1:31 p.m. October 5, 2011

Preface

Bill Casselman
University of British Columbia
cass@math.ubc.ca

Preview of the spring seminar

Bill Casselman

This course will be concerned with explaining the following formulas, which are in fact all special cases of one theorem:

1. The fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$

The group $\mathrm{SL}_2(\mathbb{R})$ acts on the upper half-plane $\mathcal{H}$ by linear fractional transformations. The invariant area form is

$$\frac{dx\,dy}{y^2}\,.$$

The discrete subgroup $\mathrm{SL}_2(\mathbb{Z})$ has fundamental domain

$$\mathcal{D} = \{z = x + iy \,|\, |x| \le 1/2,\ |z| \ge 1\}\,.$$

Its area is

$$\int_{-1/2}^{1/2} dx \int_{\sqrt{1-x^2}}^{\infty} \frac{dy}{y^2} = \int_{-1/2}^{1/2} \frac{dx}{\sqrt{1-x^2}} = [\arcsin x]_{-1/2}^{1/2} = \pi/6 - (-\pi/6) = \pi/3\,.$$

It is not an accident that, as Euler (and one of the Bernoullis before him?) knew,

$$\frac{\pi^2}{6} = 1 + 1/4 + 1/9 + 1/16 + \cdots$$

which is the value of the ζ-function

$$1 + 1/2^s + 1/3^s + 1/4^s + \cdots$$

at $s = 2$.

2. Dirichlet

Let K be imaginary quadratic extension $\mathbb{Q}(\sqrt{-D})$ of $\mathbb{Q}$ (with D the discriminat of the field, which may have some square factors), $\mathfrak{o}$ its ring of integers, made up of those x in K satisfying a monic quadratic polynomial equation with integral coefficients. An $\mathfrak{o}$-lattice in K is an $\mathfrak{o}$ module contained in K. Two of these are said to be equivalent if one is a scalar multiple of the other, in which case they are isomorphic. Let h_K be the number of equivalence classes, which is finite. Also let m be the number of roots of unity in K, $\chi = \mathrm{sgn}_K$ on $(\mathbb{Z}/D)^\times$.

$$\frac{h_K}{m} = \frac{\sqrt{D}}{2\pi} L(1, \chi)\,,$$

where

$$L(s,\chi) = \prod_{p\not| D} \Big(1 - \frac{\chi(p)}{p^s}\Big)^{-1}.$$

It is absolutely convergent for $\Re(s) > 1$, but may be extended to a holomorphic function on $\Re(s) > 0$.

If $K = \mathbb{Q}(\sqrt{-1})$, for example, then $\mathfrak{o}$ is a principal ideal domain so $h_K = 1$, $m = 4$, $D = 4$, and

$$\chi(p) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{otherwise.} \end{cases}$$

Here

$$L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots$$

This is, according to Leibniz, equal to $\pi/4$, and sure enough

$$\frac{1}{4} = \frac{2}{2\pi}\frac{\pi}{4}.$$

The series above is the value at $s = 1$ of the L-function

$$1 - 1/3^s + 1/5^s - 1/7^s + \cdots$$

3. Siegel

Let Q be a positive definite, symmetric, integral, $n \times n$ matrix, and for $m \in \mathbb{N}$ and prime power q set

$$\begin{aligned} N(Q,n) &= \#\{x \,|\, Q(x) = n\} \\ N(Q) &= \#\{X \,|\, {}^tXQX = Q\} \\ N_q(Q,m) &= \#\{{}^tQ(x) \equiv m \bmod q^{n-1}\}. \end{aligned}$$

The limit

$$\nu_p(Q,m) = \lim_{k\to\infty} \frac{N_{p^k}(Q,m)}{p^{k(n-1)}}$$

exists. Define also

$$\nu_\infty(Q,m) = \lim_{U\to\{m\}} \frac{\operatorname{meas} Q^{-1}(U)}{\operatorname{meas} U}.$$

Define two such quadratic forms to be equivalent if one of them is obtained from the other by an integral unimodular change of coordinates, and in the same genus if they are equivalent modulo q for every prime power q. Thus the $N_q(Q_i)$ are all the same. Let $\{Q_i\}$ be the finite set of representatives of classes in the genus of Q. Siegel's formula is

$$\frac{\sum \frac{N(Q_i,n)}{N(Q_i)}}{\sum \frac{1}{N(Q_i)}} = \nu_\infty(Q,n) \prod_p \nu_p(Q,n).$$

Let's see how this works in a simple example, solving $x^2 + y^2 = 5$, for which there are 8 solutions. First of all, because $\mathbb{Z}[i]$ is a unique factorization domain, there is only one form in the genus.

Second, to calculate the term for the Euclidean sphere, we look at the set of (x, y) with $x^2 + y^2$ in the interval $1 \pm \varepsilon$. This has area $\pi(1+\varepsilon) - \pi(1-\varepsilon) = 2\pi\varepsilon$, so the correct factor is $2\pi\varepsilon/2\varepsilon = \pi$.

Next we have to solve $x^2 + y^2 = 5$ modulo various prime powers p^n. There are four different cases: $p = 2$, $p = 5$, $p \equiv 1$, $p \equiv -1$ modulo 4.

Lemma. *For any prime p, the ratio*

$$\frac{|\{(x,y) \in (\mathbb{Z}/p^k)^2 \,|\, x^2 + y^2 \equiv 5\}|}{p^k}$$

becomes constant for $n \gg 0$.

