For lenge siden:

- Gitt elliptiske kurver E_1, E_2, definerte vi isogenigruppa $\mathrm{Hom}(E_1, E_2)$, og gitt en elliptisk kurve E, endomorfiringen $\mathrm{End}(E) = \mathrm{Hom}(E, E)$.
- Brukte den *duale isogenien* til å vise at for alle n så har endomorfien $[n]\colon E \to E$ grad lik n^2, og videre (hvis $\mathrm{char}\, K = 0$) så er gruppa
$$E[n] = \{P \in E \mid nP = O\} \cong \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

Spørsmål: Hvordan beskrive $\mathrm{Hom}(E_1, E_2)$ og $\mathrm{End}(E)$?

Ide: Gitt en isogeni $\phi\colon E_1 \to E_2$, se på hva ϕ gjør med torsjonsgruppene $E_i[n]$. For å utnytte dette skikkelig trenger vi *Tate-modulen*. Først litt bakgrunn om l-adiske heltall.

l-adiske heltall

La l være et primtall. I ringen $\mathbb{Z}$ har vi idealene (l^n), som gir en kjede av ringer og surjeksjoner
$$\cdots \to \mathbb{Z}/l^3 \xrightarrow{\delta_3} \mathbb{Z}/l^2 \xrightarrow{\delta_2} \mathbb{Z}/l \xrightarrow{\delta_1} 0.$$

Definisjon. La l være et primtall. Ringen av l-adiske heltall, $\mathbb{Z}_l$, er ringen av sekvenser $a_1, a_2, \ldots$, hvor $a_i \in \mathbb{Z}/(l^i)$, og vi krever at $\delta_i(a_i) = a_{i-1}$.

Addisjon og multiplikasjon er komponentvis:
$$(a_i)(b_i) = (a_i b_i) \qquad (a_i) + (b_i) = (a_i + b_i)$$

l-adiske tall som rekker. Et element $a_i \in \mathbb{Z}/(l^i)$ kan representeres av et tall mellom 0 og $l^i - 1$. Dermed kan a_i skrives unikt som
$$a_i = c_0 + c_1 l + c_2 l^2 + \cdots + c_{i-1} l^{i-1}$$
med $c_j \in \{0, \ldots, l-1\}$ (en base l-representasjon). Vi har da
$$\delta_i(a_i) = a_i \bmod l^{i-1} = c_0 + c_1 l + \cdots + c_{i-2} l^{i-2},$$
Dermed vil et l-adisk tall $a = (a_i)_{i=1}^{\infty}$ kunne skrives som
$$a_1 = c_0$$
$$a_2 = c_0 + c_1 l$$
$$a_3 = c_0 + c_1 l + c_2 l^2, \text{ osv.}$$
Vi kan dermed representere a ved en uendelig rekke
$$a = c_0 + c_1 l + c_2 l^2 + \cdots$$
med alle $c_i \in \{0, \ldots, l-1\}$.

Addisjon i $\mathbb{Z}_l$ fungerer da slik:
$$\left(\sum_{i=0}^{\infty} c_i l^i\right) + \left(\sum_{i=0}^{\infty} b_i' l^i\right) = \sum_{i=0}^{\infty} c_i'' l^i,$$
hvor for alle k, så er
$$\sum_{i=0}^{k-1} c_i l^i + \sum_{i=0}^{k-1} b_i' l^i = \sum_{i=0}^{k-1} c_i'' l^i \pmod{l^k},$$

Produktet fungerer på tilsvarende måte.

Alternativt: Still opp som på barneskolen (lat som $l = 10$):

$$\begin{array}{cccccc} & \cdots & c_2 & c_1 & c_0 \\ + & \cdots & c_2' & c_1' & c_0' \\ \hline = & \cdots & c_2'' & c_1'' & c_0'' \end{array}$$

Eksempel. Et heltall n gir et l-adisk tall $\phi(n) = (a_i)_{i=1}^{\infty}$ hvor $a_i = n \pmod{l^i}$. (Alternativt: Skriv $n = \sum_{i=0}^{k} c_i l^i$.) Dette gir en ringinklusjon $\phi\colon \mathbb{Z} \hookrightarrow \mathbb{Z}_l$.

Eksempel. La $a = 1 + l + l^2 + l^3 + \cdots \in \mathbb{Z}_l$. Da er $(1 - l)a = 1 \in \mathbb{Z}_l$.

Proposisjon. *Ringen $\mathbb{Z}_l$ er*

- *et helområde.*
- *lokal, med unikt maksimal ideal*
$$(l) = \{c_1 l + c_2 l^2 + \cdots\} \in \mathbb{Z}_l.$$
- *en DVR, og idealene i $\mathbb{Z}_l$ er (l^i) og (0).*

Merknad. Brøkkroppen til $\mathbb{Z}_l$ skrives $\mathbb{Q}_l$, og er ringen av elementer på formen $\sum_{i=n}^{\infty} c_i l^i$ for $n \in \mathbb{Z}$.

Tate-modulen til en elliptisk kurve

Vi har sett at hvis $\phi\colon E_1 \to E_2$ er en isogeni, så gir ϕ en avbildning av torsjonspunktene, $\phi[n]\colon E_1[n] \to E_2[n]$, for alle n. Vi vil utnytte dette til å forstå mengden isogenier bedre. For å gjøre det, må vi introdusere *Tate-modulen* til en elliptisk kurve.

