Indhold

1 Etablering af gruppestrukturen

I dette kapitel vil vi introducere elliptiske kurver. Det viser sig, at være muligt at påføre de elliptiske kurver en gruppestruktur ved en geometrisk addition af punkter fra en sådan kurve. Vi vil indføre denne additionslov og vise, at det resulterer i en abelsk gruppe. For at kunne gøre dette skal vi desuden anvende projektiv geometri, som også vil blive introduceret.

1.1 Elliptiske kurver

For at kunne snakke om elliptiske kurver skal vi først og fremmest have defineret, hvad en elliptisk kurve er. Vi vil i denne tekst benytte følgende definition:

Definition 1. En elliptisk kurve E er grafen for en ligning

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

hvor $A, B \in K$ er konstanter og $4A^3 + 27B^2 \neq 0$. Denne type elliptisk kurve siges at være på Weierstrass normalform.

Da $\Delta = -16(4A^3 + 27B^2)$ er diskriminanten for (1.1) betyder det, at vi ikke tillader multiple rødder for en elliptisk kurve. Altså har kurvens rødder alle multiplicitet 1. Der findes mere generelle definitioner af elliptiske kurver, men når vi arbejder over legemer som ikke har karakteristik 2 eller 3, kan vi altid skrive en elliptisk kurve på Weierstrass normalform.

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".

1.3 Gruppeloven

Lad nu E være en elliptisk kurve over K som i 1.1. 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

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

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.

2 Elliptiske kurver over endelige legemer

Vi skal i dette kapitel undersøge elliptiske kurver over endelige legemer. Lad $\mathbb{F}$ være et endeligt legeme og lad E være en elliptisk kurve på formen

$$y^2 = x^3 + Ax + B,$$

som er defineret over $\mathbb{F}$. Da er gruppen $E(\mathbb{F})$ endelig, da der kun findes endeligt mange talpar (x, y) så $x, y \in \mathbb{F}$. Lad E være den elliptiske kurve $y^2 = x^3 - x$ over $\mathbb{F}_5$. For at bestemme ordenen af $E(\mathbb{F})$ laver vi en tabel over mulige værdier for x, $x^3 - x \pmod 5$ og for y som er kvadratrødderne af $x^3 - x$. Dette giver os samtlige punkter på kurven:

x	$x^3 - x$	y	Punkter
0	0	0	$(0, 0)$
1	0	0	$(1, 0)$
2	1	± 1	$(2, 1), (2, 4)$
3	4	± 2	$(3, 2), (3, 3)$
4	2	–	–
∞		∞	∞

Bemærk, at $\sqrt{2} \notin \mathbb{Z}$ og derfor har 2 ikke en kvadratrod i $\mathbb{F}_5$. Dette giver os, at $E(\mathbb{F}_5)$ har orden 7 og vi skriver $\#E(\mathbb{F}_5) = 7$. Vi skal i dette kapitel vise Hasses sætning, som giver en vurdering for antallet af punkter på en elliptisk kurve over et endeligt legeme:

Sætning 1 (Hasse)**.** *Lad E være en elliptisk kurve over et endeligt legeme $\mathbb{F}_q$. Da gælder der, at*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Vi vil i kapitel 3 se på en af anvendelserne, som disse elliptiske kurver over endelige legemer har, nemlig indenfor faktorisering af heltal.

2.1 Endomorfier

Vi skal først have etableret nogle resultater vedrørende endomorfier på endelige legemer, som er nødvendige for beviset af Hasses sætning. Lad K være et legeme og $\overline{K}$ dens tilhørende algebraiske aflukning. Når vi skriver om en elliptisk kurve E menes den at være på formen $y^2 = x^3 + Ax + B$.

Vi begynder da med følgende definition:

Definition 3. En endomorfi på E er en homomorfi $\alpha : E(\overline{K}) \to E(\overline{K})$ givet ved rationale funktioner.

