Kapitel 3

Elliptiske kurver over endelige legemer

Vi skal i dette kapitel betragte elliptiske kurver over endelige legemer. Lad $\mathbb{F}$ være et endeligt legeme og lad E være en elliptisk kurve over $\mathbb{F}$. Da er gruppen $E(\mathbb{F})$ endelig, da der kun findes endeligt mange talpar (x, y) hvor $x, y \in \mathbb{F}$. Et endeligt legeme har p^n elementer for et primtal p, hvor $n \geq 1$ (se bilag A.1). Derfor lader vi $\mathbb{F}_q$ være det endelige legeme med $q = p^n$ elementer.

Vi vil vise Hasses sætning, som giver os en vurdering på antallet af punkter i gruppen $E(\mathbb{F}_q)$. Denne vurdering viser sig, at have en anvendelse indenfor heltalsfaktorisering, som vi ser på i kapitel 4. Vi ser også på en måde, hvorpå vi kan bestemme den eksakte orden af en gruppe $E(\mathbb{F}_{q^n})$, hvis vi kender ordenen af $E(\mathbb{F}_q)$, som er let at bestemme for legemer med få elementer.

3.1 Eksempler

Lad E være en elliptisk kurve på formen

$$E : y^2 = x^3 - x,$$

defineret over $\mathbb{F}_5$. Da er gruppen $E(\mathbb{F}_5)$ endelig, som nævnt ovenfor. For at bestemme den eksakte orden af $E(\mathbb{F}_5)$ laver vi en tabel over alle mulige værdier for x, $x^3 - x \pmod 5$ og for kvadratrødderne y af $x^3 - x \pmod 5$. 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	–	–
∞		∞	∞

Vi kan da tælle punkterne og vi ser, at $E(\mathbb{F}_5)$ har orden 7, hvilket vi skriver som $\#E(\mathbb{F}_5) = 7$. Bemærk at $\sqrt{2} \notin \mathbb{Z}_5$, hvilket er hvorfor der ikke er en tilhørende værdi for y til $x = 4$.

Additionen af punkterne på en sådan kurve over et endeligt legeme foretages på samme måde, som i formlerne i gruppeloven, men de foretages modulo p. Eksempelvis hvis vi ville bestemme $(1,0) + (3,3)$ får vi, at

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{3-0}{3-1} = \frac{3}{2} \equiv 4 \pmod 5.$$

Dermed har vi, at

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 = 4^2 - 1 - 3 = 12 \equiv 2 \pmod 5, \\ y_3 &= m(x_1 - x_3) - y_1 = 4(1-2) - 0 = -4 \equiv 1 \pmod 5. \end{aligned}$$

Vi får altså punktet

$$(1,0) + (3,3) = (2,1),$$

som netop er ét af punkterne vi har opgivet i tabellen.

3.2 Frobenius endomorfien

I det forrige kapitel så vi på endomorfier for generelle legemer. Nu vil vi se på en endomorfi som er defineret over endelige legemer, som viser sig at have en kritisk rolle i vores bevis for Hasses sætning. Denne endomorfi er Frobenius endomorfien ϕ_q. For en elliptisk kurve E over et endeligt legeme $\mathbb{F}_q$ er denne givet ved

$$\phi_q(x,y) = (x^q, y^q), \quad \phi_q(\infty) = \infty. \tag{3.1}$$

Vi skal nu vise nogle af de egenskaber, som denne endomorfi besidder:

Lemma 2 *Lad E være en elliptisk kurve over $\mathbb{F}_q$. Da er ϕ_q en endomorfi for E af grad q, som ikke er separabel.*

Vi skal bruge, at $(a+b)^q = a^q + b^q$ når $q = p^n$ hvor p er et primtal (se appendiks A.1).

Bevis. Vi vil først 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 $x_1 \neq x_2$. Det følger da fra gruppeloven, at summen af de to punkter $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ er givet ved

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2, \\ y_3 &= m(x_1 - x_3) - y_1, \end{aligned}$$

hvor $m = (y_2 - y_1)/(x_2 - x_1)$. Opløfter vi til q'ende potens får vi videre, at

$$x_3^q = m'^2 - x_1^q - x_2^q,$$
$$y_3^q = m'(x_1^q - x_3^q) - y_1^q,$$

hvor $m' = (y_2^q - y_1^q)/(x_2^q - x_1^q)$. Sammensætter vi de resultater har vi netop, at $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$, hvilket er hvad ϕ_q skal opfylde for at være en homomorfi (for alle punkter).

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 $\infty^q = \infty$ 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 vi har endnu engang, at $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$.

