve danner en gruppe, som vi hevder i følgende teorem.

THEOREM 3.4. *La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve med heltalls koeffisienter, og la $E(\mathbb{Q})$ være mengden av alle punkter på E med rasjonale koordinater. Da vil $(E(\mathbb{Q}), +)$ være en abelsk gruppe med $\mathcal{O}$ som identitet.*

BEVIS. Fra formlene for addisjon av punkter vi kom fram til i Seksjon 2, sammen med det faktum om at $\mathbb{Q}$ er en kropp, ser vi at $E(\mathbb{Q})$ er lukket under binæropperasjonen $+$.

Det er greit å se at operasjonen $P * Q$ er kommutativ, ettersom to punkter definerer en unik linje, og fra dette får vi at $P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q + P$ som viser at $+$ også er kommutativ.

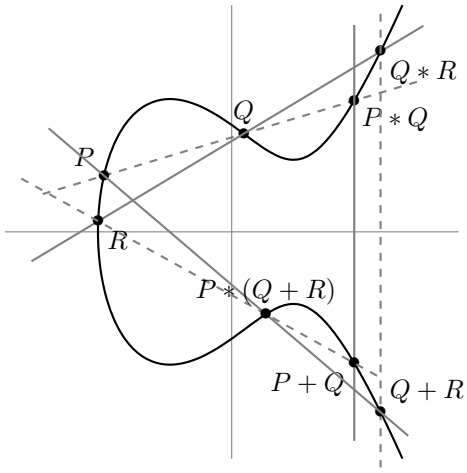
Vi har også sett at $\mathcal{O}$ fungerer som en venstre identitet i $E(\mathbb{Q})$, og ettersom $+$ er kommutativ vil $\mathcal{O}$ også fungere som en høyre identitet.

For alle punkter $(x, y) \in E(\mathbb{Q})$ så vil $(x, y) + (x, -y) = \mathcal{O}$, som viser at alle punkter har en invers.

For å vise assosiativitet trenger vi å benytte oss av Lemma 3.3. Så la oss anta vi har tre punkter $P, Q, R \in E(\mathbb{Q})$. For å vise at $P + (Q + R) = (P + Q) + R$ er det nok å vise at $P * (Q + R) = (P + Q) * R$. Vi brukeer Lemma 3.3 ved å se på de 10 punktene

$$\mathcal{O},\ P,\ Q,\ R,\ Q * R,\ Q + R,\ P * Q,\ P + Q,\ P * (Q + R),\ (P + Q) * R.$$

Nå ønsker vi å konstruere to kurver av grad tre ved å multiplisere tre likninger som representerer tre linjer. Vi ser en ilustrasjon av dette i Figur 3.9.



FIGUR 3.9. En illustrasjon av assosiativiteten til addisjon av punkter

Første kurve lager vi fra disse tre linjene:

(1) $L_1 : \ \alpha_1 X + \beta_1 Y + \gamma_1 Z = 0$ som går igjennom Q, R og $Q * R$.
(2) $L_2 : \ \alpha_2 X + \beta_2 Y + \gamma_2 Z = 0$ som går igjennom $\mathcal{O}$, $P * Q$ og $P + Q$.
(3) $L_3 : \ \alpha_3 X + \beta_3 Y + \gamma_3 Z = 0$ som går igjennom P, $Q + R$ og $P * (Q + R)$

Hvis vi multipliserer disse likningene får vi en kurve av grad tre som går gjennom alle de 9 punktene linjene går igjennom.

Den andre kurven vi ønsker å konstruere blir konstruert av følgende linjer:

(1) $L_1' : \ \alpha_1' X + \beta_1' Y + \gamma_1' Z = 0$ som går igjennom P, Q og $P * Q$.
(2) $L_2' : \ \alpha_2' X + \beta_2' Y + \gamma_2' Z = 0$ som går igjennom $\mathcal{O}$, $Q * R$ og $Q + R$.
(3) $L_3' : \ \alpha_3' X + \beta_3' Y + \gamma_3' Z = 0$ som går igjennom $P + Q$, R og $(P + Q) * R$

Ved å multplisere sammen disse tre likningene får vi enda en kurve av grad tre, som skjærer E i de nevnte punktene. Vi ser også at begge kurvene har til felles at de skjærer E i de åtte punktene

$$\mathcal{O},\ P,\ Q,\ R,\ R * Q,\ R + Q,\ P * R,\ P + R$$

Dermed får vi fra Lemma 3.3 at de må dele det niende skjæringspunktet, som betyr at

$$P * (Q + R) = (P + Q) * R,$$

og fra dette får vi at

$$P + (Q + R) = (P + Q) + R.$$

□

KAPITTEL 4

Nagell-Lutz Teorem

I dette kapittelet kommer vi til å vise Nagell-Lutz Teorem, som er et av de to store resultatene vi skal ta for oss i denne oppgaven. Nagell-Lutz Teorem gir en enkel måte å finne alle punkter av endelig orden på en elliptisk kurve over de rasjonale tallene. Teoremet sier at alle punkter av endelig orden vil ha heltalls koordinater og at y-koordinatet vil enten være lik 0 eller dele diskriminanten til kurven. Vi starter med å definere diskriminanten til en elliptisk kurve.

DEFINISJON 4.1. La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve med heltalls koeffisienter, hvor $f(x)$ har $\alpha_1, \alpha_2, \alpha_3$ som sine røtter. Da er diskriminanten D til kurven gitt ved følgende formel

$$D = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2. \tag{2}$$

Ettersom det er vanskelig å finne de komplekse røttene til et polynom av grad tre, så vil det være bedre å ha en enklere formel for diskriminanten, det får man ut ifra følgende proposisjon.

PROPOSISJON 4.2. *La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve med heltalls koeffisienter og diskriminant D, da gjelder følgende*

(a) $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$

(b) Det eksisterer polynomer $r(x), s(x) \in \mathbb{Z}[x]$ slik at $D = r(x)f(x) + s(x)f'(x)$

BEVIS. (a) Hvis vi lar $\alpha_1, \alpha_2, \alpha_3$ være de tre komplekse røttene til $f(x)$, får vi at $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. Ut i fra dette får man følgende uttrykk for a, b og c

$$\begin{aligned} a &= -(\alpha_1 + \alpha_2 + \alpha_3) \\ b &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 \\ c &= -\alpha_1\alpha_2\alpha_3 \end{aligned}$$

Hvis vi substituerer ut a, b og c i (a) og ganger ut, samt ganger ut (2) får vi at disse to uttrykkene blir det samme.

(b) Hvis vi gir følgende uttrykk for $r(x)$ og $s(x)$

$$\begin{aligned} r(x) &= (18b - 6a^2)x - (4a^3 - 15ab + 27c), \\ s(x) &= (2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2), \end{aligned}$$

og ganger ut $r(x)f(x) + s(x)f'(x)$ vil alle x-leddene kanselleres og vi står igjen med diskriminanten slik som i (a).

□

Da er vi klare til å starte på første resultat på veien til å vise Nagell-Lutz Teorem.

LEMMA 4.3. *La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve med heltalls koeffisienter og diskriminant D, og la $P \in E(\mathbb{Q})$ være et punkt på kurven slik at $P = (x_1, y_1)$ og $2P = P + P$ begge har heltalls koordinater. Da vil enten $y_1 = 0$ eller $y_1|D$.*

BEVIS. Hvis $y_1 = 0$ er vi allerede ferdig, så anta at $y_1 \neq 0$, da får vi at $P \neq -P$ som impliserer at $2P \neq \mathcal{O}$. Dette betyr at vi kan skrive $2P$ som (x_2, y_2) hvor x_2 og y_2 fra antagelsen er heltall. Fra formelene for addisjon av punkter på en elliptiske kurver får vi da følgende

$$2x_1 + x_2 = \lambda^2 - a, \quad \lambda = \frac{f'(x)}{2y_1}.$$

Vi vet at $2x_1, x_2$ og a alle er heltall, som betyr at λ^2 også må å være et heltall. Siden vi vet λ er ransjonalt, så må λ også være et heltall. Dette impliserer da at $y_1|f'(x_1)$. I tillegg siden $P = (x_1, y_1)$ er et punkt på kurven vet vi at $y_1^2 = f(x_1)$, og da vil $y_1|f(x_1)$.

Fra Proposisjon 4.2 (b) har vi at det eksisterer polynomer $r(x), s(x) \in \mathbb{Z}[x]$ slik at

$$D = r(x_1)f(x_1) + s(x_1)f'(x_1).$$

Siden y_1 deler både $f(x_1)$ og $f'(x_1)$, vil $y_1|D$.

□

Nagell-Lutz Teorem beskriver de rasjonale punktene an endelig orden på to måter, det ene er at de har heltalls koordinater og den andre er at y-koordinatet er null eller deler diskriminanten. For å vise at punkter med endelig orden har heltalls koordinater kommer vi til å trenge å definere enda et nyttig verktøy.

DEFINISJON 4.4. La $q \neq 0$ være et rasjonalt tall og p et primtall. Skriv q på følgende måte: $q = \frac{m}{n}p^\nu$, hvor $\nu \in \mathbb{Z}$ og p verken deler m eller n. Da definerer vi p-ordenen til q som

$$\mathrm{ord}_p(q) = \nu.$$

Som konvensjon definerer vi $\mathrm{ord}_p(0) = \infty$.

La oss nå se på hvordan p-ordenen til koordinatene til et rasjonalt punkt på en elliptiske kurve $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ ser ut. La $(x, y) \in E(\mathbb{Q})$ være et punkt på kurven og la

$$x = \frac{m}{np^\mu}, \quad y = \frac{u}{wp^\sigma}$$

hvor p ikke deler m, n, u eller w. Vi setter dette inn i likningen for kurven og samler høyresiden på felles nevner og får

$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}.$$

Her ser man at på høyre side av likningen så er p en divisor av alle leddene i telleren utenom m^3. Dermed får vi at p ikke deler telleren på verken høyre eller venstre side av likningen. Dette fører til at $\sigma > 0$ hvis og bar hvis $\mu > 0$, og at $3\mu = 2\sigma$, som betyr at vi har $\mu = 2\nu$ og $\sigma = 3\nu$ for et heltall ν.

Nå som vi har en sammenheng mellom primtall i nevneren til alle rasjonale punkter på en elliptisk kurve, gir det mening å se på følgende delmengder for en elliptisk kurve E når $\nu \geq 1$.

$$E(p^\nu) := \{(x, y) \in E(\mathbb{Q}) \mid \text{ord}_p(x) \leq -2\nu \text{ og } \text{ord}_p(y) \leq -3\nu\} \cup \{\mathcal{O}\}.$$

Her følger det naturlig at

$$E(\mathbb{Q}) \supseteq E(p) \supseteq E(p^2) \supseteq \cdots \supseteq E(p^\nu) \supseteq \cdots .$$

Dette fører oss videre til følgende proposisjon

PROPOSISJON 4.5. *La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve med heltalls koeffisienter og p et primtall. La R_p være ringen gitt ved*

$$R_p := \{q \in \mathbb{Q} \mid ord_p(q) \geq 0\},$$

og la $E(p^\nu)$ være definert som over. Da gjelder følgende.

