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, $x^3 - x$ (mod 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

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

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

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

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

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

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. $\square$

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. $\square$

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. $\square$

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.