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

$$x_3 = m^2 - 2x_1,$$
$$y_3 = m(x_1 - x_3) - y_1,$$

hvor $m = (3x_1^2 + A)/2y_1$. På samme måde som før opløfter vi dette til den q'ende potens og får, at

$$x_3^q = m'^2 - 2x_1^q,$$
$$y_3^q = m'(x_1^q - x_3^q) - y_1^q,$$

hvor $m' = (3^q(x_1^q)^2 + A^q)/2^q y_1^q$. Idet, at $2, 3, A \in \mathbb{F}_q$ følger det, at $2^q = 2, 3^q = 3$ og $A^q = A$. Dette er altså netop formlen for fordoblingen af punktet (x_1^q, y_1^q) på den elliptiske kurve E. Hvis $A^q \neq A$ ville vi have været på en anden elliptisk kurve. Vi har dermed 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. □

Bemærkning 1. 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 $\mathbb{F}_q$, da gælder der*

1. $\phi_q(x,y) \in E(\overline{\mathbb{F}}_q)$,
2. $(x,y) \in E(\mathbb{F}_q) \Leftrightarrow \phi_q(x,y) = (x,y)$,

for alle $(x,y) \in E(\overline{\mathbb{F}}_q)$.

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

$$\begin{aligned}(y^q)^2 &= (x^q)^3 + A^q(x^q) + B^q \\ &= (x^q)^3 + A(x^q) + B.\end{aligned}$$

hvor vi har brugt, at $(a+b)^q = a^q + b^q$ når q er en potens af legemets karakteristik og at $a^q = a$ for alle $a \in \mathbb{F}_q$ (se appendiks A.1). 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). □

Følgende proposition er vigtig, da den skaber en sammenhæng mellem kernen for $\phi_q^n - 1$ og antallet af punkter på en elliptisk kurve E over et endeligt legeme $\mathbb{F}_q$.

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. Betragter vi $(\phi_q^n - 1)$ som en endomorfi har vi, at

$$(\phi_q^n - 1)(x,y) = 0 \Leftrightarrow (x^{q^n}, y^{q^n}) - (x,y) = 0 \Leftrightarrow (x^{q^n}, y^{q^n}) = (x,y).$$

Da ϕ_q^n er Frobenius afbildningen for $\mathbb{F}_{q^n}$ følger det at

$$\ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$$

fra lemma 3. At $\phi_q^n - 1$ er separabel vil vi ikke vise, men et bevis kan findes i [4, s. 58]. Da $\phi_q^n - 1$ er separabel følger det fra proposition 1, at

$$\#E(E_{q^n}) = \deg(\phi_q^n - 1).$$

Vi har dermed vist det ønskede. □

3.3 Hasses sætning

Vi skal i dette afsnit vise Hasses sætning nu, da vi har fået etableret de nødvendige resultater vedrørende endomorfier på elliptiske kurver over endelige legemer.

Sætning 4 (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 skal i kapitel 4 hvordan elliptiske kurver over endelige legemer kan benyttes til heltalsfaktorisering, hvilket bl.a. hviler på Hasses sætning. Det skal nævnes, at der også findes et elementært bevis for Hasses sætning af Manin, CITE, men vi vil benytte teorien om endomorfier til at bevise sætningen. Lad i det følgende

$$a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\phi_q - 1). \tag{3.2}$$

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*

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

Bevis. Vi vil ikke give beviset her, da det bygger på en række af tekniske resultater. For et bevis se [4, s. 100]. □

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 $\mathbb{R}$ følger det, at $qx^2 - ax + 1 \geq 0$, for alle $x \in \mathbb{R}$ (se proposition 4 i A.3). 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. □

3.4 Torsionspunkter

Det viser sig, at proposition 2 også har andre interessante konsekvenser, som vi vil se på her.

Ordenen af et element P fra en gruppe over en elliptisk kurve er det mindste positive heltal k sådan at $kP = P + P + \ldots P = \infty$. Hvis der ikke findes et sådan k siges ordenen af P at være uendelig. Torsionspunkterne er netop de punkter, som har endelig orden. For en elliptisk kurve E og et legeme K definerer vi

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

Vi bemærker at alle punkter over et endeligt legeme er et torsionspunkt. Følgende sætning karakteriserer disse grupper af torsionspunkter:

Sætning 5 *Lad E være en elliptisk kurve over et legeme K og lad n være et positivt heltal. Hvis karakteristikken for K ikke deler n, eller ikke er 0, da er*

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Hvis karakteristikken for K er $p > 0$ og $p \mid n$, lader vi $n = p^r n'$ sådan at $p \nmid n'$. Da er

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad \textit{eller} \quad \mathbb{Z}_n \oplus \mathbb{Z}_{n'}.$$

Bevis. Et bevis for denne sætning kan findes i [4, s. 79]. □

En konsekvens af sætning 5 er, at vi snakke om en basis for $E[n]$, da vi nu ved hvordan den ser ud.

