Sist:

- Generelt om separable morfier
- Viste, vha. differensialer, at for en elliptisk kurve E definert over $\mathbb{F}_q$, så er isogenien $1 - \mathrm{Fr}_q \in \mathrm{End}(E)$ separabel.
- $\rightsquigarrow E(\mathbb{F}_q) = |\ker(1 - \mathrm{Fr}_q)| = \deg(1 - \mathrm{Fr}_q)$.

I dag: Bruk dette for å estimere $|E(\mathbb{F}_q)|$ (Hasses teorem).

Telle punkter, et grovt anslag. La nå $K = \mathbb{F}_q$, og la E være en elliptisk kurve definert over $\mathbb{F}_q$, med Weierstrass-ligning

$$y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{F}_q.$$

Vi viser to måter å estimere $|E(\mathbb{F}_q)|$ på.

*Måte 1:*La $g = x^3 + Ax + B$, vi har da

$$E(\mathbb{F}_q) = \{O\} \sqcup \{(\alpha, \beta) \in \mathbb{F}_q^2 \mid \beta^2 = g(\alpha)\}.$$

Se på avbildningen $\beta \mapsto \beta^2$, som sender 0 til 0, og som er 2-til-1 på $\mathbb{F}_q \setminus \{0\}$. Vi har

$$\mathbb{F}_q = \{0\} \sqcup R \sqcup S,$$

hvor

$$R = \{\gamma \in \mathbb{F}_q \mid x^2 = \gamma \text{ har 2 røtter}\}, \quad |R| = \frac{q-1}{2}$$
$$S = \{\gamma \in \mathbb{F}_q \mid x^2 = \gamma \text{ har 0 røtter}\}, \quad |S| = \frac{q-1}{2}$$

Vi har altså

$$|E(\mathbb{F}_q)| = 1 + |\{\alpha \in \mathbb{F}_q \mid g(\alpha) = 0\}| + 2|\{\alpha \in \mathbb{F}_q \mid g(\alpha) \in R\}| + 0|\{\alpha \in \mathbb{F}_q \mid g(\alpha) \in S\}|.$$

Hvis vi nå antar at verdiene $g(\alpha)$ tar er *tilfeldig* (uniformt) fordelt, får vi estimatet

$$|E(\mathbb{F}_q)| \approx 1 + 1 + 2\left(\frac{q-1}{2}\right) + 0\left(\frac{q-1}{2}\right) = q + 1.$$

Måte 2: Se på funksjonen $h\colon \mathbb{F}_q^2 \to \mathbb{F}_q$ gitt ved $h(\alpha, \beta) \mapsto \beta^2 - (\alpha^3 + A\alpha + B)$, og anta at h kan approksimeres som en tilfeldig (uniformt fordelt) funksjon av α, β. Sannsynligheten for at $h(\alpha, \beta) = 0$ da er q^{-1} og $|\mathbb{F}_q^2| = q^2$, så vi får $|\{(\alpha, \beta \in \mathbb{F}_q^2 \mid h(\alpha, \beta) = 0\}| \approx q$, som gir $|E(\mathbb{F}_q)| \approx q + 1$.

Hasses teorem sier at dette estimatet ikke er altfor gæli:

Teorem (Hasses teorem)**.** *Vi har*[1]

$$|E(\mathbb{F}_q) - (1 + q)| \leq 2\sqrt{q}$$

[1] I forelesningen påstod jeg at $2\sqrt{q}$ ikke kunne være et heltall, og at ulikheten derfor blir en streng ulikhet. For å si det med Guri Melby: Dette kom HELT FEIL UT. Jeg tenkte at q skulle være et primtall, men q er en primtallspotens, så $\sqrt{q}$ kan godt være et heltall, og ulikheten kan godt være en likhet.

Første steg i beviset har vi gjort, vi vet at $|E(\mathbb{F}_q)| = \deg(1 - \mathrm{Fr}_q)$. Det gjenstår å få has på $\deg(1 - \mathrm{Fr}_q)$.

