Elliptic Curves. Sheet 5. To be handed in during 6th Week.

1. Prove that, if $d \in \mathbb{Z}_p$ is non-square, then

$$|a + b\sqrt{d}|_p = |a^2 - b^2 d|_p^{1/2}, \text{ for any } a, b \in \mathbb{Q}_p,$$

defines a non-Archimedean valuation on $\mathbb{Q}_p(\sqrt{d})$ which extends the usual $|\ |_p$ on $\mathbb{Q}_p$. [Hint: First show that, for any $\alpha \in \mathbb{Q}_p(\sqrt{d})$, $|\alpha|_p \leqslant 1 \Rightarrow |\alpha + 1|_p \leqslant 1$].

2. Let $\mathcal{E} : Y^2 = X^3 + 17$, defined over $\mathbb{Q}$, and $\widetilde{\mathcal{E}} : Y^2 = X^3 + 2$, defined over $\mathbb{F}_5$. What does $(-64/25, 59/125) \in \mathcal{E}(\mathbb{Q})$ map to under the reduction map modulo 5?

3. Let $\mathcal{E} : Y^2 = X^3 + p$, defined over $\mathbb{Q}_p$, and $\widetilde{\mathcal{E}} : Y^2 = X^3$, defined over $\mathbb{F}_p$, where $p \neq 2$. Show that $(0, 0)$ on $\widetilde{\mathcal{E}}$ does not lift to a point in $\mathcal{E}(\mathbb{Q}_p)$.

4. Give examples of elliptic curves defined over $\mathbb{Z}_p$ ($p \neq 2$) such that $\widetilde{\mathcal{E}}$, defined over $\mathbb{F}_p$, has:
(a). A cusp which lifts to a point in $\mathcal{E}(\mathbb{Q}_p)$.
(b). A cusp which does not lift to a point in $\mathcal{E}(\mathbb{Q}_p)$.
(c). A node which lifts to a point in $\mathcal{E}(\mathbb{Q}_p)$.
(d). A node which does not lift to a point in $\mathcal{E}(\mathbb{Q}_p)$.

5. A *non-commutative formal group* over a ring R is a power series $F(X, Y) \in R[[X, Y]]$ which satisfies:
$F(X, Y) = X + Y +$ terms of degree $\geqslant 2$,
and
$F(X, F(Y, Z)) = F(F(X, Y), Z)$ [associativity],
but not $F(X, Y) = F(Y, X)$ [commutativity]. Let $R = \mathbb{F}_p[t]/I$, where $I = t^2\mathbb{F}_p[t]$. Find a non-commutative formal group over R.

The following question is compulsory for students taking the MSc in MFoCS (Mathematics and the Foundations of Computer Science). For everyone else, it is optional.

6. Let $\mathcal{E} : Y^2 = X^3 + AX$, where $A \in \mathbb{Z}$ and $A \neq 0$. Let $F(X, Y)$ be the formal group associated to $\mathcal{E}$ [as in lectures] and let $F(X, Y) = \sum F_n(X, Y)$, where each $F_n(X, Y)$ is homogeneous of degree n. Show that $F_n(X, Y) = 0$ unless $n \equiv 1 \pmod 4$. What is the similar result when the elliptic curve is of the form $\mathcal{E} : Y^2 = X^3 + B$?