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) sådan at $x, y \in \mathbb{F}$. Et endeligt legeme har p^n elementer for et primtal p, hvor $n \geq 1$ (se bilag A). 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 $E(\mathbb{F})$. 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 blot kender ordenen af $\mathbb{F}_q$.

3.1 Eksempler

Lad E være en elliptisk kurve på formen

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

som er 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 ordenen 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 egenskaber, som denne endomorfi beisdder.

Lemma. 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. □

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

3.3 Hasses sætning

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.

Med de foregående resultater er vi nu næsten klar til at vise Hasses sætning (sætning 1). Lad i det følgende afsnit

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

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

Lemma. Lad $r, s \in \mathbb{Z}$ så $\gcd(s, q) = 1$. Da er

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

Bevis. Vi vil ikke give beviset her, da det bygger på en række af tekniske resultater. Et bevis kan findes i [LW]. $\square$

Nu er vi da i stand til, at gives beviset for Hasses sætning:

Bevis (Bevis for Hasses sætning). Da graden af en endomorfi altid er ≥ 0 følger det fra lemma 4, at

$$r^2 q + s^2 - rsa = q\left(\frac{r^2}{s^2}\right) - \frac{rsa}{s^2} + 1 \geq 0,$$

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. $\square$

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. 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

$$a \equiv \mathrm{Trace}((\phi_q)_m) \pmod{m},$$

for alle m, hvor $\gcd(m, q) = 1$. $\square$

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 (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 (3.2) 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. □

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. 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. 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 (Bevis for sætning 4). Lad nu

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

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 appendiks). 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 3. Idet vi husker, at $\phi_q^n = \phi_{q^n}$ giver sætning 3 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. Eksempel på 4.12 i aktion. □

Bilag A

Legemer

Lad p være et primtal. Heltallene modulo p giver os et legeme $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der indeholder p elementer. Antallet af elementer i ethvert endeligt legeme er på formen p^n. For at se dette lader vi K være et endeligt legeme. Dets karakteristik må være p for et eller andet primtal, da et legeme med karakteristik 0 er uendeligt. Derfor må K være endeligt frembragt som et vektorrum over $\mathbb{Z}/p\mathbb{Z}$. Så lad $x_1, \ldots, x_n$ være en basis for K. Elementerne i K kan da skrives entydigt som

$$x = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n, \quad \text{hvor} \quad \alpha_i \in \mathbb{Z}/p\mathbb{Z}.$$

Da hvert $\alpha_i \in K$ har vi altså p forskellige valg for hver af $\alpha_1, \alpha_2, \ldots, \alpha_n$. Dette betyder, at vi har p^n valg for x, som også giver os hele legemet K. Antallet af elementer i K er altså p^n.

Vi benytter notationen $\mathbb{F}_q = \mathbb{F}_{p^n}$ for det endelige legeme med $q = p^n$ elementer. Bemærk, at $\mathbb{Z}/p^n\mathbb{Z}$ ikke er et legeme for $n \geq 2$, da p ikke har nogen multiplikativ invers.

Bilag B

Talteoretiske resultater

Her samler vi nogle af de (hovedsagligt) mindre resultater, som benyttes igennem kapitlerne. De præsenteres her kort og henvises til i opgaven, når de er blevet anvendt.

Proposition. Et element $a \in \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ har ikke en invers i $\mathbb{Z}_n$ hvis $\gcd(a, n) > 1$. □

Bevis. Antag for modstrid, at $d = \gcd(a, n) > 1$, men at der samtidigt eksisterer en invers c til a modulo n. Da $d = \gcd(a, n)$ findes et heltal e, som ikke er nul, sådan at $de = n$. Da $d > 1$ har vi også, at $|e| < |n|$ så e er ikke nul modulo n. Da d deler a har vi, at $n = de$ deler ae så $ae = 0 \pmod{n}$. Vi har altså, at

$$e = e \cdot 1 = eac = 0 \cdot c = 0 \pmod{n},$$

hvilket er i modstrid med at e ikke kunne være 0 modulo n. Altså har a ikke en invers når $\gcd(a, n) > 1$. □

Vi giver nu beviset for sætning

Bevis (Bevis for Fermats lille sætning). Vi ser først på de $p-1$ positive multipla af a

$$a, 2a, \ldots, (p-1)a. \tag{B.1}$$

Hvis $ra = sa \pmod{p}$ har vi, at $r = s \pmod{p}$, så elementerne listet i (B.1) er forskellige og ikke-nul. De må altså være kongruente til $1, 2, \ldots, p-1$ men ikke nødvendigvis i den opskrevne rækkefølge. Ganger vi elementerne sammen må de to kongruenser være de samme, altså er

$$a \cdot 2a \cdots (p-1)a = 1 \cdot 2 \cdots (p-1) \pmod{p},$$

hvilket giver os, at

$$a^{p-1}(p-1)! = (p-1)! \pmod{p} \Rightarrow a^{p-1} = 1 \pmod{p}.$$ □