LECTURE 3, MONDAY 16.02.04

FRANZ LEMMERMEYER

Last time I talked about the arithmetic of conics and elliptic curves: the structure of the group of integral points on conics and of rational points on elliptic curves, and similar results over finite fields and over the p-adic numbers. This time I will present the analytic machinery that is essential for understanding the beauty of the subject.

1. The Congruence Zeta Function

Both for conics and elliptic curves over $\mathbb{Q}$ there is an analytic method that sometimes provides us with a generator for the group of integral or rational points on the curve. Before we can describe this method, we have to talk about zeta functions of curves over finite fields, whose classical name is the "congruence zeta function".

Take a conic C or an elliptic curve E defined over the finite field $\mathbb{F}_p$; let N_r denote the cardinalities of the groups of $\mathbb{F}_{p^r}$-rational points on C and E respectively, where we count solutions in the affine plane for C and in the projective plane for E. Then

$$Z_p(T) = \exp\Big(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\Big)$$

is called the zeta function of C or E over $\mathbb{F}_p$.

For the parabola $C : y = x^2$, we clearly have $N_r = C\#(\mathbb{F}_q) = p^r$, and we find

$$Z_p(T) = \exp\Big(\sum_{r=1}^{\infty} p^r \frac{T^r}{r}\Big) = \exp(-\log(1-pT)) = \frac{1}{1-pT}.$$

For the conic $X^2 - \Delta Y^2 = 4$ we will prove that

$$Z_p(T) = \frac{1}{(1-pT)(1-\chi(p)T)},$$

where χ is the Dirichlet character defined by $\chi(p) = (\Delta/p)$. The substitution $T = p^{-s}$ turns this into

$$\zeta_p(s;\mathcal{C}) = \frac{1}{(1-p^{1-s})(1-\chi(p)p^{-s})}.$$

1.1. **L-Functions for Conics.** Now we take the zeta function for each p and multiply them together to get a global zeta function. The first factor $1/(1-p^{1-s})$ gives us the product

$$\prod_p \frac{1}{1-p^{1-s}} = \zeta(s-1),$$

that is, essentially the Riemann zeta function.

The other factor, on the other hand, is more interesting:

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}}$$

is a Dirichlet L-function for the quadratic character $\chi = (\Delta/\cdot)$. This function converges on the right half plane $\Re s > 1$ and can be extended to a holomorphic function on the complex plane.

Now the nice thing discovered by Dirichlet (in his proof that every arithmetic progression $ax+b$ with $(a,b)=1$ contains infinitely many primes) is that, for every nontrivial (quadratic) character χ, $L(s,\chi)$ has a nonzero value at $s=1$. In fact, he was able to compute this value:

$$L(1,\chi) = \begin{cases} h \cdot \frac{2\pi}{w\sqrt{|\Delta|}} & \text{if } \Delta < 0, \\ h \cdot \frac{2\log\varepsilon}{\sqrt{\Delta}} & \text{if } \Delta > 0 \end{cases}$$

where $\chi(p) = (\Delta/p)$, and where w, Δ, h and $\varepsilon > 1$ are the number of roots of unity, the discriminant, the class number and the fundamental unit of $\mathbb{Q}(\sqrt{\Delta}\,)$.

The functional equation of Dirichlet's L-function allows us to rewrite Dirichlet's formula as

$$\lim_{s\to 0} s^{-r} L(s,\chi) = \frac{2hR}{w},$$

where $r=0$ and $R=1$ for $\Delta<0$, and $r=1$ and $R=\log\varepsilon$ for $\Delta>0$.

Observe that the evaluation of the L-funtion (which was defined using purely local data) at $s=0$ yields (h times) a generator of the free part of the group $\mathcal{C}(\mathbb{Z})$ (which is a global object)!

1.2. **L-Functions for Elliptic Curves.** The really amazing thing is that exactly the same thing works for elliptic curves of rank 1: by counting the number N_r of $\mathbb{F}_{p^r}$-rational points on E, we get a zeta function $Z_p(T)$ that can be shown to have the form

$$Z_p(T) = \frac{P(T)}{(1-T)(1-pT)}$$

for some polynomial $P(T) \in \mathbb{Z}[T]$ of degree 2 (if p does not divide the discriminant of E). In fact, if $p \nmid \Delta_E$ we have $P(T) = 1 - a_pT + pT^2$, where $a_p = p+1-\#E(\mathbb{F}_p)$, and there are similar (but simpler) expressions for P if $p \mid \Delta_E$).

Put $L_p(s) = 1/P(p^{-s})$ and define the L-function

$$L(s,E) = \prod_p L_p(s).$$

Hasse conjectured that this L-function can be extended analytically to the whole complex plane; moreover, there exists an $N \in \mathbb{N}$ such that

$$\Lambda(s,E) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(s,E)$$

satisfies the functional equation $\Lambda(s-2,E) = \pm\Lambda(s,E)$ for some choice of signs. For curves with complex multiplication, this was proved by Deuring; the general conjecture is a consequence of the now proved Taniyama-Shimura conjecture.

