Indhold

0.1 Etablering af gruppestrukturen

Det er muligt at påføre de elliptiske kurver en gruppestruktur, ved en geometrisk addition af punkter fra en sådan kurve. Vi skal i dette kapitel indføre denne gruppelov og vise, at det resulterer i en abelsk gruppe.

0.1.1 Elliptiske kurver

Først og fremmest skal vi have defineret, hvad en elliptisk kurve er. Her følger definitionen, som vi vil benytte igennem dette projekt.

Definition 1 (Elliptisk kurve)**.** En elliptisk kurve er grafen for en ligning på formen

$$y^2 = x^3 + Ax + B \tag{1}$$

for $A, B \in K$. Denne form kaldes for Weierstrass normalform.

Bemærkning 1. I tilfældet hvor karakteristikken af K er 2 eller 3 kan vi ikke opnå at få funktionen på Weierstrass normalform.

Vi kræver desuden for en elliptisk kurve, at

$$\Delta = -16(4A^3 + 27B^2) \neq 0,$$

hvor Δ er diskriminanten. Dette er tilsvarende til, at kurvens rødder har multiplicitet 1.

0.1.2 Det projektive plan

Som tidligere nævnt vil vi etablere en gruppestruktur på de elliptiske kurver. For at kunne gøre dette får vi brug for det projektive plan $\mathbb{P}^2$. Rent intuitivt kan man se det projektive plan, som værende den affine plan

$$\mathbb{A}^2(K) = \{(x, y) \in K \times K\},$$

hvor K et et legeme, med en ekstra linje "i uendelig". Vi ønsker at formalisere dette begreb. For $x, y, z \in K$ ikke alle nul og $\lambda \in K$, $\lambda \neq 0$, definerer vi en ækvivalensrelation. To tripler (x_1, y_1, z_1) og (x_2, y_2, z_2) siges at være ækvivalente hvis

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2),$$

og vi skriver $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$. Vi vil fremover skrive $(x : y : z)$ for en sådan ækvivalensklasse. I de tilfælde hvor $z \neq 0$ har vi, at

$$(x, y, z) = (x/z, y/z, 1),$$

hvilket er de punkter vi kalder for de "endelige"punkter i $\mathbb{P}^2(K)$. Vi er nemlig i stand til at associere et punkt fra $\mathbb{A}^2(K)$ med et sådan punkt. Vi har en afbildning (en inklusion for at være mere præcis) $\mathbb{A}^2(K) \to \mathbb{P}^2(K)$ givet ved

$$(x, y) \mapsto (x, y, 1).$$

Dette kan vi selvfølgelig ikke gøre, når $z = 0$ og vi ser det som at vi har ∞ i enten x- eller y-koordinaten. Vi kalder dermed punkterne $(x, y, 0)$ for punkterne i "uendelig".

0.1.3 Gruppeloven

Lad nu E være en elliptisk kurve over K som i 1. Mængden af punkter på E med koordinater i K er givet ved

$$E(K) = \{\mathcal{O}\} \cup \{(x, y) \in K \times K \mid y^2 = x^3 + Ax + B\},$$

hvor $\mathcal{O}$ er punktet i uendelighed, som vi vil definere senere. Vi definerer da en binær operator/funktion + på $E(K)$ ved følgende algoritme:

Definition 2 (Gruppeloven for elliptiske kurver)**.** Givet to punkter $P_1, P_2 \in E(K)$, $P_i = (x_i, y_i)$. Et tredje punkt $R = P_1 + P_2 = (x_3, y_3)$ findes da som følger

1. Hvis $x_1 \neq x_2$ da er

   $$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1,$$

   hvor $m = (y_2 - y_1)/(x_2 - x_1)$.

2. Hvis $x_1 = x_2$, men $y_1 \neq y_2$ da er $R = P_1 + P_2 = \mathcal{O}$.

3. Hvis $P_1 = P_2$ og $y_1 \neq 0$ da er

   $$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1,$$

   hvor $m = (3{x_1}^2 + A)/2y_1$.

