HOMEWORK 3

TOPICS IN AG: ELLIPTIC CURVES

Due April 19, 2004

(1) Compute the torsion group $E(\mathbb{Q})_{\text{tors}}$ for the elliptic curve $y^2 = x^3 + 1$. (Euler proved that these are the only rational points on E).
(2) Consider the elliptic curve $E : y^2 = x^3 + b$ with $b \in \mathbb{Z}$; For any odd prime $p \equiv 2 \bmod 3$ we have $\#E(\mathbb{F}_p) = p + 1$.
(3) Let $E : y^2 = x^3 + b$ be an elliptic curve, where $b \in \mathbb{Z}$ is not divisible by a sixth power $\neq 1$. Then

$$E(\mathbb{Q})_{\text{tors}} \simeq \begin{cases} \mathbb{Z}/6\mathbb{Z}, & \text{if } b = 1; \\ \mathbb{Z}/3\mathbb{Z}, & \text{if } b = -432 \text{ or } 1 \neq b \text{ is a square}; \\ \mathbb{Z}/2\mathbb{Z} & \text{if } 1 \neq b \text{ is a cube}; \\ 0 & \text{otherwise.} \end{cases}$$

(4) Consider the conic $\mathcal{P} : X^2 - dY^2 = 1$ for squarefree integers d.
   (a) Show that
   $$\mathcal{P}^{(n)} = \{(x, y) \in \mathcal{P}(\mathbb{Z}_p) : x - 1 \equiv y \equiv 0 \bmod p^n\}$$
   are subgroups of $\mathcal{P}(\mathbb{Z}_p)$ for all $n \geq 0$.
   (b) Show that, for $p > 2$, the map $u : \mathcal{P}^{(1)} \longrightarrow \mathbb{Z}_p$ that sends $P = (x, y)$ to $u(P) = \frac{x-1}{y}$ is well defined. Give a convincing reason why we should put $u((1, 0)) = 0$. Show that for $p = 2$, u is defined on $\mathcal{P}^{(2)}$.
   (c) Show that $|u(kP)| = |k| \cdot |u(P)|$ for all $P \in \mathcal{P}^{(1)}$ and all $k \geq 1$; here $|a|$ denotes the p-adic absolute value on $\mathbb{Z}_p$. (Try $k = 2$ first; I also suspect that $|u(P + Q) - u(P) - u(Q)| < \max\{|u(P)|^2, |u(Q)|^2\}$, but haven't found a proof yet).
   (d) Show that $\mathcal{P}^{(1)}$ is torsion free for $p > 2$, and that $\mathcal{P}^{(2)}$ is torsion free for $p = 2$.