(a) $E(p)$ inneholder alle punkter $P = (x, y) \in E(\mathbb{Q})$ hvor enten nevneren i x eller nevneren i y har p som en divisor.
(b) For alle $\nu \geq 1$, så er $E(p^\nu)$ en undergruppe av $E(\mathbb{Q})$.
(c) Avbildningen

$$t : \frac{E(p^\nu)}{E(p^{3\nu})} \longrightarrow \frac{p^\nu R_p}{p^{3\nu} R_p}, \quad P = (x, y) \longmapsto t(P) = \frac{x}{y},$$

er en injektiv gruppehomomorfi hvor $\mathcal{O} \longmapsto 0$.

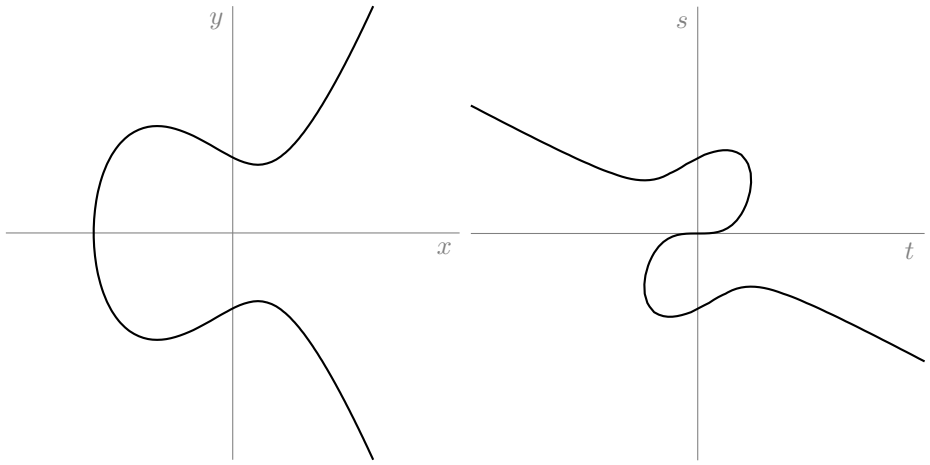
BEVIS. Først ser vi på ringen R_p. Vi kan se at hvis vi har to elementer $r, s \in R_p$ så vil både $r \pm s$ og rs være inneholdt i R_p. Siden $\text{ord}_p(0) = \infty \geq 0$ og $\text{ord}_p(1) = 0$ vil også $0, 1 \in R_p$. I tillegg så har R_p de distributive lovene sine fra $\mathbb{Q}$ dermed er det greit å se at R_p er en kommutativ ring med enhet. Legg også merke til at enhetene i ringen er alle ellementer som har sin p-orden lik null, og alle idealer til R_p er på formen $p^i R_p$ for en $i \geq 1$.

(a) Er allerede vist over, ettersom vi ikke antok noe om hvor store σ og μ skulle være.

(b) Det at inverser og $\mathcal{O}$ er inneholdt i $E(p^\nu)$ følger direkte fra definisjonen av $E(p^\nu)$, men for å vise at mengden er lukket under addisjon, gjør vi et bytte av koordinater fra (x, y)-planet til (t, s)-planet definert ved

$$t = \frac{x}{y} \text{ og } s = \frac{1}{y},$$

hvor $\mathcal{O}$ er definert til å bli sendt til punktet $(0, 0)$. Vi kan se at dette vil være et injektivt skifte av koordinater som inkluderer alle punktene på E utenom de hvor



FIGUR 4.1. En elliptisk kurve i xy-planet og i ts-planet

$y = 0$, som er punktene av orden 2. Vi kan se at alle løsninger av

$$0 = x^3 + ax^2 + bx + c, \tag{3}$$

er heltallsløsninger ved å la

$$x = \frac{m}{np^\mu},$$

hvor $p \geq 0$ ikke deler m eller n, være en løsning av 3. Da får vi at

$$0 = \frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}.$$

Vi ser fra dette uttrykket at p^μ må dele m^3, som betyr at $\mu = 0$. Dette gjelder for alle primtall, som betyr at x må være et heltall. Fra dette vil ikke noen punkter av orden to være inneholdt i $E(p^\nu)$, som betyr at vi kan se bort ifra dem når vi skal vise at $E(p^\nu)$ er lukket under addisjon.

Ved dette byttet av koordinater får vi at likningen for E kan bli uttrykt som

$$E_{ts} : \ s = t^3 + at^2s + bts^2 + cs^3.$$

Og hvis vi har en linje $y = \alpha x + \beta$ i (x, y)-planet, så vil denne korrespondere med en linje i (t, s)-planet ved å dele på βy på begge sider for å få

$$\frac{1}{\beta} = \frac{\alpha}{\beta}\frac{x}{y} + \frac{1}{y},$$

som impliserer

$$s = -\frac{\alpha}{\beta}t + \frac{1}{\beta}.$$

Dermed kan vi addere punkter i (t, s)-planet på akkurat samme måte som i (x, y)-planet.

La oss nå se på hvordan punker i $E(p^\nu)$ fra (x,y)-planet vil se ut i (s,t)-planet. Vi vet fra før at et element i $E(p^\nu)$ i (x,y)-planet vil være på formen.

$$x = \frac{m}{np^{2(\nu+i)}}, \quad y = \frac{u}{wp^{3(\nu+i)}}$$

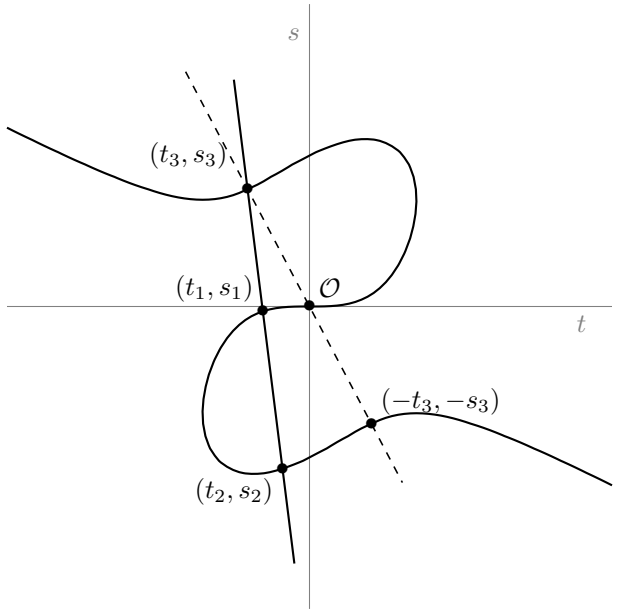
for en $i \geq 0$. Dermed får vi at i (t,s)-planet vil

$$t = \frac{x}{y} = \frac{mw}{nu}p^{\nu+i}, \quad s = \frac{1}{y} = \frac{w}{u}p^{3(p+i)}.$$

Dette betyr at for elementer fra $E(p^\nu)$ i (t,s)-planet så vil $t \in p^\nu R_p$ og $s \in p^{3\nu}R_p$. Og fra det vi så tidligere så er $t \in p^\nu R_p$ hvis og bare hvis $s \in p^{3\nu}R_p$, som fører til at det er nok å vise at $\text{ord}_p(t) \geq \nu$ for å vise at $(t,s) \in E(p^\nu)$.

For å få vist at $E(p^\nu)$ er en undergruppe av $E(\mathbb{Q})$ må vi vise at den er lukket under addisjon i (t,s)-planet, men da trenger vi formler for å addere punker i (t,s)-planet.

Første ting å legge merke til er at $\mathcal{O} = (0,0)$ og hvis (t,s) er en løsning av likningen for E_{ts}, så er $(-t,-s)$ også det, dermed er $(-t,-s)$ alltid det tredje skjæringspunktet til linjen som går igjennom (t,s) og $\mathcal{O}$ og kurven. La $P_1 = (t_1,s_1)$ og $P_2 = (t_2,s_2)$ være to distinkte punkter i $E(p^\nu)$. Først ser vi på tilfellet hvor $t_1 = t_2$ og $s_1 \neq s_2$. Da får vi at linjen som går igjennom P_1 og P_2 er den vertikale linjen $t = t_1$ som da skjærer igjennom et tredje punkt $P_3 = (t_1,s_3)$. Dermed er $P_1 + P_2 = (-t_1,-s_3)$, og siden vi vet $t_1 \in p^\nu R_p$ impliserer det at $(P_1+P_2) \in E(p^\nu)$.



FIGUR 4.2. Addisjon av punkter i ts-planet

La nå $t_1 \neq t_2$ og sett $s = \gamma t + \delta$ til å være linjen som går igjennom P_1 og P_2. Da vil stigningstallet γ være gitt ved

$$\gamma = \frac{s_2 - s_2}{t_2 - t_1}.$$

Ettersom vi vet at koordinatene til P_1 og P_2 må tilfredsstille likningen for E_{ts}, så får vi følgende uttrykk

$$\begin{aligned} s_2 - s_1 &= (t_2^3 - t_1^3) + a(t_2^2 s_2 - t_1^2 s_1) + b(t_2 s_2^2 - t_1 s_1^2) + c(s_2^3 - s_1^3) \\ &= (t_2^3 - t_1^3) + a((t_2^2 - t_1^2)s_2 + t_1^2(s_2 - s_1)) \\ &\qquad + b((t_2 - t_1)s_2^2 + t_1(s_2^2 - s_1^2)) + c(s_2^3 - s_1^3). \end{aligned}$$

Ved andre likhet har vi lagt til og trukket fra $at_1^2 s_2 + bt_1 s_2^2$. Hvis vi nå fordeler alle ledd med $(s_2 - s_1)$ som divisor på en side og alle med $(t_2 - t_1)$ som divisor på den andre får vi

$$\begin{aligned} &(1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2))(s_2 - s_1) \\ &= ((t_2^2 + t_1 t_2 + t_1^2) + a(t_2 + t_1)s_2 + bs_2^2)(t_2 - t_2). \end{aligned}$$

Dermed kan vi få et uttrykk får stigningstallet

$$\gamma = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)}. \tag{4}$$

I det tilfellet hvor $P_1 = P_2$ vil man få at stigningstallet γ til tangenten i P_1 vil være gitt på følgende måte

$$\gamma = \frac{ds}{dt}(P_1) = 3t_1^2 + 2at_1 s_1 + bs_1^2 + (at_1^2 + 2bt_1 s_1 + 3cs_1^2)\frac{ds}{dt}(P_1)$$

Fra dette får vi følgende formel for γ

$$\gamma = \frac{3t_1^2 + 2at_1 s_1 + bs_1^2}{1 - at_1^2 - 2bt_1 s_1 - 3cs_1^2}. \tag{5}$$

Hvis vi ser litt nøye på uttrykk (5) for γ, ser vi at dette er det samme som vi har for γ i uttrykk (4), bare evaluert i $t_2 = t_1$ og $s_2 = s_1$. Dermed er det nok å kun se på det første tilfellet av γ. Hvis vi ser på nevneren i uttrykk (4) for γ, ser vi at siden $t_1, t_2, s_1, s_2 \in p^\nu R_p$ får vi at utrykket

$$-at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)$$

vil være inneholdt i $p^{2\nu} R_p$. Dermed vil

$$1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)$$

være en enhet i R_p, som impliserer at $\gamma \in p^{2\nu} R_p$ siden telleren i uttrykket for γ er innholdt i $p^{2\nu} R_p$.