4. Hvis $P_1 = P_2$ og $y_1 = 0$ da er $R = P_1 + P_2 = \mathcal{O}$.

Vi definerer desuden, at

$$P + \mathcal{O} = \mathcal{O},$$

for alle $P \in E(K)$.

Vælg to punkter

$$P = (x_p, y_p), \quad Q = (x_q, y_q)$$

på en elliptisk kurve E. Vi kan da trække en ret linje, L, igennem punkterne P og Q, som vil skære kurven for E i et tredje punkt $P * Q$. Reflektér dette punkt og vi definerer $P+Q$ til at være dette punkt. Lad desuden $\mathcal{O}$ betegne punktet i uendelighed.

Vi skal nu udlede formlerne for additionen af disse punkter. Lad først $P \neq Q$ og lad P og Q være forskellige fra $\mathcal{O}$. Da har vi, at hældningen for linjen igennem P og Q er

$$m = \frac{y_q - y_p}{x_q - x_p}.$$

Hvis $x_p = x_q$ er linjen lodret, hvilket er et tilfælde vi behandler senere. Så lad $x_p \neq x_q$, da får vi videre at

$$y_q = m(x_q - x_p) + y_p.$$

Vi indsætter dette i ligningen for E og får, at

$$(m(x - x_p) + y_p)^2 = x^3 + Ax + B.$$

Skriver vi dette ud får vi, at

$$\begin{aligned} 0 &= x^3 + Ax + B - 2y_p m(x - x_p) - m^2(x - x_p)^2 - y_p^2 \\ &= x^3 + Ax + B - 2y_p mx - 2y_p mx_p - m^2(x^2 - 2xx_p + x_p^2) - y_p^2 \\ &= x^3 - m^2x^2 + (A - 2my_p + 2m^2x_p)x - 2my_p x_p - m^2x_p^2 - y_p^2 + B. \end{aligned}$$

Denne har tre rødder, som netop er de tre punkter, hvor L skærer E. Pr. vores konstruktion kender vi allerede de to rødder x_p og x_q, og vi ønsker at finde den tredje. Generelt for et kubisk polynomium $x^3 + ax^2 + bx + c$, med rødder r, s, t, har vi at

$$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + \ldots,$$

hvilket giver os, at $-a = r + s + t$. Hvis de to rødder vi kender er r og s kan vi finde den sidste som

$$t = -a - r - s.$$

I vores tilfælde er $a = -m^2$ så vi har, at

$$x = m^2 - x_p - x_q.$$

Vi mangler da blot at reflektere dette punkt for at have fundet punktet punktet $P + Q = (x, y)$. Vi reflekterer over x-aksen og finder, at

$$x = m^2 - x_p - x_q, \quad y = m(x_p - x) - y_p.$$

Vi vender nu tilbage til tilfældet, hvor $x_p = x_q$. Da vil linjen igennem P og Q være lodret, så den skærer E i $\mathcal{O}$. Vi husker, at når $\mathcal{O}$ reflekteres over x-aksen får vi igen $\mathcal{O}$. Vi får altså, at $P + Q = \mathcal{O}$.

Tilfældet hvor $P = Q = (x, y)$ kræver lidt flere overvejelser, da ikke ligeså let kan udvælge en linje. For to punkter der ligger tæt på hinanden vil linjen igennem punkterne nærme sig tangenten til et af punkterne. Derfor vælger vi i dette tilfælde, at lade linjen der går igennem punkterne være deres tangentlinje.

Blah blah blah.

Hvis $P = \mathcal{O}$ er linjen igennem P og Q en lodret linje der skærer E i refleksionen af Q. Derfor får vi, at

$$\mathcal{O} + Q = Q.$$

Der gælder derfor også, at $\mathcal{O} + \mathcal{O} = \mathcal{O}$.

Vi har nu dækket de mulige tilfælde og kan opstille gruppeloven som følger.

Kapitel 1

Faktoriseringsalgoritmer

Vi vil i dette kapitel introducere nogle forskellige algoritmer der kan benyttes til faktorisering. Først introduceres Pollards $p-1$ algoritme, hvilket er den algoritme som var inspirationen for Lenstras algoritme, der benytter elliptiske kurver.