Hvordan ser funksjonen $\deg\colon \mathrm{End}(E) \to \mathbb{Z}$ ut? Vi vet

- $\deg(\mathrm{Fr}_q) = q$,
- $\deg([n]) = n^2$ for alle $n \in \mathbb{Z}$.
- Vi vet at $\deg(\phi\psi) = \deg(\phi)\deg(\psi)$ for alle $\phi, \psi \in \mathrm{End}(E)$, slik at for eksempel
$$\deg(n\phi) = \deg([n]\phi) = n^2 \deg(\phi).$$
.

Denne siste ligningen hinter til at $\deg(\phi)$ er en *kvadratisk* funksjon av ϕ.

Definisjon. La G være en abelsk gruppe, og la $d\colon G \to \mathbb{R}$ være en funksjon. Definer $b\colon G \times G \to \mathbb{R}$ ved
$$b(\alpha, \beta) = \frac{q(\alpha + \beta) - q(\alpha) - q(\beta)}{2}.$$
Vi sier at d er en *kvadratisk form* hvis

(1) For alle $\alpha \in G$, så er $d(\alpha) = d(-\alpha)$

(2) Funksjonen b er bilineær.

Vi sier d er *positiv definitt* hvis $d(\alpha) \geq 0$ for alle $\alpha \in G$ og $d(\alpha) = 0 \Leftrightarrow \alpha = 0$.

Den kvadratiske formen d bestemmer altså en bilineær avbildning b, og motsatt er d bestemt av b, siden
$$b(\alpha, \alpha) = -b(\alpha, -\alpha) = -\frac{d(0) - d(\alpha) - d(-\alpha)}{2} = d(\alpha).$$
Skriver man ut dette får man en bijeksjon
$$\{\text{Kvadratiske former på } G\} \leftrightarrow \{\text{Symmetriske bilineære avbildninger } G \times G \to \mathbb{R}\}$$
$$q \mapsto b(\alpha, \beta) = \frac{q(\alpha + \beta) - q(\alpha) - q(\beta)}{2}$$
$$q(\alpha) = b(\alpha, \alpha) \leftarrow\!\shortmid b$$

Lemma. *Hvis $G = \mathbb{Z}^n$, så er det en bijektiv korrespondanse mellom (positiv definitte) kvadratisk former $d\colon G \to \mathbb{R}$ og (positiv definitte) symmetriske reelle $(n \times n)$-matriser, gitt ved*
$$M = (a_{ij}) \in M_n(\mathbb{R}) \leftrightarrow d((b_i)_{i=1}^n) = \sum_{i,j} b_i b_j a_{ij}.$$

Bevis. Bijeksjonen over er komposisjonen av naturlige bijeksjoner
$$\begin{aligned}\{\text{Kvadratiske former på } \mathbb{Z}^n\} &\leftrightarrow \{\text{Symmetriske bilineære avbildninger } \mathbb{Z}^n \times \mathbb{Z}^n \to \mathbb{R}\}\\ &\leftrightarrow \{\text{Symmetriske avbildninger } \mathbb{Z}^n \otimes \mathbb{Z}^n \to \mathbb{R}\}\\ &\leftrightarrow \{\text{Symmetriske reelle } (n \times n)\text{-matriser}\},\end{aligned}$$
og det er lett å se at M er positiv definitt hvis og bare hvis d er det. $\square$

For $\mathrm{End}(E) = \mathbb{Z}^n$ har vi altså en konkret beskrivelse av kvadratiske former på gruppen. Poenget med den abstrakte definisjonen over er at den er lett å sjekke.[2]

Proposisjon. *Funksjonen* $\deg\colon \mathrm{End}(E) \to \mathbb{Z}$ *er en positiv definitt kvadratisk funksjon.*

Bevis. Vi må vise at funksjonen

$$b(\phi, \psi) = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

er bilineær. Vi bruker at for alle $\alpha \in \mathrm{End}(E)$, så er

$$\deg(\alpha) = \alpha\hat{\alpha}.$$

Altså er

$$b(\phi, \psi) = (\phi + \psi)(\hat{\phi} + \hat{\psi}) - \phi\hat{p}hi - \psi\hat{\psi} = \phi\hat{\psi} + \psi\hat{\phi}$$

som opplagt er lineært i både ϕ og ψ.

