LECTURE 13, THURSDAY APRIL 1, 2004

FRANZ LEMMERMEYER

1. Parametrizing Curves of Genus 0

As a special case of the theorem that curves of genus 0, in particular those with the maximal number of double points, can be parametrized we present a proof of

Proposition 1.1. *Every quartic with three double points is birational isomorphic to a conic (hence to a line if the latter has a rational point).*

Proof. By a linear projective transformation we can move the singularites of the quartic C to the points $[0:0:1]$, $[0:1:0]$ and $[1:0:0]$. The fact that $[0:0:1]$ is singular implies that the equation of C now has no terms in Z^4, Z^3X or Z^3Y. Thus a quartic with singularities in $[0:0:1]$, $[0:1:0]$ and $[1:0:0]$ necessarily has the form

$$F(X,Y,Z) = aX^2Y^2 + bY^2Z^2 + cX^2Z^2 + dXYZ^2 + eYZX^2 + fXZY^2.$$

We now apply the quadratic transformation

$$X = \frac{1}{x}, \quad Y = \frac{1}{y}, \quad Z = \frac{1}{z}.$$

Clearing denominators in the resulting equation yields a conic:

$$G(x,y,z) = az^2 + bx^2 + cy^2 + dxy + eyz + fxz.$$

Since the quartic was irreducible, so is the conic (a factorization of the conic into two linear factors would give a factorization of the quartic into two quadratic factors by transforming back); but irreducible conics can be parametrized (over algebraically closed fields). □

Note that this result allows us to parametrize the lemniscate in a way that differs from the one used above (which was rather tricky). Also observe that the "quadratic transformation" used in the proof transformed the singular lemniscate into a smooth (in general, at least) conic.

Also observe that the quartic $x^2y^2 + x^2 + y^2 = 0$ has the three rational double points $[0:0:1]$, $[0:1:0]$ and $[1:0:0]$; the above procedure leads to the conic $X^2 + Y^2 + Z^2 = 0$, which does not have any rational point. In fact, the quartic cannot have a rational parametrization defined over $\mathbb{Q}$ since it only has finitely many rational points, namely the three singular points.

2. Blow Ups

In this section I will briefly touch upon an important technique, namely the resolution of singularities by blow ups.

Consider the map $\phi : (u,v) \longmapsto (x,y) : x = u, y = uv$ between affine planes; since $u = x$, $v = y/x$, the map ϕ is birational. It projects the line $u = 0$ (the v-axis)

down to a single point $(0,0)$ in the $x-y$-plane, and ϕ is bijective outside of this line.

We can use the map ϕ to pull back curves $\mathcal{C}_f : f(x,y)=0$ in the $x-y$-plane to curves $\mathcal{C}_g : g(u,v)=0$ in the $u-v$-plane by setting $g = f\circ\phi$, i.e., $g(u,v)=f(u,uv)$. As we have said before, if the curve $\mathcal{C}_f$ does not pass through the origin, then this map will induce a birational isomorphism between $\mathcal{C}_f$ and $\mathcal{C}_g$.

But what if $f(0,0)=0$? Let m denote the multiplicity of the point $O=(0,0)$; writing $f(x,y)=\sum a_{ij}x^iy^j$, and plugging in some line equation $y=tx$ we find $f(x,tx)=\sum_{a_{ij}} t^jx^{i+j}$, and the largest power of x dividing $f(x,tx)$ is the smallest degree $m=i+j$ of a term occurring in $f(x,y)$. Now we find $g(u,v)=f(u,uv)=u^mh(u,v)$ with $h(0,v)\neq 0$. Thus the curve $\mathcal{C}_g$ will contain the line $u=0$ as a multiple component; putting $f_1(u,v)=f(u,uv)u^{-m}$ we find that the other component of $\mathcal{C}_g$ is the curve $\mathcal{C}' : f_1(u,v)=0$.

Example 1. Consider the cuspidal cubic $y^2-x^3=0$; blowing up at the origin gives us a new curve $g(u,v)=u^2(v^2-u)$, hence $\mathcal{C}' : u-v^2=0$ is a parabola. The map ϕ sends the points (u,v) on the parabola to the points $(x,y)=(u,uv)$ on the cuspidal cubic $y^2-x^3=0$; conversely, $u=x$ and $v=\frac{y}{x}$ map the cubic to the parabola, and this map is defined outside of O. Thus ϕ is a birational map, and it induces a bijection outside of O.

Example 2. Consider the nodal cubic $y^2-x^3-x^2=0$. A blow up at the origin gives us the nonsingular parabola $v^2=u+1$.