Motivationen for disse hurtigere metoder er, at en naiv tilgang er meget langsom. Antag at n er et sammensat tal, som vi ønsker at faktorisere. Hvis n faktoriseres som $n = n_1 n_2$ er det klart, at $\min\{n_1, n_2\} \leq \sqrt{n}$. Vi kan da finde en faktor ved at undersøge om først $2 \mid n$, dernæst om $3 \mid n$ osv. Vi vil da finde en faktor senest når vi kommer til $\sqrt{n}$.

1.1 Pollards $p-1$ metode

Før vi beskriver algoritmen skal vi først bruge følgende definition.

Definition 3 (B-potensglat)**.** Lad $B \in \mathbb{Z}^+$. Hvis $n \in \mathbb{Z}^+$ har primtalsfaktoriseringen $n = \prod {p_i}^{e_i}$, da siges n at være B-potensglat hvis ${p_i}^{e_i} \leq B$ for alle i.

Eksempel 1. Da $50 = 2 \cdot 5^2$ følger det, at 50 er 25-potensglat. Bemærk, at den netop ikke er 5-potensglat.

Med disse detaljer på plads er vi nu klar til, at beskrive Pollards $p-1$ algoritme. Antag at det sammensatte tal n, som vi ønsker at faktorisere, har en primfaktor p sådan, at $p-1$ har mange små primtalsfaktorer. Fra Fermats lille sætning ved vi, at

$$a^{p-1} \equiv 1 \pmod{p},$$

hvilket betyder at $p \mid \gcd(a^{p-1} - 1, n)$. Men da vi ikke kender p (det er jo den faktor vi leder efter)

Algoritme 1 (Pollards $p-1$ algoritme)**.** Lad $n \geq 2$ være et sammensat tal, som er tallet vi ønsker at finde en faktor for.

1. Vælg et tal $k \in \mathbb{Z}^+$ sådan, at k er et produkt af mange små primtal opløftet i små potenser. F.eks. kan k vælges som

   $$k = \text{LCM}[1, 2, \ldots, K],$$

   for $K \in \mathbb{Z}^+$.

2. Vælg et heltal a sådan, at $1 < a < n$.

3. Udregn $\gcd(a, n)$. Hvis $\gcd(a, n) > 1$ har vi fundet en ikke-triviel faktor for n og vi er færdige. Ellers fortsæt til næste trin.

4. Udregn $D = \gcd(a^k - 1, n)$. Hvis $1 < D < n$ er D en ikke-triviel faktor for n og vi er færdige. Hvis $D = 1$ gå da tilbage til trin 1 og vælg et større k. Hvis $D = n$ gå da til trin 2 og vælg et nyt a.

Følgende er et eksempel på anvendelsen af Pollards algoritme, hvor det går godt, altså hvor $p-1$ har små primfaktorer.

Eksempel 2. Vi vil forsøge at faktorisere

$$N = 30042491.$$

Vi ser at $2^{N-1} = 2^{30042490} \equiv 25171326 \pmod{30042491}$, så N er ikke et primtal. Vi vælger som beskrevet i algoritmen

$$a = 2 \quad \text{og} \quad k = \text{LCM}(1, 2, 3, 4, 5, 6, 7) = 420.$$

Da $420 = 2^2 + 2^5 + 2^7 + 2^8$ skal vi udregne 2^{2^i} for $0 \leq i \leq 8$. Vi springer de første par udregninger over.

i	$2^{2^i} \pmod{N}$
5	28933574
6	27713768
7	10802810
8	16714289

Denne tabel gør det forholdsvist let for os, at bestemme

$$\begin{aligned} 2^{420} &= 2^{2^2+2^5+2^7+2^8} \\ &\equiv 16 \cdot 28933574 \cdot 10802810 \cdot 16714289 \pmod{30042491} \\ &\equiv 27976515 \pmod{30042491} \end{aligned}$$

Ved anvendelse af den euklidiske algoritme finder vi dernæst, at

$$\gcd(2^{420}-1, N) = \gcd(27976514, 30042491) = 1.$$

Her fejler testen altså og vi er nået frem til, at N ikke har nogle primtalsfaktorer p sådan, at $p-1$ deler 420.

