# Vragen algorithme René Schoof

Gijsbert van Vliet

October 14, 2014

- In het algorithme van René Schoof wordt een afbeelding

$$(1) End_{\mathbb{F}_q} E \to End_{Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)} E[l]$$

gedefinieerd.
Ik weet dat $End_{\mathbb{F}_q} E$ precies de endomorphismen $\phi$ van $E$ zijn zodanig dat voor iedere $\sigma \in Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ geldt dat

$$\phi(P^\sigma) = \phi(P)^\sigma$$

Is het nu ook zo dat $End_{Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)} E[l]$ precies de endomorphismen $\phi : E[l] \to E[l]$ zijn die commuteren met ieder element $\sigma \in Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ en dat afbeelding (1) simpelweg gegeven is door restrictie van endomorphismen van $E$ tot endomorphismen van $E[l]$?

- Verderop in het algorithme wordt een onderscheid gemaakt tussen twee gevallen. Het eerste geval is het geval dat er een $P \in E[l]$ bestaat met $\phi_l^2 P = \pm qP$.
In het speciale geval dat $\phi_l^2 P = qP$ wordt in één zin de conclussie getrokken dat als $\left(\frac{q}{l}\right) = -1$, dat dan $t \equiv 0 \pmod{l}$. Ik zie niet in waarom deze conclussie zo snel getrokken kan worden.
Ook wordt in dit gedeelte van het algorithme gesproken over de eigenwaarde van $\phi_l$. Is dit gewoon de eigenwaarde van $\phi_l$ waarbij deze geïntepreteerd wordt als element van $Gl_2(\mathbb{Z}_l)$?