Math 497A Homework 1
Fall 2008
Due: Friday, September 5

(1) Let C be the conic given by the equation

$$F(x,y) = ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

A point (x,y) on C is *singular* if

$$\frac{\partial F}{\partial x}(x,y) = \frac{\partial F}{\partial y} = 0.$$

Let

$$\delta := \det \begin{pmatrix} 2a & b & d \\ b & 2c & e \\ d & e & 2f \end{pmatrix}$$

(a) Show that if $\delta \neq 0$, then C has no singular points.
(b) Show that of $\delta = 0$ and $b^2 - 4ac \neq 0$, then there is a unique singular point on C.
(c) Let L be the line $y = \alpha x + \beta$ with $\alpha \neq 0$. Prove that the intersection of L and C either has $0, 1$ or 2 points.
(d) Determine conditions on the coefficients which ensure that the intersection consists of exactly one point. What is the geometric significance of these conditions? (There will be more than one case to consider.)

(2) For each of the following conics, either find a rational point or prove that there are no rational points.
(a) $x^2 + y^2 = 6$
(b) $3x^2 + 5y^2 = 4$
(c) $3x^2 + 6y^2 = 4$

(3) Prove that for every exponent $e \geq 1$, the congruence

$$x^2 + 1 \equiv 0 \mod 5^e$$

has a solution $x_e \in \mathbb{Z}/5^e\mathbb{Z}$. Prove that these solutions can be chosen to satisfy

$$x_1 \equiv 2 \mod 5 \quad \text{and} \quad x_{e+1} \equiv x_e \mod 5^e \quad \text{for all } e \geq 1.$$

This is a special case of Hensel's lemma. *Hint:* Use induction on e.

(4) Define a composition law on the points of a cubic C by the following rule: Given $P, Q \in C$, define $P * Q$ to be the point on C so that P, Q, and $P * Q$ are colinear (i.e. they lie on a line).
(a) Explain why this law is commutative.
(b) Prove that there is no identity element for this composition law.
(c) Prove that this composition law is not associative.
(d) Explain why $P * (P * Q) = Q$.
(e) Suppose that the line through two points $\mathcal{O}$ and S is tangent to C at $\mathcal{O}$. Show that

$$\mathcal{O} * (Q * (Q * S)) = \mathcal{O}.$$

(5) Prove that the equation

$$y^2 = x^3 + 7$$

has no solutions in integers $x, y \in \mathbb{Z}$.

(6) $(*)$ Find all solutions to the equation

$$y^2 = x^3 - 2$$

with $x, y \in \mathbb{Z}$ and prove that your list is complete.

Note: Problems labeled $(*)$ do not have to be handed in.