For alle $\phi \in \mathrm{End}(E)$ har vi $\deg(\phi) = \deg(-\phi)$, $\deg(\phi) \geq 0$, og $\deg(\phi) = 0 \Leftrightarrow \phi = 0$, som fullfører beviset. □

Vi har nå den kvadratiske formen $\deg\colon \mathrm{End}(E) \to \mathbb{Z}$, som vi skal evaluere i $1 - \mathrm{Fr}_q$. Vi lar $b\colon \mathrm{End}(E) \times \mathrm{End}(E) \to \mathbb{R}$ være den assosierte bilineære formen.

Proposisjon (Cauchy–Schwarz' ulikhet)**.** *La* $\phi, \psi \in \mathrm{End}(E)$*. Da er*

$$\deg(\phi)\deg(\psi) \geq (b(\phi, \psi))^2$$

Bevis. Siden $\mathrm{End}(E) = \mathbb{Z}^n$, så er $\deg\colon \mathrm{End}(E) \to \mathbb{R}$ definert av en positiv definitt $(n \times n)$-matrise. Vi kan dermed si at b definerer et indreprodukt på $\mathrm{End}(E) \otimes \mathbb{R} = \mathbb{R}^n$, og resultatet over er da den vanlige Cauchy–Schwarz' ulikhet. □

Korollar. *Hvis* $\phi, \psi \in \mathrm{End}(E)$*, så er* $|\deg(\phi+\psi) - \deg(\phi) - \deg(\psi)| \leq 2\sqrt{\deg(\phi)\deg(\psi)}$.

Bevis. Vi har

$$\begin{aligned}\deg(\phi + \psi) &= b(\phi + \psi, \phi + \psi)\\ &= b(\phi, \phi) + b(\psi, \psi) + b(\phi, \psi) + b(\psi, \phi) = \deg(\phi) + \deg(\psi) + 2b(\phi, \psi).\end{aligned}$$

Dermed er

$$|\deg(\phi + \psi) - \deg(\phi) - \deg(\psi)| = 2|b(\phi, \psi)| \leq 2\sqrt{\deg(\phi)\deg(\psi)}.$$

□

[2] Ett annet poeng er at Silvermans fullstendige bevis for at $\mathrm{End}(E)$ er endeliggenerert bruker den kvadratiske formen deg på $\mathrm{End}(E)$, så man ønsker å bruke begrepet "kvadratisk form" også for grupper som man ikke veit at er endelig genererte.

Bevis for Hasses teorem. Anvend lemmaet over på $\phi = 1$ og $\psi = -\operatorname{Fr}_q$.

Vi får da

$$|\deg(1 - \operatorname{Fr}_q) - \deg(1) - \deg(-\operatorname{Fr}_q)| \leq 2\sqrt{\deg(1)\deg(-\operatorname{Fr}_q)},$$

og siden $\deg(1) = 1$, og $\deg(-\operatorname{Fr}_q) = q$, gir dette

$$|\deg(1 - \operatorname{Fr}_q) - 1 - q| \leq 2\sqrt{q},$$

og altså

$$|E(\mathbb{F}_q) - 1 - q| \leq 2\sqrt{q}.$$

□

Bonus: Weil-formodningene

Denne delen er med for dannelsens skyld, og er ikke pensum.

La E være en elliptisk kurve definert over $\mathbb{F}_q$. Kroppen $\mathbb{F}_q$ er inneholdt i større kropper $\mathbb{F}_{q^n}$ for alle n, så kurven E er også definert over $\mathbb{F}_{q^n}$ for alle n. Det gir dermed mening å spørre om størrelsen til mengden $E(\mathbb{F}_{q^n})$, og hvordan denne avhenger av n.

