LECTURE 1, MONDAY FEB. 09, 2004

FRANZ LEMMERMEYER

We will start our journey to the land of algebraic geometry by discussing the simplest algebraic varieties, namely plane algebraic curves. These are zero sets of polynomials $F(X,Y)$ in two variables with coefficients in some field (or, sometimes, in a ring). The simplest algebraic curves are lines, that is, zero sets of linear polynomials $aX+bY+c$. Slightly more complicated are curves described by quadratic polynomials: conics. We will now discuss the simplest of these: the unit circle.

1. Pythagorean Triples

Let us consider one of the oldest[1] diophantine problems: finding all Pythagorean triples, that is, all triples (a,b,c) of integers such that $a^2+b^2=c^2$. The simplest and best known solution is the triple $(3,4,5)$.

We will discuss various methods for solving this problem: a geometric, an analytic and an algebraic method.

The Geometric Method: Parametrization. The geometric solution turns the problem of finding integral solutions of $a^2+b^2=c^2$ into the equivalent one of finding rational points on the unit circle $\mathcal{C}: X^2+Y^2=1$. This is easy: any Pythagorean triple (a,b,c) corresponds to a rational point $x=\frac{a}{c}$, $y=\frac{b}{c}$ on the unit circle $\mathcal{C}$ and vice versa.

In order to find all rational points on $\mathcal{C}$ we start with an obvious solution, say $P=(-1,0)$ (any rational point on $\mathcal{C}$ would do). A line through P with rational slope t will intersect the circle $\mathcal{C}$ in two points, namely P and one other point, say P_t It is easy to see that P_t is a rational point if t is rational, and that in fact every rational point $\ne P$ on $\mathcal{C}$ is one of these points P_t: in fact, if $Q=(x,y)\ne P$ is a rational point on $\mathcal{C}$, then $t=\frac{y}{x+1}$ (the slope of the line PQ) gives $Q=P_t$.

The actual calculation gives the formulas

$$x=\frac{1-t^2}{1+t^2},\quad y=\frac{2t}{1+t^2}. \tag{1}$$

Note that the point $P=(-1,0)$ does not correspond to a rational value of t (we could get P by admitting the value $t=\infty$; this will be made precise once we know about projective planes).

Note that, over the field of rational numbers, dividing through by $1+t^2$ is not a problem since $1+t^2\ne 0$. When determining the solutions of $X^2+Y^2=1$ in arbitrary fields K, one has to be careful if K contains a primitive fourth root of unity.

Consider for example the finite fields $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ for odd primes p. The formulas (1) still give points on the unit circle over $\mathbb{F}_p$, one for each value $t\in\mathbb{F}_p$, except for

[1]It is not so clear just how old this problem is: already the Babylonians compiled tables of Pythagorean triples, the Pythagoreans found formulas for generating infinitely many such triples, but not even Diophantus asked for *all* solutions to $x^2+y^2=z^2$.

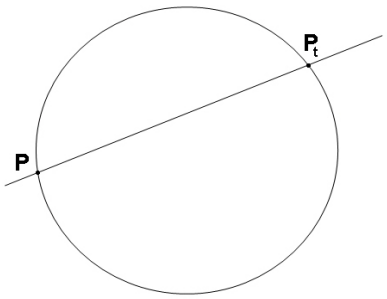

FIGURE 1. Parametrizing the Unit Circle

those values of t for which $1+t^2=0$. We know from elementary number theory that the congruence $t^2 \equiv -1 \bmod p$ has a solution (in fact exactly two) if and only if $p \equiv 1 \bmod 4$. Thus the parametrization (1) provides us with p points on $\mathcal{C}$ if $p \equiv 3 \bmod 4$, and with $p-2$ points if $p \equiv 1 \bmod 4$. The same argument as over $\mathbb{Q}$ shows that every point $\neq P$ is actually parametrized by (1), which finally shows that the set $\mathcal{C}(\mathbb{F}_p)$ of points on the unit circle with coordinates in $\mathbb{F}_p$ has cardinality

$$\#\mathcal{C}(\mathbb{F}_p) = \begin{cases} p+1 & \text{if } p \equiv 3 \bmod 4, \\ p-1 & \text{if } p \equiv 1 \bmod 4. \end{cases}$$

Note that $\#\mathcal{C}(\mathbb{F}_p)$ is always divisible by 4; this will be explained later by giving $\mathcal{C}(\mathbb{F}_p)$ a group structure and showing that the point $(0,1)$ has order 4.