For å finne P_3 substituerer vi s med $\gamma t + \delta$ i likningen til E_{ts}, for å få et polynom med t_1, t_2 og t_3 som sine røtter, og vi får

$$\gamma t + \delta = t^3 + at^2(\gamma t + \delta) + bt(\gamma t + \delta)^2 + c(\gamma t + \delta)^3.$$

Hvis vi deretter ganger ut og samler med tanke på eksponenter av t får vi at

$$0 = (1 + a\gamma + b\gamma^2 + c\gamma^3)t^3 + (\gamma\delta + 2b\gamma\delta + 3c\gamma^2\delta)t^2 + \cdots . \tag{6}$$

Etter som (6) har løsningene t_1, t_2 og t_3, vet vi at høyre side skal være lik

$$(1 + a\gamma + b\gamma^2 + c\gamma^3)(t - t_1)(t - t_2)(t - t_3)$$

Hvis vi sammenligner disse to og deler med $(1 + a\gamma + b\gamma^2 + c\gamma^3)$ på begge sider, og så sammenligner t^2 leddene får vi at

$$t_1 + t_2 + t_3 = -\frac{\gamma\delta + 2b\gamma\delta + 3c\gamma^2\delta}{1 + a\gamma + b\gamma^2 + c\gamma^3}. \tag{7}$$

Vi vet at $\gamma \in p^{2\nu}R_p$, $s_1 \in p^{3\nu}$ og $t_1 \in p^{\nu}R_p$ så kan vi se fra uttrykket $\delta = s_1 - \gamma t_1$, at $\delta \in p^{3\nu}R_p$. Dermed på samme vis som med γ, kan vi se at nevneren i uttrykket for $t_1 + t_2 + t_3$ er en enhet i R_p, som viser at $t_3 \in p^{\nu}R_p$. Siden vi vet $P_1 + P_2 = (-t_3, -s_3)$ så har vi vist at $E(p^{\nu})$ er lukka under addisjon. Dermed har vi vist at $E(p^{\nu})$ er en undergruppe av $E(\mathbb{Q})$ for alle $\nu \geq 1$.

(c) I tillegg til at vi viste at $t_3 \in p^{\nu}R_p$, så kan vi se fra (7) at $t_1 + t_2 + t_3 \in p^{3\nu}R_p$. Hvis vi definerer $t(P) = t'$ når $P = (t', s')$ så har vi vist at

$$(t(P_1) + t(P_2) - t(P_1 + P_2)) \in p^{3\nu}R_p, \quad \text{for alle } P_1, P_2 \in E(p^{\nu}).$$

Dette er det samme som å si

$$t(P_1) + t(P_2) + p^{3\nu}R_p = t(P_1 + P_2) + p^{3\nu}R_p.$$

Videre så vet vi også at $P \in E(p^{3\nu})$ hvis og bare hvis $t(P) \in p^{3\nu}R_p$. Dermed har vi vist at

$$t : \frac{E(p^{\nu})}{E(p^{3\nu})} \longrightarrow \frac{p^{\nu}R_p}{p^{3\nu}R_p}$$

er en injektiv gruppehomomorfi.

□

Med dette er vi klare til å vise Nagell-Lutz Teorem.

THEOREM 4.6 (Nagell-Lutz). *La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve med heltalls koeffisienter og diskriminant D, og la $P = (x_1, y_1) \in E(Q)$ være et punkt slik at $mP = \mathcal{O}$ for et positivt heltall $m \geq 1$. Da vil x_1 og y_1 begge være heltall hvor $y_1 = 0$ eller $y_1 | D$.*

BEVIS. La oss starte med å anta at P ikke har heltalls koordinater og vi lar t være gruppehomomorfien definert som i Proposisjon 4.5 (c). Da vil det eksistere et primtall p slik at $P \in E(p)$. Ettersom ordenen til både x_1 og y_1 må være endelig, må det eksistere en $\nu \geq 1$ slik at P er inneholdt i $E(p^{\nu})$, men ikke $E(p^{\nu+1})$.

Anta først at p ikke deler m. Fra Proposisjon 4.5 (c) får vi

$$mt(P) + p^{3\nu}R_p = t(mP) + p^{3\nu}R_p = t(\mathcal{O}) + p^{3\nu}R_p = 0 + p^{3\nu}R_p.$$

Ettersom p ikke er en divisor av m, så er m en enhet i R_p. Dette fører til

$$t(P) + p^{3\nu}R_p = 0 + p^{3\nu}R_p,$$

men dette betyr at $t(P) \in E(p^{3\nu}) \subseteq E(p^{\nu+1})$, som da er en motsigelse.

Nå antar vi at p deler m, da er $m = pn$ for en eller annen $n \geq 1$. La $P' = nP$, da vil P' ha orden p, og siden $P \in E(p)$, som er en undergruppe av $E(Q)$, så vil $P' \in E(p)$. På samme måte som over kan vi la μ være slik at P' er inneholdt i $E(p^\mu)$, men ikke $E(p^{\mu+1})$. Så nå vil vi få

$$pt(P') + p^{3\mu}R_p = 0 + p^{3\mu}R_p,$$

så deler vi på p på begge sider og får

$$t(P') + p^{3\mu-1}R_p = 0 + p^{3\mu-1}R_p.$$

Dette betyr at $P' \in E(p^{3\mu-1})$, men siden $3\mu - 1 \geq \mu + 1$, får vi igjen en motsigelse. Dette vil si at $P \notin E(p)$ for alle primtall p, og dette betyr fra Proposisjon 4.5 (a) at x_1 og y_1 må begge være heltall.

Siden P har endelig orden, så betyr det at $2P$ også må ha endelig orden, som betyr at $2P$ også har heltallskoordinater. Da får vi fra Lemma 4.3 at $y_1 = 0$ eller $y_1 | D$.

□

Fra Teorem 4.6 følger det som et korollar at det kun kan finnes endelig mange rasjonale punkter av endelig orden på en elliptisk kurve over de rasjonale tallene.

KOROLLAR 4.7. *For alle elliptiske kurver $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ med heltalls koeffisienter, så er det endelig mange punkter i $E(\mathbb{Q})$ av endelig orden.*

BEVIS. For alle punkter $P = (x_0, y_0) \in E(\mathbb{Q})$ med heltalls koordinater vil enten $y_0 = 0$, eller $y_0 | D$, hvor D er diskriminanten til kurven. Vi vet at diskriminanten $D \neq 0$, siden den er gitt med formelen

$$\begin{aligned} D &= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \\ &= (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2, \end{aligned}$$

hvor α_1, α_2 og α_3 er distinkte, siden $f(x)$ har distinkte komplekse røtter. Dermed må det være et endelig antall divisorer av D, som betyr at det er endelig mange y_0 som kan dele D. Vi vet også at for en gitt y_0 er det maksimalt 3 rasjonale løsninger av polynomet

$$y_0^2 = x^3 + ax^2 + bx + c.$$

Dette impliserer at det er endelig mange punkter på E med heltalls koordinater, som betyr at det er endelig mange punkter av endelig orden.

□

KAPITTEL 5

Fire nyttige lemmaer

For å bevise Mordells teorem kommer vi til å trenge fire lemmaer, og det er disse vi kommer til å bruke dette kapittelet på å vise. Disse lemmaene gjelder generelt for alle rasjonale elliptiske kurver, men når vi skal vise det fjerdet lemmaet kommer vi til å gjøre antagelsen om at den elliptiske kurven vi jobber med har minst ett punkt av orden to. De tre første av lemmaene vi skal vise, kommer til å omhandle en høydefunksjon som vi vil definere.

1. Høyden til P

Definisjon 5.1. La $\frac{m}{n}$ være et rasjonalt tall skrevet slik at m relativt primisk til n, eller $m = 0$ og $n = 1$. Da definerer vi høyden og den lille høyden til $\frac{m}{n}$ ved

$$H\left(\frac{m}{n}\right) = \max\{|n|, |m|\}, \qquad h\left(\frac{m}{n}\right) = \log H\left(\frac{m}{n}\right).$$

Vi definerer også høyden til et punkt $P = (x, y)$ som høyden til x-koordinatet. Ved konvensjon definerer vi $H(\mathcal{O}) = 1$.

Og med dette er vi allerede klar til å vise det første lemmaet.

Lemma 5.2. *La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve med heltalls koeffisienter, da vil mengden*

$$\{P \in E(\mathbb{Q}) \mid h(P) \leq M\},$$

være endelig for alle reelle tall M.

Bevis. La M være et reelt tall og sett $M' = \exp(M)$. Vi kan se at høyden til et punkt er et positivt heltall, og vi vet at det kun er endelig mange heltall med absoluttverdi mindre enn M'. Ettersom et rasjonalt tall kan uttrykkes ved to heltall, vil det fortsatt kun være endelig mange kombinasjoner av to heltall, som begge har absoluttverdi mindre enn M'.
Med det vet vi at det kun kan være en endelig mengde x-verdier til punkter med $H(x) \leq M'$. En x-verdi kan kun høre til to y-verdier som punkter på en elliptisk kurve. Dermed kan vi si at det kun er endelig mange punkter P som kan ha $H(P) \leq M'$.
Hvis vi tar logoritmen får vi at det er endelig mange punkter P med $h(P) \leq M$.
□

2. Høyden til $P + P_0$

I denne seksjonen skal vi bevise det andre lemmaet vårt. Dette sier at gitt et punkt P_0 så er høyden til $P+P_0$ "nesten" mindre enn den doble høyden til P. Før vi beviser dette er det lurt å notere seg noen få ting. Vi så i Seksjon 4.1 at hvis vi har et rasjonalt punkt $P = (x, y)$ på en elliptisk kurve

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c$$

med heltalls koeffisienter, og et primtall p som deler nevneren til enten x-koordinatet eller y-koordinatet, vil $P = (\frac{m}{up^{2\nu}}, \frac{n}{wp^{3\nu}})$ for en $\nu \geq 1$. Siden dette gjelder for alle primtal, får vi at alle rasjonale punkter $P \neq \mathcal{O}$ på en elliptisk kurve med heltalls koeffisienter vil være på formen

$$P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right),$$

for et positivet heltall e, som ikke har noen felles divisorer med n eller m.

