Vi vil her give et bevis for Hasse's sætning, der giver os en (optimal) vurdering af antallet af punkter på en elliptisk kurve. Til dette formål skal vi først opbygge nogle resultater vedrørende endomorfier på endelige legemer, som benyttes i beviset for dette.

Definition 4. 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 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 $(x,y) \in E(\overline{K})$. Dette giver os også, da α er en homomorfi, at $\alpha(\infty) = \infty$. 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

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}. \tag{3.6}$$

Det er endda muligt, at gøre dette endnu simplere ved at gange udtrykket i (3.6) 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

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{3.7}$$

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 (3.7) 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).

Definition 5. Graden af en endomorfi α er givet ved

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

hvis α er ikke-triviel. Hvis α er den trivielle endomorfi lader vi $\deg(\alpha) = 0$.

Vi siger, at α er en separabel endomorfi, hvis den afledede $r_1'(x)$ ikke er lig nul.

Definition 6 (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 $\overline{K}$.

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

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

hvilket fuldfører beviset for (2). □

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.*

Bevis. Beviset går på at vise, at $\phi_q : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ er en homomorfi. Dette gøres vha. additionsformlerne. Se f.eks. [1]. □

Dette betyder, at ${\phi_q}^2 = \phi_q \circ \phi_q$ også er en endomorfi, hvilket vi kan udvide til ${\phi_q}^n$ for $n \geq 1$ er en endomorfi. Da multiplikation samtidigt er en endomorfi følger det, at ${\phi_q}^n - 1$ også er det.

Det næste resultat bliver afgørende for beviset for Hasses sætning. Det fortæller os om graden af en endomorfi for en elliptisk kurve E, som eksempelvis ϕ_q er det.

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 det opfylder følgende

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 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

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

En hurtig omskrivning giver os 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.

□