Elliptic curves

Problem sheet 3

December 10, 2009

1. For each triple p, m, r below, find an $x \in \mathbb{Z}$ such that $|r - x|_p \leq p^{-m}$:

(i) $p = 257$, $r = 1/2$, $m = 1$

(ii) $p = 3$, $r = 7/8$, $m = 2$

(iii) $p = 3$, $r = 7/8$, $m = 7$

(iv) $p = 3$, $r = 5/6$, $m = 9$

(v) $p = 5$, $r = 1/4$, $m = 4$

2. One can explicitly work out the group $E(k)$ if E is a given elliptic curve over a given finite field k—one can just count all the solutions and then add them to each other until one finds out what's going on. For the following equations find all the solutions, and work out explicitly what the group is.

(i) $y^2 = x^3 + x$ over $k = \mathbb{Z}/5$.

(ii) $y^2 = x^3 + 2x$ over $k = \mathbb{Z}/5$.

(iii) $y^2 = x^3 + x$ over $k = \mathbb{Z}/3$.

(iv) $y^2 + y = x^3 + x^2$ over $k = \mathbb{Z}/2$ (Note however that the inverse of (x, y) is not $(x, -y)$; this formula only works for cubics of the form $y^2 = f(x)$).

(v) Can $\mathbb{Z} \times \mathbb{Z}/6 \times \mathbb{Z}/8 \times \mathbb{Z}/10$ be realized as the group of points of some elliptic curve over some field? Why can't an arbitrary abelian group show up?

3. Compute the torsion subgroups of the following elliptic curves over $\mathbb{Q}$:

(i) $Y^2 = X^3 + 4X$

(ii) $Y^2 = X^3 - 9X$

(iii) $Y^2 = X^3 - 43X + 166$

(iv) $Y^2 = X^3 - 219X + 1654$ (The numbers can get a bit big so you may want to use a calculator; the point of the last two questions is that there are points of large order).

4 Prove that the equation $y^2 + y = x^3 - x^2$ defines a non-singular curve $E \subset \mathbb{P}^2_{\mathbb{Q}}$. Determine all the points $P = (x, y)$ in $E(\mathbb{Q})$ such that x, $y \in \mathbb{Z}$, $|x| \leq 1$, $|y| \leq 1$, and the subgroup of $E(\mathbb{Q})$ generated by them.

5 Determine the primes p such that $y^2 + y = x^3 - x$ defines a non-singular curve over a field of characteristic p. Check that 2 and 3 are among these primes.