1.2 Lenstras elliptiske kurve metode

Vi vil nu se på Lenstras metode til at avende elliptiske kurver til at faktorisere heltal. Idéerne til denne algoritme bygger videre på Pollards $p-1$ metode, men den har den fordel, at hvor vi før kun havde en gruppe, $\mathbb{Z}/n\mathbb{Z}$, at arbejde over, kan vi nu skifte imellem en masse.

Eksempel 3. Vi vil nu give et eksempel for anvendelsen af Lenstras algoritme.

Vi har nu demonstreret, hvordan Lenstras faktoriseringsalgoritme anvendes i praksis og vil nu se på, hvorfor den er en effektiv algoritme til dette problem. Vi vil vise Hasses sætning, som giver en grænse for antallet af punkter på en elliptisk kurve over et endeligt legeme.

Sætning 1 (Hasses sætning)**.** *Lad $q = p^m$, hvor et primtal så $p \neq 2, 3$ og lad $A, B \in \mathbb{F}_q$ med $\Delta = 4a^3 + 27b^2 \neq 0$. Hvis vi lader $\#E(\mathbb{F}_q)$ være antallet af løsninger til*

$$y^2 = x^3 + Ax + B, \tag{1.1}$$

over $\mathbb{F}_q$, da vil

$$|\#E(\mathbb{F}_q) - q| \leq 2\sqrt{q}. \tag{1.2}$$

Lad E være en elliptisk kurve, som i (2.1). Til denne elliptiske kurve tilknytter vi endnu en elliptisk kurve E_λ. For polynomiet

$$\lambda(t) = t^3 + At + B,$$

i $\mathbb{F}_q[t]$ lader vi E_λ være en elliptisk kurve over $\mathbb{F}_q(t)$ givet ved

$$\lambda y^2 = x^3 + Ax + B. \tag{1.3}$$

Da dette er ikke den sædvanlige form skal vi justere additionsformlerne for, at vi stadigvæk opnår en gruppestruktur. Det kan ses, at $(t, 1)$ og $-(t, 1) = (t, -1) \in E_\lambda(K)$ ved indsættelse i (2.3).

Vi får altså en veldefineret funktion

$$d : \mathbb{Z} \to \{0, 1, 2, \ldots\},$$

som er givet ved

$$d(n) = d_n = \begin{cases} 0 & \text{hvis } P_n = \mathcal{O} \\ \deg f_n & \text{ellers.} \end{cases}$$

Forbindelsen mellem denne funktion $d(n)$ og Hasses sætning er følgende forhold mellem d_n og N_q, som vi vil bevise:

Lemma 1. *Der gælder for funktionen d_n og antallet af punkter N_q på E følgende lighed*

$$d_{-1} - d_0 - 1 = N_q - q. \tag{1.4}$$

Bevis. Bemærk først at $d_0 = q$ da $\deg t^q = q$. Vi mangler da at vise, at $d_{-1} = N_q + 1$. For at vise ligheden vil vi reducere X_{-1}, fra de modificerede additionsformler finder vi, at

$$\begin{aligned} X_{-1} &= (t^3 + at + b)\left(\frac{(t^3 + at + b)^{(q-1)/2} + 1}{t^q - t}\right)^2 - (t^q + t) \\ &= (t^3 + at + b)\frac{\left((t^3 + at + b)^{(q-1)/2} + 1\right)^2}{(t^q - t)^2} - (t^q + t) \\ &= \frac{t^{2q+1} + R(t)}{(t^q - t)^2}, \end{aligned}$$

hvor $R(t)$ er et polynomium hvor $\deg R(t) \leq 2q$. Vi bemærker, at over $\mathbb{F}_q$ kan vi skrive

$$t^q - t = \prod_{\alpha \in \mathbb{F}_q} (t - \alpha) = t(t-1)\dots(t-q+1).$$

Der er kun to forskellige faktorer over $\mathbb{F}_q$, som kan udgå. Da en faktor af den første type er relativt primisk til en faktor af den anden type har vi nu, at

$$d_{-1} = \deg f_{-1} = 2q + 1 - 2m - n,$$

hvor vi husker at for den første type er det en dobbeltrod. Idet vi husker, at $d_0 = q$ følger det, at

$$d_{-1} - d_0 = q + 1 - 2m - n.$$

□

Vi ønsker nu, at se nærmere på funktionen $d(n)$ og vi vil vise følgende lemma:

