LECTURE 3, MONDAY FEB. 16, 2004

FRANZ LEMMERMEYER

So far we have seen that the rational points on the unit circle can be described easily using the techniques of sweeping lines; except for one point, we get a bijection between the rational points on the unit circle and the rational numbers. Is it possible to do this for any algebraic curve? As a matter of fact, it is not; below we will give a few examples of curves that cannot be parametrized.

1. Unique Factorization Domains

Let us briefly recapitulate some basic results from algebra. A ring (for us, a ring is always commutative and has a unit element 1) is called a domain if it has no zero divisors, that is, if $ab = 0$ for $a, b \in R$ implies that $a = 0$ or $b = 0$. For example, $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain because $2 \cdot 3 = 0$, but $2 \neq 0$ and $3 \neq 0$ in this ring. Domains R have the cancellation property: if $ab = ac$ for $a, b, c \in R \setminus \{0\}$, then $b = c$; this can be proved by constructing the field of quotients and then multiplying through by a^{-1}. Rings with zero divisors do not have the cancellation property: for example, $3 \cdot 2 = 3 \cdot 4 = 0$, but $2 \neq 4$ in $\mathbb{Z}/6\mathbb{Z}$.

Now let R be a domain. We say that $b \mid a$ for elements $a, b \in R$ if there is a $c \in R$ such that $a = bc$. Elements dividing 1 are called units and form a group $R^\times$, the unit group of R. A simple observation is that if $a \mid b$ and $b \mid a$, then $a = bu$ for some unit u: in fact, $a \mid b$ implies $b = ac$ for some $c \in R$, and $b \mid a$ shows $a = bd$ for some $d \in R$. Thus $a = bd = acd$

An element $p \in R \setminus R^\times$ is called

- irreducible if every factorization $p = ab$ in R is trivial, that is, if $p = ab$ implies that a or b is a unit;
- prime if it has the property that, whenever $p \mid ab$ divides a product, it divides one of the factors: $p \mid a$ or $p \mid b$.

It is easy to see that primes are always irreducible: in fact, if a prime p has the factorization $p = ab$, then $p \mid ab$; since p is prime, it divides one of the factors, say a; but then we have $p \mid a$, i.e. $a = pc$ for some $c \in R$. Thus $a = pc = abc$, and from the cancellation law we conclude that $bc = 1$, hence b is a unit and any factorization of p is trivial.

The converse, namely that irreducibles are prime, is not true in general, but it holds for unique factorization domains (UFDs). These are domains in which every nonunit has a factorization into primes that is unique up to units and the order of the factors.

It is known that any Euclidean ring is a UFD; a Euclidean ring is a ring with a Euclidean algorithm, that is, a function $f : R \longrightarrow \mathbb{N}$ with the property that

- $f(a) = 0$ if and only if $a = 0$;
- for any pair $a, b \in R \setminus \{0\}$, there is a $q \in R$ such that $f(a - bq) < f(b)$.

The standard examples of Euclidean rings are $\mathbb{Z}$, where f can be taken to be the absolute value (although there exist other possible choices as well), and the polynomial ring $K[X]$ in one variable over a *field* K, where f is the function $f(r) = 2^{\deg r}$ for polynomials $r \in K[X]$.

From what we have seen above, any irreducible element in $K[X]$ is prime; for example, $X-4$ and X^2+1 are primes in $\mathbb{Q}(X)$ (what about $\mathbb{C}[X]$?).

The reason we have inserted this section on UFDs is that we will need the following result below:

Proposition 1.1. *Let R be a UFD. If a, b, m are nonzero elements of R such that $a \mid m$ and $b \mid m$, and if $\gcd(a,b) = 1$, then $ab \mid m$.*

Proof. Just look at the prime factorizations: we know $m = ac$ for some c, and that $b \mid m = ac$. Since the prime factors of b do not occur in the prime factorization of a, they must all occur in the prime factorization of c, which implies $b \mid c$ and therefore $m = abd$, that is, $ab \mid m$. □

For Euclidean domains R there is a simpler proof using only the fact that if $\gcd(a,b) = d$, then there are $r, s \in R$ with $d = ar + bs$ (Bezout's Lemma). Now assume that $m = ac = bd$, and write $ar + bs = 1$ (a and b are coprime). Then $bd = mr = arc = (1-bs)c = c - bsc$, which immediately implies that $b \mid c$, and we are done.

2. Mason's Theorem

A few years ago, the high school student (now Harvard undergraduate) Noah Snyder [*An alternate proof of Mason's theorem*, Elem. Math. **55** (2000), 93–94] came up with a 'proof from the Book' for Mason's ABC theorem. The following version of his proof is lifted from an article of Dan Bernstein.