The Analytic Method: Trigonometry. As is well known, every real point (x,y) on the unit circle can be written as $x=\cos\alpha$, $y=\sin\alpha$ for some real number $\alpha \in [0,2\pi)$. Using the identities $\cos^2\alpha - \sin^2\alpha = \cos 2\alpha$ and $\cos^2\alpha + \sin^2\alpha = 1$ we find

$$\begin{aligned} x &= \cos\alpha = \frac{\cos^2\frac{\alpha}{2} - \sin^2\frac{\alpha}{2}}{\cos^2\frac{\alpha}{2} + \sin^2\frac{\alpha}{2}} = \frac{1-m^2}{1+m^2}, \\ y &= \sin\alpha = \frac{2\sin\frac{\alpha}{2}\cos\frac{\alpha}{2}}{\cos^2\frac{\alpha}{2} + \sin^2\frac{\alpha}{2}} = \frac{2m}{1+m^2}, \end{aligned}$$

where we have put $m = \tan\frac{\alpha}{2}$. Every rational number m now gives us a rational point on the unit circle. Conversely, if x and $y \neq 0$ are rational, then so is $m = \frac{1-x}{y}$. Since the point $(1,0)$ corresponds to $m=0$ (although $m=\frac{1-x}{y}$ does not make any sense here), this parametrization gives us all rational points $\neq (-1,0)$ on $\mathcal{C}$.

The Algebraic Method: Unique Factorization. Consider the equation $a^2 + b^2 = c^2$, and assume that (a,b,c) is a solution in coprime natural numbers (such solutions are called primitive). It is easy to see that c must be odd and that one of a or b is even. Assume that b is even and write $b^2 = c^2 - a^2 = (c+a)(c-a)$. Since $\gcd(c-a, c+a) = 2$ (it divides $2c$ and $2a$, hence 2; now observe that a and c are both odd, hence their sum and difference are even), we conclude using unique factorization that $c+a = 2r^2$, $c-a = 2s^2$, and $b = 2rs$; this shows $c = r^2+s^2$, $a = r^2-s^2$, and we have found: the primitive Pythagorean triples (a,b,c) with b

even are given by

$$a = r^2 - s^2, \quad b = 2rs, \quad c = r^2 + s^2, \tag{2}$$

where r and s are coprime integers.

The rational points on the unit circle corresponding to these solutions are $x = \frac{r^2-s^2}{r^2+s^2} = \frac{1-t^2}{1+t^2}$ and $y = \frac{2rs}{r^2+s^2} = \frac{2t}{1+t^2}$, where we have put $t = \frac{r}{s}$.

It is of course easy to verify without using unique factorization that (2) are solutions of the equation $X^2 + Y^2 = Z^2$. Showing that this set of solutions is complete, however, requires unique factorization, at least if we want to use the algebraic method.

The Galois Theoretic Method. This method is a lame excuse to introduce some Galois theory. Let F be a field, and $m \in F$ a nonsquare; then the set $K = F(\sqrt{m}) = \{a + b\sqrt{m} : a, b \in F\}$ forms a field with respect to the natural addition and multiplication. We say that K/F is a quadratic extension.

The set of all ring homomorphisms $K \longrightarrow K$ leaving the elements of the base field F fixed forms a group called the Galois group of K/F, which is denoted by $\mathrm{Gal}(K/F)$. It has two elements, the identity map and the conjugation $\sigma : a + b\sqrt{m} \longmapsto a - b\sqrt{m}$. Note that the set of elements in K fixed by σ is just F.

For general Galois extensions K/F we have the norm map $N : K \longrightarrow F$ defined by $N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$. For quadratic extensions, the norm is given by

$$N(a + b\sqrt{m}) = (a + b\sqrt{m})(a - b\sqrt{m}) = a^2 - mb^2 \in F.$$

For cyclic extensions (field extensions whose Galois group is cyclic, i.e. generated by one element σ) we have Hilbert's Theorem 90: if $\alpha \in K^\times$ has norm 1, then α can be written in the form $\alpha = \beta^{1-\sigma} = \frac{\beta}{\sigma(\beta)}$ (the converse, by the way, is trivial).

For quadratic extensions, there is a simple proof of Hilbert's Theorem 90: if $\alpha = -1$, just take $\beta = \sqrt{m}$. If $\alpha \neq -1$, put $\beta = \alpha + 1$: then $\beta^{1-\sigma} = \frac{\alpha+1}{\sigma(\alpha)+1} = \frac{\alpha(\alpha+1)}{N(\alpha)+\alpha} = \alpha$.

Now let us apply Hilbert 90 to the problem of finding all Pythagorean triples (x, y, z). Assume that $z \neq 0$; then $\frac{x+iy}{z}$ is an element of norm 1 in $\mathbb{Q}(i)$, hence by Hilbert's Theorem 90 there is some $a+bi \in \mathbb{Z}[i]$ such that $\frac{x+iy}{z} = \frac{a+bi}{a-bi} = \frac{a^2-b^2+2abi}{a^2+b^2}$. Thus (x, y, z) is proportional to $(a^2 - b^2, 2ab, a^2 + b^2)$.

Remark. The methods are not equivalent. The analytic method requires trigonometric functions and thus, at least at present, only works for subfields of $\mathbb{C}$. The algebraic version works for (fields that are quotients of) unique factorization domains, and the geometric version over general fields. Moreover, the analytic and geometric methods can be applied only to curves of genus 0; the algebraic method gives at least some information as long as one has a factorization to work with.

Moral. For solving certain problems in arithmetic, there usually are a variety of possible methods you can choose from. Of course in order to have a choice you have to be familiar with these methods. During the first weeks we shall discuss some of the more elementary techniques, in particular rational parametrization and its applications.