MATH CIRCLE - ELLIPTIC CURVES WEEK 3

SAM LICHTENSTEIN

Today we reviewed the congruent number problem and how it becomes a problem about finding rational points on an elliptic curve. After drawing the real locus (the points in $\mathbb{R}^2$) defined by such a curve, say $y^2 = x^3 - n^2x$, we began considering whether this was really the best set of points to look at.

A digression into degenerate conics convinced us that while a conic like $x^2 + y^2 = 0$ has only a *single* point in $\mathbb{R}^2$, it consists of *two whole lines* when viewed in $\mathbb{C}^2$. Thus, to get the "real story" about a curve, such an elliptic curve, it is important to consider the complex locus – the locus in $\mathbb{C}^2$.

However, is that the *whole* story? Recalling the line parametrizing the rational points on the circle

$$x^2 + y^2 = 1$$

we remembered that a "point at ∞" corresponds to a finite point on the circle. This suggests that a full understanding of various curves (such as a line in the plane) requires "filling them in" with extra points at infinity.

The rest of the class today was an attempt to do this in a meaningful way, without relying upon a notion of *limits* that disguises the algebraic machinery underlying the curves. (For example, in the case of the rational points on the circle above, we can get the "extra" point on the circle, $(-1, 0)$, by allowing t to tend to ∞ in the equation $x = \frac{2y-t}{t}$ of the line passing through $(-1, 0)$ and $(1, t)$. In the limit, the line has equation $x = -1$ since $\lim_{t\to\infty} \frac{2y-t}{t} = -1$. Indeed, the line $x = -1$ intersects the circle "twice" at $(-1, 0)$ so we get the last rational point as desired. But having to take limits is a pain.)

To get this, we used the idea that *points on a line correspond to lines through the origin in the plane.* For example, if we take our line A to be $x = 1$ then any point $(1, t)$ corresponds to a unique line ℓ passing through $(0, 0)$ and $(1, t)$. In fact, *any* point (x, y) corresponds to a unique line $\ell_{(x,y)}$ through the origin, unless $x = y = 0$ – so we throw out this case. We thus have the correspondence

$$\text{lines through } (0,0) \leftrightsquigarrow \text{points} \neq (0,0).$$

However, it is not a one-to-one correspondence because (x, y) and $(\alpha x, \alpha y)$ determine the same line for any α. (Check this!) If $x \neq 0$ we can always divide by x to get (x, y) and $(1, \frac{y}{x})$ determining the same line. So the points on A get us *almost* all the lines. But there is *one extra* line in the plane we *don't* get, namely the y-axis defined by $x = 0$. (Given any points $(0, y)$ on this line, we cannot divide by 0 to get it into the form $(1, t)$.) However, we can choose a distinguished point $(0, 1)$ on this line. So we have a one-to-one correspondence between lines in the plane and points $[1, t]$ on the line A, *plus an additional point* $[0, 1]$ "at ∞". The set of lines in the plane, or equivalently, points on A plus an additional point $[0, 1]$, is called a *projective line.* The coordinates $[a, b]$ (which cannot *both* be zero), which are defined only up to scaling by nonzero constants, determine a point on the projective line. For example, when $a \neq 0$ the point $[a, b]$ will determine a "finite" point on the line, $[1, t]$ for $t = b/a$. And when $a = 0$ the point $[a, b] = [0, b] = [0, 1]$ is the point at ∞, the vertical line through zero in the plane, the y-axis. (These are three names for the same thing!)

Next we remembered that we were dealing with curves in the *plane*, $\mathbb{C}^2$. To get extra stuff at ∞ we need to know how to extend the regular plane to the horizon, in the way we extended the regular line to infinity. We did this in an analogous way, with A the *plane* in $\mathbb{C}^3$ defined by $x = 1$. An arbitrary point on this plane looks like $(1, y, z)$ for some y, z. The plane A is just like the regular yz plane $\mathbb{C}^2$. And if we look at the set of lines in $\mathbb{C}^3$ which pass through $(0, 0, 0)$ we see that *most* of them are parametrized by the points of A. Some of them lie in the regular yz-plane however, and have $x = 0$. To define one of these you must choose a point $(0, y, z)$ with y or z nonzero. If we again denote a line through zero by $[a, b, c]$ if it passes through a point $(a, b, c) \neq (0, 0, 0)$ then we have a set of bracket-coordinates for the lines through the origin in $\mathbb{C}^3$. In this case, the points $[1, b, c]$ correspond 1-1 with the regular points of a plane A. The points $[0, b, c]$ correspond to a "line at ∞" – and in fact this line at ∞ is a *projective* line. (It is a horizon, where opposite points of the horizon are identified with one another.)

We will review projective geometry next week and use it to talk about *projective* points on an elliptic curve. This will be important if we want **every line to meet an elliptic curve in exactly three points**!