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. Vi vil fremover antage, at α ikke er den trivielle endomorfi, altså 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

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

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 $r_2(x)$ er rationale funktioner. Skriv da $r_1(x) = p(x)/q(x)$ (opgave om den rent faktisk er defineret).