Med en rational funktion forstår vi en kvotient af polynomier. Det vil altså sige, at en endomorfi α skal opfylde, at $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ og der skal findes rationale funktioner $R_1(x, y)$ og $R_2(x, y)$, begge med koefficienter i $\overline{K}$, så

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

for alle $(x, y) \in E(\overline{K})$. da α er en homomorfi gælder der, at $\alpha(\infty) = \infty$. Den trivielle endomorfi angives med 0 og er den endomorfi, som sender ethvert punkt til ∞. Vi vil fremover antage, at α ikke er den trivielle endomorfi, hvilket betyder at der findes (x, y) sådan at $\alpha(x, y) \neq \infty$.

Eksempel 1. Skal vi have en endomorfi her?

Vi ønsker nu, at finde en standard repræsentation for de rationale funktioner, som en endomorfi er givet ved. Følgende sætning gør dette muligt for os:

Sætning 2. *Lad E være en elliptisk kurve over et legeme K. En endomorfi α kan da skrives som*

$$\alpha(x, y) = (r_1(x), r_2(x)y) = \left(\frac{p(x)}{q(x)}, \frac{s(x)}{t(x)}y\right),$$

hvor p, q henholdsvis s, t ikke har nogen fælles faktor.

Bevis. For et punkt $(x, y) \in E(\overline{K})$ gælder der, at $y^2 = x^3 + Ax + B$ så vi har også, at

$$y^{2k} = (x^3 + Ax + B)^k \quad \text{og} \quad y^{2k+1} = y^{2k}y = (x^3 + Ax + B)^k y, \quad k \in \mathbb{N}.$$

Vi kan altså erstatte en lige potens af y med et polynomium der kun afhænger af x, og en ulige potens med y ganget med et polynomium der kun afhænger af x. For en rational funktion $R(x, y)$ kan vi da beskrive en anden

rational funktion, som stemmer overens med denne på punkter fra $E(\overline{K})$. Vi kan altså antage, at

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}. \tag{2.1}$$

Vi kan endda gøre det endnu simplere ved at gange udtrykket i (2.1) med $p_3(x) - p_4(x)$, hvilket giver

$$(p_3(x) - p_4(x)y)(p_3(x) + p_4(x)y) = p_3(x)^2 - p_4(x)^2y^2,$$

hvorefter vi kan erstatte y^2 med $x^3 + Ax + B$. Dette giver os altså, at

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{2.2}$$

Da α er en endomorfi er den givet ved

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)),$$

hvor R_1 og R_2 er rationale funktioner. Da α specielt er en homomorfi bevarer den strukturen for en elliptisk kurve så vi har, at

$$\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y).$$

Dette medfører, at

$$R_1(x,-y) = R_1(x,y) \quad \text{og} \quad R_2(x,-y) = -R_2(x,y).$$

Skriver vi R_1 på samme form som i (2.2) må $q_2(x) = 0$, og ligeledes må vi for R_2 have at $q_1(x) = 0$. Vi kan altså antage, at

$$\alpha(x,y) = (r_1(x), r_2(x)y),$$

hvor $r_1(x)$ og $r_2(x)$ er rationale funktioner. Skriv da

$$r_1(x) = \frac{p(x)}{q(x)} \quad \text{og} \quad r_2(x) = \frac{s(x)}{t(x)}y,$$

hvor p, q henholdsvis s, t ikke har nogen fælles faktorer. Hvis $q(x) = 0$ for et punkt (x,y) lader vi $\alpha(x,y) = \infty$. Hvis $q(x) \neq 0$ giver (ii) i lemma 1, at $r_2(x)$ da også vil være defineret. □

Lemma 1. *Lad α være en endomorfi givet ved*

$$\alpha(x,y) = \left(\frac{p(x)}{q(x)}, \frac{s(x)}{t(x)}y\right),$$

for en elliptisk kurve E. Lad p, q henholdsvis s, t være sådan, at de ikke har nogen fælles rødder. Da har vi, at

(i) For et polynomium $u(x)$, som ikke har en fælles rod med $q(x)$ har vi, at

$$\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3}.$$

(ii) $t(x_0) = 0$ hvis og kun hvis $q(x_0) = 0$.

