Elliptic Curves. Sheet 4. To be handed in during 5th Week.

1. Decide whether there exists $x \in \mathbb{Q}_p$ such that $x^2 = -28$ for each of: $p = 2, 3, 5, 7, 11$.

2. Show that $(X^2 - 2)(X^2 - 17)(X^2 - 34)$ has a root in $\mathbb{R}$ and in every $\mathbb{Q}_p$, but not in $\mathbb{Q}$.

3. Is 4 a cube in $\mathbb{Q}_3$? Is 28 a cube in $\mathbb{Q}_3$? Is 13 a cube in $\mathbb{Q}_7$?

4. 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].

5. 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 $x^3 = a$.

6. Let K be any field with 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 $a \in R$.

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.

7. Show that $f(X) = 5X^3 - 7X^2 + 3X + 6$ has a root $\alpha \in \mathbb{Z}_7$ with $|\alpha - 1|_7 < 1$. Find $a \in \mathbb{Z}$ such that $|\alpha - a|_7 \leqslant 7^{-4}$.