Ved estimatet vi ga tidligere, har vi at $|E(\mathbb{F}_{q^n})| \approx 1 + q^n$. Setter vi $\epsilon_n = (1 + q^n) - |E(\mathbb{F}_{q^n})|$, så sier Hasses teorem at

$$|\epsilon_n| \leq 2\sqrt{q^n}.$$

Teorem (“Weil-formodningene[3] for en elliptisk kurve”)**.** *Gitt en E definert over $\mathbb{F}_q$, så finnes det et komplekst tall α med $|\alpha| = \sqrt{q}$ slik at for alle n har vi*

$$\epsilon_n = \alpha^n + \bar{\alpha}^n = 2Re(\alpha^n).$$

Siden

$$2|\mathrm{Re}(\alpha^n)| \leq 2|\alpha^n| = 2\sqrt{q^n},$$

så er Hasses teorem et korollar av dette teoremet.

Fra $\alpha + \alpha^{-1} = \epsilon_1$ og $|\alpha| = \sqrt{q}$, følger det at α må være en av de to konjugerte røttene til polynomet

$$x^2 - \epsilon_1 x + q$$

og α er derfor entydig bestemt av ϵ_1. Dermed er $|E(\mathbb{F}_{q^n})|$ bestemt for alle n straks man kjenner $|E(\mathbb{F}_q)|$.

Eksempel. Ta kurven definert av ligningen $y^2 = x^3 - x$. Denne er definert over $\mathbb{F}_5$ (den er for så vidt definert over alle K!), så la oss ta $q = 5$. Man sjekker at $|E(\mathbb{F}_5)| = 7$, så $\epsilon_1 = 1 + 5 - |E(\mathbb{F}_5)| = -1$. Dermed er α en rot av

$$x^2 + x + 5,$$

så

$$\alpha = -\frac{1}{2} \pm \frac{\sqrt{19}}{2}i,$$

[3]Hvorfor ikke “Weil-formodningen” i entall? Weil-formodningene kan formuleres mer generelt for algebraiske varieteter definert over $\mathbb{F}_q$, og i den generelle formen er det naturlig å presentere dette som flere underformodninger. For en elliptisk kurve er resultatet enklere, så vi dropper å stykke det opp.

og vi får
$$E(\mathbb{F}_{5^n}) = 1 + 5^n - 2\mathrm{Re}(\alpha^n)$$
for alle n.

Beviset for Weil-formodningene. På samme måte som $E(\mathbb{F}_q) = \ker(1 - \mathrm{Fr}_q)$, har vi at
$$|E(\mathbb{F}_{q^n})| = |\ker(1 - \mathrm{Fr}_{q^n})| = \deg(1 - \mathrm{Fr}_{q^n}).$$
Siden $\mathrm{Fr}_{q^n}(\alpha) = \alpha^{q^n}$ for alle $\alpha \in \overline{\mathbb{F}}_q$, har vi at $\mathrm{Fr}_{q_n} = \mathrm{Fr}_q^n$, hvor vi tenker på Fr_q som et element i ringen $\mathrm{End}(E)$. For å bestemme $\deg(1 - \mathrm{Fr}_{q^n})$ analyserer vi mer generelt hvordan man kan beregne $\deg(1 - \phi^n)$ for en vilkårlig $\phi \in \mathrm{End}(E)$.

Vi har tidligere vist et teorem som sier at ringen $\mathrm{End}(E)$ enten er $\mathbb{Z}$, en orden i en kvadratisk kropp, eller en orden i en kvaternionisk algebra. I dette beviset viste vi også at for alle $\phi \in \mathrm{End}(E)$, så er trasen $T(\phi) = \phi + \hat{\phi}$ inneholdt i $\mathbb{Z} \subset \mathrm{End}(E)$.

