Übung 9 Elliptische Kurven

17.12.21

Aufgabe 1) Ergänzung zu Blatt 8, Aufgabe 3 (Silverman Ex. 3.15)

a) **Zeige:** $e_{[m]} = e_m$

b) **Zeige:** $e_\phi(S,T) = e_{\hat{\phi}}(T,S)^{-1}$

c) Kann man den Zusammenhang

$$e_{\hat{\phi}\circ\phi}(S,T) = e_{\hat{\phi}}(\phi(S),T)$$

$$\| $$

$$e_{[m]}(S,T) \qquad \forall\, S \in \ker([m]) = E[m]$$

$$T \in \ker(\phi)$$

zusammen mit a) und b) nutzen, um die Bilinearität von e_ϕ aus der Bilinearität von e_m herzuleiten.

Aufgabe 2) Silverman, Aufgabe III. 3.23

Aufgabe 3) Silverman, Aufgabe IX. 3.32