Math 445 Number Theory

December 3, 2004

Elliptic curves: $f(x,y) = y^2 - (ax^3 + bx^2 + cx + d) = y^2 - q(x)$ $\mathcal{C}_f(\mathbb{R})$ is an *elliptic curve* if f has no linear factors and $\mathcal{C}_f(\mathbb{R})$ has no singular points.

Verifying this, over $\mathbb{R}$ can be hard! But if we work over $\mathbb{C}$, we have

Fact: $\mathcal{C}_f(\mathbb{C})$ is an elliptic curve (which implies that $\mathcal{C}_f(\mathbb{R})$ is) $\Leftrightarrow$ $q(x)$ has no repeated root.

An elliptic curve is a cubic curve. So two points on the curve A, B can be used to find a third, C, as $C =$ the other point lying on $L \cap \mathcal{C}_f(\mathbb{R})$, where $L =$ the line through A and B . This can be used to define a <u>product</u> on $\mathcal{C}_f(\mathbb{R})$, $C = AB$. (If $A = B$, we can use $L =$ the tangent line through A.) This product, unfortunately, is not very well-behaved; for example it isn't associative. An example: of $AA = B$, then $AB = A$, so $A(AB) = AA = B$. But $(AA)B = BB =$ the third point on the tangent line through B, which is can't be A, since then the line through A and B is tangent at both A and B, so the cubic equation $f(x, mx + r) = 0$ has two double roots!

But this can be remedied, by introducing a second binary operation, $+$, defined as follows. Let $\underline{0} \in \mathcal{C}_f(\mathbb{R})$ be any point, and define, for $A, B \in \mathcal{C}_f(\mathbb{R})$, $A + B = \underline{0}(AB)$. This addition <u>is</u> associative, and in fact, turns $\mathcal{C}_f(\mathbb{R})$ into an abelian group! In particular, we have

$A + B = B + A$ (since $AB = C = BA$ is the third point on the line through A, B)

$A + \underline{0} = A$ (since if $A\underline{0} = C$, then $A + \underline{0} = \underline{0}(A\underline{0}) = \underline{0}C = A$, since $\underline{0}, A, C$ are the three points of some $L \cap \mathcal{C}_f(\mathbb{R})$

For every A there is exactly one B with $A + B = \underline{0}$; $A + B = \underline{0}(AB) = \underline{0}$ means that the line through $\underline{0}$ and AB is tangent at $\underline{0}$. There is only only such line, so AB must be $\underline{00}$. So $B = A(AB) = A(\underline{00})$ is determined by A, and we can check that in fact $A + B = \underline{0}(AB) = \underline{0}(\underline{00}) = \underline{0}$.

Associativity is the fun one! See the second page.....

But what does this mean? It means that an elliptic curve $\mathcal{C}_f(\mathbb{R}$ forms an (abelian) group under this addition! And if $\underline{0}$ is chosen with rational coordinates (assuming $\mathcal{C}_f(\mathbb{R}$ has a rational point), then the chord-and-tangent claculations in the addition will always give rational points when starting from rational points. That is, $\mathcal{C}_f(\mathbb{Q}$ is <u>also</u> an abelian group under this operation!

For the case of elliptic curves, with polynomial $f(x,y) = y^2 - (ax^3 + bx^2 + cx + d)$, a particularly nice choice for $\underline{0}$ is the "point at infinity", since it simplifies many calculations. A formal approach to this requires us to projectivize everything, which means to think, instead of f, of the homogeneous polynomial $F(x,y) = y^2z - (ax^3 + bx^2z + cxz^2 + dz^3)$, which has solution $(0,1,0)$, which "represents" vertical lines in the plane. But the upshot of choosing $\underline{0}$ at infinity is that if $A = (a_1, a_2)$, then $\underline{0}A = (a_1, -a_2)$ (since the line from A to "vertical lines" is the vertical line through A !). This allows us to write <u>formulas</u> for $A + B = \underline{0}(AB)$ and $2A = \underline{0}(AA)$. For the "normalized" polynomials $y^2 = x^3 + ax + b$, if $A = (a_1, a_2)$ and $B = (b_1, b_2)$, then a little computation with chords and tangents reveals:

