# HOMEWORK 1

TOPICS IN AG: ELLIPTIC CURVES

Due Monday, Feb. 23, 2004

(1) Show that the map from the quartic $\mathcal{C} : z^2 = x^4+1$ to the Weierstrass cubic $E_1 : u^2 = v^3 - 4v$ is defined for all points of a field except finitely many. Show that the same is true for the inverse map. Thus the map $\mathcal{C} \longrightarrow E$ is an example of a birational isomorphism (a map defined by rational functions, giving a bijection between the (complex) points on the curves except for finitely many exceptions).

(2) Transform the Fermat quartic $\mathcal{C}_2 : z^2 = x^4 - 4$ into Weierstrass form $E_2 : u^2 = v^3 + v$, and show that the map you find is a birational isomorphism.

(3) Consider the two 'curves' $C_1 : X^4 + Y^4 = Z^2$ and $C_2 : X^4 - 4Y^4 = Z^2$ occurring in the proof of FLT for exponent 4. In our proof we started with a rational point $(x, y, z)$ on $C_1$ and obtained a rational point $(a, b, x)$ on $C_2$. Express $x, y, z$ as rational functions of $r, s, a$; this defines a rational map $\phi : C_2 \longrightarrow C_1$.

Is the rational map that you get birational (i.e., can the converse map $C_1 \longrightarrow C_2$ be expressed using rational functions)?

(4) Consider the following diagram:

$$\begin{array}{ccc} C_2 & \longrightarrow & E_2 \\ {\scriptstyle\phi}\downarrow & & \\ C_1 & \longrightarrow & E_1 \end{array}$$

Since the horizontal maps are (essentially) bijective, you can define a map $\psi : E_2 \longrightarrow E_1$ (i.e. rewrite $\phi$ in terms of the new coordinates $u, v$). Do this.

(5) Show that $7 = a^3 + b^3$ for *positive* rational numbers. Hint: starting with the point $P = (2, 1)$ on the cubic $C : x^3 - y^3 = 7$, construct the tangent to $C$ at $P$ and compute their point of intersection $Q \neq P$.