2. Modular Curves

Among the elliptic curves defined over $\mathbb{Q}$, there are certain curves with very special properties: curves with elliptic multiplication (CM). Although the explanation for their special behavior requires class field theory, some aspects of curves with CM can be seen at a very elementary level.

One property of CM elliptic curves not shared by other curves is that there are *very simple* formulas for the number $\mathbb{F}_p$-rational points. In fact, such formulas were already known to Gauss, though of course he used a different language.

Let us explain the pattern by examining the elliptic curves E_n that come up in the proof of Fermat's Last Theorem for the exponents $n = 3$, 4 and 7:

n	E_n
3	$y^2 = x^3 - 432$
4	$y^2 = x^3 - 4x$
7	$y^2 = x^3 - 3 \cdot 7^2 x^2 + 2^4 \cdot 7^3 x$

Define integers $a_p = a_p(n) = p + 1 - \#E_n(\mathbb{F}_p)$; the following table gives a_p for the primes $3 \leq p \leq 47$ and these curves:

p	$a_p(E_3)$	$a_p(E_4)$	$a_p(E_7)$
3	0	0	0
5	0	2	0
7	−1	0	0
11	0	0	4
13	5	−6	0
17	0	2	0
19	−7	0	0
23	0	0	8
29	0	10	2
31	−4	0	0
37	11	2	−6
41	0	10	0
43	8	0	−12
47	0	0	0

Of course you can compute these numbers by counting the number of points in $E(\mathbb{F}_p)$; it is faster to let a computer do the work. Pari offers a function that allows you to do just that. First you have to initialize the elliptic curve; if its equation is given by

$$y^2 - a_1 y - a_3 xy = x^3 + a_2 x^2 + a_4 x + a_6,$$

then you should type

$$\mathtt{e} = \mathtt{ellinit}([\mathtt{a1}, \mathtt{a2}, \mathtt{a3}, \mathtt{a4}, \mathtt{a6}]).$$

In the special case of the curve $E_3 : y^2 = x^3 - 432$, we thus type

$$\mathtt{e} = \mathtt{ellinit}([0, 0, 0, 0, -432])$$

The output is (not yet) interesting for us. But if we now type

$$\mathtt{ellap}(\mathtt{e}, 7)$$

then the output -1 is exactly the a_7 we are interested in.

The following little program computes the coefficients a_p for all primes $p \le 47$:

```
{e = ellinit([0,0,0,0,-432]) :
for(p = 2,50,if(isprime(p),
print(p," ",ellap(e,p)),))}
```

Note that if you write this program into some tex file and copy it, right clicking the pari window with the mouse will let you paste the whole thing right into pari.

It is easy to see that $a_p = 0$ if p is a quadratic nonresidue modulo 3, 4, or 7 respectively. The cases where $a_p \ne 0$ are much more interesting:

(1) $y^2 = x^3 - 432$: If $p \equiv 1 \bmod 3$, then $4p = L^2 + 27M^2$ for unique positive integers L, M, and we have $a_p = \pm L$, where the sign is chosen in such a way that $a_p \equiv 2 \bmod 3$.
(2) $y^2 = x(x^2 - 4)$: If $p \equiv 1 \bmod 4$, then $p = a^2 + 4b^2$ for unique positive integers a, b, and we have $a_p = \pm 2a$, where the sign is chosen in such a way that $a_p \equiv 2 \bmod 8$.
(3) $y^2 = x(x^2 - 3\cdot 7^2 x + 2^4 \cdot 7^3)$: If $p \equiv 1, 2, 4 \bmod 7$, then $p = c^2 + 7d^2$ for unique positive integers c, d, and we have $a_p = \pm 2c$, where the sign is chosen in such a way that $a_p \equiv 1, 2, 4 \bmod 7$.

The first two results essentially go back to Gauss; Deuring generalized this to all elliptic curves with complex multiplication. The curves above do have complex multiplication: for the first curve $y^2 = x^3 - 432$, the map $x \longmapsto \rho x$, where $\rho = \frac{1}{2}(-1 + \sqrt{-3}\,)$ is a primitive cube root of unity, leaves the defining equation of the elliptic curve invariant. For the second curve $y^2 = x(x^2 - 4)$, the map $x \longmapsto -x$, $y \longmapsto iy$ has this property. The last curve can be checked to have complex multiplication defined over the ring of integers in $\mathbb{Q}(\sqrt{-7}\,)$, but this is already quite technical.

The problem with these extremely nice results is that they don't generalize easily. What we need is a completely different type of formula for the a_p.

