**Sist:**

- For et primtall $l$, definerte ringen av $l$-adiske heltall: Sekvenser $(a_i)$ med $a_i \in \mathbb{Z}/l^i$, slik at $a_i = a_{i-1} \pmod{l^{i-1}}$.
- For en elliptisk kurve $E$, definerte den $l$-adiske Tate-modulen til $E$, skrevet $T_l(E)$, hvor elementene er sekvenser $P_1, P_2, \ldots$, med $P_i \in E[l^i]$ og $lP_i = P_{i-1}$.
- Viste at (når $l \neq \operatorname{char} K$), så er $T_l(E) \cong \mathbb{Z}_l \oplus \mathbb{Z}_l$ som $\mathbb{Z}_l$-moduler.

Vil bruke $T_l(E)$ til å forstå isogenigruppa $\operatorname{Hom}(E_1, E_2)$ og endomorfiringen $\operatorname{End}(E)$.

La $\phi\colon E_1 \to E_2$ være en isogeni. Da får vi, for alle $n$, en gruppehomomorfi $\phi[n]\colon E_1[n] \to E_2[n]$, og spesielt får vi homomorfier $\phi[l^i]\colon E_1[l^i] \to E_2[l^i]$ for alle $i$.

La $p = (P_i)_{i=1}^{\infty} \in T_l(E_1)$, og la $Q_i = \phi(P_i) \in E_2$ for alle $i$. Siden $P_i \in E_1[l^i]$, er $\phi(P_i) \in E_2[l^i]$, og siden $lP_i = P_{i-1}$, har vi

$$lQ_i = l\phi(P_i) = \phi(lP_i) = \phi(P_{i-1}) = Q_{i-1}$$

Dermed er $q = (Q_i)_{i=1}^{\infty}$ et veldefinert element i $T_l(E_2)$.

**Proposisjon.** *Gitt en isogeni $\phi\colon E_1 \to E_2$, får vi en homomorfi av $\mathbb{Z}_l$-moduler*

$$\phi_l\colon T_l(E_1) \to T_l(E_2)$$

*ved*

$$(P_i)_{i=1}^{\infty} \mapsto (\phi(P_i))_{i=1}^{\infty}$$

*Bevis.* Vi har vist at dette er veldefinert, og det er lett å sjekke at dette er en homomorfi av $\mathbb{Z}_l$-moduler.[1] □

**Proposisjon.** *La $\phi\colon E_1 \to E_2$ og $\psi\colon E_2 \to E_3$ være isogenier. Da er*

$$(\psi \circ \phi)_l = \psi_l \circ \phi_l\colon T_l(E_1) \to T_l(E_3).$$

*Bevis.* Rett fram fra definisjonen av $\phi_l, \psi_l$.[2] □

**Endomorfiringen til Tate-modulen.** La nå $E$ være en elliptisk kurve, og se på $\operatorname{End}_{\mathbb{Z}_l}(T_l(E)) = \operatorname{Hom}_{\mathbb{Z}_l}(T_l(E), T_l(E))$, gruppa av $\mathbb{Z}_l$-homomorfier fra $T_l(E)$ til $T_l(E)$. Vi kan definere et produkt på $\operatorname{End}(T_l(E))$ ved å sette $fg = f \circ g$, og med dette produktet blir $\operatorname{End}(T_l(E))$ en ring.

Siden $T_l(E) \cong \mathbb{Z}_l^{\oplus 2}$ som $\mathbb{Z}_l$-modul, så har vi en ringisomorfi

$$\operatorname{End}(T_l(E)) = \operatorname{Hom}_{\mathbb{Z}_l}(T_l(E), T_l(E)) \cong \operatorname{Hom}_{\mathbb{Z}_l}(\mathbb{Z}_l^{\oplus 2}, \mathbb{Z}_l^{\oplus 2}) = M_2(\mathbb{Z}_l),$$

hvor $M_2(\mathbb{Z}_l)$ angir ringen av $(2 \times 2)$-matriser med koeffisienter i $\mathbb{Z}_l$.