Bevis. (i) For et punkt $(x, y) \in E(K)$ har vi også, at $\alpha(x, y) \in E(K)$, da α er en endomorfi. Derfor har vi, at

$$\begin{aligned}\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} &= \frac{y^2 s(x)^2}{t(x)^2} = \left(\frac{s(x)}{t(x)}y\right)^2 \\ &= \left(\frac{p(x)}{q(x)}\right)^3 + A\left(\frac{p(x)}{q(x)}\right) + B \\ &= \frac{p(x)^3 + Ap(x)q(x)^2 + Bq(x)^3}{q(x)^3} = \frac{u(x)}{q(x)^3},\end{aligned}$$

hvor $u(x) = p(x)^3 + Ap(x)q(x)^2 + Bq(x)^3$. Antag nu, at $q(x_0) = 0$. Hvis nu også $u(x_0) = 0$ følger det, at

$$\begin{aligned}u(x_0) = p(x_0)^3 + Ap(x_0)q(x_0)^2 + Bq(x_0)^3 = 0 &\Rightarrow p(x_0)^3 = 0 \\ &\Rightarrow p(x_0) = 0,\end{aligned}$$

men p og q havde pr. antagelse ingen fælles rødder. Så hvis $q(x_0) = 0$ må $u(x_0) \neq 0$ og de har dermed ingen fælles rødder.

(ii) Vi ved fra (i), at

$$(x^3 + Ax + B)s(x)^2 q(x)^3 = u(x)t(x)^2. \tag{2.3}$$

Hvis $q(x_0) = 0$ følger det direkte fra (2.3), at

$$u(x_0)t(x_0)^2 = 0.$$

Da q og u ikke har nogen fælles rødder følger det, at $t(x_0) = 0$. Antag nu, at $t(x_0) = 0$, da har vi fra (2.3), at

$$({x_0}^3 + Ax_0 + B)s(x_0)^2 q(x_0)^3 = 0.$$

Da s og t pr. antagelse ikke har nogen fælles rødder giver det yderligere, at

$$({x_0}^3 + Ax_0 + B)q(x_0)^3 = 0.$$

Hvis ${x_0}^3 + Ax_0 + B \neq 0$ er $q(x_0)^3 = 0$ og dermed må $q(x_0) = 0$. Hvis vi derimod har, at ${x_0}^3 + Ax_0 + B = 0$ er det klart, at $(x - x_0) \mid (x^3 + Ax + B)$. Med andre ord findes et polynomium $Q(x)$ sådan, at

$$(x^3 + Ax + B) = (x - x_0)Q(x),$$

hvor $Q(x_0) \neq 0$, da $x^3 + Ax + B$ ikke har nogen dobbeltrødder. Da $t(x_0) = 0$ findes der også et polynomium $T(x)$ sådan, at

$$t(x) = (x - x_0)T(x).$$

Udtrykket fra (2.3) kan da skrives, som

$$(x - x_0)Q(x)s(x)^2q(x)^3 = u(x)((x - x_0)T(x))^2,$$

hvilket med division med $(x - x_0)$ giver os, at

$$Q(x)s(x)^2q(x)^3 = u(x)(x - x_0)T(x)^2.$$

I tilfældet, hvor $x = x_0$ har vi så, at

$$Q(x_0)s(x_0)^2q(x_0)^3 = 0,$$

men da $Q(x_0) \neq 0$ og $s(x_0) \neq 0$ må $q(x_0)^3 = 0$ så $q(x_0) = 0$. □

Med den nu etablerede standard repræsentation for endomorfier, er vi i stand til at give en definition for graden af en endomorfi:

Definition 4. Graden af en endomorfi α er givet ved

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\},$$

når α ikke er den trivielle endomorfi, altså for $\alpha \neq 0$. For $\alpha = 0$ lader vi $\deg(\alpha) = 0$.

En endomorfi siges at være separabel hvis den afledede $r_1'(x) \neq 0$.

Eksempel 2. Eksempel på en separabel endomorfi. Bogen ser på $2P$ som også er oplagt, men måske skulle man vælge en mere interessant.

Den følgende proposition er essentiel idet, at det tilknytter graden af en endomorfi til antallet af elementer i kernen for selvsamme endomorfi, hvilket vi skal benytte direkte i beviset for Hasses sætning.

