Suggested Exercises

Total: 4+13+4 =21 questions.

Koblitz Section I.5: 2(a,b,c), 4
Koblitz Section I.6: 1(a,b,c,d), 4, 6, 11 (c,d), 12(a,b), 13, 14(b,c)

Let E_1, E_2 be elliptic curves defined over $\mathbb{C}$ (simply viewed as complex tori). Denote $\text{Hom}(E_1, E_2)$ the ring of isogenies from E_1 to E_2, and $\text{End}(E)$ the ring of endomorphisms of the elliptic curve E:

$$\text{End}(E) := \text{Hom}(E, E) = \{ \text{ isogenies from } E \text{ to } E\}.$$

(1) Show that $\text{End}(E)$ contains $\mathbb{Z}$.
(2) Let $L = \mathbb{Z}\tau + \mathbb{Z}$ be a lattice in $\mathbb{C}$ with $\tau \in \mathbb{H}$. Show that End $(\mathbb{C}/L)$ is $\mathbb{Z}$ unless $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$, in which case it is a subring of $\mathbb{Q}(\tau)$ of rank 2 as a $\mathbb{Z}$-module.

In the case $\text{End}(E) \neq \mathbb{Z}$, we say that E has *complex multiplication.*

Let $\phi \in \text{Hom}(E_1, E_2)$. The degree of ϕ can be defined as

$$\deg(\phi) := |\ker \phi|.$$

For a given positive integer d and a fixed elliptic curve $\mathbb{C}/L$, let

$$N_d := \#\left(\{\mathbb{C}/L' : \text{ there exists an isogeny } \mathbb{C}/L' \longrightarrow \mathbb{C}/L \text{ of degree } d\}/\simeq\right).$$

(3) Show that
$$N_d = \#\{L' : L' \leq L, \, [L : L'] = d\}.$$
(4) Show that $N_d = \displaystyle\sum_{n|d} n$, i.e, $N_d = \sigma(d)$.