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

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

Med disse detaljer på plads er vi i stand til at vise følgende sætning:

Sætning 6 *Lad E være en elliptisk kurve over $\mathbb{F}_q$. Lad a være som i (3.2). 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 $\gcd(m, q) = 1$.

Bevis. Det følger direkte fra lemma 1 at hvis $\phi_q^2 - a\phi_q + q \neq 0$ (hvis den ikke er nul-endomorfier) 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 (se proposition 2) følger det fra proposition 1 og fra det faktum, at $\det(\alpha_n) \equiv \deg(\alpha) \pmod{n}$ (se [4, proposition 3.15]), at

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

Videre har vi, at $sv - tu = \det((\phi_q)_m) \equiv q \pmod{m}$. Fra (3.2) har vi, at $\#\ker(\phi_q - 1) = q + 1 - a$, så

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

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

$$(\phi_q)_m^2 - a(\phi_q)_m + qI \equiv 0 \pmod{m},$$

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.

For at vise entydigheden af a lader vi nu $a_1 \neq a$ være sådan, at

$$\phi_q^2 - a_1\phi_q + q = 0,$$

er opfyldt. Da har vi også, at (ved at lægge 0 til)

$$(a - a_1)\phi_q = (\phi_q^2 - a_1\phi_q + q) - (\phi_q^2 - a\phi_q + q) = 0$$

Da $\phi_q : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ er surjektiv betyder det, at $(a - a_1)$ annihilerer $E(\overline{\mathbb{F}}_q)$ (dvs. for hvert element $x \in E(\overline{\mathbb{F}}_q)$ er $(a-a_1)x = 0$). Specielt har vi, at $(a-a_1)$ annihilerer $E[m]$ for hvert $m \geq 1$. Men da der er punkter i $E[m]$ med orden m når $\gcd(m, q) = 1$ har vi, at $a - a_1 \equiv 0 \pmod{m}$ for sådan et m. Dermed er $a - a_1 = 0$ og vi har vist, at a er entydig. □

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 7 *Lad $\#E(\mathbb{F}_q) = q + 1 - a$. Skriv $X^2 - aX + q = (X - \alpha)(X - \beta)$. Da er*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n),$$

for alle $n \geq 1$.

Vi har brug for, at $\alpha^n + \beta^n$ er et heltal, hvilket følgende lemma giver os:

Lemma 5 *Lad $s_n = \alpha^n + \beta^n$. Da er $s_0 = 2$, $s_1 = a$ og $s_{n+1} = as_n - qs_{n-1}$ for alle $n \geq 1$.*

Bevis. Bemærk først, at $s_0 = \alpha^0 + \beta^0 = 2$ og $s_1 = a$. Vi ser, at

$$(\alpha^2 - a\alpha + q)\alpha^{n-1} = \alpha^{n+1} - a\alpha^n + q\alpha^{n-1} = 0,$$

da α er en rod i $X^2 - aX + q$. Altså har vi, at $\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}$. På samme måde har vi, at $\beta^{n+1} = a\beta^n - q\beta^{n-1}$, da β også er en rod. Lægges disse udtryk sammen får vi, at

$$\begin{aligned} s_{n+1} = \alpha^{n+1} + \beta^{n+1} &= a\alpha^n - q\alpha^{n-1} + a\beta^n - q\beta^{n-1} \\ &= a(\beta^n + \beta^n) - q(\alpha^{n-1} + \beta^{n-1}) \\ &= as_n - qs_{n-1}. \end{aligned}$$

Dermed er s_n et heltal for alle $n \geq 0$. □

Bevis for sætning 7. Lad først

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n.$$

Da deler $X^2 - aX + q = (X - \alpha)(X - \beta)$ polynomiet $f(X)$. Kvotienten er et polynomium $Q(X)$ med heltallige koefficienter, da $X^2 - aX + q$ er monisk og $f(X)$ har heltallige koefficienter (se sætning 10 i appendikset). Derfor er

$$f(\phi_q) = (\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0, \tag{3.3}$$

som endomorfier for E pr. sætning 6. Idet vi husker, at $\phi_q^n = \phi_{q^n}$ giver sætning 6 også, at der findes entydigt $k \in \mathbb{Z}$ sådan at $\phi_{q^n}^2 - k\phi_q^n + q^n = 0$. Sådan et k er givet ved $k = q^n + 1 - \#E(\mathbb{F}_{q^n})$, og dette sammen med (3.3) giver os netop, at

$$\alpha^n + \beta^n = q^n + 1 - \#E(\mathbb{F}_{q^n}),$$

hvilket netop var hvad vi ønskede at vise. □

Eksempel 2. Eksempel på 4.12 i aktion. □