Vi ser videre fra definisjonen av høyde at

$$|m| \leq H(P) \text{ og } e^2 \leq H(P).$$

Hvis vi også substituerer x-verdien og y-verdien for P i likningen for E, og multipliserer alt med e^6 får vi

$$n^2 = m^3 + am^2e^2 + bme^4 + ce^6.$$

Videre tar vi absoluttverdien og bruker trekantulikheten og ulikhetene over for å få

$$\begin{aligned} |n^2| &\leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6| \\ &\leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3. \end{aligned}$$

Fra dette ser vi at

$$|n| \leq KH(p)^{3/2},$$

hvor $K = \sqrt{1 + |a| + |b| + |c|}$.

LEMMA 5.3. *La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve med heltalls koeffisienter, og fikser et punkt $P_0 \in E(\mathbb{Q})$, da vil det eksistere en κ_0 som kun avhenger av P_0, a, b og c, slik at*

$$h(P + P_0) \leq 2h(P) + \kappa_0, \qquad \textit{for alle } P \in E(\mathbb{Q})$$

BEVIS. Det første vi noterer oss er at for $P_0 = \mathcal{O}$ så gjelder ulikheten med $\kappa_0 = 0$. Så fra nå anta at $P_0 \neq \mathcal{O}$, men heller ha $P_0 = (x_0, y_0)$. Videre kan vi notere at det er nok å vise ulikheten for alle P uten om en endelig mengde, ettersom det eventult bare er å legge til et stort nok tall til slutt for å få det til å gjelde for de punktene også. Derfor er det også greit å anta $P \notin \{\mathcal{O}, P_0, -P_0\}$ så vi kan anta at $P = (x, y)$. Grunnen til at vi gjør dette er for å kun trenge å se på formelen for å addere to punkter hvor $x_0 \neq x$.

La

$$P + P_0 = (\xi, \eta).$$

Da kan vi gi et uttrykk for ξ med formelen for addisjon av distinkte punkter,

$$\xi = \lambda^2 - x - x_0 - a, \qquad \lambda = \frac{y - y_0}{x - x_0}.$$

Ved videre utregning får vi at

$$\begin{aligned}\xi &= \frac{(y-y_0)^2}{(x-x_0)^2} - x - x_0 - a \\ &= \frac{(y-y_0)^2 - (x-x_0)^2(x+x_0+a)}{(x-x_0)^2}.\end{aligned}$$

Hvis vi ganger ut uttrykket får vi leddet $y^2 - x^3$ i telleren, som vi kan bytte ut med $ax^2 + bx + c$, ettersom P er et punkt på E. Da får vi et utrykk for ξ på formen

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G},$$

hvor A, B, C, D, E, F, G er rasjonale tall kun avhenig av x_0, y_0, a, b og c. Hvis vi utvider ξ med største felles multiplum av nevnerne til A, B, C, D, E, F, G så får vi at alle leddene vil ha heltall forran seg, som impliserer at vi kan anta at A, B, C, D, E, F, G alle er heltall.

Hvis vi nå substituerer x og y med $\frac{m}{e^2}$ og $\frac{n}{e^3}$ og utvider ξ med e^4 får vi et uttrykk for ξ hvor både teller og nevner er heltall, nemlig

$$\xi = \frac{Ane + +Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

Så da har vi et uttrykk for en øvre grense for høyden til $P + P_0$ nemlig

$$H(P + P_0) \leq \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}.$$

Som vi så tidligere har vi følgende tre ulikheter

$$|e| \leq H(P)^{1/2}, \quad |m| \leq H(P), \quad |n| \leq KH(P)^{3/2}.$$

Hvis vi ser på nevneren og telleren til ξ hver for seg og bruker disse tre ulikhetene i tillegg til trekantulikheten får vi

$$\begin{aligned}|Ane + Bm^2 + Cme^2 + De^4| &\leq |Ane| + |Bm^2| + |Cme^2| + |De^4| \\ &\leq |A|KH(P)^2 + |B|H(P)^2 + |C|H(P)^2 + |D|H(P)^2 \\ &\leq (|A|K + |B| + |C| + |D|)H(P)^2,\end{aligned}$$

og

$$\begin{aligned}|Em^2 + Fme^2 + Ge^4| &\leq |Em^2| + |Fme^2| + |Ge^4| \\ &\leq (|E| + |F| + |G|)H(P)^2.\end{aligned}$$

Fra dette har vi da

$$H(P + P_0) \leq K_0 H(P)^2,$$

hvor $K_0 = \max\{|A|K+|B|+|C|+|D|, |E|+|F|+|G|\}$. Vi har sett at A, B, C, D, E, F, G, K kun er avhengig av x_0, y_0, a, b og c, så impliserer dette at K_0 er det samme. Så hvis vi tar logoritmen på begge sider får vi

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

hvor $\kappa_o = \log K_0$.

□

3. Høyden til $2P$

Det tredje lemmaet vi skal vise sier at høyden til et punkt addert med seg selv er "nesten" større enn fire ganger høyden til punktet. Før vi er klare til å vise dette lemmaet beviser vi en proposisjon som lemmaet kommer til å følge fra uten alt for mye arbeid.

PROPOSISJON 5.4. *La $\phi(X)$ og $\psi(X)$ være to polynomer med heltalls koeffisienter, og anta at $\phi(X)$ og $\psi(X)$ har ingen felles komplekse røtter. La d være den største av graden til $\phi(X)$ og graden til $\psi(X)$.*

(a) Det eksisterer et heltall $R \geq 1$ avhengig av ϕ og ψ slik at for alle rasjonale tall $\frac{m}{n}$ vil

$$\gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right)$$

dele R.

(b) Det eksisterer konstanter κ_1 og κ_2 som avhenger av ϕ og ψ slik at for alle rasjonale tall $\frac{m}{n}$ vil

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2.$$

BEVIS. (a) Legg merke til at $n^d\phi(\frac{m}{n})$ og $n^d\psi(\frac{m}{n})$ er begge heltall siden ϕ og ψ har grad mindre eller lik d. Dermed gir det mening å se på deres største felles divisor. Uten tap av generalitet anta at ϕ har grad d og at ψ har grad $e \leq d$. Da kan vi skrive

$$n^d\phi\left(\frac{m}{n}\right) = a_0m^d + a_1m^{d-1}n + ... + a_dn^d,$$
$$n^d\psi\left(\frac{m}{n}\right) = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e+1} + ... + b_en^d.$$

For enklere notasjon la $\Phi(m,n) = n^d\phi(\frac{m}{n})$ og $\Psi(m,n) = n^d\psi(\frac{m}{n})$ slik at problemet vårt blir å finne en R som har $\gcd(\Phi(m,n), \Psi(m,n))$ som en divisor.

Ettersom $\phi(X)$ og $\psi(X)$ ikke har noen felles røtter, betyr det at de er relativt primisk i den Euklidiske ringen $\mathbb{Q}[X]$. Derfor kan vi finne rasjonale polynomer $F(X)$ og $G(X)$ slik at

$$F(X)\phi(X) + G(X)\psi(X) = 1. \tag{8}$$

Velg A til å være det minste felles multiplummet av nevnerne til koeffisientene til F og G og velg D til å være den største graden til F og G. Legg merke til at hverken A eller D er avhengig av n eller m.

Vi evaluerer nå identiteten (8) i $X = \frac{m}{n}$ og multipliserer med An^{d+D}, og får at

$$n^DAF\left(\frac{m}{n}\right)\Phi(m,n) + n^DAG\left(\frac{m}{n}\right)\Psi(m,n) = An^{d+D}.$$

La γ være største felles divisor til $\Phi(m,n)$ og $\Psi(m,n)$. Da ser vi at γ deler An^{d+D}, men dette er ikke nok ettersom vi ønsker å finne et multiplum av γ som er uavhengig av n. Vi vet at γ deler $\Phi(m,n)$ derfor vet vi at γ må dele

$$An^{D+d-1}\Phi(m,n) = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + ... + Aa_dn^{D+2d-1}.$$

Vi ser her at γ deler alle leddene uten om det første ettersom γ deler An^{D+d}, men dette betyr at γ må dele $Aa_0m^dn^{D+d-1}$ siden γ skal dele hele uttrykket. Da får vi at γ også deler

$$\gcd(An^{D+d}, Aa_0m^dn^{D+d-1}).$$

Siden m og n er relativt primiske får vi at γ må dele Aa_0n^{D+d-1}. Hvis vi videre ser på $Aa_0n^{D+d-2}\Phi(m,n)$ får vi på samme måte at γ deler $Aa_0^2n^{D+d-2}$. Ved å fortsette med dette videre, vil vi til slutt få at γ deler Aa_0^{D+d}, som er uavhengig av både n og m. Og da har vi vist (a).

(b) Først viser vi den øvre grensen til $h(\frac{\phi(m/n)}{\psi(m/n)})$. Det er verdt å notere seg at høyden til et rasjonalt tall ikke avhenger av hvilket tall som er over eller under brøkstreken, derfor er det greit igjen å anta at ϕ har grad d og ψ har grad $e \leq d$. Hvis vi lar $\xi = \frac{\phi(m/n)}{\psi(m/n)}$ får vi

$$H(\xi) = H\left(\frac{\phi(m/n)}{\psi(m/n)}\right) = H\left(\frac{n^d\phi(m/n)}{n^d\psi(m/n)}\right).$$

Så nå har vi et uttrykk med heltall i både nevner og teller og hvis vi bruker trekantulikheten og det faktum om at $|m| \leq H(\frac{m}{n})$ og $|n| \leq H(\frac{m}{n})$ får vi

$$\begin{aligned}\left|n^d\phi\left(\frac{m}{n}\right)\right| &= |a_0m^d + a_1m^{d-1}n + ... + a_dn^d| \\ &\leq (|a_0| + |a_1| + ... + |a_d|)H\left(\frac{m}{n}\right)^d,\end{aligned}$$

og

$$\begin{aligned}\left|n^d\psi\left(\frac{m}{n}\right)\right| &= |b_0m^en^{d-e} + b_1m^{e-1}n^{d-e+1} + ... + b_en^d| \\ &\leq (|b_0| + |b_1| + ... + |b_e|)H\left(\frac{m}{n}\right)^d.\end{aligned}$$

Fra dette får vi

$$H(\xi) \leq K_2H\left(\frac{m}{n}\right)^d,$$

Hvor $K_2 = \max\{|a_0|+|a_1|+...+|a_d|, |b_0|+|b_1|+...+|b_e|\}$. Hvis vi nå tar logoritmen på begge sider får vi det vi ønsker

$$h(\xi) = h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2.$$

Her er det viktig å notere at κ_2 kun er avhengig av ϕ og ψ.