This is a mild generalization of Hensel's Lemma:

Lemma. *If $f(x) = 0$ is a polynomial in n variables with coefficients in $\mathbb{Z}$, and x_n in $(\mathbb{Z}/p^n)^d$ satisfies (a) $f(x_n) \equiv 0 \bmod p^n$ and (b) $\langle \nabla f, x\rangle \neq 0 \bmod p^n$ then there exist exactly p solutions (x_{n+1}, y_{n+1}) with*

$$x_{n+1} \equiv x_n \bmod p^{n+1}$$
$$f(x_{n+1}) \equiv 0 \bmod p^{n+1}$$

Here ∇f is the linear function with coordinates $(\partial f/\partial x_i)$. If x is any point in $(\mathbb{Z}/p^{n+1})^d$ congruent to x_n modulo p^n, then We have

$$f(x + p^n \Delta x) = f(x) + p^n \langle \nabla f, \Delta x\rangle + O(p^{2n}) \equiv f(x) + p^n \langle \nabla f, \Delta x\rangle \text{ modulo } p^{n+1}\,.$$

But then the solutions modulo p^{n+1} are in bijection with the solutions of the linear equation

$$(f(x)/p^n) + \langle \nabla f, \Delta x\rangle = 0 \text{ modulo } p\,.$$

If $p \neq 2$ or 5 the curve $X^2 + y^2 = 5$ is non-singular modulo p. Hence, in these circumstances, for every solution of $f(x,y) = 0$ in the field $\mathbb{Z}/p$ there exist exactly p^{n-1} modulo p^n. In our case, quadratic reciprocity tells us that the number of solutions of $x^2 + y^2 = 5$ modulo p is $p - 1$ if $p \equiv 1$ and $p + 1$ if $p \equiv 3$ modulo 4, as long as $p \neq 5$. Hence the limiting ratio is $1 - 1/p$ if $p \equiv 1$ and $1 + 1/p$ if $p \equiv 3$ modulo 4 and $p \neq 5$. Thus Siegel's formula has on the right hand side the product

$$\prod p \neq 2, 5 \left(1 - \frac{\chi(p)}{p}\right)^{-1}$$

which is, up to a single factor, what we saw in the first example.

In general, a non-singular point of the algebraic curve $f(x,y) = 0$ will behave in the same way, but singular ones behave differently. Modulo 5, the equation $x^2 + y^2 = 5$ is the cone $x^2 + y^2 = 0$, with a singular point at $(0,0)$. Modulo 2 the curve $x^2 + y^2 = 5$ is singular everywhere.

Modulo powers of 2 or 5 things are more complicated. For example, $(1,0)$ is a solution modulo 4, and $(1,0)$ in $(\mathbb{Z}/8)^2$ is congruent to it modulo 4 but there do not exist any solutions of $x^2 + y^2 = 5$ modulo 8 that are congruent to $(1,0)$ modulo 4, since $(1+4a)^2 + (0+4b)^2 \equiv 1$ modulo 4. On the other hand, $(1,4)$ is congruent to $(1,0)$ modulo 4 and every one of the four points $(1+4a, 4+4b)$ in $(\mathbb{Z}/8)^2$ will be a solution modulo 8. So the naive extsension of Hensel's Lemma fails in this case.

Similarly, the equation $x^2 + y^2 = 5$ modulo 5 becomes the singular cone $x^2 + y^2 = 0$, and again a naive extension of Hensel's Lemma fails.

I leave it as an exercise to see what happens for $p = 2$ and $p = 5$. (Hint: Try working out a systematic algorithm that will produce all solutions modulo any 2^k or 5^k, and then calculate the limit ratio. Take as a simple model the equation $x^2 = 1$: Prove that if $x_n \equiv 1$ modulo 2^n then there exist 2 solutions

$x_{n+1} \equiv x_n$ modulo 2^{n-1}, as long as $n \geq 3$. Deduce that there exist 4 solutions of $x^2 \equiv 1$ modulo all 2^n for $n \geq 3$.)

In any event, the explicit evaluation of Siegel's formula involves again values of certain L-functions associated to quadratic characters at integral points. Siegel's formula is also the canonical example of how global phenomema (the number of solutions of an equation in integers) are related to local phenomena (the solutions in local fields), and has motivated much subsequent work along these lines, such the celebrated Birch and Swinnerton-Dyer conjecture.

4. Minkowski, Siegel

The group $\mathrm{SL}_n(\mathbb{Z})$ acts discretely on the space X_n of positive definite symmetric matrices of determinant 1. On X_n we can assign a volume form to be The volume of the quotient $\Gamma\backslash X_n$ is ...

5. Tamagawa, Weil

If Q is a positive definite symmetric matrix with coefficients in $\mathbb{Q}$, the volume of $\mathrm{SO}_Q(\mathbb{Q})\backslash\mathrm{SO}_Q(\mathbb{A})$ with respect to a rational differential form of highest degree is two.

6. Weil, Langlands, Kottwitz

Let G be a semi-simple, simply connected group defined over $\mathbb{Q}$—for example $G = \mathrm{SL}_n$. Choose on G a rational differential form of highest degree. It determines on each $G(\mathbb{Q}_v)$ an invariant Haar measure, and also one on $G(\mathbb{A})$. The volume of $G(\mathbb{Q})\backslash G(\mathbb{A})$ is one.