DIOPHANTINE EQUATIONS

September 15–19 2015, Baskerville Hall, Hay-on-Wye

ELLIPTIC CURVES

1. Show that $y^2 + y = x^3 - x$ has infintely many rational solutions.
(You may assume that the curve is smooth over $\mathbb{Q}$ and over $\mathbb{F}_p$ for all primes $p \neq 37$.)

(*Hint: Prove that it has no non-trivial points of finite order.*)

2. Let $E/\mathbb{Q}$ be the elliptic curve given by $y^2 = (x+1)(x+4)(x-5)$.

(i). Prove that the group of rational points is isomorphic to $\mathrm{C}_2 \times \mathrm{C}_2 \times \mathbb{Z}$. You may find it helpful to note that $Q = (-3, 4)$ lies on the curve.

(*Hint: Bound the torsion by reducing the curve modulo 5 and modulo 7. Find the rank by doing 2-descent and bounding the image by looking at $E(\mathbb{R})$ and $E(\mathbb{Q}_3)$.*)

(ii). Find all rational solutions to the equation defining E. You may assume that for this curve

$$-5.60 \leq h(P) - \hat{h}(P) \leq 1.58$$

for all $P \in E(\mathbb{Q})$, and may find it helpful to know that $10Q$ has x-coordinate

$$\frac{661822357518174342999917659646891158606732140305553705}{311668667097257198712027230911109622652235276597856l6}.$$

(*Hint: Find an upper bound on $h(R)$ for the generator R of the copy of $\mathbb{Z}$ in $E(\mathbb{Q})$.*)

3. (i). Let $E : y^2 = f(x)$ be an elliptic curve, $K = \mathbb{Q}(\sqrt{d})$ a quadratic extension, and E_d the curve $dy^2 = f(x)$, the *quadratic twist* of E by d. Show that

$$\mathrm{rk}\, E/\mathbb{Q}(\sqrt{d}) = \mathrm{rk}\, E/\mathbb{Q} + \mathrm{rk}\, E_d/\mathbb{Q}.$$

(ii). Although the following holds true for all elliptic curves over all number fields and in all quadratic extensions, it is slightly easier to do one explicit example. Take

$$E/\mathbb{Q} : y^2 = x^3 - x \qquad (\Delta_E = 64),$$

and show that

$$L(E/\mathbb{Q}(\sqrt{-3}), s) = L(E/\mathbb{Q}, s) L(E_{-3}/\mathbb{Q}, s).$$

4*. Assuming either the Birch–Swinnerton-Dyer conjecture or finiteness of the Tate-Shafarevich group show that there is algorithm to determine whether a polynomial equation $f(x, y) = 0$ with $\mathbb{Z}$-coefficients has infinitely many rational solutions.