Section C

Elliptic Curves

Victor Flynn 2/6/2006

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

C9.1b. Elliptic Curves

C9.1b1. (i) Let K be a field, complete with respect to a non-Archimedean valuation $|\ |$, with valuation ring $R = \{x \in K : |x| \leqslant 1\}$. Prove Hensel's Lemma, that if $f(x) \in R[x]$ and $a_0 \in R$ satisfies $|f(a_0)| < |f'(a_0)|^2$, then there exists a unique $a \in R$ such that $f(a) = 0$ and $|a - a_0| \leqslant |f(a_0)|/|f'(a_0)|$.

(ii) For which primes p do there exist $x, y \in \mathbb{Z}_p$ such that $3y^2 = 4x^3 - 10$?

(iii) For prime $p \neq 2$, determine how many elements there are in the set $\mathbb{Q}_p^*/\left(\mathbb{Q}_p^*\right)^2$. Determine how many elements there are in the set $\mathbb{Q}_2^*/\left(\mathbb{Q}_2^*\right)^2$.

C9.1b2. 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].

(iii) Let $m, n \in \mathbb{Z}$, with $n \neq 0$. Show that the curve $Y^2 = X^3 - (m^2+1)^2X + 9n^2$ has infinitely many $\mathbb{Q}$-rational points.

C9.1b3. (i) Find a proper factor of $N = 1517$ by applying the Elliptic Curve Method, using the curve $Y^2 = X^3 + 7X - 7$ and $4P$, where $P = (1, 1)$.

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

(iii) Let $\mathcal{E}_k$ be the elliptic curve $Y^2 = X^3 + k$, where $k \in \mathbb{Q}$ and $k \neq 0$. Show that there is always a point of order 3 in $\mathcal{E}_k(\mathbb{C})$ which is not in $\mathcal{E}_k(\mathbb{Q})$.

C9.1b4. (i) Find the rank of the elliptic curve $Y^2 = X(X^2 + 3X + 5)$.

(ii) For any prime $p \equiv 5 \pmod 8$, show that the elliptic curve $Y^2 = X^3 + p^2X$ has rank 0.

End of Last Page