Nå gjenstår det bare å vise den nedre grensen til $h(\xi)$. Vi vet at $H(\xi)$ er lik det største tallet av $n^d\phi(m/n)$ og $n^d\psi(m/n)$ delt på deres største felles divisor. I

(a) fikk vi en øvre grense på den største felles divisoren som kun var avhengig av ϕ og ψ nemlig R. Dermed får vi

$$\begin{aligned} H(\xi) &\geq \frac{1}{R}\max\{|n^d\phi(m/n)|, |n^d\psi(m/n)|\} \\ &\geq \frac{1}{2R}(|n^d\phi(m/n)| + |n^d\psi(m/n)|). \end{aligned}$$

Hvis vi nå deler på $H(\frac{m}{n})^d = \max\{|m^d|, |n^d|\}$ på begge sider får vi

$$\begin{aligned} \frac{H(\xi)}{H(m/n)^d} &\geq \frac{1}{2R}\frac{|n^d\phi(m/n)| + |n^d\psi(m/n)|}{\max\{|m^d|, |n^d|\}} \\ &= \frac{1}{2R}\frac{|\phi(m/n)| + |\psi(m/n)|}{\max\{|(\frac{m}{n})^d|, 1\}}. \end{aligned}$$

Vi definerer funksjonen

$$p(t) = \frac{|\phi(t)| + |\psi(t)|}{\max\{|t|^d, 1\}}.$$

Vi ser at når $t \to \pm\infty$ så vil $p(t)$ gå mot $|a_0|$ hvis $e < d$ og $|a_0| + |b_0|$ hvis $e = d$. Siden p er kontinuerlig betyr dette at p må være begrenset nedenifra av en positiv konstant $C_1 > 0$ over alt utenom et begrensett lukket intervall I. Ettersom I er lukket og begrenset i $\mathbb{R}$ er det også kompakt, som betyr at $p(t)$ må ha et positivt minimum C_2 på I, og siden ϕ og ψ ikke har noen felles røtter, vil $p(t)$ aldri være lik 0, som betyr at $C_2 > 0$. Sett nå $C = \min\{C_1, C_2\}$, da får vi at $p(\frac{m}{n}) \geq C$, hvor C er kun avhengig av ϕ og ψ.
Vi så over at

$$\frac{H(\xi)}{H(m/n)^d} \geq \frac{1}{2R}p\left(\frac{m}{n}\right).$$

Fra dette kan vi da se

$$H(\xi) \geq \frac{C}{2R}H\left(\frac{m}{n}\right)^d.$$

Og hvis vi tar logoritmen på begge sider får vi til slutt at

$$h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \geq dh\left(\frac{m}{n}\right) - \kappa_1,$$

hvor $\kappa_1 = \log\left(\frac{2R}{C}\right)$, som konkluderer (b).

□

Med dette er vi klar til å bevise det tredje lemmaet vi skal se på.

LEMMA 5.5. *La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve med heltalls koeffisienter. Da eksisterer det en κ kun avhengig av a, b og c slik at*

$$h(2P) \geq 4h(P) - \kappa \text{ for alle } P \in E(\mathbb{Q}).$$

BEVIS. Akkurat som i bevist for Lemma 5.3, er det nok å vise ulikheten for alle utenom et endelig antall punkter, ettersom vi bare kan justere κ i etterkant, slik at

det stemme for de resterende punktene. Så anta $2P \neq \mathcal{O}$. Da har vi at $2P = (\xi, \eta)$, og vi har fra formlene for addisjon av punkter

$$\xi = \lambda^2 - 2x - a, \qquad \lambda = \frac{f'(x)}{2y}.$$

Fra dette får vi videre

$$\begin{aligned}\xi &= \frac{f'(x)^2}{4y^2} - 2x - a \\ &= \frac{f'(x)^2 - (8x - 4a)y^2}{4y^2} \\ &= \frac{f'(x)^2 - (8x - a)f(x)}{4f(x)}.\end{aligned}$$

I det siste steget har vi brukt det faktum at P er et punkt på kurven vår, så (x, y) må tilfredstille likningen for E. Ettersom E er ikkesingulær fra definisjonen av elliptiske kurver, så vil $f(x)$ og $f'(x)$ ikke ha noen felles røtter, derfor vil

$$f'(x)^2 - (8x - a)f(x) \text{ og } 4f(x)$$

være to polynomer med heltalls koeffisienter av grad 4 og 3 som ikke har noen felles røtter. Dermed kan vi bruke Proposisjon 5.4 (b), og få at for en κ avhengig av kun a, b og c at

$$h(\xi) \geq 4h(x) - \kappa$$

som er det samme som å si at

$$h(2P) \geq 4h(P) - \kappa.$$

□

4. Restklassene til $2E(\mathbb{Q})$

Det siste lemmaet vi skal vise i dette kapittelet sier at for en elliptisk kurve E over de rasjonale tallene, så har $2E(\mathbb{Q})$ endelig mange restklasser i $E(\mathbb{Q})$. Dette resultatet i likhet med Mordells Teorem gjelder for alle elliptiske kurver med heltalls koeffisienter, men vi kommer til å gjøre antagelsen om at E har minst ett rasjonalt punkt med orden to. Hvis en elliptisk kurve $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ har et rasjonalt punkt av orden to, så betyr det at det ligger en $T = (x_1, 0)$ på E. og vi kan substituere x med $x - x_1$ i likningen for E, da vil vi få utrykket til den elliptiske kurven på formen

$$E : y^2 = f(x) = x^3 + ax^2 + bx, \quad \text{for } a, b \in \mathbb{Z}.$$

Hvor vi vil ha et punk $T = (0, 0)$ av orden to, som ligger på E.

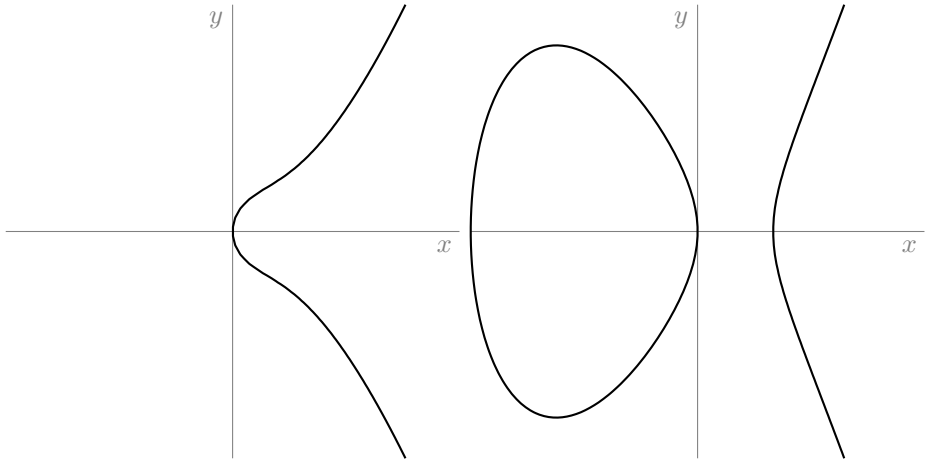
I tillegg til E kommer vi til å se på en kurve $\bar{E} : y^2 = \bar{f}(x) = x^3 + \bar{a}x^2 + \bar{b}x$ som er definert ved

$$\bar{a} = -2a, \quad \text{og} \quad \bar{b} = a^2 - 4b.$$

Hvis vi bruker samme transformasjon på $\bar{E}$ får vi at

$$\begin{aligned}\bar{\bar{a}} &= -2\bar{a} = 4a,\\ \bar{\bar{b}} &= \bar{a}^2 - 4\bar{b}\\ &= 4a^2 - 4a^2 + 16b\\ &= 16b.\end{aligned}$$

Fra dette får vi at $\bar{\bar{E}} : y^2 = \bar{\bar{f}}(x) = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x = x^3 + 4ax^2 + 16bx$, som man kan se er isomorf med E ved å substituere $x = 4x$ og $y = 8y$ og så dele likningen med 64. Kurven $\bar{E}$ kommer til å bli veldig nyttig for å få bevist det fjerdet lemmaet vårt, men først viser vi følgende proposisjon.



FIGUR 5.1. elliptisk kurve $E:\ y^2 = x^3 - x^2 + x$ og tilhørende elliptisk kurve $\bar{E}:\ y^2 = x^3 + 2x^2 - 3x$

PROPOSISJON 5.6. *La E og $\bar{E}$ være to elliptiske kurver med heltalls koeffisienter gitt ved likningene*

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c \quad og \quad \bar{E} : y^2 = \bar{f}(x) = x^3 + \bar{a}x^2 + \bar{b}x,$$

hvor

$$\bar{a} = -2a \quad og \quad \bar{b} = a^2 - 4b.$$

La $T = (0,0) \in E(\mathbb{Q})$.

(a) Det eksisterer en gruppehomomorfi $\phi : E \to \bar{E}$ definert ved

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right), & \text{hvis } P = (x,y) \neq \mathcal{O}, T\\ \bar{\mathcal{O}}, & \text{hvis } P = \mathcal{O} \text{ eller } P = T. \end{cases}$$

Kjernen til ϕ er $\{\mathcal{O}, T\}$.