La l være et primtall, og anta nå at $\operatorname{char} K = 0$ eller $\operatorname{char} K = p$, $p \neq l$. Vi ser på de endelige gruppene $E[l^i]$, som vi har beregnet til[1]

$$E[l^i] \cong \mathbb{Z}/l^i\mathbb{Z} \oplus \mathbb{Z}/l^i\mathbb{Z}$$

Hvis $P \in E[l^i]$, så ligger $[l](P) = lP \in E[l^{i-1}]$. Vi har dermed en kjede av abelske grupper

$$\cdots \xrightarrow{[l]} E[l^3] \xrightarrow{[l]} E[l^2] \xrightarrow{[l]} E[l]$$

Definisjon. Den l-adiske Tate-modulen til E, skrevet $T_l(E)$, er den abelske gruppa av sekvenser $P_1, P_2, P_3, \ldots$, hvor $P_i \in E[l^i]$ og $[l](P_i) = P_{i-1}$.

Proposisjon. *Den abelske gruppa $T_l(E)$ blir en modul over $\mathbb{Z}_l$ ved å sette, for $a = (a_i)_{i=1}^{\infty} \in \mathbb{Z}_l$ og $v = (P_i)_{i=1}^{\infty} \in T_l(E)$, at*

$$av = (a_i P_i)_{i=1}^{\infty} \in T_l(E).$$

Proposisjon. *Vi har en isomorfi av $\mathbb{Z}_l$-moduler: $T_l(E) \cong \mathbb{Z}_l \oplus \mathbb{Z}_l$.*

[1] Vi har hoppet over å vise dette for $\operatorname{char} K = p \neq l$.

Bevis. Har en isomorfi $E[l] \cong \mathbb{Z}/l \oplus \mathbb{Z}/l$. La $P_1, Q_1 \in E[l]$ være slik at $P_1 = (1,0)$ og $Q_1 = (0,1)$ under denne isomorfien. Velg så, for alle i, punkter $P_i, Q_i \in E[l^i]$ slik at $lP_i = P_{i-1}$ og $lQ_i = Q_{i-1}$.

Vi påstår at P_i, Q_i genererer $E[l^i]$. Mer presist:

Lemma. *For alle i er avbildningen*

$$\psi\colon \mathbb{Z}/l^i \oplus \mathbb{Z}/l^i \to E[l^i]$$

definert ved $(a,b) \mapsto aP_i + bQ_i$ en isomorfi.

Bevis. Opplagt for $i = 1$, vi bruker (sterk) induksjon på i.

Vi vet at $E[l^i] \cong \mathbb{Z}/l^i \oplus \mathbb{Z}/l^i$, så ved å telle elementer i gruppene, holder det å vise at ψ er en injeksjon. Med andre ord må vi sjekke at hvis $a, b \in \mathbb{Z}$ er slik at $aP_i + bQ_i = 0$, så er både a, b delelig med l^i.

Skriv $a = a'l^j$ og $b = b'l^k$ med $a', b' \neq 0 \pmod{l}$, og anta WLOG[2] at $j \leq k$. Anta for en motsigelse at $j < i$. Da er

$$aP_i + bQ_i = a'l^jP_i + b'l^{k-j}l^jQ_i = a'P_{i-j} + b'l^{k-j}Q_{i-j} = 0.$$

Ved induksjonsantagelsen brukt på $i - j$, må vi da ha at l^{i-j} deler a' (og $b'l^{k-j}$), som gir en motsigelse. □

Definer nå en avbildning $\phi\colon \mathbb{Z}_l \oplus \mathbb{Z}_l \to T_l(E)$ ved å sette

$$\phi((a_i),(b_i)) = (a_iP_i + b_iQ_i)$$

Lett å sjekke at dette er en avbildning av $\mathbb{Z}_l$-moduler.

La $v = (R_i) \in T_l(E)$. Lemmaet ovenfor viser at vi for alle i kan finne unike $a_i, b_i \in \mathbb{Z}/l^i$ slik at $a_iP_i + b_iQ_i = R_i$.

Lett å sjekke[3] at $a_i = a_{i-1} \pmod{l^{i-1}}$ og $b_i = b_{i-1} \pmod{l^{i-1}}$, så $((a_i),(b_i))$ definerer et element i $\mathbb{Z}_l \oplus \mathbb{Z}_l$ slik at $\phi((a_i),(b_i)) = (R_i)$. Siden a_i, b_i alltid finnes og er unike, har vi vist at ϕ er en isomorfi. □

Merknad. Det finnes ingen kanonisk isomorfi $\mathbb{Z}_l \oplus \mathbb{Z}_l \cong T_l(E)$, vi har bare definert den ved å gjøre uendelig mange valg.

Merknad. Hvis E er definert over K, så har $\mathbb{Z}_l$-modulen $T_l(E)$ mer struktur: Enhver kroppautomorfi $\sigma \in \mathrm{Gal}(\overline{K}/K)$ virker på $E[l^i]$ på en slik måte at σ også virker på $T_l(E)$. Dette gir en gruppehomomorfi $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_l(E))$ som forteller mye om E.

[2] UTAG?

[3] $(a_i - a_{i-1})P_{i-1} + (b_i - b_{i-1})Q_{i-1} = a_ilP_i + b_ilQ_i - a_{i-1}P_{i-1} - b_{i-1}Q_{i-1} = lR_i - R_{i-1} = 0$, som betyr at $a_i - a_{i-1} = b_i - b_{i-1} = 0 \pmod{l^{i-1}}$.