Lemma. *For alle $\phi \in \mathrm{End}(E)$ gjelder*
$$\phi^2 - T(\phi)\phi + \deg(\phi) = 0,$$

Bevis. Bruk $\deg(\phi) = \phi\hat{\phi} = \hat{\phi}\phi$ og skriv ut. □

For $\phi \in \mathrm{End}(E)$, la $R_\phi \subseteq \mathrm{End}(E)$ være underringen av $\mathrm{End}(E)$ generert av ϕ.

Lemma. *Hvis $\phi \notin \mathbb{Z}$, har vi $R_\phi \cong \mathbb{Z}[x]/(x^2 - T(\phi)x + \deg(\phi))$.*

Bevis. Ringen R_ϕ er bildet av avbildningen $\chi\colon \mathbb{Z}[x] \to \mathrm{End}(E)$ gitt ved $x \mapsto \phi$. Ved lemmaet over, er $x^2 - T(\phi)x + \deg(\phi) \in \ker(\chi)$, så $(x^2 - T(\phi)x + \deg(\phi)) \subseteq \ker(\chi)$.

Homomorfien χ faktoriserer dermed gjennom en surjeksjon $\mathbb{Z}[x]/(x^2 - T(\phi) + \deg(\phi))$, og vi har at $\mathbb{Z}[x]/(x^2 - T(\phi) + \deg(\phi))$ har rang 2 som $\mathbb{Z}$-modul. Siden $\phi \notin \mathbb{Z}$, har R_ϕ rang ≥ 2 som $\mathbb{Z}$-modul, og dermed må surjeksjonen $\mathbb{Z}[x]/(x^2 - T(\phi) + \deg(\phi)) \to R_\phi$ være en isomorfi. □

La $\phi \in \mathrm{End}(E) \setminus \mathbb{Z}$, og la $\alpha \in \mathbb{C}$ være en rot av $x^2 - T(\phi)x + \deg(\phi)$. Vi kan definere en homomorfi $\iota\colon R_\phi \to \mathbb{C}$ ved $\iota(\phi) = \alpha$.

Lemma. *For alle $\psi \in R_\phi$, så er $\hat{\psi} \in R_\phi$, og*
$$\iota(\hat{\psi}) = \overline{\iota(\psi)}.$$

Bevis. Siden R_ϕ er genererert av ϕ, holder det å vise at $\hat{\phi} \in R_\phi$ og at $\iota(\hat{\phi}) = \overline{\iota(\phi)}$.

For den første påstanden: $\hat{\phi} = T(\phi) - \phi$.

For den andre påstanden: Vi har at $\iota(\phi) = \alpha$ er en rot av $x^2 - T(\phi)x + \deg(\phi)$, og $\bar{\alpha}$ er den andre roten av dette polynomet. Dermed er $\bar{\alpha} = T(\phi) - \alpha$, som betyr at
$$\iota(\hat{\phi}) = \iota(T(\phi) - \phi) = T(\phi) - \iota(\phi) = T(\phi) - \alpha = \bar{\alpha} = \overline{\iota(\phi)}.$$
□

Proposisjon. *Med α som over, har vi*

$$\deg(1-\phi^n) = 1 + \deg(\phi)^n - (\alpha^n + \bar{\alpha}^n).$$

Bevis. Vi har

$$\deg(1-\phi^n) = (1-\phi^n)(1-\hat{\phi}^n).$$

Siden $(1-\phi^n)(1-\hat{\phi}^n) \in \mathbb{Z}$, har vi

$$(1-\phi^n)(1-\hat{\phi}^n) = \iota((1-\phi^n)(1-\hat{\phi}^n)) = (1-\alpha^n)(1-\bar{\alpha}^n) = 1 + (\alpha\bar{\alpha})^n - (\alpha^n + \bar{\alpha}^n),$$

og siden $\deg(\phi) = \phi\hat{\phi} = \alpha\bar{\alpha}$, er vi i mål. $\square$

Bruker vi proposisjonen over på $\phi = \mathrm{Fr}_q$, har vi vist Weil-formodningene for elliptiske kurver.