Section C

Elliptic Curves

Victor Flynn 3/3/2008

Do not turn this page until you are told that you may do so

C9.1b. Elliptic Curves

C9.1b1. (i) Decide whether there exists $x \in \mathbb{Q}_p$ such that $x^3 = 5$ for each of: $p = 3, 5, 13$.

(ii) Find the 3-adic expansion of $-\frac{13}{8}$. For any prime p, and $a_0, a_1, a_2 \in \{0, \ldots, p-1\}$, express $a_0, \overline{a_1 a_2} = a_0 + a_1 p + a_2 p^2 + a_1 p^3 + a_2 p^4 + \ldots$ in the form m/n, where $m, n \in \mathbb{Z}$.

(iii) Let $\mathcal{E} : x^3 + y^3 = p$, defined over $\mathbb{Q}_p$, and let $\widetilde{\mathcal{E}} : x^3 + y^3 = 0$, defined over $\mathbb{F}_p$, be the reduction of $\mathcal{E}$ modulo p. Show that $(0,0)$ is a singular point on $\widetilde{\mathcal{E}}(\mathbb{F}_p)$ and that it does not lift to a point on $\mathcal{E}(\mathbb{Q}_p)$. Find a curve $\mathcal{D}$, nonsingular and defined over $\mathbb{Q}_p$, such that $\widetilde{\mathcal{D}} = \widetilde{\mathcal{E}}$ and such that $(0,0) \in \widetilde{\mathcal{D}}(\mathbb{F}_p)$ does lift to a point on $\mathcal{D}(\mathbb{Q}_p)$.

(iv) Let $p \neq 2$ be prime and let $a, b, c \in \mathbb{Z}_p$ satisfy $|a|_p = |b|_p = |c|_p = 1$. Show that there exist $x, y \in \mathbb{Z}_p$ such that $ax^2 + by^2 = c$.

[You might first wish to consider, for any $\alpha, \beta, \gamma \in \mathbb{F}_p \backslash \{0\}$, the sizes of the sets $\{\alpha x^2 : x \in \mathbb{F}_p\}$ and $\{\gamma - \beta y^2 : y \in \mathbb{F}_p\}$.]

C9.1b2. (i) State and prove the Nagell-Lutz Theorem for $\mathbb{Q}$-rational torsion points on the elliptic curve $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$. [You may assume the result that any $\mathbb{Q}$-rational torsion point (x, y) on such a curve satisfies $x, y \in \mathbb{Z}$. You may also use the polynomial identity: $\phi_1(X)\psi_1(X) + \phi_2(X)\psi_2(X) = 4A^3 + 27B^2$, where $\phi_1(X) = 3X^2 + 4A$, $\psi_1(X) = (3X^2 + A)^2$, $\phi_2(X) = -27(X^3 + AX - B)$ and $\psi_2(X) = X^3 + AX + B$.]

(ii) Find the torsion group over $\mathbb{Q}$ for the elliptic curve $y^2 = x^3 + x + 1$, and deduce that this curve has infinitely many rational points.

(iii) Let $D \in \mathbb{Z}$ satisfy $D \not\equiv 0 \pmod 5$ and $D \equiv 2 \pmod 7$. Suppose also that there exists a prime $p \equiv 1 \pmod 3$ such that D is not a quadratic residue mod p. Find the torsion group over $\mathbb{Q}$ for the elliptic curve $y^2 = x^3 + D$.

(iv) Let $\mathcal{E} : y^2 = x(x-1)(x-4)$. Show that $(2, 2i), (1 - i\sqrt{3}, 3 + i\sqrt{3}), (4 + 2\sqrt{3}, 6 + 4\sqrt{3})$ each have order 4 in $\mathcal{E}(\mathbb{C})$. Show that $\#\widetilde{\mathcal{E}}(\mathbb{F}_p)$ is divisible by 8, for all primes $p \neq 2, 3$. Show that the torsion group of $\mathcal{E}(\mathbb{Q})$ has order 4.

C9.1b3. Let $\mathcal{C} : Y^2 = X(X^2 + aX + b)$ and $\mathcal{D} : Y^2 = X(X^2 + a_1X + b_1)$, where $a, b \in \mathbb{Z}$ with $b(a^2 - 4b) \neq 0$ and $a_1 = -2a$, $b_1 = a^2 - 4b$. Let the map ϕ [which you may assume to be a homomorphism] be defined as usual by

$$\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q}) : (x, y) \mapsto \Big(\frac{y^2}{x^2},\ y - \frac{by}{x^2}\Big) = \Big(\frac{x^2 + ax + b}{x},\ y - \frac{by}{x^2}\Big).$$

Let q be defined as usual by

$$q : \mathcal{D}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 : (u, v) \mapsto u \text{ when } u \neq 0,$$

$$q : (0, 0) \mapsto b_1,\ \ q : \underline{\mathbf{o}} \mapsto 1.$$

(i) Show that the image of q is a subset of the finite set

$$\{r : r \text{ is a square free integer and } r|b_1\}.$$

(ii) Find the rank of the elliptic curve $Y^2 = X(X^2 + 3X - 3)$. [Standard results may be used without proof, provided they are accurately stated.]

C9.1b4. (a) For any elliptic curve $\mathcal{E}$ and $(s, t) \in \mathcal{E}(\mathbb{Q})$ with $s, t \in \mathbb{Q}$ and $s = \frac{c}{d}$, $c, d \in \mathbb{Z}$, $\gcd(c, d) = 1$, let the height function $h_x(s, t)$ be defined, as usual, by:

$$h_x\big((s, t)\big) = \log\max\big(|c|, |d|\big),$$

and define $h_x(\underline{\mathbf{o}}) = 0$.

(i) Show that, for any $m \geq 1$, there is a constant C_m, independent of P, such that $|h_x(mP) - m^2 h_x(P)| \leq C_m$, for all $P \in \mathcal{E}(\mathbb{Q})$.

(ii) Show that, for any $P \in \mathcal{E}(\mathbb{Q})$, the sequence $4^{-n} h_x(2^n P)$ is Cauchy and therefore convergent in $\mathbb{R}$ as $n \to \infty$.

[You may use the result that there exists a constant C, independent of P, Q, such that $|h_x(P + Q) + h_x(P - Q) - 2h_x(P) - 2h_x(Q)| \leq C$, for all $P, Q \in \mathcal{E}(\mathbb{Q})$.]

(b) Let K be field, complete with respect to a discrete non-Archimedean valuation, $R = \{x \in K : |x| \leqslant 1\}$, $\mathcal{M} = \{x \in K : |x| < 1\}$, and assume that $R/\mathcal{M}$ is of characteristic p, for some prime p. Let $F(X, Y)$ be a formal group defined over R, and let $F(\mathcal{M})$ denote the set $\mathcal{M}$ together with the group operation: $x \oplus y = F(x, y)$. For any $m \geq 1$, let $[m](x)$ denote, as usual, $x \oplus \ldots \oplus x$ [m times]. Show that, for any $x \in \mathcal{M}$, the sequence $[p^n](x) \to 0$ as $n \to \infty$.

(c) Let $p \equiv 1 \pmod{12}$ and $q \equiv 5 \pmod{12}$ be primes. Show that there exists an elliptic curve of the form $y^2 = x^3 + ax - a$, with $a \in \mathbb{Z}$, for which the Elliptic Curve Method, using $3(1, 1)$, successfully factorises $N = pq$.