Example 3. Consider the curve $y^2-x^5=0$, which has singularities at $(0,0)$ and at its point at infinity $[0:1:0]$. A blow up at $(0,0)$ gives the curve $v^2-u^3=0$, which is still singular at 0. Another blow up finally resolves the singularity.

It can be proved that for every irreducible plane curve $\mathcal{C}$ there is a birational map to some smooth curve (in general in some higher dimensional space); also, every irreducible plane curve can be transformed by birational maps into a plane curve whose only singular points are ordinary (a point P of multiplicity m is called ordinary if the curve has m distinct tangents at P).

3. Quadrics

Quadrics are the higher dimensional analogs of conics: zero sets of quadratic polynomials in projective spaces of dimension ≥ 2. The simplest example is the unit sphere $x^2+y^2+z^2=1$, or rather its projective closure $X^2+Y^2+Z^2=W^2$ in $\mathbb{P}^3K$, Using lines through the rational point $(x,y,z)=(-1,0,0)$, the unit sphere is easily parametrized. The same method works for any quadric with a rational point, so these objects offer nothing new.

4. Cubic Surfaces

By now we have applied geometric techniques to find parametric solutions to quite a few plane curves. But what if we are given a diophantine equation with more than two variables? Well, in this case, we need to employ higher dimensional algebraic geometry. No there are dozens of textbooks out there dealing with the theory of plane algebraic curves; on the other hand, sources for the arithmetic of surfaces are scarce, mainly because the theory is quite complicated. Nevertheless there are a few techniques that can be explained very easily and yet are powerful

enough to solve a few nontrivial problems. Below, I will present some of those techniques.

4.1. **A Singular Cubic Surface.** Consider the cubic surface

$$F(X,Y,Z) = (X+Y+Z)^3 - dYZ(X+Z) = 0.$$

We find that the partial derivatives

$$\begin{aligned} F_X &= 3(X+Y+Z)^2 - dYZ, \\ F_Y &= 3(X+Y+Z)^2 - dXZ - dZ^2, \\ F_Z &= 3(X+Y+Z)^2 - dXY - 2dYZ \end{aligned}$$

vanish simultaneously on the line $Y = X + Z = 0$. (You should draw the surface, e.g. for $d = 1$, with `singsurf` and have a look at the singular line). The planes containing this line have the form $tY = X + Z$; elimination of X gives

$$0 = (t+1)^3Y^3 - dtY^2Z.$$

The solution $Y = 0$ gives us the known line; the other points of intersection satisfy

$$(t+1)^3Y = dtZ.$$

Since the equation is homogeneous, we may set $Z = (t+1)^3$ and get the parametrization

$$\begin{aligned} X &= dt^2 - (t+1)^3, \\ Y &= dt, \\ Z &= (t+1)^3. \end{aligned}$$

4.2. **Ramanujan's Taxicab Problem.** Hardy, when visiting Ramanujan in the hospital, remarked that he had arrived in a taxicab with the rather dull number 1729. Ramanujan replied that 1729 was quite interesting: it is the smallest integer that can be written in two different ways as the sum of two positive cubes: $9^3+10^3 = 1^3 + 12^3$.

Let us look more generally at the diophantine equation $a^3+b^3 = c^3+d^3$. Dividing through by d^3 (note that $d \neq 0$ by Fermat's Last Theorem) and introducing new variables, we get the cubic surface

$$x^3 + y^3 = z^3 + 1.$$

This cubic surface (whose rational points were already found by Euler!) has a couple of trivial solutions such as

$$(x,y,z) = (t,1,t), (1,t,t), (t,-t,-1)$$

for all rational numbers t. Geometrically, the solutions $(x,y,z) = (t,1,t)$ form a line ℓ, which can be described as the intersection of the planes $x - z = 0$ and $y = 1$.

In order to find nontrivial solutions, let us consider the planes through ℓ; they can be described by the equation $y = 1 + \lambda(x - z)$ for $\lambda \in \mathbb{Q}$. Intersecting this plane with the cubic surface, we expect to get a cubic curve; actually the cubic must contain the line ℓ, so the cubic is reducible, and its components are the line ℓ and some conic $\mathcal{C}$.

If we could find a rational point on one of these conics, we could find infinitely many (hopefully less trivial) rational solutions. Let's do the calculation: we have

$$\begin{aligned} 0 &= x^3 + y^3 - z^3 - 1 \\ &= x^3 + [1 + \lambda(x-z)]^3 - z^3 - 1 \\ &= (x-z)[x^2 + xz + z^2 + 3\lambda + 3\lambda^2(x-z) + \lambda^3(x-z)^2]. \end{aligned}$$

The first factor $x - z = 0$ leads to $y = 1$ and thus to ℓ. The problem now is to find a rational point on some of the conics.

