HOMEWORK 3

TOPICS IN AG: ELLIPTIC CURVES

Here's the last problem:

Consider the conic $\mathcal{P} : X^2 - dY^2 = 1$ *for squarefree integers* d.

(1) *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* $n \geq 0$.

(2) *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* $\mathcal{P}^{(2)}$.

(3) *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).*

(4) *Show that* $\mathcal{P}^{(1)}$ *is torsion free for* $p > 2$, *and that* $\mathcal{P}^{(2)}$ *is torsion free for* $p = 2$.

Consider the claim that $|u(kP)| = |k| \cdot |u(P)|$. This is trivial for $k = 0, 1$; now consider $k = 2$ and $P = (x, y)$. Then $2P = (x^2 + dy^2, 2xy) = (2x^2 - 1, 2xy)$, hence $u(2P) = \frac{2x^2-2}{2xy} = \frac{x-1}{y}\frac{x+1}{x}$. If $p > 2$, then $x \equiv 1 \bmod 2$ implies that $p \nmid x(x + 1)$, hence $|u(2P)| = |u(P)|$. If $p = 2$ and $n \geq 2$, then $x \equiv 1 \bmod 4$, hence $\frac{x+1}{x} \equiv 2 \bmod 4$ and therefore $|u(2P)| = |2| \cdot |u(P)|$.

Now consider the general case. We have

$$\begin{aligned}
(x + y\sqrt{d}\,)^k &= x^k + \binom{k}{2}x^{k-2}y^2d + \binom{k}{4}x^{k-4}y^4d^2 + \dots \\
&\quad + \binom{k}{1}x^{k-1}y\sqrt{d} + \binom{k}{3}x^{k-3}y^3d\sqrt{d} + \dots \\
&= x^k + \binom{k}{2}x^{k-2}(x^2 - 1) + \binom{k}{4}x^{k-4}(x^2 - 1)^2 + \dots \\
&\quad + \Big[\binom{k}{1}x^{k-1} + \binom{k}{3}x^{k-3}(x^2 - 1) + \dots\Big]y\sqrt{d} \\
&= f(x) + g(x)y\sqrt{d}.
\end{aligned}$$

Thus $kP = (f(x), g(x)y)$ and therefore

$$u(kP) = \frac{f(x) - 1}{g(x)y} = \frac{x - 1}{y} \cdot \frac{f(x) - 1}{(x - 1)g(x)}. \tag{1}$$

Assume first that $p \nmid k$. Then

$$\begin{aligned}\frac{f(x)-1}{x-1} &= 1 + x + x^2 + \ldots + x^{k-1} + \binom{k}{2} x^{k-2}(x+1) \\ &\equiv k + k(k-1) \equiv k^2 \bmod p.\end{aligned}$$

On the other hand we have $g(x) \equiv k \bmod p$, hence the second factor in (1) is a p-adic unit, and we find that $|u(kP)| = |u(P)|$ in this case.

Now assume that $k = p > 3$. Then the denominator $g(x) \equiv px^{p-1} \equiv p \bmod p^2$ because of Fermat's Little Theorem. We need to show that the numerator is divisible exactly by p^2, which requires working modulo p^3.

A better way of proceeding might use the following observation: there exist polynomials $r_k(x), s_k(x)$ such that

$$f_k(x) - 1 = (x-1)r_k(x)^2, \quad g_k(x) = r_k(x)s_k(x).$$

This was discovered while playing around with pari. I'm almost sure this is well known since the polynomials f are closely connected to Chebyshev polynomials.

Assuming this factorization, we have

$$u(kP) = u(P) \cdot \frac{r_k(x)}{s_k(x)}.$$

This should be easier to handle than the original fraction.

I'll keep working on this problem and let you know the outcome.