Section C

Elliptic Curves

Victor Flynn 3/3/2007

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

C9.1b. Elliptic Curves

C9.1b1. (i) Find an $x \in \mathbb{Z}$ such that $|x^2+2|_3 < 3^{-2}$. Show that there does not exist $x \in \mathbb{Z}$ such that $|x^2+3|_3 < 3^{-2}$.

(ii) Let $p \neq 2$ be prime. Find the p-adic expansion of $\frac{1+2p}{p-p^3}$.

(iii) Does there exist a prime p such that $p = p^p$ in $\mathbb{Q}_p^*/\left(\mathbb{Q}_p^*\right)^p$?

(iv) Let q, r be distinct primes, and let $\alpha, \beta \in \mathbb{Q}$. Show that there exists a sequence $x_n \in \mathbb{Q}$ such that $x_n \to \alpha$ with respect to $|\ |_q$, and $x_n \to \beta$ with respect to $|\ |_r$, as $n \to \infty$. Does there exist a sequence $y_n \in \mathbb{Q}^*$ such that $y_n \to 0$ with respect to $|\ |_p$ for all primes p, and $y_n \to 0$ with respect to $|\ |_\infty$, as $n \to \infty$?

C9.1b2. (i) 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 suppose that $z \in \mathcal{M}$ has exact order p^n, for some $n \geqslant 1$, with respect to the group operation $x \oplus y = F(x, y)$ on $\mathcal{M}$. Show that:

$$|z| \geqslant |p|^{\frac{1}{p^n - p^{n-1}}}.$$

[You may assume the result that, for any prime p, the multiplication by p map $[p](T)$ can be written as $[p](T) = pf(T) + g(T^p)$, for some $f(T) = T + \ldots \in R[[T]]$ and $g(T) \in R[[T]]$.]

(ii) Let $\mathcal{E} : y^2 = x^3 + Ax + B$, be an elliptic curve, where $A, B \in \mathbb{Z}_p$, and let $\widetilde{\mathcal{E}}$ denote the reduction of $\mathcal{E}$ modulo p. Show that any $(x, y) \in \mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ satisfies $|x|_p \leqslant 1, |y|_p \leqslant 1$. When $\widetilde{\mathcal{E}}$ is non-singular, show that $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_p)$.

(iii) Let $D \in \mathbb{Z}$, $D > 0$, $D \equiv 2 \pmod 3$. Describe the torsion group over $\mathbb{Q}$ of the elliptic curve $Y^2 = X^3 + DX$.

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 q is a homomorphism.
[You are only required to show that $q(P + Q) = q(P)q(Q)$ in the typical case when none of $P, Q, P + Q$ are $(0, 0)$ or $\underline{\mathbf{o}}$.]

(ii) Show that q has kernel $\phi(\mathcal{C}(\mathbb{Q}))$.

(iii) Find the rank of the elliptic curve $Y^2 = X(X^2 + X - 2)$.

C9.1b4. (i) Find a proper factor of $N = 10573$ by applying the Elliptic Curve Method, using the curve $Y^2 = X^3 - X - 5$ and $3P$, where $P = (2, 1)$.

(ii) 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 $h_x(\underline{\mathbf{o}}) = 0$.
Let $\mathcal{C}, \mathcal{D}, \phi$ be as defined in the previous question. Find a constant k, which depends only on a, b, such that $h_x\big(\phi(P)\big) \leqslant 2\big(h_x(P)\big) + k$, for all $P \in \mathcal{C}(\mathbb{Q})$. Find a constant ℓ, which depends only on a, b, such that $h_x\big(2P\big) \leqslant 4\big(h_x(P)\big) + \ell$, for all $P \in \mathcal{C}(\mathbb{Q})$.

(iii) Let $p \neq 2$ be prime, let $m \in \mathbb{F}_p^*$ and let $\mathcal{E}$ be the elliptic curve $Y^2 = X(X^2 + m^2)$, defined over $\mathbb{F}_p$. Show that $\#\mathcal{E}(\mathbb{F}_p)$ is always divisible by 4.
[You may wish to consider separately the cases $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$.]