One thing we could try is look where the other two lines intersect the plane. Take e.g. $(x, y, z) = (1, t, t)$, which is the line $x - 1 = y - z = 0$. It intersects the plane in $(x, y, z) = (1, 1, 1)$, which is a point on the line and not on the conic (except for $\lambda = -1$).

If $\lambda = -1$, the conic has the equation

$$0 = x^2 + xz + z^2 - 3 + 3(x-z) - (x-z)^2 = 3xz - 3 + 3(x-z),$$

or, after cancelling 3,

$$\mathcal{C} : xz + x - z - 1 = (x-1)(z+1) = 0.$$

Thus in this case the conic splits into two lines, and these are lines we already know.

Thus we have to keep looking for another approach. Let us compute the points of intersection of the line $x - z = 0$ and the conic. We immediately get $x^2 + \lambda = 0$. In general, the two points of intersection will not be rational; but if $\lambda = -b^2$, then $(x, z) = (b, b)$ will be a rational point on the conic

$$\mathcal{C} : x^2 + xz + z^2 - 3b^2 + 3b^4(x-z) - b^6(x-z)^2 = 0.$$

Now consider the lines $z = a(x-b) + b$ through (b, b); they intersect $\mathcal{C}$ in (b, b) and ... well, let us ask `pari`:

```
z=a*(x-b)+b: x^2 + x*z + z^2 - 3*b^2 + 3*b^4*(x-z) - b^6*(x-z)^2
```

gives some huge expression. We know that this expression must be divisible by $x - b$, hence we type in

```
%/(x-b)
```

and get a much nicer expression which is linear in x; solving for x then gives

$$x = b\frac{(b^6-1)a^2 - (2b^6+3b^3-2)a + (b^6+3b^3+2)}{(b^6-1)a^2 - (2b^6+1)a + b^6 - 1}.$$

Plugging this into $z = a(x-b) + b$, we find with `pari`:

$$z = b\frac{(b^6-3b^3+2)a^2 + (-2b^6+3b^3+2)a + b^6 - 1}{(b^6-1)a^2 - (2b^6+1)a + b^6 - 1}.$$

Finally, $y = 1 + \lambda(x-z) = 1 - b^2(x-z)$ gives

$$y = \frac{(-2b^6+3b^3-1)a^2 + (4b^6-1)a + -2b^6 - 3b^3 - 1}{(b^6-1)a^2 - (2b^6+1)a + b^6 - 1}.$$

Finally, let us check the solution: after typing in

```
x^3+y^3-z^3
```

`pari` gives the result 1. Moreover, for $a = -1$ and $b = -\frac{1}{2}$ we get $x = \frac{1}{10}$, $y = \frac{6}{5}$ and $z = \frac{9}{10}$, which gives us back Ramanujan's solution $(a, b, c, d) = (1, 12, 9, 10)$.

Thus we have found a 2-parameter family of solutions. Are there any solutions not covered by this family? Actually this would be equivalent to the claim that our conic $\mathcal{C}$ only has a rational point if $-\lambda$ is a square; this seems too good to be true.

Can we find all rational points on this cubic surface? In fact we can, using the following beautiful result due to Mordell (*Diophantine Equations*, p. 83, Thm. 1):

Theorem 4.1. *Let C be a cubic surface defined over $\mathbb{Q}$ and containing two rational lines. Then all rational points on C can be found.*

Proof. Let P_1 and P_2 be rational points on the lines ℓ_1 and ℓ_2. Then the line P_1P_2 meets C in a third point P whose coordinates are necessarily rational.

Conversely, let P be a rational point on the surface and not on one of the lwo lines. Then P and L_1 determine a plane, which will meet L_2 in a rational point P_2, and the line PP_2 will meet L_1 in a rational point P_1. □

Let us now find all rational points on the surface. Take the two lines given by

$$\ell_1 : (x, y, z) = (0, 1, 0) + \lambda(1, 0, 1)$$
$$\ell_3 : (x, y, z) = (0, 0, -1) + \mu(1, -1, 0).$$

We now write down the equation of the line through $P_\lambda \in \ell_1$ and $P_\mu \in \ell_3$: it is

$$(x, y, z) = (\mu, -\mu, -1) + \nu(\lambda - \mu, 1 + \mu, \lambda + 1).$$

Plugging this into our equation of the surface, we get a cubic in ν with roots $\nu = 0$ and $\nu = 1$ and

$$\nu = \frac{\mu - 1}{\mu - \lambda}.$$

With $t = \frac{\lambda\mu - 1}{\mu - \lambda}$, this gives the family of rational points $(x, y, z) = (1, t, t)$, which is exactly the second line ℓ_2.