(b) *Ved å benytte samme prosess på $\bar{E}$ får vi en avbildning $\bar{\phi} : \bar{E} \to \bar{\bar{E}}$. Kurven $\bar{\bar{E}}$ er isomorf til kurven E via avbildningen $(x, y) \mapsto (\frac{1}{4}x, \frac{1}{8}y)$. Det er dermed en gruppehomomorfi $\psi : \bar{E} \to E$ definert ved*

$$\psi(\bar{P}) = \begin{cases} (\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2 - \bar{b})}{8\bar{x}^2}), & \text{hvis } \bar{P} = (\bar{x}, \bar{y}) \neq \bar{\mathcal{O}}, \bar{T} \\ \mathcal{O}, & \text{hvis } \bar{P} = \bar{\mathcal{O}} \text{ eller } \bar{P} = \bar{T}. \end{cases}$$

(c) *Komposisjonen $\psi \circ \phi : E \to E$ er det samme som å multiplisere med 2*

$$\psi \circ \phi(P) = 2P.$$

Bevis. (a) Først starter vi med å vise at ϕ er veldefinert. Dette gjør vi ved å vise at $\phi(P) = (\bar{x}, \bar{y})$ er et punkt på $\bar{E}$.

$$\begin{aligned} \bar{x}^3 + \bar{a}\bar{x}^2 + \bar{b}\bar{x} &= \bar{x}(\bar{x}^2 - 2a\bar{x} + (a^2 - 4b)) \\ &= \frac{y^2}{x^2}\left(\frac{y^4}{x^4} - 2a\frac{y^2}{x^2} + (a^2 - 4b)\right) \\ &= \frac{y^2}{x^2}\left(\frac{y^4 - 2ay^2x^2 + x^4(a^2 - 4b)}{x^4}\right) \\ &= \frac{y^2}{x^2}\left(\frac{(y^2 - ax^2)^2 - 4bx^4}{x^4}\right) \\ &= \frac{y^2}{x^6}\left((x^3 + bx)^2 - 4bx^4\right) \\ &= \frac{y^2}{x^6}(x^6 - 2bx^4 + b^2x^2) \\ &= \left(\frac{y(x^2 - b)}{x^2}\right)^2 \\ &= \bar{y}^2. \end{aligned}$$

Da gjenstår det å vise at

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2), \quad \text{for alle } P_1, P_2 \in E(\mathbb{Q}).$$

Vi ser fort at hvis enten $P_1 = \mathcal{O}$ eller $P_2 = \mathcal{O}$ så fungerer det fint. Vi kan også se at

$$\phi(T + T) = \phi(\mathcal{O}) = \bar{\mathcal{O}} = \bar{\mathcal{O}} + \bar{\mathcal{O}} = \phi(T) + \phi(T).$$

La oss nå se på $T + P$, hvor $P = (x, y) \neq (0, 0)$, da handler det om å vise at $\phi(P + T) = \phi(P)$ ettersom $\phi(T) = \bar{\mathcal{O}}$. Vi får fra formelen for addering av punkter at

$$P + T = (x, y) + (0, 0) = \left(\frac{b}{x}, -\frac{by}{x^2}\right).$$

Hvis vi skriver

$$P + T = (x(P + T), y(P + T)) \quad \text{og} \quad \phi(P + T) = (\bar{x}(P + T), \bar{y}(P + T)),$$

får vi

$$\bar{x}(P + T) = \frac{(by/x^2)^2}{(b/x)^2} = \frac{y^2}{x^2} = \bar{x}(P).$$

Og på samme måte får vi

$$\begin{aligned}\bar{y}(P+T) &= \frac{(-by/x^2)((b/x)^2-b)}{(b/x)^2} \\ &= (-y)\left(\frac{b}{x^2}-1\right) \\ &= \frac{y(x^2-b)}{x^2} \\ &= \bar{y}(P).\end{aligned}$$

Så da ser vi at $\phi(P+T)=\phi(P)$.

Det neste vi ser er at ϕ tar negative til negative

$$\phi(-P)=\phi(x,-y)=\left(\frac{(-y)^2}{x^2},\frac{-y(x^2-b)}{x^2}\right)=(\bar{x},-\bar{y})=-\phi(P).$$

Får å videre vise at ϕ er en homomorfi er det nok å vise at hvis $P_1+P_2+P_3=\mathcal{O}$ så er også $\phi(P_1)+\phi(P_2)+\phi(P_3)=\bar{\mathcal{O}}$. Dette er fordi hvis vi vet dette vet vi også at

$$\phi(P_1+P_2)=\phi(-P_3)=-\phi(P_3)=\phi(P_1)+\phi(P_2).$$

Men det å si at $P_1+P_2+P_3=\mathcal{O}$ er det samme som å si at P_1,P_2 og P_3 ligger på samme linje, $y=\lambda x+\nu$. Derfor kan vi vise at $\phi(P_1)+\phi(P_2)+\phi(P_3)=\bar{\mathcal{O}}$ ved å vise at $\phi(P_1),\phi(P_2)$ og $\phi(P_3)$ ligger på samme linje som skjærer $\bar{E}$. Vi kan anta at ingen av P_1,P_2,P_3 er lik T eller $\mathcal{O}$ ettersom vi allerede har vist det for dem. Dermed vet vi også at $\nu\neq 0$, ettersom da ville T vært på linjen. Linjen vi kommer til å se på er

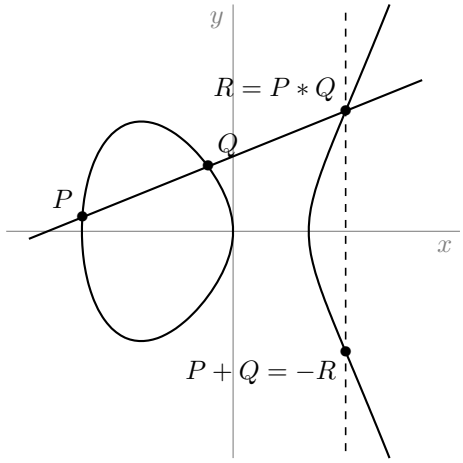
$$y=\bar{\lambda}x+\bar{\nu},\ \text{hvor}\ \bar{\lambda}=\frac{\nu\lambda-b}{\nu}\ \ \text{og}\ \ \bar{\nu}=\frac{\nu^2-a\nu\lambda+b\lambda^2}{\nu}.$$

Vi ser at punktet $\phi(P_i)=\phi(x_i,y_i)=(\bar{x}_i,\bar{y}_i)$ for $i=1,2,3$ ligger på linjen ved følgende utregning

$$\begin{aligned}\bar{\lambda}\bar{x}_i+\bar{\nu} &= \frac{\nu\lambda-b}{\nu}\left(\frac{y_i}{x_i}\right)^2+\frac{\nu^2-a\nu\lambda+b\lambda^2}{\nu} \\ &= \frac{(\nu\lambda-b)y_i^2+(\nu^2-a\nu\lambda+b\lambda^2)x_i^2}{\nu x_i^2} \\ &= \frac{\nu\lambda(y_i^2-ax_i^2)-b(y_i-\lambda x_i)(y_i+\lambda x_i)+\nu^2x_i^2}{\nu x_i^2},\end{aligned}$$

og ved å bruke at $y_i^2 - ax_i^2 = x_i^3 + bx_i$ og $y_i - \lambda x_i = \nu$, får vi

$$\begin{aligned}
&= \frac{\lambda(x_i^3 + bx_i) - b(y_i - \lambda x_i) + \nu x_i^2}{x_i^2} \\
&= \frac{x_i^2(\lambda x_i + \nu) - by_i}{x_i^2} \\
&= \frac{(x_i^2 - b)y_i}{x_i^2} \\
&= \bar{y}.
\end{aligned}$$



FIGUR 5.2. Illustrasjon av å addere tre punkt på samme linje blir $\mathcal{O}$

Merk at det ikke er nok å bare vise at $\phi(P_1), \phi(P_2)$ og $\phi(P_3)$ ligger på linjen $y = \bar{\lambda}x + \bar{\nu}$. For å si at $\phi(P_1) + \phi(P_2) + \phi(P_3) = \bar{\mathcal{O}}$ må vi også vise at $\bar{x}(P_1), \bar{x}(P_2)$ og $\bar{x}(P_1)$ er de eneste løsningene av polynomet $(\bar{\lambda}x + \bar{\nu}) = \bar{f}(x)$, hvor $\bar{x}_i(P_i) = \bar{x}_i = \frac{y_i^2}{x_i^2}$. Ettersom $P_1 + P_2 + P_3 = \mathcal{O}$ vet vi at x_1, x_2 og x_3 er de eneste løsningene av $(\lambda x + \nu)^2 = f(x)$. Fra dette får vi

$$\begin{aligned}
0 &= x^3 - (\lambda^2 - a)x^2 + (b - 2\nu\lambda)x - \nu^2 \\
&= (x - x_1)(x - x_2)(x - x_3) \\
&= x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x - x_1x_2x_3.
\end{aligned}$$

Fra dette får vi følgene tre uttrykk

$$\begin{aligned}
(\lambda^2 - a) &= (x_1 + x_2 + x_3), \\
(b - 2\nu\lambda) &= (x_1x_2 + x_2x_3 + x_3x_1), \\
\nu^2 &= x_1x_2x_3.
\end{aligned}$$

Hvis vi ser på polynomet $(\bar{\lambda}x + \bar{\nu})^2 = \bar{f}(x)$, ser vi at dette er det samme som

$$0 = x^3 - (2a + \bar{\lambda}^2)x^2 + (a^2 - 4b - 2\bar{\nu}\bar{\lambda})x + \bar{\nu}^2. \tag{9}$$

Hvis $\bar{x}_1, \bar{x}_2$ og $\bar{x}_3$ skal være de eneste løsningene av dette polynomene betyr det at høyre siden av (9) må være lik $(x-\bar{x}_1)(x-\bar{x}_2)(x-\bar{x}_3)$. Derfor starter vi med å se på

$$\begin{aligned}
&\bar{x}_1+\bar{x}_2+\bar{x}_3\\
&=\frac{y_1^2}{x_1^2}+\frac{y_2^2}{x_2^2}+\frac{y_3^2}{x_3^2}\\
&=\frac{f(x_1)}{x_1^2}+\frac{f(x_2)}{x_2^2}+\frac{f(x_3)}{x_3^2}\\
&=\frac{x_1^2+ax_1+b}{x_1}+\frac{x_2^2+ax_2+b}{x_2}+\frac{x_3^2+ax_3+b}{x_3}\\
&=\frac{x_1x_2x_3(x_1+x_2+x_3)+3ax_1x_2x_3+b(x_1x_2+x_2x_3+x_3x_1)}{x_1x_2x_3}\\
&=\frac{\nu^2(\lambda^2-a)+3a\nu^2+b(b-2\nu\lambda)}{\nu^2}\\
&=2a+\frac{\lambda^2\nu^2-2\lambda\nu+b^2}{\nu^2} \;=\; 2a+\bar{\lambda}^2.
\end{aligned}$$

Videre ser vi på uttrykket

$$x_1x_2+x_2x_3+x_3x_1=\frac{f(x_1)f(x_2)}{x_1^2x_2^2}+\frac{f(x_2)f(x_3)}{x_2^2x_3^2}+\frac{f(x_3x_1)}{x_1^2x_3^2}.$$

Hvis vi samler på felles brøk får vi $x_1x_2x_3=\nu^2$ i nevneren, og i telleren får vi

$$\begin{aligned}
&x_1x_2x_3(x_1x_2+x_2x_3+x_3x_1)+2ax_1x_2x_3(x_1+x_2+x_3)\\
&+b((x_1+x_2+x_3)(x_1x_2+x_2x_3+x_3x_1)-3x_1x_2x_3)\\
&+3a^2x_1x_2x_3+2ab(x_1x_2+x_2x_3+x_3x_1)+b^2(x_1+x_2+x_3)\\
&=\nu^2(b-2\nu\lambda)+2a\nu^2(\lambda^2-a)+b((\lambda^2-a)(b-2\nu\lambda)-3\nu^2)\\
&+3a^2\nu^2+2ab(b-2\nu\lambda)+b^2(\lambda^2-a).
\end{aligned}$$