Vi har vist tidligere at $\operatorname{End}(E)$ er en ring, med multiplikasjon $\phi\psi = \phi \circ \psi$.

---

[1] Gitt $(P_i)$ og $(P_i')$ i $T_l(E_1)$, sendes $(P_i)+(P_i') = (P_i + P_i')$ til $(\phi(P_i + P_i')) = (\phi(P_i) + \phi(P_i')) = (\phi(P_i)) + (\phi(P_i'))$, så avbildningen er additiv.

Hvis $a = (a_i) \in \mathbb{Z}_l$, så er $\phi(a(P_i)) = \phi((a_i P_i)) = (a_i \phi(P_i)) = a(\phi(P_i))$, så avbildningen respekterer $\mathbb{Z}_l$-modulstrukturen.

[2] For $(P_i) \in T_l(E_1)$, er $\psi_l \circ \phi_l((P_i)) = \psi_l((\phi(P_i)) = (\psi(\phi(P_i))) = ((\psi \circ \phi)(P_i)) = (\psi \circ \phi)_l((P_i))$.

**Proposisjon.** *Avbildningen* $\mathrm{End}(E) \to \mathrm{End}(T_l(E))$ *gitt ved* $\phi \mapsto \phi_l$ *er en ringhomomorfi.*

*Bevis.* Vi vet at avbildningen er en gruppehomomorfi, så vi må vite at den respekterer multiplikasjon. Men vi har

$$(\phi\psi)_l = (\phi \circ \psi)_l = \phi_l \circ \psi_l = \phi_l \psi_l.$$

□

## Injektivitet

Vi har altså en gruppehomomorfi $\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$, og når $E_1 = E_2$, er dette også en ringhomomorfi.

**Proposisjon.** *La* $E_1, E_2$ *være elliptiske kurver. Avbildningen*

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$$

*er injektiv.*

*Bevis.* La $\phi \in \mathrm{Hom}(E_1, E_2)$ være slik at $\phi_l = 0$. La $0 \neq p = (P_i) \in T_l(E_1)$. Da finnes en $i$ slik at $P_i \neq O$.

Vi påstår at punktene $P_i, P_{i+1}, P_{i+2}, \ldots$ alle er forskjellige. Anta for en motsigelse at $P_i = P_j$ med $i < j$. Da er $P_j = P_i = l^{i-j} P_j$. Dermed er $P_j = l^{i-j} l^{i-j} \cdots l^{i-j} P_j = l^{n(i-j)} P_j$ for alle $n \geq 0$. Men siden $l^j P_j = O$, betyr det at $P_j = O$, som motsier at $P_j = P_i \neq O$.

Hvis $\phi_l = 0$, så er $\phi_l(p) = (\phi(P_i))_{i=1}^{\infty} = 0$, som betyr at $\phi(P_i) = O$ for alle $i$. Men da er $|\ker \phi| = \infty$, som bare kan skje hvis $\phi = 0$. □

Altså sitter $\mathrm{Hom}(E_1, E_2)$ inni $\mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2)) \cong \mathrm{Hom}_{\mathbb{Z}_l}(\mathbb{Z}_l^{\oplus 2}, \mathbb{Z}_l^{\oplus 2}) = \mathbb{Z}_l^{\oplus 4}$. Dessverre er gruppa $\mathbb{Z}_l^{\oplus 4}$ en veldig stor gruppe, som f.eks. inneholder frie grupper på formen $\mathbb{Z}^N$ for alle $N$, så det er vanskelig å få konkret informasjon om $\mathrm{Hom}(E_1, E_2)$ ut av dette.

