I'd like to start with the story of the Siegel mass formula. The mass formula is a statement about integral quadratic form, a homogeneous quadratic polynomial in some number of variables. I'll say it's over R if the coefficients are in R. So, for example, $x^2 + y^2$ or $x^2 - y^2$, which are quadratic over $\mathbb{Z}$.

I can ask if I can convert one to the other with a change of coordinates. These are equivalent over $\mathbb{C}$ because I can multiply y by i. They're inequivalent over $\mathbb{Z}$ and indeed $\mathbb{R}$ since the first is positive definite. Over the reals, any quadratic form can be diagonalized, so it can be written $\sum \pm x_i^2$. The only invariant is how many plus and minus signs you get. They are equivalent if they have the same number of variables and the same signature.

So $x^2 + y^2$ and $x^2 + 3y^2$ are equivalent over the reals, but not over the integers. Mod 3, the first form is nondegenerate, but the second is degenerate. You can ask if two forms are equivalent over the integers by looking at the signature, or looking modulo an integer. This motivates the following definition, which I will restrict for simplicity to positive definite forms.

Definition 1. *Two positive definite quadratic forms q and q' over $\mathbb{Z}$ in some fixed number of variables are* in the same genus *if $q \cong q' \mod N$ for all N.*

Do two quadratic forms in the same genus have to be equivalent? No, but there are a finite number of them, and there's a formula for how many of them there are. This is a weighted count of how many there are.

Suppose that q is a quadratic form over $\mathbb{Z}$ and R is a commutative ring. I'll write $O_q(R)$ is the set of invertible $n \times n$ matrices so that $q \circ A = q$, for example, if q is the standard quadratic form, then this is the usual orthogonal group. If q is positive definite, then $O_q(\mathbb{Z})$ is a finite group, a group of invertible integer-valued matrices, so they leave invariant a lattice and a quadratic form, so $q(v) = q(w)$. There are only finitely many lattice points you can go to, so there can be only finitely many transformations in total.

These are always finite groups. You can define the mass of the genus of q as follows:

$$\sum \frac{1}{|O_q(\mathbb{Z})|}$$

If all these summands were one, this would be the number of forms in a genus. Every quadratic form has at least one, so these coefficients are never one. This is a weighted count of the number of quadratic forms in a genus up to equivalence. The mass formula is a formula for what this mass is.

If q is a positive definite quadratic form over $\mathbb{Z}$ then the mass of q is something that I'll tell you about in a second. Let me tell you the right hand side in the simplest case.

To explain what I mean in the simplest case, I need to introduce a little terminology.

Definition 2. *If q is a positive definite quadratic form over $\mathbb{Z}$ then q is* unimodular *if it is nondegenerate mod p for every prime p.*

The claim is that unimodular forms in n variables comprise a genus. If you have two forms in the same genus, and one is unimodular, then the other is as well. This is the converse, if you have two unimodular forms, this says they are in the same genus.

This is the simplest genus, and for this genus, well, fix a number $n = 8k$. If there are going to exist unimodular forms at all, then the dimension has to be divisible by 8. What is the left hand side in this case? It's the sum over unimodular quadratic forms q in n variables (isomorphism classes) and what you sum is

$$\sum \frac{1}{|O_q(\mathbb{Z})} = \frac{\Gamma(\frac{1}{2})\Gamma(1)\cdots\Gamma(\frac{n}{2})\zeta(2)\zeta(4)\cdots\zeta(n-2)\zeta(\frac{n}{2})}{2^{n-1}\pi^{\frac{n(n+1)}{4}}}$$

It's not obvious that this is even rational.

What are some examples? Suppose that $n = 8$. In eight variables, there is only one unimodular form up to isomorphism, which is the E_8 lattice, so the left hand side is $\frac{1}{|Aut\ E_8|}$. You can evaluate the right hand side, and you can get that the right hand side is $\frac{1}{2^{14}3^5 5^2 7}$, so you get the order of the Weyl group of E_8. This might make you think this is an equality between numbers that look very small.

This is atypical. Once you start multiplying factorials together, you get something very large, very quickly. For $n = 32$, the thing on the right hand side is in the millions, and each summand on the left is less than one. So there are lots of pairwise inequivalent unimodular quadratic forms. This tells you they're out there without describing them explicitly.

Let me spend this lecture giving a modern reformulation of this statement and how you would prove it.

Let's take as a temporary goal justifying this formula. Let's try to prove that all forms in the same genus are equivalent, and we'll fail because it's not true, and the method of our failure will suggest something.