Proposition 1. *Lad E være en elliptisk kurve. Lad $\alpha \neq 0$ være en separabel endomorfi for E. Da er*

$$\deg \alpha = \#\ker(\alpha),$$

hvor $\ker(\alpha) =$ *angiver kernen for homomorfien $\alpha : E(\overline{K}) \to E(\overline{K})$. I tilfældet hvor $\alpha \neq 0$ ikke er separabel gælder der, at*

$$\deg \alpha > \#\ker(\alpha).$$

Bevis. Vi skriver α på standardformen, som vi introducerede tidligere, altså sættes

$$\alpha(x, y) = (r_1(x), r_2(x)y)),$$

hvor $r_1(x) = p(x)/q(x)$. Da α er antaget til at være separabel er $r_1' \neq 0$ og dermed er $pq' - p'q$ ikke nulpolynomiet. Lad nu

$$S = \{x \in \overline{K} \mid (pq' - p'q)(x)q(x) = 0\}.$$

Lad da $(a, b) \in E(\overline{K})$ være valgt sådan, at følgende er opfyldt

1. $a \neq 0$, $b \neq 0$ og $(a, b) \neq \infty$,
2. $\deg(p(x) - aq(x)) = \max\{\deg p(x), \deg q(x)\} = \deg \alpha$,
3. $a \notin r_1(S)$,
4. $(a, b) \in \alpha(E(\overline{K}))$.

Da $pq' - p'q$ ikke er nulpolynomiet er S en endelig mængde, hvilket dermed også betyder, at $\alpha(S)$ er en endelig mængde. Funktionen $r_1(x)$ antager uendeligt mange forskellige værdier når x gennemløber $\overline{K}$, da en algebraisk aflukning indeholder uendeligt mange elementer. Da der for hvert x er et punkt $(x, y) \in E(\overline{K})$ følger det, at $\alpha(E(\overline{K}))$ er en uendelig mængde. Det er altså muligt, at vælge et punkt $(a, b) \in E(\overline{K})$ med egenskaberne ovenfor.

Vi ønsker at vise, at der netop er $\deg \alpha$ punkter $(x_1, y_1) \in E(\overline{K})$ sådan, at $\alpha(x_1, y_1) = (a, b)$. For et sådan punkt gælder der, at

$$\frac{p(x_1)}{q(x_1)} = a, \quad r_2(x_1)y_1 = b.$$

Da $(a, b) \neq \infty$ er $q(x_1) \neq 0$. Da $b \neq 0$ har vi også, at $y_1 = b/r_2(x_1)$. Dette betyder, at y_1 er bestemt ved x_1, så vi behøver kun at tælle værdier for x_1. Fra antagelse (2) har vi, at $p(x) - aq(x) = 0$ har $\deg \alpha$ rødder talt med

multiplicitet. Vi skal altså vise, at $p - aq$ ikke har nogen multiple rødder. Antag for modstrid, at x_0 er en multipel rod. Da har vi, at

$$p(x_0) - aq(x_0) = 0 \quad \text{og} \quad p'(x_0) - aq'(x_0) = 0.$$

Dette kan omskrives til ligningerne $p(x_0) = aq(x_0)$ og $aq'(x_0) = p'(x_0)$, som vi ganger med hinanden og får, at

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0).$$

Da $a \neq 0$ pr. (1) giver det os, at x_0 er en rod i $pq' - p'q$ så $x_0 \in S$. Altså er $a = r_1(x_0) \in r_1(S)$, hvilket er i modstrid med (3). Dermed har $p - aq$ netop $\deg \alpha$ forskellige rødder. Da der er præcist $\deg \alpha$ punkter (x_1, y_1) så $\alpha(x_1, y_1) = (a, b)$ har kernen for α netop $\deg \alpha$ elementer. □

2.2 Frobenius endomorfien

En endomorfi med en absolut kritisk rolle for teorien om elliptiske kurver over endelige legemer er Frobenius endomorfien ϕ_q. For en elliptisk kurve E over et endeligt legeme $\mathbb{F}_q$ er denne givet ved

$$\phi_q(x, y) = (x^q, y^q), \tag{2.4}$$

og $\phi_q(\infty) = \infty$. Denne endomorfi spiller en vigtig rolle i beviset for Hasses sætning, men vi skal først vise nogle af dens egenskaber.