Clearly this is not the general solution. What went wrong? Actually, there is a problem with Mordell's proof: in order to show that P arises from intersecting the line P_1P_2 with C, we have to make sure that $P_1 \neq P_2$. But in the case where the lines ℓ_1 and ℓ_2 are coplanar, we always get $P_1 = P_2$ whenever P does not lie in the plane L_1L_2, and do not even have well defined points P_1 and P_2 is P lies in L_1L_2. Thus the theorem is only true if the lines are skew.

In our example, all three lines are coplanar: the first two intersect in $(1, 1, 1)$, the first and the third in $(-1, 1, -1)$.

What now? I do not know whether our cubic surface contains two rational skew lines. Fortunately, we don't need that much:

Theorem 4.2. *Let C be a cubic surface defined over $\mathbb{Q}$ and containing two skew lines ℓ, ℓ' defined over a quadratic number field k such that $\ell^\sigma = \ell'$ for the nontrivial automorphism of $k/\mathbb{Q}$. Then all rational points on C can be found.*

The assumptions of this theorem are satisfied in our example: consider the lines

$$\ell : x + \rho y = 0,\ z = -\rho;$$
$$\ell' : x + \rho^2 y = 0,\ z = -\rho^2.$$

where $\rho = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity, are lines with the property that $\ell^\sigma = \ell'$ for $\sigma : \rho \longmapsto \rho^2$.

The proof of this theorem proceeds exactly as above:

Proof. Let P be a point on ℓ with coordinates in k; then $P' = P^\sigma$ is a point on ℓ' with conjugate coordinates. The line $L = PP'$ is rational, since it is fixed by σ, and it will therefore intersect C in a third rational point Q.

Conversely, assume that Q is a rational point on C and not on one of the lwo lines. Then Q and ℓ determine a plane, which will meet ℓ' in a point P', and the line QP' will meet ℓ in some point P; clearly P and P' are conjugate since Q is rational. □

Let us return to our two skew lines and fix two points:

$$(x,y,z) = (0,0,-\rho) + \lambda(\rho,-1,0), \quad (x,y,z) = (0,0,-\rho^2) + \lambda'(\rho^2,-1,0).$$

The line through these points is given by

$$\begin{aligned} x &= \lambda\rho + \nu(\lambda'\rho^2 - \lambda\rho), \\ y &= -\lambda + \nu(\lambda - \lambda'), \\ z &= -\rho + \nu(\rho - \rho^2). \end{aligned}$$

Putting $\lambda = a + b\rho$, $\lambda' = a + b\rho^2$, plugging these equations into the one for the cubic surface and factoring out $\nu(\nu-1)$ we find

$$\nu = \frac{(1+\rho)a^3 - (2+\rho)ba^2 + (2+\rho)b^2a - b^3 + \rho + 1}{a^3 - 3ba^2 + 3b^2a - 2b^3 + 1}$$

This in turn shows that

$$\begin{aligned} x &= \frac{a^4 - 2ba^3 + 3b^2a^2 + (-2b^3+1)a + (b^4 - 2b)}{a^3 - 3ba^2 + 3b^2a - 2b^3 + 1}, \\ y &= \frac{-a^4 + 2ba^3 - 3b^2a^2 + (2b^3-1)a + (-b^4 - b)}{a^3 - 3ba^2 + 3b^2a - 2b^3 + 1}, \\ z &= -\frac{a^3 + b^3 + 1}{a^3 - 3ba^2 + 3b^2a - 2b^3 + 1}, \end{aligned}$$

and in fact `pari` confirms that $x^3 + y^3 - z^3 - 1 = 0$.

Note that the denominator is $(a-b)^3 - b^3 + 1$, which by Fermat's Last Theorem for the exponent 3 vanishes if and only if $(a,b) = (1,1), (1,0)$; these values correspond to $\lambda = 1+\rho$ and $\lambda = 1$. If $\lambda = 1$, the line through the two conjugate points becomes $y+1 = x+z = 0$, which intersects C in the rational point $(1,-1,-1)$. If $\lambda = 1+\rho$, the line becomes $x+1 = y-z+1 = 0$, which intersects C in the two conjugate points and the rational point $[0:1:1:0]$ at infinity.

Introducing the new variables $A = a - b$ and $B = -b$, the formulas simplify somewhat:

$$\begin{aligned} x &= \frac{A^4 - 2BA^3 + 3B^2A^2 + (1-2B^3)A + B^4 + B}{A^3 + B^3 + 1}, \\ y &= \frac{-A^4 + 2BA^3 - 3B^2A^2 + (2B^3-1)A - B^4 + 2B}{A^3 + B^3 + 1}, \\ z &= \frac{-A^3 + 3BA^2 - 3B^2A + 2B^3 - 1}{A^3 + B^3 + 1}. \end{aligned}$$