Since $K[X]$ is a UFD, we can factor every polynomial into irreducible factors. If $f = p_1^{a_1} \cdots p_r^{a_r}$, then the product of the distinct prime factors of f is called the radical of f: $\operatorname{rad} f = p_1 \cdots p_r$.

Lemma 2.1. *We have $\frac{f}{\operatorname{rad} f} \mid f'$.*

Proof. In fact, if $f(X) = p_1(X)^{a_1} \cdots p_r(X)^{a_r}$ is the prime factorization of f, then $\operatorname{rad} f = p_1(X) \cdots p_r(X)$ and $\frac{f}{\operatorname{rad} f} = p_1(X)^{a_1-1} \cdots p_r(X)^{a_r-1}$. On the other hand, $f'(X) = a_1 p_1(X)^{a_1-1} p_2(X)^{a_2} \cdots p_r(X)^{a_r} + p_1(X)^{a_1} \frac{d}{dx} p_2(X)^{a_2} \cdots p_r(X)^{a_r}$, hence $p_1(X)^{a_1-1} \mid f'(X)$. Similarly $p_j(X)^{a_j} \mid f'(X)$, and since the p_j are coprime, the result follows. □

Theorem 2.2. *Let K be a field and A, B, C nonzero elements of $K[X]$ with $A + B + C = 0$ and $\gcd(A,B,C) = 1$. If $\deg A \ge \deg \operatorname{rad} ABC$, then $A' = 0$.*

What this theorem says is that if $A + B = C$, then the number of prime factors of ABC cannot be too small (unless the derivative of one of the factors is 0).

If the field K has characteristic 0, we can say more. In fact, in this case $A' = 0$ implies that A is constant (not so in characteristic p, where the polynomial t^p has derivative 0). Thus if ABC is not constant, then $\deg A \le \deg \operatorname{rad} ABC - 1$, and by symmetry we have

Corollary 2.3. *Let K be a field of characteristic 0. If A, B, C are nonzero polynomials in $K[X]$ with $A + B + C = 0$ and $\gcd(A, B, C) = 1$, then*

$$\max\{\deg A, \deg B, \deg C\} \leq \deg \operatorname{rad} ABC - 1. \tag{1}$$

Note that this is best possible: if $A = 1$, $B = t^n$ and $C = 1 + t^n$, then $\operatorname{rad} ABC = t(t^n + 1)$ (note that $t^n + 1$ is squarefree since it is coprime to its derivative) and $n = \max\{\deg A, \deg B, \deg C\} = \deg \operatorname{rad} ABC - 1$.

If K has characteristic p (where p is odd), the example $(1 - t)^p + t^p = 1$ has $\operatorname{rad} ABC = t(1 - t)$ and $\max\{\deg A, \deg B, \deg C\} = p$, so the inequality (1) is not satisfied.

Proof of Theorem 2.2. First observe that

$$\gcd(A, B) = \gcd(A, B, -A - B) = \gcd(A, B, C) = 1.$$

Similarly, $\gcd(B, C) = \gcd(C, A) = 1$.

By Lemma 2.1, $\frac{C}{\operatorname{rad} C}$ divides both C and C', hence $C'B - CB'$. Similarly, $\frac{B}{\operatorname{rad} B} \mid (C'B - CB')$. Finally, $C' = -A' - B'$, hence $C'B - CB' = (-A' - B')B + (A + B)B' = AB' - A'B$, hence $\frac{A}{\operatorname{rad} A} \mid (C'B - CB')$. Since the quotients $\frac{A}{\operatorname{rad} A}$, $\frac{B}{\operatorname{rad} B}$ and $\frac{C}{\operatorname{rad} C}$ are coprime, we conclude that

$$\frac{A}{\operatorname{rad} A} \frac{B}{\operatorname{rad} B} \frac{C}{\operatorname{rad} C} \mid (C'B - CB').$$

Since A, B, C are pairwise coprime, we have $(\operatorname{rad} A)(\operatorname{rad} B)(\operatorname{rad} C) = \operatorname{rad}(ABC)$, hence

$$\frac{ABC}{\operatorname{rad}(ABC)} \mid (C'B - CB').$$

By hypothesis, we have

$$\begin{aligned} \deg \frac{ABC}{\operatorname{rad}(ABC)} &= \deg ABC - \deg \operatorname{rad} ABC \\ &\geq \deg ABC - \deg A = \deg BC \\ &> \deg(C'B - CB'). \end{aligned}$$

This implies that $0 = C'B - CB' = AB' - A'B$. But then $A \mid A'B$, hence $A \mid A'$ since $(A, B) = 1$. Since $\deg A > \deg A'$, this implies $A' = 0$. □

3. Fermat's Last Theorem for Polynomials

As you all know, Fermat's Last Theorem states that there are no nonzero integers such that $X^n + Y^n = Z^n$ for $n > 2$. Equivalently, after dividing through by Z^n it claims that there are no nontrivial rational points on the Fermat curve $x^n + y^n = 1$.