$$A + B = \left(\frac{m^2 - b}{a} - a_1 - b_1, -\left(a_2 + m\left(\frac{m^2 - b}{a} - 2a_1 - b_1\right)\right)\right) \text{, where } m = \frac{b_2 - a_2}{b_1 - a_1} .$$

$$2A = \left(\frac{M^2 - b}{a} - 2a_1, -\left(a_2 + m\left(\frac{M^2 - b}{a} - 3a_1\right)\right)\right) \text{, where } M = \frac{3a_1^2 + 2aa_1 + b}{2a_2}$$

Note that, in the first case, when $a_1 = b_1$, and in the second case, when $a_2 = 0$, that the resulting point is the point at infinity (the line used in the calculation is a vertical line). So we must treat $[0:1:0]$ (as it is usually written) as a (rational) point on the curve!

$A+(B+C)=(A+B)+C$: this is the fun one! This *says* that $\underline{0}(A(\underline{0}(BC)))=\underline{0}((\underline{0}(AB))C)$, so we need to show that $A(\underline{0}(BC))=(\underline{0}(AB))C$. And how do you show this?! Well, we use a little

Lemma: If $f(x,y), g(x,y)$ are cubic polynomials, and $P_1,\ldots,P_9 \in \mathcal{C}_f(\mathbb{R} \cap \mathcal{C}_g(\mathbb{R}$, with P_1,P_2,P_3 lying on a line L (which is *not* contained in $\mathcal{C}_f(\mathbb{R})$, then there is a quadratic polynomial $q(x,y)$ with $P_4,\ldots,P_9 \in \mathcal{C}_q(\mathbb{R}$.

And the point to this result is that, typically, you can't expect 6 points chosen at random to lie on a quadratic (i.e., on a conic section). so this is really saying something.

Setting the proof of this aside for the moment, to show associativity, start with a cubic curve $\mathcal{C}_f(\mathbb{R}$ (which contains no line), and set

$P_1=B, P_4=AB, P_7=A$ (all on a line $L_1 : L_1(x,y)=0$)
$P_2=B, P_5=\underline{0}, P_8=\underline{0}(BC)$ (on a line $L_2(x,y)=0$)
$P_3=C, P_6-\underline{0}(AB), P_9=(\underline{0}(AB))C$ (on a line $L_3(x,y)=0$

These points all lie on $\mathcal{C}_f(\mathbb{R}$ (since $A,B,C,\underline{0}$ do), and they also lie on $\mathcal{C}_g(\mathbb{R}$, where $g(x,y)=L_1(x,y)L_2(x,y)L_3(x,y)$. Furthermore, P_1,P_2,P_3 lie on a line L. In the generic case, where all 9 of these points are distinct, the lemma lets us conclude that the remaining 6 points $P_4,\ldots,P_9$ lie on a quadratic. But! P_4,P_5,P_6 <u>also</u> lie on a lineL' , so $L' \subseteq \mathcal{C}_f q\mathbb{R}$, since L hits the quadratic in $3>2$=degree(q) points. So, q is really a product of linear functions, implying that P_7,P_8,P_9 lie on a line, since otherwise one of these lies on L', implying that it hits $\mathcal{C}_f(\mathbb{R}$ in $4>3$=degree(f) points, so $L' \subseteq \mathcal{C}_f(\mathbb{R}$, a contradiction. But this means that $P_7P_8=P_9$, i.e., $A(\underline{0}(BC))=(\underline{0}(AB))C$!

If these 9 points are not all distinct, we appeal to "continuity", by finding a nearby generic situation; the limits of 3 sequences of points lying on lines is 3 points on a line. The details of this can (sort of) be found in the text.....