Hvis vi regner ut dette videre får vi til slutt

$$a^2-4b-2\frac{\nu^3\lambda-a\nu^2\lambda^2+b\nu\lambda^3-b\nu^2ab\nu\lambda-b^2\lambda^2}{\nu^2}=a^2-4b-2\bar{\nu}\bar{\lambda}.$$

Og til slutt ser vi på uttrykket

$$x_1x_2x_3=\frac{f(x_1)f(x_2)f(x_3)}{x_1^2x_2^2x_3^2}.$$

Hvis vi multipliserer ut så får vi igjen $x_1x_2x_3 = \nu^2$ i nevneren og i telleren får vi

$$\begin{aligned}
&(x_1x_2x_3)^2 + ax_1x_2x_3(x_1x_2 + x_2x_3 + x_3x_1) \\
&+ b((x_1x_2 + x_2x_3 + x_3x_1)^2 - 2x_1x_2x_3(x_1 + x_2 + x_3)) \\
&+ a^2x_1x_2x_3(x_1 + x_2 + x_3) + a^3x_1x_2x_3 \\
&+ ab((x_1 + x_2 + x_3)(x_1x_2 + x_2x_3 + x_3x_1) - 3x_1x_2x_3) \\
&+ b^2((x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1)) \\
&+ a^2b(x_1x_2 + x_2x_3 + x_3x_1) + ab^2(x_1 + x_2 + x_3) + b^3.
\end{aligned}$$

Nå til slutt hvis vi substituerer og kansellerer det vi kan får vi

$$\frac{\nu^4 - 2a\nu^3\lambda + (2b - a^2)\nu^2\lambda^2 - 2ab\nu\lambda^3 + b^2\lambda^4}{\nu^2} = \bar{\nu}^2.$$

Med dette kan vi konkludere med at $\bar{x}_1, \bar{x}_2$ og $\bar{x}_3$ er de eneste løsningene på likningen $(\bar{\lambda}x + \bar{\nu})^2 = \bar{f}(x)$, og har vist at ϕ er en gruppehomomorfi. At $\{\mathcal{O}, T\}$ er kjernen til ϕ følger direkte fra måten ϕ er definert på.

(b) Avbildningen $\bar{\phi}$ vil være en gruppehomomorfi ved samme argument som i (a) og vi så tidligere at $\bar{\bar{E}}$ er isomorf til E. Fra dette får vi at ψ er en gruppehomomorfi.

(c) Vi kan se fra hvordan ϕ er definert at $\phi(P) = 2P$ for $P = \mathcal{O}$ og $P = T$. Hvis vi antar at $P = (x, y)$ er et annet punkt hvor $y = 0$, men $x \neq 0$, da ser vi at $\psi \circ \phi(x, 0) = \psi(0, 0) = \mathcal{O}$. Dermed kan vi anta at $P = (x, y)$ hvor $x \neq 0$ og $y \neq 0$. Hvis vi da regner ut $2P$ med formelen for å addere et punkt på kurven med seg selv får vi

$$\begin{aligned}
2P &= 2(x, y) \\
&= \left(\frac{(3x^2 + 2ax + b)^2 - 8xy^2 - 4ay^2}{4y^2}, y(2P) \right) \\
&= \left(\frac{x^4 - (2b - 4a^2)x^2 + b^2 + 4ax^3 + 4abx - 4af(x)}{4y^2}, y(2P) \right) \\
&= \left(\frac{(x^2 - b)^2}{4y^2}, \frac{\left(3x^2 + 2ax + b\right)\left(x - \frac{(x^2-b)^2}{4y^2}\right) - 2f(x)}{2y} \right) \\
&= \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3} \right).
\end{aligned}$$

Videre regner vi ut

$$\begin{aligned}\psi \circ \phi(x,y) &= \psi\left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) \\ &= \left(\frac{\left(\frac{y(x^2-b)}{x^2}\right)^2}{4\left(\frac{y^2}{x^2}\right)^2}, \frac{\frac{y(x^2-b)}{x^2}\left(\left(\frac{y^2}{x^2}\right)^2 - (a^2-4b)\right)}{8\left(\frac{y^2}{x^2}\right)^2}\right) \\ &= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(y^4-(a^2-4b)x^4)}{8y^3x^2}\right).\end{aligned}$$

Og til slutt hvis vi substituerer $y^4 = x^2(x^2+ax+b)$, får vi at $\psi \circ \phi(P) = 2P$, som fullfører beviset.

□

Det er verdt å legge merke til at ved akkurat samme argument som i (c) så vil $\phi \circ \psi : \bar{E}(\mathbb{Q}) \to \bar{E}(\mathbb{Q})$ være det samme som å addere et punkt med seg selv i $\bar{E}(\mathbb{Q})$.

Videre skal vi vise noen egenskaper for ϕ og ψ, det som er verdt å legge merke til da er at alle argumentene kommer til å holde for begge gruppehomomorfiene. Dette er fordi ϕ og $\bar{\phi}$ er definert nesten helt likt.

Først ønsker vi å se på bildet til ϕ, som vi kommer til å donere $\phi(E)$. Vi hevder følgende tre påstander om $\phi(E)$:

i. $\bar{\mathcal{O}} \in \phi(E)$.
ii. $\bar{T} = (0,0) \in \phi(E)$ hvis og bare hvis $\bar{b} = a^2 - 4b$ er et kvadrattall.
iii. La $\bar{P} = (\bar{x}, \bar{y}) \in \bar{E}(\mathbb{Q})$ hvor $\bar{x} \neq 0$, da er $\bar{P} \in \phi(E)$ hvis og bare hvis $\bar{x}$ er kvadratet av et rasjonalt tall.

Vi kan greit se at i. stemmer ettersom $\phi(\mathcal{O}) = \bar{\mathcal{O}}$.

Vi vet at hvis $\bar{T}$ skal være i bildet til ϕ så må det eksistere et rasjonalt punkt $P = (x,y)$ på E slik at $y = 0$ og $x \neq 0$. For at dette skal stemme må $f(x) = x(x^2+ax+b)$ ha en annen rasjonal løsning enn $x = 0$. Som vil si at $\bar{T}$ er i bildet hvis og bare hvis

$$x = \frac{-a \pm \sqrt{a^2-4b}}{2}$$

har rasjonale løsninger, og vi kan se at dette stemmer hvis og bare hvis $a^2 - 4b = \bar{b}$ er et kvadrattall.

Fra definisjonen av ϕ ser vi helt klart at hvis $\bar{P} = (\bar{x}, \bar{y}) \in \phi(E)$ så er $\bar{x}$ kvadratet av et rasjonalt tall. Men anta at $\bar{x} = w^2$ hvor $w \neq 0$ er et rasjonalt tall. Ettersom det er to elementer i kjernen til ϕ, vet vi at hvis $\bar{P} = (\bar{x}, \bar{y})$ er i bildet,

vil det være to elementer i $E(\mathbb{Q})$ som blir sendt til $\bar{P}$. La

$$x_1 = \frac{1}{2}\left(w^2 - a + \frac{\bar{y}}{w}\right), \qquad y_1 = wx_1,$$
$$x_2 = \frac{1}{2}\left(w^2 - a - \frac{\bar{y}}{w}\right), \qquad y_2 = -wx_2.$$

La oss nå se på følgende uttrykk

$$\begin{aligned} x_1x_2 &= \frac{1}{4}\left((w^2-a)^2 - \frac{\bar{y}^2}{w^2}\right) \\ &= \frac{1}{4}\left((\bar{x}-a)^2 - \frac{\bar{y}^2}{\bar{x}}\right) \\ &= \frac{1}{4}\left(\frac{\bar{x}^3 - 2a\bar{x}^2 + a^2\bar{x} - \bar{y}^2}{\bar{x}}\right) \\ &= b. \end{aligned}$$

Vi får den siste likheten fra likningen for $\bar{E}: \ \bar{y}^2 = \bar{x}^3 - 2a\bar{x}^2 + (a^2 - 4b)\bar{x}$. Hvis vi skal vise at $P_1 = (x_1, y_1)$ og $P_2 = (x_2, y_2)$ ligger på E kan vi se at det er nok å vise at

$$\frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i},$$

for $i = 1, 2$. Videre kan vi se fra hvordan vi har definert y_i at $\frac{y_i}{x_i} = \pm w$. Dermed for å vise at P_i er på E står vi igjen med å vise at

$$w^2 = x_1 + a + x_2,$$

som følger direkte fra slik x_1 og x_2 er definert. Vi regner også ut ved å bruke at $b = x_1x_2$ og $y_i = \pm wx_i$

$$\frac{y_1(x_1^2 - b)}{x_1^2} = \frac{x_1w(x_1^2 - x_1x_2)}{x_1^2} = w(x_1 - x_2) = \bar{y},$$
$$\frac{y_2(x_2^2 - b)}{x_2^2} = \frac{x_2w(x_1x_2 - x_2^2)}{x_2^2} = w(x_1 - x_2) = \bar{y}.$$

Ved dette ser vi at P_i er på kurven E og at $\phi(P_i) = \bar{P}$ for $i = 1, 2$.

Legg merke til at bildet til ψ vil ha akkurat samme egenskaper ved samme argument. Grunnen til at vi ser på bildet til ϕ og ψ er fordi det kommer til nytte i en proposisjon om en avbildning $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$, hvor $\mathbb{Q}^*$ er den multiplikative gruppen av alle rasjonale tall uten om 0, og $(\mathbb{Q}^*)^2$ er undergruppen av alle kvadrater av rasjonale tall. Vi kommer til å studere denne avbildningen i følgende proposisjon

PROPOSISJON 5.7. *La $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ være en avbildning definert ved*

$$\alpha(P) = \begin{cases} 1, & \text{hvis } P = \mathcal{O} \\ b, & \text{hvis } P = T \\ x, & \text{hvis } P = (x, y),\ x \neq 0 \end{cases}.$$

Da vil følgende gjelde

(a) α er en gruppehomomorfi.

(b) Kjernen til α er lik bildet til ψ. Dermed induserer α en injektiv gruppehomomorfi

$$\alpha : E(\mathbb{Q})/\psi(\bar{E}) \hookrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2.$$

(c) La $p_1, p_2, ..., p_t$ være de distinkte primtallsfaktorene til b. Da vil bildet til α være inneholdt i undergruppen av $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ som inneholder alle elementer på formen

$$\{\pm p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_t^{\epsilon_t} \mid \epsilon_i \text{ er enten } 1 \text{ eller } 0\}.$$

(d) $\psi(\bar{E})$ har maksimalt 2^{t+1} ulike restklasser i $E(\mathbb{Q})$.