Is Fermat's Last Theorem true for polynomials? According to Ribenboim's books, it was Liouville (not the J. Liouville famous for his theorems on elliptic functions) in 1879 who proved that it actually does hold, even for $n = 2$. I don't understand his proof, which is not too bad since we actually know a counterexample: our parametrization of the unit circle showed that

$$(1 - t^2)^2 + (2t)^2 = (1 + t^2)^2.$$

The correct version of Fermat's Last Theorem for polynomials states

Theorem 3.1. *The Fermat curve $x^n + y^n + 1 = 0$ does not have a nontrivial $\mathbb{C}(t)$-rational point for $n > 2$.*

Proof. Assume that the curve is rational. Clearing denominators we find polynomials such that $x(T)^n + y(T)^n + z(T)^n = 0$. Hence $\deg x(T)^n \le h(xyz) \le s-1$, where s is the number of distinct roots of xyz. Thus $s - 1 < \deg xyz$, and therefore $n \deg x = \deg x^n \le \deg x + \deg y + \deg z - 1$. The same inequality holds for y and z; adding them gives $n(\deg x + \deg y + \deg z) \le 3(\deg x + \deg y + \deg z) - 3$, which implies that $n < 3$. □

Note that if the Fermat curve does not have nontrivial $\mathbb{C}(t)$-rational points, then the same is true for $\mathbb{Q}(t)$-rational points.

Fermat's Last Theorem for polynomials can be proved in many different ways; Shanks, in his book *Solved and Unsolved Problems in Number Theory*, discusses a proof given by Chebyshev using integration.

Proof by descent. (This proof was not discussed in class).

Here's a proof similar to Kummer's proof of FLT (for regular prime exponents) in the integers (see N. Greenleaf, *On Fermat's equation in* $\mathbb{C}(t)$, Amer. Math. Monthly **76** (1969), 808–809): assume that there exist coprime polynomials $a, b, c \in \mathbb{C}[x]$ with $a^n + b^n = c^n$ for some $n > 2$, and pick one for which $N = \max\{\deg a, \deg b, \deg c\}$ is minimal. Since the roots of $x^n + 1$ are $-\zeta^j$ for a primitive n-th root of unity (such as $\zeta = \exp\frac{2\pi i}{n}$) and $j = 0, 1, \ldots, n-1$, we have the factorization

$$a^n + b^n = (a+b)(a+b\zeta)(a+b\zeta^2)\cdots(a+b\zeta^{n-1}).$$

We claim that these factors are relatively prime. In fact, let $d = \gcd(a+b\zeta^r, a+b\zeta^s)$; then d divides the difference $b(\zeta^r - \zeta^s)$, hence b (as $\zeta^r - \zeta^s \in \mathbb{C}$ is a unit). Moreover, d divides $\zeta^{s-r}(a+b\zeta^r) - (a+b\zeta^s) = a(\zeta^{s-r}-1)$, i.e., $d \mid a$. Since $\gcd(a,b) = 1$ by assumption, this proves our claim.

Since c^n has factors with multiplicity divisible by n, each factor $a + b\zeta^r$ must be an n-th power:

$$a + b = f_0^n, \quad a + b\zeta = f_1^n, \quad \ldots, a + b\zeta^{n-1} = f_{n-1}^n.$$

Thus

$$a = \frac{f_1^n - \zeta f_0^n}{1-\zeta}, \quad b = \frac{f_1^n - f_0^n}{\zeta - 1},$$

hence (here we use $n > 2$)

$$f_2^n = (\zeta+1)f_1^n - \zeta f_0^n.$$

Now put $a_1 = \sqrt[n]{\zeta+1}\, f_1$ and $b_1 = -\sqrt[n]{\zeta}\, f_0$; then (a_1, b_1, f_2) is a triple of polynomials in $\mathbb{C}[t]$ satisfying the Fermat equation of exponent n.

Now $\deg a_1 = \deg f_1 \le \frac{1}{n}\max\{\deg a, \deg b\} \le \frac{N}{n}$, and similarly $\deg b_1 \le \frac{N}{n}$ and $\deg f_2 \le \frac{N}{n}$. This contradicts the minimality of N, and the proof is complete.

Proof using algebraic geometry. The simplest proof uses concepts from algebraic geometry we have not yet talked about. A polynomial solution of the Fermat equation is a rational map from the projective line $\mathbb{P}^1\mathbb{C}$ to the Fermat curve. It is known that rational maps from the projective line to a curve exist only if the curve has genus 0. But the Fermat curve has genus $\frac{(n-1)(n-2)}{2}$, which is > 0 for $n > 2$.