Lemma 2. *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.*

Bevis. Vi skal vise, at $\phi_q : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ er en homomorfi. Lad da $(x_1, y_1), (x_2, y_2) \in E(\overline{\mathbb{F}}_q)$, hvor $x_1 \neq x_2$. Da følger det fra gruppeloven, at summen af de to punkter $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ er givet ved

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{hvor } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Opløftes dette i q'ende potens får vi, at

$$x_3{}^q = m'^2 - x_1{}^q - x_2{}^q, \quad y_3{}^q = m'(x_1{}^q - x_3{}^q) - y_1{}^q, \quad \text{hvor } m' = \frac{y_2{}^q - y_1{}^q}{x_2{}^q - x_1{}^q}.$$

Dette giver os, at $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$, hvilket netop er hvad ϕ_q skal opfylde for at være en homomorfi. I tilfældet hvor $x_1 = x_2$ har vi fra gruppeloven, at $(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = \infty$. Men hvis $x_1 = x_2$ må

${x_1}^q = {x_2}^q$ hvilket betyder, at $\phi_q(x_1, y_1) + \phi_q(x_2, y_2) = \infty$. Så da $\infty^q = \infty$ (lægges ∞ sammen q gange er det stadigvæk ∞) får vi, at

$$\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2).$$

Hvis ét af punkterne er ∞, eksempelvis $(x_1, y_1) = \infty$, har vi fra gruppeloven, at $(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = (x_2, y_2)$. Bruger vi igen, at $\infty^q = \infty$ følger det direkte, at $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$.

Når $(x_1, y_1) = (x_2, y_2)$ hvor $y_1 = 0$ er $(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = \infty$. Når $y_1 = 0$ er ${y_1}^q = 0$ så $\phi_q(x_1, y_1) + \phi_q(x_2, y_2) = \infty$ og dermed er $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$.

Det resterende tilfælde er når $(x_1, y_1) = (x_2, y_2)$ og $y_1 \neq 0$. Fra gruppeloven har vi, at $(x_3, y_3) = 2(x_1, y_1)$, hvor

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{hvor } m = \frac{3{x_1}^2 + A}{2y_1}.$$

Som tidligere opløftes dette til den q'ende potens

$${x_3}^q = {m'}^2 - 2{x_1}^q, \quad {y_3}^q = m'({x_1}^q - {x_3}^q) - {y_1}^q, \quad \text{hvor } m' = \frac{3^q({x_1}^q)^2 + A^q}{2^q {y_1}^q}.$$

Idet, at $2, 3, A \in \mathbb{F}_q$ følger det, at $2^q = 2, 3^q = 3$ og $A^q = A$. Vi står altså tilbage med formlen for fordoblingen af punktet $({x_1}^q, {y_1}^q)$ på den elliptiske kurve E.

Dermed har vi vist, at ϕ_q er en homomorfi for E. Da $\phi_q(x, y) = (x^q, y^q)$ er givet ved polynomier, som specielt er rationale funktioner, er ϕ_q en endomorfi. Den har tydeligvis grad q. Da $q = 0$ i $\mathbb{F}_q$ er den afledte af x^q lig nul, hvilket betyder at ϕ_q ikke er separabel. □

Bemærk, at da ϕ_q er en endomorfi for E er ${\phi_q}^2 = \phi_q \circ \phi_q$ det også og dermed også ${\phi_q}^n = \phi_q \circ \phi_q \circ \ldots \circ \phi_q$ for $n \geq 1$. Da multiplikation med -1 også er en endomorfi er ${\phi_q}^n - 1$ også en endomorfi for E.

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, at $(a+b)^q = a^q + b^q$ når q er en potens af legemets karakteristik (detaljer placeres i appendiks?). 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

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

hvilket fuldfører beviset for (2). □

Proposition 2. *Lad E være en elliptisk kurve over $\mathbb{F}_q$ og lad $n \geq 1$. Da gælder der, at*

1. $\ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$.
2. *$\phi_q^n - 1$ er separabel, så* $\#E(\mathbb{F}_{q^n}) = \deg(\phi_q^n - 1)$.