Lemma 2. *For funktionen $d(n)$ gælder der, at*

$$d_n = n^2 - (d_{-1} - d_0 - 1)n + d_0. \tag{1.5}$$

Bevis. Vi vil vise lemmaet vha. induktion. For $n = 0$ og $n = -1$ ser vi først, at

$$\begin{aligned} d_{-1} &= (-1)^2 + (d_{-1} - d_0 - 1) + d_0 = 1 + d_{-1} - d_0 - 1 + d_0 = d_{-1}, \\ d_0 &= d_0 = 0^2 - 0 \cdot (d_{-1} - d_0 - 1) + d_0 = d_0. \end{aligned}$$

Antag da, at (2.5) er sandt for $n - 1$ og n, hvor $n \geq 0$. □

Vi vil her give et bevis for Hasse's sætning. Til dette formål skal vi først opbygge nogle resultater vedrørende endomorfier på endelige legemer.

Definition 4 (Algebraisk aflukning)**.** En algebraisk aflukning af et legeme K, er et legeme $K \subseteq \overline{K}$, hvor $\overline{K}$ er en algebraisk udvidelse af K samt, at ethvert ikke-konstant polynomium fra $\overline{K}[X]$ har en rod i $\overline{K}$.

Det kan vises, at ethvert legeme har en algebraisk aflukning og at to algebraiske aflukninger for det samme legeme vil være isomorfe. Derfor giver det mening for os, at snakke om *den* algebraiske aflukning for et givent legeme. Lad nu $\mathbb{F}_q$ være et endeligt legeme med algebraisk aflukning $\overline{\mathbb{F}}_q$. Vi ser på Frobenius afbildningen

$$\phi_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q,$$

som er givet ved, at $x \mapsto x^q$. For en elliptisk kurve E over $\mathbb{F}_q$ virker ϕ_q på koordinaterne $E(\overline{\mathbb{F}}_q)$ ved, at

$$\phi_q(x, y) = (x^q, y^q), \quad \phi_q(\infty) = \infty.$$

I det følgende udnytter vi, at q er et primtal (men bogen arbejder måske blot med at $q = p^r$, hvor p er et primtal. Da skal der tilføjes lidt resultater.

Lemma 3. *Lad E være en elliptisk kurve over $\mathbb{F}_q$, og lad $(x, y) \in E(\overline{\mathbb{F}}_q)$. Da gælder der, at*

1. $\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$,
2. $(x, y) \in E(\mathbb{F}_q) \Leftrightarrow \phi_q(x, y) = (x, y)$.

Bevis. Vi har, at $y^2 = x^3 + ax + b$, hvor $a, b \in \mathbb{F}_q$. Vi opløfter denne ligning til den q'ende potens og får, at

$$(y^q)^2 = (x^q)^3 + (a^q x^q) + b^q,$$

hvor vi har brugt Freshman's dream. Men dette betyder netop, at $(x^q, y^q) \in E(\overline{\mathbb{F}}_q)$, hvilket viser (1). For at vise (2) husker vi, at $\phi_q(x) = x \Leftrightarrow x \in \mathbb{F}_q$. Det følger da, at

$$\begin{aligned}(x, y) \in E(\mathbb{F}_q) &\Leftrightarrow x, y \in \mathbb{F}_q \\ &\Leftrightarrow \phi_q(x) = x \text{ og } \phi_q(y) = y \\ &\Leftrightarrow \phi_q(x, y) = (x, y).\end{aligned}$$

□

Lemma 4. *Lad E være en elliptisk kurve over $\mathbb{F}_q$. Da er ϕ_q en endomorfi for E af grad q, desuden er ϕ_q ikke seperabel.*