MATH 124 HOMEWORK #9

INNA ZAKHAREVICH

(1) We know that elliptic curves are zero sets of the equations $y^2 = x^3 + Ax + B$. In $\mathbb{Z}/5\mathbb{Z}$ there are 5 values for each of A and B, so there are 25 elliptic curves.

An elliptic curve is zero exactly when its discriminant is zero; this will happen exactly when $4A^3 + 27B^2 = 0$. Considering this mod 5 and multiplying by 3, we get that this happens exactly when

$$-2A^3 \equiv B^2 \pmod 5.$$

For $A = 0$, the only time the discriminant is 0 is if $B = 0$. For $A = 1$ or -1 there are no solutions. When $A = 2$ we get that we want $B^2 \equiv 1$, which means that $B = \pm 2$. When $A = -2$ we get that we want $B^2 \equiv 1$, which happens exactly when $B \equiv \pm 1$. Thus we see that there are 5 pairs (A, B) for which the discriminant is zero, so there are 5 singular elliptic curves.

So now we want to compute equivalence classes of elliptic curves. We know that the curve $y^2 = x^3 + Ax + B$ is equivalent to $y^2 = x^3 + ax + b$ if and only if there is some $n \neq 0$ such that $A = n^4 a$ and $B = n^6 b$. However, $n^4 \equiv 1$ and $n^6 \equiv n^2 \equiv \pm 1$. Thus the elliptic curves are equal if and only if $A = a$ and $B = \pm b$. Thus each equivalence class of curves has 2 curves in it, and therefore there are 10 non-equivalent non-singular curves.

(2) (a) Consider a point $(a, b) \in P$. If $a, b \in \mathbb{Q}$ then $b/a \in \mathbb{Q}$ unless $a = 0$. $a = 0$ only when $P = (0, 0)$, when the point is clearly on a line of the form $y = mx$. Otherwise, the point is on the line $y = (b/a)x$.

(b) Suppose that $y = mx$ meets (1) at 3 rational points. First, note that m must be rational, since it is the ratio of the coordinates of the points. Plugging in to (1) for y, we get

$$x(x^2 - m^2 x - 4) = 0.$$

The solutions to this equation are the x-coordinates of the given points, so we know that $x^2 - m^2 x - 4$ has two rational solutions, which means that its discriminant must be the square of a rational number. Thus we see that there is a rational n such that

$$n^2 = (m^2)^2 - 4(-4)(1) = m^4 + 16.$$

(c) Suppose that there is a nontrivial solution (U, V, W) to $U^4 + W^4 = V^2 W^2 = (VW)^2$. Then setting $x = U$, $y = V$, $z = VW$ we see that we have a nontrivial solution to $x^4 + y^4 = z^2$. However, we know that no such solutions exist. Contradiction. Thus the equation has no nontrivial solutions.

(d) We need to find all solutions to the equation $m^4 + 16 = n^2$. Putting m and n over a common denominator d, we get

$$\left(\frac{k}{d}\right)^4 + 16 = \left(\frac{\ell}{d}\right)^2.$$

Thus we see that m, n must satisfy

$$k^4 + (2d)^4 = (\ell d)^2.$$

If we had a nontrivial solution to this, we would have a nontrivial solution to $x^4 + y^4 = z^2$, which we know that we don't have. Thus we must have either k or d be zero. Since d clearly can't be 0, we must have $k = 0$, which means that $m = 0$. Thus all rational points of $y^2 = x^3 - 4x$ are on the line $y = 0$, so they are the points $(0, 0), (2, 0), (-2, 0)$ (and, also, the point at infinity).

(3) Suppose that $P = (x_0, y_0)$. Let $f = x^3 - y^2 - Ax - B$. We know that

$$\frac{\partial f}{\partial x} = 3x^2 - A \qquad \frac{\partial f}{\partial y} = -2y.$$

Thus the slope of a tangent line at P is

$$m := \frac{3x_0^2 - A}{2y_0}.$$

The equation of the tangent line is $y = m(x - x_0) + y_0$. Notice that if we find the third root, a, of the given expression, we will have that

$$y = -m(a - x_0) + y_0 = m(x_0 - a) + y_0,$$

exactly the formula we want. Thus it remains to show that the third root of the expression will be given by the formula we want. Plugging in for y, we get

$$f(x) = x^3 - (m(x - x_0) - y_0)^2 - Ax - B = 0.$$

We know that two roots of the equation are the double root x_0. Thus to find the third root it suffices to write the given equation in terms of $x - x_0$. Notice that we don't need to worry about terms that are linear or constant in $x - x_0$, since we know that these will cancel out (since x_0 is a double root).

$$\begin{aligned} f(x) &= ((x - x_0)^3 + 3x^2x_0 - 3xx_0^2 + x_0^3) - m^2(x - x_0)^2 \\ &\quad + 2y_0m(x - x_0) - y_0^2 - A(x - x_0) - Ax_0 - B \\ &= ((x - x_0)^3 + 3((x - x_0)^2 + 2xx_0 - x_0^2) - m^2(x - x_0)^2 + \cdots \\ &= (x - x_0)^3 + (3x_0 - m^2)(x - x_0)^2 + \cdots \end{aligned}$$

Thus the third root is $x - x_0 = m^2 - 3x_0$, so

$$a = m^2 - 2x_0$$

as desired.