18.781 Problem Set 10 solutions

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

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

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.)

This is done in the text at the beginning of Section 5.6: $\boxed{x^2 + y^2 - 3}$ works.

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

This is impossible, by Example 8 in Section 5.6 of the text. As soon as there is at least one rational point (x_0, y_0), then you get each of the others as the intersection with $C_f(\mathbb{Q})$ of the line through (x_0, y_0) of rational slope m: one point for each slope, so infinitely many points.

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

This is impossible. Suppose $(x_0, y_0) = (p_1/q_1, p_2/q_2)$ is a rational point, with p_i integers and q_i nonzero integers. Choose a prime p dividing neither q_1 nor q_2. Then q_i has an inverse $r_i(p)$ modulo p, and a little thought or trying examples should convince you that $(x_0(p), y_0(p)) = (p_1 \cdot r_1(p), p_2 \cdot r_2(p))$ is a point on the curve modulo 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.)

This is only possible for $p = 2$. A curve that works is

$$f(x, y) = x^2 - x + y^2 - y.$$

You know from our early work on $\mathbb{Z}/p\mathbb{Z}$ that *every* x satisfies the equation $x^p - x \equiv 0 \pmod{p}$. So every x and y satisfy f.

5. A degree two smooth curve having $p-1$ points modulo infinitely many primes p. Essentially I did this in class: $xy - 1$ works. (Then x can be anything nonzero modulo p ($p - 1$ choices), and y must be its unique inverse.

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

This one I stated but did not prove in class: the equation $x^2 + y^2 = 1$ has $p+1$ points modulo any prime congruent to 3 modulo 4. (For example, the points modulo 3 are $(0, 1), (0, 2), (1, 0), (2, 0)$.) To prove this, start with the obvious point $(1, 0)$ on the curve. The line of slope m through this point is $(1 + t, mt)$. It meets the curve where

$$[1 + 2t + t^2 + m^2t^2 = 1, \qquad (m^2 + 1)t^2 + 2t = 0.$$

One of those points is $t = 0$ (the original point $(1, 0)$), and the other is the root of

$$(m^2 + 1)t + 2 = 0, \qquad t = -2/(m^2 + 1).$$

Notice that p is 3 modulo 4, so $m^2 + 1 = 0$ has no solutions; so the denominator $m^2 + 1$ is always nonzero. Each of the p possible slopes m gives a new point, so we have found $p + 1$ altogether.

You should worry about two things: first, that the case of the tangent line returns the original point $(1, 0)$ (so I overcounted by 1) and second, that I omitted the vertical line and *its* point of intersection (which means that I undercounted by 1). Both of these concerns are valid. The tangent line at $(1, 0)$ is in the direction perpendicular to the gradient $(2x, 2y) = (2, 0)$, which is to say the direction $(0, 1)$, which is to say vertical. So "all lines of finite slope" was by good fortune equal to "all non-tangent lines through $(1, 0)$." Each of these p lines gives exactly one new point.

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

This is harder. By now you may have the idea that curves $x^2 + y^2 + c = 0$ are reasonable to investigate. An easy way to get no rational points is no real points, which requires $b > 0$ and $c < 0$. So let's try

$$f(x, y) = x^2 + y^2 + 1.$$

Modulo 2 it's easily seen to have 2 points, so that's OK. I proved in class that if $p \equiv 1 \pmod{4}$ then a change of variables makes the equation

$$x^2 - (y')^2 + 1 = 0,$$

which has the $p - 1$ points

$$(x, y') = ((u + u^{-1})/2, -(u - u^{-1})/2) \qquad u \not\equiv 0 \pmod{p}.$$

If $p \equiv 3 \pmod{4}$, we know there can be no points with x or y equal to zero. As soon as there is *one* point, the $p+1$ lines through that point intersect the curve in $p+1$ distinct points, two of which may be at infinity; so we get at least $p - 1$ points. We therefore need to find just *one* point.

To find a point, we want to solve the equation

$$(\text{quadratic residue}) + (\text{quadratic residue}) + 1 = 0,$$

or

$$(\text{quadratic residue}) + 1 = -(\text{quadratic residue})$$

Since $p \equiv 3 \pmod 4$, -1 is a non-residue. Since the Legendre symbol is multiplicative, the equation is

$$(\text{quadratic residue}) + 1 = (\text{quadratic non-residue}).$$

This will have a solution (r_1, r_2) chosen from $\{1, 2, \ldots, p-1\}$ *unless* the first $(p-1)/2$ nonzero classes

$$1, 2, \ldots, (p-1)/2$$

are all quadratic *non-residues*, and the last $(p-1)/2$

$$(p+1)/2, \ldots, p-1$$

are all quadratic *residues*. In particular this requires that 1 should be a non-residue (which never happens) and -1 should be a residue (which does not happen in our case).

The conclusion is that $\boxed{f(x,y) = x^2 + y^2 + 1}$ has at least $p-1$ points mod p for all primes p.

More precisely, in this last case, the secant construction never produces points at infinity; so it always leads to $p+1$ points. (The reason is the same as the reason for the non-vanishing of denominators in the solution to Problem 6.) So

$$\text{number of points modulo } p = \begin{cases} 2 & (p = 2) \\ p-1 & (p \equiv 1 \pmod 4) \\ p+1 & (p \equiv 3 \pmod 4). \end{cases}$$