Bevis. Da $(\phi_q^n - 1)(x,y) = 0 \Leftrightarrow (x^q, y^q) = (x,y)$ følger det fra lemma 3, at $\ker(\phi_q^n - 1) = E(\mathbb{F}_q)$. Da ϕ_q^n er Frobenius afbildningen for $\mathbb{F}_{q^n}$ følger (1) fra lemma 3. At $\phi_q^n - 1$ er separabel vil vi ikke vise, men et bevis kan findes i [LW]. Da følger det fra proposition 1, at $\#E(E_{q^n}) = \deg(\phi_q^n - 1)$. □

2.3 Hasses sætning

Med de foregående resultater er vi nu næsten klar til at vise Hasses sætning (sætning 1). Lad i det følgende afsnit

$$a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\phi_q - 1). \tag{2.5}$$

Da skal vi vise, at $|a| \leq 2\sqrt{q}$ for at vise Hasses sætning. Først har vi dog følgende lemma

Lemma 4. *Lad $r, s \in \mathbb{Z}$ så* $\gcd(s,q) = 1$. *Da er*

$$\deg(r\phi_q - s) = r^2 q + s^2 - rsa.$$

Bevis. Vi vil ikke give beviset her, da det bygger på en række af tekniske resultater. Et bevis kan findes i [LW]. □

Nu er vi da i stand til, at gives beviset for Hasses sætning:

Bevis for Hasses sætning. Da graden af en endomorfi altid er ≥ 0 følger det fra lemma 4, at

$$r^2q + s^2 - rsa = q\left(\frac{r^2}{s^2}\right) - \frac{rsa}{s^2} + 1 \geq 0,$$

for alle $r, s \in \mathbb{Z}$ med $\gcd(s, q) = 1$. Da mængden

$$\left\{\frac{r}{s} \mid \gcd(s, q) = 1\right\} \subseteq \mathbb{Q},$$

er tæt i $\mathbb{R}$ (se appendiks?) følger det, at $qx^2 - ax + 1 \geq 0$, for alle $x \in \mathbb{R}$. Dette medfører at diskrimanten må være negativ eller lig 0. Altså har vi, at

$$a^2 - 4q \leq 0 \Rightarrow |a| \leq 2\sqrt{q},$$

hvilket viser Hasses sætning. □

Eventuelt afsnit for torsionspunkter?

Følgende sætning følger også fra proposition 2, som vil vise sig at være nyttigt til at udvide resultatet fra Hasses sætning.

Sætning 3. *Lad E være en elliptisk kurve over $\mathbb{F}_q$. Lad a være som i* (2.5)*. Da er a det entydige heltal så*

$$\phi_q{}^2 - a\phi_q + q = 0,$$

set som endomorfier. Med andre ord er a det entydige heltal sådan, at

$$(x^{q^2}, y^{q^2}) - a(x^q, y^q) + q(x, y) = \infty,$$

for alle $(x, y) \in E(\overline{\mathbb{F}}_q)$. Desuden er a det entydige heltal der opfylder, at

$$a \equiv \mathit{Trace}((\phi_q)_m) \pmod{m},$$

for alle m, hvor $\gcd(m, q) = 1$.

Før vi starter på beviset for sætning 3 skal vi først se på torsions punkterne for en elliptisk kurve. For en elliptisk kurve E givet over et legeme K lader vi

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty\}.$$

Det er altså de punkter, hvis orden er endelig (alle punkter over et endeligt legeme er torsions punkter).

Opskriv eventuelt sætning 3.2?

