Section C

Elliptic Curves

Victor Flynn 23/2/2009

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

C9.1b. Elliptic Curves

C9.1b1. (a) Let $\mathcal{C}$ be a non-singular cubic curve, defined over a field K, with a K-rational point $\mathbf{o}$. Describe the standard law for adding two points on $\mathcal{C}$, and prove that it is associative.

(b) For which primes p do there exist $x, y \in \mathbb{Z}_p$ such that $y^2 = x^3 - x - 1$? [You may find it helpful first to compute $h(-2), h(0), h(3)$ for $h(x) = x^3 - x - 1$.]

(c) Find a proper factor of $N = 221$ by applying the Elliptic Curve Method, using the curve $Y^2 = X^3 + 5X - 5$ and $3P$, where $P = (1, 1)$.

(d) Find a sequence $x_n \in \mathbb{Q}_p$ such that $\sum_{n=1}^{\infty} x_n$ is convergent in $\mathbb{Q}_p$ but $\sum_{n=1}^{\infty} |x_n|_p$ is not convergent in $\mathbb{R}$.

C9.1b2. (a) Let R be any ring (commutative, with 1), and let F, G be formal groups over R.

(i) Show that there exists a unique normalised invariant differential for F, which is given by $\omega = F_X(0, T)^{-1} \mathrm{d}T \in R[[T]]\mathrm{d}T$, and that every invariant differential for F is of the form $a\omega$ for some $a \in R$.

(ii) Let f be a homomorphism over R from F to G. Let ω_F, ω_G be the normalised invariant differentials on F, G, respectively. Show that $\omega_G \circ f = f'(0)\ \omega_F$. Deduce that, for any prime p, there exist $f, g \in R[[T]]$ such that $[p](T) = pf(T) + g(T^p)$ [where $[p]$ represents the multiplication-by-p map on F].

(b) Find the torsion group over $\mathbb{Q}$ for the elliptic curve $Y^2 = X^3 - 9$.

(c) Let $n \in \mathbb{Z}$ be not divisible by 15, let n and $-n$ both be nonsquare, and let $\mathcal{E}, \mathcal{F}$ be the elliptic curves $\mathcal{E} : Y^2 = X^3 + nX$ and $\mathcal{F} : Y^2 = X^3 - nX$. Show that at least one of $\mathcal{E}(\mathbb{Q})$ or $\mathcal{F}(\mathbb{Q})$ has torsion group given by $\{\mathbf{o}, (0, 0)\}$.

C9.1b3. (a) Find the rank of the elliptic curve $Y^2 = X(X^2 + 5X - 5)$.

(b) Let p be prime. Show that the elliptic curve $Y^2 = X^3 + pX$ has rank at most 2.

(c) Let $\alpha \in \mathbb{Z}$, $\alpha \neq 0, -4$, and let $\mathcal{C}$ be the elliptic curve $Y^2 = X^3 + \alpha X^2 - \alpha X$. Show that $(1, 1) \in 2\mathcal{C}(\mathbb{Q}) \iff \alpha$ or $\alpha + 4$ is the square of an integer. [You may find it helpful first to construct a curve $\mathcal{D}$ with 2-isogenies $\phi : \mathcal{C} \to \mathcal{D}$, $\hat{\phi} : \mathcal{D} \to \mathcal{C}$, and find the preimages of $(1, 1)$ under $\hat{\phi}$.]

End of Last Page