Here's what happens in general: consider the formal power series

$$f(q) = \sum_{n=1}^{\infty} c_n q^n \;=\; q \prod_{n=1}^{\infty} (1 - q^{3n})^2 (1 - q^{9n})^2.$$

A little pari program readily computes the first few values of c_n:

$$f(q) = q - 2q^4 - q^7 + 5q^{13} + \dots$$

```
{f=q:(for(n=1,10,f=f*(1-q^(3*n))^2*(1-q^(9*n))^2)):print(f)}
```

outputs a huge polynomial whose first few terms are

$$f(q) = q - 2q^4 - q^7 + 5q^{13} + 4q^{16} - 7q^{19} \dots$$

If you compare this with the a_p computed above, you will notice after a while that $a_p = c_p$ for the primes $p \le 13$. As a matter of fact, Eichler and Shimura have proved that this is true for all primes: the numbers a_p coming from counting the number of $\mathbb{F}_p$-rational points of E coincide with the c_p coming from this weird power series.

Now what about this function f? Here are some more surprises: put $q = e^{2\pi i z}$; then f becomes a function defined on the upper half plane, and turns out to be a cusp form of weight 2 of nebentypus of level $N = 27$. I might explain what

this all means at one point, but for now suffice it to say that modular forms are meromorphic functions on the upper half plane with lots of symmetries: since they can be expressed as functions of q, they clearly have to be invariant under the map $z \to z+1$; in addition, they are invariant under the action of subgroups of SL $_2(\mathbb{Z})$.

Elliptic curves whose a_p come from a modular form are called modular. It was the Japanese mathematician Taniyama who asked in 1955 whether maybe all elliptic curves defined over $\mathbb{Q}$ are modular. Shimura made his conjecture precise, and Weil, whose first reaction to hearing this conjecture was to make fun of it, came up with a criterium that allowed to test whether a given elliptic curve is modular or not. Over the years, hundreds of elliptic curves were checked to be modular, and eventually Wiles succeeded in proving the Taniyama-Shimura-Weil conjecture for semistable elliptic curves; later, Breuil, Conrad, Diamond, and Taylor proved the full conjecture.

Here's an example of an elliptic curve without complex multiplication: $E : y^2 - y = x^3 - x^2$. This curve has conductor $N = 11$, and Eichler-Shimura gives $a_p = p + 1 - \#E(\mathbb{F}_p) = c_p$ for all primes p, where

$$\sum_{n=1}^{\infty} c_n q^n \;=\; q \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2.$$

3. Birch–Swinnerton-Dyer

3.1. **Birch and Swinnerton-Dyer for Elliptic Curves.** The conjecture of Birch and Swinnerton-Dyer for elliptic curves predicts that $L(s, E)$ has a zero of order r at $s = 1$, where r is the rank of the Mordell-Weil group. More exactly, it is believed that

$$\lim_{s \to 1} \;(s-1)^{-r} L(s; E) = \frac{\Omega \cdot \#\mathbf{Ш}(E/\mathbb{Q}) \cdot R(E/\mathbb{Q}) \cdot \prod c_p}{(\#E(\mathbb{Q})_{\text{tors}})^2},$$

where r is the Mordell-Weil rank of $E(\mathbb{Q})$, $\Omega = c_\infty$ the real period, $\mathbf{Ш}(E/\mathbb{Q})$ the Tate-Shafarevich group, $R(E/\mathbb{Q})$ the regulator of E (some matrix whose entries are canonical heights of basis elements of the free part of $E(\mathbb{Q})$), c_p the Tamagawa number for the prime p (trivial for all primes not dividing the discriminant), and $E(\mathbb{Q})_{\text{tors}}$ the torsion group of E.

The weak form of the conjecture only claims that the order of the zero of $L(s, E)$ at $s = 1$ (called the analytic rank) is equal to the Mordell-Weil rank (the arithmetic rank) r of the group of rational points on E: $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$.

Dirichlet's class number formula for quadratic fields can be interpreted as a Birch and Swinnerton-Dyer conjecture for Pell conics.

The following result was proved by Coates and Wiles in 1977:

Theorem 1. *Let E be an elliptic curve over some number field $\mathbb{Q}$ with complex multiplication. If the arithmetic rank of E is positive, then $L(1, E) = 0$.*

Thus $\text{rk}_{\text{arith}} > 0$ implies that $\text{rk}_{\text{anal}} > 0$. The condition that E have complex multiplication ensures that L has an analytic continuation to the whole complex plane.

Gross and Zagier proved in 1983 a kind of converse:

Theorem 2. *Let E be a modular elliptic curve over $\mathbb{Q}$. If $L(s, E)$ has a simple zero at $s = 1$, then $E(\mathbb{Q})$ is infinite.*

In other words: if the analytic rank is 1, then the arithmetic rank is ≥ 1.