Lad da $\{\beta_1, \beta_2\}$ være en basis for $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$. Ethvert element fra $E[n]$ kan altså skrives som $\beta_1 m_1 + \beta_2 m_2$, hvor $m_1, m_2 \in \mathbb{Z}$ er entydige mod n. For en homomorfi $\alpha : E(\overline{K}) \to E(\overline{K})$ afbilleder α torsionspunkterne $E[n]$ til $E[n]$, derfor findes $a, b, c, d \in \mathbb{Z}$ sådan, at

$$\alpha(\beta_1) = a\beta_1 + b\beta_2, \quad \alpha(\beta_2) = c\beta_1 + d\beta_2.$$

Vi kan altså repræsentere en sådan homomorfi med matricen

$$\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Bevis for sætning 3. Det følger direkte fra lemma 1, at hvis ${\phi_q}^2 - a\phi_q + q \neq 0$, altså hvis den ikke er nul-endomorfien, da er dens kerne endelig. Så hvis vi kan vise, at kernen er uendelig, da må endomorfien være lig 0.

Lad nu $m \geq 1$ være valgt sådan, at $\gcd(m, q) = 1$. Lad da $(\phi_q)_m$ være den matricen, som beskriver virkningen af ϕ_q på $E[m]$, som vi beskrev ovenfor. Lad da

$$(\phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}.$$

Da $\phi_q - 1$ er separabel følger det fra proposition 1 og 3.15 (nævn resultat og henvis?, at

$$\begin{aligned} \#\ker(\phi_q - 1) = \deg(\phi_q - 1) &\equiv \det((\phi_q)_m - I) \\ &= \begin{vmatrix} s-1 & t \\ u & v-1 \end{vmatrix} \\ &= sv - tu - (s+v) + 1 \pmod{m}. \end{aligned}$$

Fra 3.15 (henvis, opskriv?) har vi, at $sv - tu = \det((\phi_q)_m) \equiv q \pmod{m}$. Fra (2.5) har vi, at $\#\ker(\phi_q - 1) = q + 1 - a$ så det følger, at

$$\mathrm{Trace}((\phi_q)_m) = s + v \equiv a \pmod{m}.$$

Idet vi husker, at $X^2 - aX + q$ er det karakteristiske polynomium for $(\phi_q)_m$ følger det fra Cayley-Hamiltons sætning fra lineær algebra, at

$${(\phi_q)_m}^2 - a(\phi_q)_m + qI \equiv I \pmod{m},$$

hvor I er 2×2 identitetsmatricen. Vi har da, at endomorfien ${\phi_q}^2 - a\phi_q + q$ er nul på $E[m]$. Da der er uendeligt mange muligheder for valget af m er kernen for $\phi^2 - a\phi_q + q$ uendelig. Dermed er endomorfien lig 0.

Mangler beviset for entydigheden af a. □

Endeligt vil vi vise en sætning, som gør det muligt at bestemme ordenen af en gruppe af punkter for en elliptisk kurve. Hvis vi kender ordenen af $E(\mathbb{F}_q)$ for et lille endeligt legeme gør følgende sætning det muligt, at bestemme ordenen af $E(\mathbb{F}_{q^n})$.

Sætning 4.12 og bevis, som afslutning på kapitlet.

3 Faktoriseringsalgoritmer

Vi vil i dette kapitel se på en af de anvendelser, som elliptiske kurver har, nemlig faktorisering af heltal. Vi ved fra aritmetikkens fundamentalsætning, at ethvert positivt heltal større end 1 enten er et primtal eller kan skrives som et entydigt produkt af primtal. Vi ønsker da for et heltal n, at bestemme sådan en primtalsfaktor. Vi vil i dette kapitel introducere to forskellige algoritmer, som kan benyttes til faktorisering. Først vil vi se på Pollards $p-1$ algoritme, som dog ikke benytter sig af elliptiske kurver, men som var inspirationen til den anden algoritme vi vil se på, nemlig Lenstras algoritme der benytter elliptiske kurver.

Motivationen for disse hurtigere metoder er, at en naiv tilgang til faktoriseringsproblemet 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 $\sqrt{n}$. Dette bliver hurtigt uoverkommeligt når n er stort.

