ELLIPTIC CURVES
Homework 2

4. $a)$ Let E be the elliptic curve over $\mathbf{Q}_p$ with affine equation $y^2 = x^3 + p$. Show that the point $(0,0)$ on the reduction of E mod p does not lift to a point in $E(\mathbf{Q}_p)$.

$b)$ Find an example of an elliptic curve E over $\mathbf{Q}_p$ with additive reduction where the point $(0,0)$ on the reduction of E mod p lifts to a point in $E(\mathbf{Q}_p)$.

5. Let E be an elliptic curve over $\mathbf{Q}$. We have seen in class that for all primes p the group $E(\mathbf{Q}_p)^{(1)}$ is uniquely m-divisible for m prime to p. Use this result to give a proof of the fact, proven in class in another way, that there are only finitely many torsion points in $E(\mathbf{Q})$. (You will need a small trick.)

6. We admit the following facts from number theory: If $\overline{\mathbf{Q}}_p$ is a fixed algebraic closure of $\mathbf{Q}_p$, for each $n > 0$ there is a unique unramified extension $K_n|\mathbf{Q}_p$ contained in $\overline{\mathbf{Q}}_p$. The union $\mathbf{Q}_p^{\mathrm{nr}}$ of the K_n for all n is the *maximal unramified extension* of $\mathbf{Q}_p$. It is the fraction field of a complete discrete valuation ring with maximal ideal (p) and residue field $\overline{\mathbf{F}}_p$.

$a)$ Let E be an elliptic curve over $\mathbf{Q}_p$. Show that for m prime to p the group $E(\mathbf{Q}_p^{\mathrm{nr}})^{(0)}$ is m-divisible, i.e. the multiplication-by-m map is surjective. Here $E(\mathbf{Q}_p^{\mathrm{nr}})^{(0)}$ denotes, as in class, the group of points in $E(\mathbf{Q}_p^{\mathrm{nr}})$ whose reduction in $\overline{E}(\overline{\mathbf{F}}_p))$ is smooth.

$b)$ Is $E(\mathbf{Q}_p^{\mathrm{nr}})^{(0)}$ always uniquely m-divisible for m prime to p? If yes, give a proof, if not, give a counterexample. [*Hint*: You may want to consider the case $m = 2$.]

7. Let E be an elliptic curve over $\mathbf{Q}$, with Tate–Shafarevich group $Ш(E)$.

$a)$ Show that $Ш(E)$ is finite if and only if $NШ(E)$=0 for some $N > 0$.

$b)$ Suppose there is a surjective morphism with finite kernel $E \to E'$ with $Ш(E')$ finite. Deduce that $Ш(E)$ is finite.

Note: In $b)$ we mean the morphism $E \to E'$ is a surjective group homomorphism on points and has finite kernel. It can be shown that any non-constant morphism $E \to E'$ (in the sense of algebraic geometry) sending O to O has this property. Such maps are called *isogenies.*