18.781 Problem Set 10

Due Monday, May 6 in class.

Remember that a *plane curve of degree d* is specified by a degree d polynomial in two variables:

$$\begin{aligned} f(x,y) = \quad & a_{d,0}x^d + a_{d-1,1}x^{d-1}y + \cdots + a_{0,d}y^d \\ & + a_{d-1,0}x^{d-1} + a_{d-2,1}x^{d-2}y + \cdots + a_{0,d-1}y^{d-1} \\ & \quad \vdots \\ & + a_{1,0}x + a_{0,1}y + a_{0,0}. \end{aligned}$$

We will mostly be concerned with curves defined over the integers $\mathbb{Z}$, which means that *all the coefficients a_{ij} are integers.* A *rational point* on the curve is a pair (x, y) of rational numbers such that $f(x, y) = 0$. The collection of *rational points* is

$$C_f(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}^2 \mid f(x,y) = 0\}.$$

The collection of *real points* is

$$C_f(\mathbb{R}) = \{(x,y) \in \mathbb{R}^2 \mid f(x,y) = 0\},$$

and the *complex points* are

$$C_f(\mathbb{C}) = \{(x,y) \in \mathbb{C}^2 \mid f(x,y) = 0\}.$$

Something not discussed as much in Chapter 5 of the text is *points modulo p*

$$C_f(\mathbb{Z}/p\mathbb{Z}) = \{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid f(x,y) \equiv 0 \pmod{p}\},$$

for a prime number p.

The curve is called *smooth* if for every complex point (x_0, y_0), the gradient vector

$$\left(\frac{\partial f}{\partial x}(x_0,y_0), \frac{\partial f}{\partial y}(x_0,y_0)\right) \neq 0.$$

(The text also assumes smoothness at points at infinity; don't worry about that.)

In each problem, either give an example of the kind of curve described (explaining why your example works) or explain why no example can exist. (You don't need to prove that your examples are smooth, but we reserve the right to deduct points in grading if they are not.)

1. A degree two smooth curve with infinitely many real points but *no* rational points. (This means you are looking for a quadratic equation $f(x, y) = 0$ (integer coefficients) with lots of real roots and no rational roots. The first condition excludes things like $x^2+y^2+1 = 0$, which has no real roots.)

2. A degree two smooth curve f with infinitely many real points but only a *finite number* (at least one) of rational points.

3. A degree two smooth curve with infinitely many rational points, but *no* points modulo any prime p.

4. A degree two smooth curve having p^2 points modulo p, for some prime p. To make it interesting, require that f is *not* divisible by p as an integer polynomial. (You want *every* pair (x, y) to be a solution modulo p.)

5. A degree two smooth curve having $p - 1$ points modulo infinitely many primes p.

6. A degree two smooth curve having $p + 1$ points modulo infinitely many primes p.

7. A degree two smooth curve having at least $p - 1$ points modulo p for every prime p, but *no* rational points.