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 6 og vi skriver $\#E(\mathbb{F}_5) = 6$. 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. Vi begynder 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 forståes 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 $(x, y) \in E(\overline{K})$. Det følger desuden, at $\alpha(\infty) = \infty$ da α specielt er en homomorfi. 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 $\alpha(x, y) \neq \infty$.

Vi ønsker da, at finde en standard repræsentation for de rationale funktioner, som beskriver en endomorfi. For en elliptisk kurve E på Weierstrass normalform gælder der, at $y^2 = x^3 + Ax + B$ for alle $(x, y) \in E(\overline{K})$, hvilket betyder at

$$y^{2k} = (x^3 + Ax + B)^k,$$

hvor $k \in \mathbb{N}$. På lignende vis har vi også, at

$$y^{2k}y = (x^3 + Ax + B)^k y.$$

Vi kan altså erstatte en lige potens af y med et polynomium der kun afhænger af x, og en ulige potens kan erstattes af y ganget med et polynomium der kun afhænger af x. For en rational funktion $R(x, y)$ kan vi nu beskrive en anden rational funktion, som stemmer overens med denne på punkter fra $E(\overline{K})$. Vi kan med andre ord antage, at

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

Det er endda muligt, at gøre dette endnu simplere ved at gange udtrykket i (2.1) med $p_3(x) - p_4(x)y$, da

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

hvorefter vi kan erstatte y^2 med $x^3 + Ax + B$. Vi får da, at

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

Lader vi nu α være en endomorfi givet ved

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

får vi, da α er en homomorfi, at

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

Dette medfører, at

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

Skrives R_1 og R_2 på samme form som i (2.2) følger det da, at $q_2(x) = 0$ for R_1 og $q_1(x) = 0$ for R_2. Vi kan altså antage, at

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

hvor $r_1(x)$ og $r_2(x)$ begge er rationale funktioner. Skriv da $r_1(x) = p(x)/q(x)$. (For $q(x) \neq 0$ giver opg. 2.19, at $r_2(x)$ er defineret, så funktionerne der giver α er defineret. Vis det.).

Vi er nu i stand til at komme 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 1. 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 α forskellige rødder. Da der er præcist deg α punkter (x_1, y_1) så $\alpha(x_1, y_1) = (a, b)$ har kernen for α netop deg α elementer. □

2.2 Frobenius endomorfien

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

$$\phi_q(x, y) = (x^q, y^q). \tag{2.3}$$

Denne endomorfi spiller en vigtig rolle i beviset for Hasses sætning, men vi skal først vise, at den har nogle specielle egenskaber:

Lemma 1. *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 bemærker først, at $\phi_q(x, y) = (x^q, y^q)$ er en funktion givet ved polynomier, som specielt er rationale. Så hvis ϕ_q er en endomorfi er graden af den q.

For at vise, at ϕ_q er en endomorfi skal vi vise, at $\phi_q : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ er en homomorfi. □

Lemma 2. *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

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

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 2, 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 2. 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

$$a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\phi_q - 1). \tag{2.4}$$

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

Lemma 3. *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 altså 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 3, 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 $\mathbb{R}$ 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. □