Fermat's Last Theorem for the exponent 4. Just as over the integers we can prove

Proposition 3.2. *The equation $x^4 + y^4 = z^2$ has only trivial solutions in $\mathbb{C}[t]$.*

Proof. Mason's Theorem. □

This can easily be generalized:

Theorem 3.3. *Let $p, q, r \in \mathbb{N}$ integers. If $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1$, then the generalized Fermat equation*

$$x^p + y^q + z^r = 0$$

does not have a solution in $\mathbb{C}[t]$.

Proof. Mason's theorem gives $p \deg x, q \deg y, r \deg z < \deg xyz$; dividing through by $\deg xyz$ and adding shows that $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$. □

4. Elliptic Curves

An elliptic curve in Weierstrass form is a curve defined by an equation $y^2 = f(x)$, where the polynomial $f(x) = x^3 + ax^2 + bx + c$ does not have multiple roots. We will see later that the curve can be parametrized if f has multiple roots.

Proposition 4.1. *The elliptic curve $y^2 = x^3 + x$ cannot be parametrized.*

Proof. Write $x = \frac{m}{M}$ and $y = \frac{n}{N}$ for polynomials $m, n, M, N \in \mathbb{C}[t]$ with $(m, M) = (n, N) = 1$. Clearing denominators we get $n^2M^3 = m^3N^2 + mM^2N^2$. Clearly we have $N^2 \mid M^3$. On the other hand, $M^2 \mid m^3N^2$, hence $M \mid N$ since $(m, M) = 1$. But then $M^3 \mid N^2$, and this implies that $M^3 = cN^2$ for some unit $c \in \mathbb{C}$.

Writing N for $\sqrt{c}N$ we may assume that $M^3 = N^2$. Unique factorization shows that $M = e^2$ and $N = e^3$ for some $e \in \mathbb{C}[t]$. Thus $n^2e^6 = m^3e^6 + me^{10}$, and therefore $n^2 = m^3 + me^4 = m(m^2 + e^4)$. Since the factors on the right hand side are coprime, $m = u^2$ is a square, and we have $n^2 = u^2(u^4 + e^4)$. This in turn implies that $u^4 + e^4 = z^2$ for some $z \in \mathbb{C}[t]$, which contradicts Prop. 3.2. □

5. ABC Conjecture.

The result for integers analogous to Mason's ABC theorem is a conjecture not likely to be proved in the near future. Define $h(A, B, C) = \max\{|A|, |B|, |C|\}$ and let $\mathrm{rad}(A)$ denote the product of the disctinct prime factors of A, that is, the largest squarefree divisor of A.

ABC Conjecture. *If A, B, C are integers such that $\gcd(A, B, C) = 1$ and $A + B = C$, then for every $\varepsilon > 0$ there is a constant $\mu(\varepsilon)$ such that*

$$h(A, B, C) \leq \mu(\varepsilon) \cdot \mathrm{rad}(ABC)^{1+\varepsilon}.$$

This would be completely analogous to Mason's ABC theorem if we could choose $\varepsilon = 0$. Unfortunately, we cannot: it can be proved rather easily that the choice $\varepsilon = 0$ leads to counterexamples, no matter how large the constant μ is chosen.

For coprime natural numbers a, b, c with $a + b = c$ define

$$P(a, b, c) = \frac{\log \max\{a, b, c\}}{\log \mathrm{rad}(abc)}.$$

Then the ABC conjecture can be stated as

ABC Conjecture. For any $\eta > 1$ there are only finitely many integers a, b, c with $P(a, b, c) > \eta$.

Triples with $P > 1.4$ are called good abc triples. The current record holder is Eric Reyssat's example $A = 2$, $B = 3^{10} \cdot 109$, $C = 23^5$ with $P(A, B, C) \approx 1.62991$. Any triple with $P(A, B, C) > 1.53$ is in the current top ten.

The analogue of the Generalized Fermat Conjecture (Theorem 3.3) is believed to be true for integers:

Fermat-Catalan Conjecture. *If p, q, r are natural numbers with $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$, then there exist only finitely many coprime integers x, y, z such that $x^p + y^q = z^r$.*

This can be deduced from the ABC conjecture. Here's the list of known solutions:

$$\begin{aligned} 1 + 2^3 &= 3^2 & 17^7 + 76271^3 &= 21063928^2 \\ 2^5 + 7^2 &= 3^4 & 1414^3 + 2213459^2 &= 65^7 \\ 7^3 + 13^2 &= 2^9 & 9262^3 + 15312283^2 &= 113^7 \\ 2^7 + 17^3 &= 71^2 & 43^8 + 96222^3 &= 30042907^2 \\ 3^5 + 11^4 &= 122^2 & 33^8 + 1549034^2 &= 15613^3 \end{aligned}$$

The first entry here is the only solution to Catalan's equation $x^p + 1 = y^q$, as was proved by Mihailescu in 2002.