Elliptic curves: exercise sheet 10

Due: 26th November 2013

Mastermath / DIAMANT, Fall 2013

René Schoof and Peter Stevenhagen

Exercise 25. Let S be the set of integers $N \in \mathbf{Z}_{>0}$ arising as the order of an elliptic curve over some finite field $\mathbf{F}_q$, with q a prime power that is not a prime. Show that S is a zero-density subset of the integers, that is, show that

$$\lim_{X\to\infty} \frac{\#\{s \in S : s \le X\}}{X} = 0.$$

Exercise 26. How many complex elliptic curves (up to isomorphism) have complex multiplication by the ring $\mathbf{Z}[\frac{1+\sqrt{D}}{2}]$ of discriminant $D = -71$? Same for $D = -163$.

Exercise 27. Let Λ_1 and Λ_2 be lattices in $\mathbf{C}$, and define the product $\Lambda_1\Lambda_2$ as the additive subgroup of $\mathbf{C}$ that is generated by all elements of the form $\lambda_1\lambda_2$, with $\lambda_i \in \Lambda_i$ for $i = 1, 2$. Show that the following are equivalent:

(a) $\Lambda_1\Lambda_2$ is a lattice

(b) Λ_1 and Λ_2 have CM by orders that have the *same* imaginary quadratic field as their field of fractions.

Exercise 28. Let Λ be a complex lattice with multiplier ring equal to the imaginary quadratic order $\mathcal{O}_D$, and define

$$\Lambda^{-1} = \{\alpha \in \mathbf{C} : \alpha\Lambda \subset \mathcal{O}_D\}.$$

Show that Λ^{-1} is a lattice with multiplier ring $\mathcal{O}_D$, and that $\Lambda\Lambda^{-1}$ is a scalar multiple of the lattice $\mathcal{O}_D$.

Exercise 29. Let D be an imaginary quadratic discriminant. Show that the set $\mathcal{C}(D)$ of isomorphism classes of complex elliptic curves with endomorphism ring $\mathcal{O}_D$ obtains a natural group structure if we define the product of isomorphism classes by

$$[\mathbf{C}/\Lambda_1] \cdot [\mathbf{C}/\Lambda_2] = [\mathbf{C}/(\Lambda_1\Lambda_2)].$$

Exercise 30. Compute the group structure of $\mathcal{C}(-68)$ and $\mathcal{C}(-195)$ as defined in the previous exercise.