3.1 Pollards $p-1$ algoritme

Lad n være et sammensat tal og lad p være en primfaktor for n. Vi ved fra Fermats lille sætning, at $a^{p-1} \equiv 1 \pmod{p}$ når $\gcd(a,p) = 1$. Hvis vi da kendte $p-1$ kunne vi bestemme p (udover den åbenlyse måde) ved

$$\gcd(a^{p-1} - 1, n) = p.$$

(måske et multiplum af p?), da hvis $x \equiv 1 \pmod{l}$, hvor l er en faktor i n, er $\gcd(x-1, n)$ divisibel med denne faktor l.

Vi kender dog ikke $p-1$ og vi kan derfor ikke foretage denne udregning. Det viser sig dog, at vi kan nøjes med et multiplum af $p-1$, da

$$a^{t(p-1)} - 1 = (a^{p-1})^k - 1 \equiv 1^k - 1 \equiv 0 \pmod{p}.$$

Idéen er da, at vi vælger et heltal

$$k = 2^{e_2} \cdot 3^{e_3} \cdot 5^{e_5} \cdots r^{e_r},$$

hvor $2, 3, \ldots, r$ er primtal og $e_1, e_2, \ldots, e_r$ er små positive heltal. Vi udregner da $\gcd(a^k - 1, n)$. Hvis vi er i det heldige tilfælde, hvor n har en faktor sådan, at $p - 1 \mid k$, da vil $p \mid a^k - 1$ og vi har så, at

$$\gcd(a^k - 1, n) \geq p > 1.$$

Hvis $\gcd(a^k - 1, n) \neq n$ har vi altså fundet en ikke-triviel faktor for n og vi kan dele n i to faktorer og gentage de ovenstående trin. Hvis vi derimod har, at $\gcd(a^k - 1, n) = n$ vælger vi et andet a og forsøger igen, og hvis $\gcd(a^k - 1, n) = 1$ vælger vi et større k.

Dette er tankegangen i Pollards $p - 1$ algoritme og vi opsummerer det i algoritmen:

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 $k \in \mathbb{Z}^+$ sådan, at k er et produkt af mange små primtal opløftet i små potenser. Eksempelvis kan k vælges til at være

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

   for et $K \in \mathbb{Z}^+$ og hvor LCM er det mindste fælles multiplum.

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 3. 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

$$a = 2 \quad \text{og} \quad k = \mathrm{LCM}[1, 2, \ldots, 7] = 420.$$

Da $420 = 2^2 + 2^5 + 2^7 + 2^8$ skal vi udregne 2^{2^i} for $0 \leq i \leq 8$. Dette resulterer i følgende tabel:

i	$2^{2^i} \pmod n$		
1	4	5	28933574
2	16	6	27713768
3	256	7	10802810
4	65536	8	16714289
5	28933574		

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

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

Her fejler testen altså og vi er nået frem til, at N ikke har nogle primtalsfaktorer p sådan, at $p-1$ deler 420. Algoritmen foreskriver da, at vi skal vælge et nyt k. Vi lader

$$k = \mathrm{LCM}[1, 2, \ldots, 11] = 27720.$$

Da $27720 = 2^{14} + 2^{13} + 2^{11} + 2^{10} + 2^6 + 2^3$ skal vi udvide tabellen til at indeholde værdierne for 2^{2^i} for $0 \leq i \leq 14$:

i	$2^{2^i} \pmod n$		
9	19694714	12	26818902
10	3779241	13	8658967
11	11677316	14	3783587

Vi fortsætter på samme måde, som vi gjorde før og bestemmer

$$\begin{aligned} 2^{27720} &= 2^{2^3+2^{2^6}+2^{2^{10}}+2^{2^{11}}+2^{2^{13}}+2^{2^{14}}} \\ &= 256 \cdot 27713768 \cdot 3779241 \cdot 11677316 \cdot 8658967 \cdot 3783587 \\ &= 16458222 \pmod{30042491}. \end{aligned}$$

Vi finder dernæst, at

$$\gcd(2^{27720} - 1 \pmod n, n) = \gcd(16458221, 30042491) = 9241,$$

hvilket betyder at vi har fundet en ikke-triviel faktor for n. Mere præcist har vi fundet faktoriseringen

$$30042491 = 3251 \cdot 9241.$$

3.2 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 4. Vi vil nu give et eksempel for anvendelsen af Lenstras algoritme.