Bevis. (a) Det første vi ser er at $\alpha(P)\alpha(\mathcal{O}) = \alpha(P)1 = \alpha(P) = \alpha(P + \mathcal{O})$ og $\alpha(2T) = \alpha(\mathcal{O}) = 1 = b^2 = \alpha(T)\alpha(T)$. Vi ser også at for $P \neq T$ at

$$\alpha(P + T) = \alpha\left(\frac{b}{x}, -\frac{by}{x^2}\right) = \frac{b}{x} = xb = \alpha(P)\alpha(T).$$

Vi kan også se at α sender inverser til inverser ved

$$\alpha(-P) = x = \frac{1}{x} = \frac{1}{\alpha(P)}.$$

Nå er det eneste som gjenstår å vise at $\alpha(P_1 + P_2) = \alpha(P_1)\alpha(P_2)$ for alle $P_1, P_2 \neq T, \mathcal{O}$. Dette gjør vi igjen ved å vise at hvis $P_1 + P_2 + P_3 = \mathcal{O}$ så er

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1.$$

Så anta at $P_1 + P_2 + P_3 = 0$ og at $P_i = (x_i, y_i) \neq T, \mathcal{O}$ for $i = 1, 2, 3$ da får vi igjen at P_1, P_2 og P_3 må ligge på samme linje $y = \lambda x + \nu$ hvor $\nu \neq 0$. Vi så tidligere at da vil $x_1 x_2 x_3 = \nu^2$, fra dette får vi at

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1 x_2 x_3 = \nu^2 = 1.$$

Med dette kan vi konkludere med at α er en gruppehomomorfi.

(b) Vi så tidligere at et punkt $P = (x, y) \in E(\mathbb{Q})$ er i bildet til ψ hvis og bare hvis $x \neq 0$ er kvadratet til et rasjonalt tall. Og at T er i bildet hvis og bare hvis $\bar{a}^2 - 4\bar{b} = 16b$ er et kvadrattall som kun stemmer om b er et kvadrattall. Fra dette følger det naturlig at bildet til ψ er inneholdt i kjernen til α.

(c) Vi har tidligere sett at hvis $P = (x, y) \in E(\mathbb{Q})$ så vil $x = m/e^2$ og $y = n/e^3$ hvor e er relativt primisk til både m og n. Hvis vi setter inn i likningen for E og multipliserer med e^6 får vi

$$n^2 = m(m^2 + e^2 am + be^4).$$

La nå $d = \gcd(m, m^2 + e^2 am + be^4)$, da får vi at d må dele både m og be^4. Siden m og e er relativt primiske må d dele b. Vi vil også få følgende

$$\left(\frac{n}{d}\right)^2 = \frac{m}{d}\left(\frac{m^2}{d} + e^2 a\frac{m}{d} + \frac{b}{d}e^4\right),$$

hvor $\frac{n^2}{d^2}$ fortsatt er et heltall og $\frac{m}{d}$ og $\frac{m^2}{d} + e^2 a\frac{m}{d} + \frac{b}{d}e^4$ er relativt primiske. Dette fører til at $\frac{m}{d}$ må være lik pluss-minus et kvadrat. Og fra dette får vi

$$\alpha(P) = \frac{m}{e^2} = me^2 = \pm k^2 d = \pm d = \pm p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_s^{\epsilon_s},$$

hvor $p_1, p_2, ..., p_s$ er primtallsfaktorene til d. Vi så at $d|b$, så det betyr at

$$\alpha(P) \in \{\pm p_1^{\epsilon_1} p_2^{\epsilon_2} ... p_t^{\epsilon_t} \mid \epsilon_i \text{ er enten 1 eller 0}\},$$

hvor $p_1, p_2, ..., p_t$ er primtallsfaktorene til b.

(d) Vi så i (c) at bildet til α er inneholdt i en mengde med 2^{t+1} elementer, og i (b) så vi at α er injektiv fra $E(\mathbb{Q})/\psi(\bar{E})$. Dette viser at $\psi(\bar{E})$ vil ha færre enn 2^{t+1} restklasser i $E(\mathbb{Q})$.

□

Det vi kommer til å bruke videre fra Proposisjon 5.7 er det at $\psi(\bar{E})$ har endelig mange restklasser i $E(\mathbb{Q})$. Legg også merke til at vi på samme måte kan vise at $\phi(E)$ har endelig mange restklasser i $\bar{E}(\mathbb{Q})$.

Med dette er vi klare til å bevise det fjerde og siste lemmaet vi trenger for å vise Mordells Teorem

LEMMA 5.8. *La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve med heltalls koeffisienter hvor $f(x)$ har minst en rasjonal rot. Da vil $2E(\mathbb{Q})$ ha endelig mange restklasser i $E(\mathbb{Q})$.*

BEVIS. Vi vet at E er isomorf med en elliptisk kurve slik at roten til $f(x)$ er flyttet til $x = 0$. Så vi kan la $E : y^2 = x^3 + ax^2 + bx$. Vi vet også at $\phi(E)$ har endelig mange restklasser i $\bar{E}$ og at $\psi(\bar{E})$ har endelig mange restklasser i E. La $R_1, R_2, ..., R_r$ være representanter fra alle restklassene til $\phi(E)$ og la $Q_1, Q_2, ..., Q_s$ være representanter til alle restklassene til $\psi(\bar{E})$. Hvis vi lar $P \in E(\mathbb{Q})$ vet vi at det eksisterer en Q_i slik at $P - Q_i \in \psi(\bar{E})$, la oss si at $P - Q_i = \psi(R)$. Da har vi også at for en R_j vil $R - R_j \in \phi(E)$, la oss si $R - R_j = \psi(P')$. Da får vi følgende

$$\begin{aligned} P = Q_i + \psi(R) &= Q_i + \psi(R_j + \phi(P')) \\ &= Q_i + \psi(R_j) + \psi \circ \phi(P') \\ &= Q_i + \psi(R_j) + 2P'. \end{aligned}$$

Med dette kan vi konkludere med at $2E(\mathbb{Q})$ kan maksimalt ha rs restklasser i $E(\mathbb{Q})$.

□

KAPITTEL 6

Mordells Teorem

I dette kapittele vil vi gi et bevis av Mordells Teorem ved å bruke Lemma 5.2, 5.3, 5.5 og 5.8 som vi viste i kapittel 5.

THEOREM 6.1 (Mordels Teorem). *La $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ være en elliptisk kurve med heltalls koeffisienter, hvor $f(x)$ har minst en rasjonal rot. La $E(\mathbb{Q})$ være gruppen av alle rasjonale punkter på E. Da er $E(\mathbb{Q})$ endelig generert.*

BEVIS. Fra Lemma 5.8 vet vi at $2E(\mathbb{Q})$ har endelig mange restklasser i $E(\mathbb{Q})$, så la $Q_1, Q_2, ..., Q_n$ være representanter fra disse restklassene. La nå $P \in E(\mathbb{Q})$ være et vilkårlig rasjonalt punkt på E. Da vet vi at for en Q_{i_1} at

$$P - Q_{i_1} \in 2E(\mathbb{Q}).$$

La oss si

$$P - Q_{i_1} = 2P_1,$$

for en $P_1 \in E(\mathbb{Q})$. Vi vil også få at det samme gjelder for P_1 med en Q_{i_2}. Hvis vi fortsetter dette videre får vi

$$\begin{aligned} P - Q_{i_1} &= 2P_1 \\ P_1 - Q_{i_2} &= 2P_2 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m, \end{aligned}$$

hvor $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_m}$ er valgt blant $Q_1, Q_2, \ldots, Q_n$. Disse likhetene kan vi nå bruke til å uttrykke P på formen

$$P = a_1Q_1 + a_2Q_2 + \cdots + a_nQ_n + 2^mP_m,$$

hvor $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Videre ser vi på høyden til P_{j-1} i forhold til P_j. Fra Lemma 5.3 vet vi at for hver $-Q_i$, $i = 1, 2, \ldots, n$ eksisterer det en κ_i slik at

$$h(R - Q_i) \leq 2h(R) + \kappa_i \quad \text{for alle } R \in E(\mathbb{Q}).$$

La κ' være den største av de endelig mange κ_i. Vi vet også fra Lemma 5.5 at det eksisterer en κ slik at

$$4h(R) \leq h(2R) + \kappa \quad \text{for alle } R \in E(\mathbb{Q}).$$

Fra dette får vi følgende

$$\begin{aligned} 4h(P_j) &\leq h(2P_j) + \kappa \\ &= h(P_{j-1} - Q_{i_j}) + \kappa \\ &\leq 2h(P_{j-1}) + \kappa' + \kappa. \end{aligned}$$

Hvis vi deler på 4 på begge sider får vi videre

$$\begin{aligned} h(P_j) &\leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa' + \kappa}{4} \\ &= \frac{3}{4}h(Pj-1) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa)). \end{aligned}$$

Fra denne ulikheten ser vi at hvis $h(P_{j-1}) \geq \kappa' + \kappa$ så vil $h(P_j) \leq \frac{3}{4}h(P_{j-1})$. Og ettersom $(\frac{3}{4})^t$ vil gå mot null når t øker, betyr det at vi kan finne en m slik at $h(P_m) \leq \kappa' + \kappa$. Så nå har vi vist at alle rasjonale punkter P på E kan skrives på formen

$$P = a_1Q_1 + a_2Q_2 + \cdots + a_nQ_n + 2^mR,$$

hvor $h(R) \leq \kappa' + \kappa$ som betyr at mengden

$$\{Q_1, Q_2, ..., Q_n\} \cup \{R \in E(\mathbb{Q}) \mid h(R) \leq \kappa' + \kappa\}$$

genererer hele $E(\mathbb{Q})$, og fra Lemma 5.2 har vi at $\{R \in E(\mathbb{Q}) \mid h(R) \leq \kappa' + \kappa\}$ er en endelig mengde. Fra dette kan vi konkludere med at $E(\mathbb{Q})$ er en endelig generert gruppe.

□

Bibliografi

[1] E. Bezout, *Théorie génerale des équations algébriques*, Paris (1779)

[2] E. Lutz, *Sur l'équation* $y^2 = x^3 - Ax - B$ *dans les corps p-adiques*, J. Reine Angew. Math, **177**, 238-247 (1937)

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

[4] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, Journal de Mathématiques Pures et Appliquées 7, 161-234 (1901)

[5] Joseph H. Silverman and John T. Tate, *Rational Points on Elliptic Curves*, Springer, New York, London, (2015)

NTNU

Kunnskap for en bedre verden