Vi trenger følgende sterkere resultat:

**Teorem.** *Gruppa* $\mathrm{Hom}(E_1, E_2)$ *er endeliggenerert, og homomorfien*

$$\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$$

*gitt ved*

$$\sum_{i=1}^{k} \phi_i \otimes a_i \mapsto \sum_{i=1}^{k} a_i (\phi_i)_l$$

*er injektiv.*

**Korollar.** *Vi har en gruppeisomorfi* $\mathrm{Hom}(E_1, E_2) \cong \mathbb{Z}^n$*, med* $n \leq 4$.

*Bevis.* Siden $\mathrm{Hom}(E_1, E_2)$ er endeliggenerert, har vi

$$\mathrm{Hom}(E_1, E_2) = \mathbb{Z}^n \oplus \bigoplus_{i=1}^{k} \mathbb{Z}/p_i^{e_i}$$

for primtall $p_i$ og heltall $e_i$. Men vi vet at $\mathrm{Hom}(E_1, E_2)$ er torsjonsfri, dvs. at $k\phi = 0 \Rightarrow \phi = 0$ for $0 \neq k \in \mathbb{Z}$. Dermed må vi ha $\mathrm{Hom}(E_1, E_2) = \mathbb{Z}^n$.

Det følger at $\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \cong \mathbb{Z}_l^n$, og siden avbildningen

$$\mathbb{Z}_l^n \cong \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2)) = \mathbb{Z}_l^4$$

er injektiv, må $n \leq 4$. □

*Bevis for Teorem.* Vi må bruke følgende tidligere resultat:

**Lemma.** *Hvis $\phi \in \mathrm{Hom}(E_1, E_2)$ er slik at $E_1[n] \subset \ker \phi$, så finnes en $\gamma \in \mathrm{Hom}(E_1, E_2)$ slik at $n\gamma = \phi$.*

$$\begin{array}{ccc} E_1 & \xrightarrow{[n]} & E_1 \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists \gamma} \\ & & E_2 \end{array}$$

Vi *antar*, og hopper over å bevise, at $\mathrm{Hom}(E_1, E_2)$ er endeliggenerert (se Silverman for fullstendig bevis). Da må vi ha $\mathrm{Hom}(E_1, E_2) \cong \mathbb{Z}^n$, siden $\mathrm{Hom}(E_1, E_2)$ er torsjonsfri.

La $\psi_1, \ldots, \psi_n$ være generatorer for $\mathrm{Hom}(E_1, E_2)$. Et element $\phi \in \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ kan da uttrykkes som

$$\phi = \sum_{i=1}^{n} \alpha_i \psi_i \qquad \alpha_i \in \mathbb{Z}_l,$$

og vi skriver $\alpha_i = \sum_{j=1}^{\infty} c_{ij} l^j$ med $c_{ij} \in \{0, \ldots, l-1\}$.

For alle $k \geq 1$, definer isogenien

$$\phi_k = \sum_{j=0}^{k-1} c_{ij} l^j \psi_i \in \mathrm{Hom}(E_1, E_2), \tag{1}$$

som vi kan tenke på som "forkortingen av $\phi$ modulo $l^k$". Gitt et element $p = (P_i)_{i=1}^{\infty} \in T_l(E_1)$, så er $\phi_l(p) = (\phi_i(P_i))_{i=1}^{\infty}$.

Anta nå at $\phi$ er slik at $\phi_l = 0$.

Fikser en $k \geq 0$, og la $P \in E[l^k]$. Det finnes en $p = (P_i) \in T_l(E)$ slik at $P_k = P$. Siden $\phi_l(p) = (\phi_i(P_i)) = 0$, så er $\phi_k(P) = \phi_k(P_k) = O$.

Siden dette gjelder for alle $P \in E[l^k]$, så er $E[l^k] \in \ker \phi_k$. Men ved lemmaet er da $\phi_k = l^k \gamma_k$ for en $\gamma_k \in \mathrm{Hom}(E_1, E_2)$. Dette kan bare skje hvis $\phi_k = 0$ (fra formen til $\phi_k$ (1)). Siden dette gjelder for alle $k$, må vi ha $\phi = 0$. □