Elliptic Curves. HT 2019/20. Sheet 3.

1. Show that the curve $2Y^2 = X^4 - 17$ has points in $\mathbb{R}$ and every $\mathbb{Q}_p$, but not in $\mathbb{Q}$.
[Hint: For showing that there are points in every $\mathbb{Q}_p$, it is helpful to use Theorem 1.15 (note also that the curve is birationally equivalent to $V^2 = 2X^4 - 34$, where $V = 2Y$). For showing there are no points in $\mathbb{Q}$, first show that, if there were points in $\mathbb{Q}$, then there would exist $r, s, t \in \mathbb{Z}$ with $\gcd(r,t) = 1$ such that $2s^2 = t^4 - 17r^4$, and then show that any prime dividing s is a quadratic residue modulo 17].

2. Let $p \equiv 2 \bmod 3$. For any $a \in \mathbb{Z}$ such that $p \nmid a$, show that there exists $x \in \mathbb{Z}_p$ with $x^3 = a$.

3. Let K be a field, complete with respect to a non-Archimedean valuation $|\ |$, and let $R = \{x \in K : |x| \leqslant 1\}$. Let $f(X) \in R[x]$ have discriminant D, and let $a_0 \in R$ satisfy $|f(a_0)| < |D|^2$. Show that $f(X)$ has a root $a \in R$.

4. 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 $\alpha \in \mathbb{Q}_p(\sqrt{d})$, $|\alpha|_p \leqslant 1 \Rightarrow |\alpha + 1|_p \leqslant 1$].

5. 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?

6. 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 $\mathcal{E}(\mathbb{Q}_p)$.

7. 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 $\mathcal{E}(\mathbb{Q}_p)$.

8. 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 $\geqslant 2$,
$F(X, F(Y,Z)) = F(F(X,Y), Z)$ [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.