Let's fix q and q' in the same genus in n variables. What does this mean? For every $N > 0$ there is a matrix $A_N \in GL_n(\mathbb{Z}/N\mathbb{Z})$ such that $q = q' \circ A_N$. You can see, without loss of generality, you can choose A_N compatible, so that if N divides N', then $A_{N'}$ reduces mod N to A_N. Then the A_N for all N give an element A of $GL_n(\hat{\mathbb{Z}})$, where $\hat{\mathbb{Z}} = \lim \mathbb{Z}/N\mathbb{Z}$, which is $\prod_p \mathbb{Z}_p$. If we wanted to prove that q and q' were equivalent, you would have $q = q' \circ A$ for $A \in GL_n(\mathbb{Z})$ but instead we get something over $GL_n(\hat{\mathbb{Z}})$. These are equivalent over $\mathbb{R}$ because they're positive definite, and equivalent over $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}]$, and the Hasse principle says that if two forms are equivalent over every completion of the rational numbers, then they are equivalent over the rationals. Then there is a matrix B in $GL_n(\mathbb{Q})$ so that $q = q' \circ B$. If you have two different isomorphisms, you can use these to build an automorphism. So we can say that $q = q' \circ A = q \circ B^{-1} \circ A$, so if I look at $B^{-1} \circ A$, this lives in the orthogonal group of q. What is this, though. It makes sense to multiply $\hat{\mathbb{Z}}$ and $\mathbb{Q}$ in a ring containing them both. So $\mathbb{A}^{fin}$ is the ring of finite adeles $\hat{\mathbb{Z}} \otimes \mathbb{Q}$. So $B^{-1} \circ A$ lives in $O_q(\mathbb{A}^{fin})$.

We started with q and q' and "defined" this element of $O_q(\mathbb{A}^{fin})$, but it's not well defined. I can multiply A by something that preserves q over $\hat{\mathbb{Z}}$, so it's only unambiguous modulo $O_q(\hat{Z})$ on the right, and on the left, similarly, by $O_q(\mathbb{Q})$. So the element of the double cosets

$$O_q(\mathbb{Q})\backslash O_q(\mathbb{A}^{fin})/O_q(\hat{\mathbb{Z}})$$

is well defined. What would it mean if this vanished? Well, then $B^{-1} \circ A$ is the identity. Then A and B would have to be in the intersection of $\hat{\mathbb{Z}}$ and $\mathbb{Q}$, which is

$\mathbb{Z}$. Then this vanishes if and only if $q \sim q'$. It turns out with a little more work that the other double cosets are the other equivalence classes.

I want to make some modifications. Let me move to the special orthogonal group. This is a different double coset space:

$$SO_q(\mathbb{Q})\backslash SO_q(\mathbb{A}^{fin})/SO_q(\hat{\mathbb{Z}})$$

We counted them before up to equivalence, but now we consider them up to orientation-preserving automorphism, so we should get something off by a factor of 2. We should also use all adeles, not finite adeles. So $\hat{\mathbb{Z}} = \prod \mathbb{Z}_p$, so $\mathbb{A}^{fin}$ might look like $\prod \mathbb{Q}_p$, but it's actually the restricted product, so only finitely many of them have denominators. There's one other completion of the rationals besides $\mathbb{Q}_p$, namely $\mathbb{R}$. So $\mathbb{A} = \mathbb{A}^{fin} \times \mathbb{R}$.

Now the middle is a bigger group, the group in the middle is $SO_q(\mathbb{A}^{fin}) \times SO_q(\mathbb{R})$. If I want to ignore this, I can mod out by it on the right.

$$SO_q(\mathbb{Q})\backslash SO_q(\mathbb{A}^{fin}) \times SO_q(\mathbb{R})/SO_q(\hat{\mathbb{Z}}) \times SO_q(\mathbb{R})$$

Now $\mathbb{A}$ has a topology: it's a locally compact ring. So $SO_q(\mathbb{A})$ is a locally compact group, which has two subgroups of interest to us, which contains $SO_q(\mathbb{Q})$ as a discrete subgroup and $SO_q(\hat{\mathbb{Z}}) \times SO_q(\mathbb{R})$ as a compact open subgroups.

We can now borrow tools from locally compact groups. We can take a Haar measure μ, invariant under left translation and unique up to scalar. This induces a measure on $SO_q(\mathbb{Q})\backslash SO_q(\mathbb{A})$, and this is acted on by $SO_q(\hat{\mathbb{Z}}) \times SO_q(\mathbb{R})$, so the number of orbits this group has on this set. The measure should restrict and be finite on the open compact subgroup. So the number of double cosets should be roughly

$$\frac{\mu(SO_q(\mathbb{Q})\backslash SO_q(\mathbb{A})}{\mu(SO_q(\hat{\mathbb{Z}}) \times SO_q(\mathbb{R})}$$

This would be true if this action were free, but since it is not, this actually turns out to be the thing we want to compute:

$$\sum \frac{1}{|SO_q(\mathbb{Z})|}$$

The fraction doesn't depend on the scalar in the Haar measure. The next step in the reasoning is to try to evaluate the numerator and denominator independently.

In fact, there's a canonical Haar measure on this locally compact group. Let's remember where Haar measures come from, so write $SO_q(\mathbb{A})$ as $SO_q(\mathbb{A}^{fin}) \times SO_q(\mathbb{R})$. As a first step, let's think on $SO_q(\mathbb{R})$. How do you write down a Haar measure? You can take a top degree differential form. If you want it to be left invariant, take an invariant top form. Let $V_{\mathbb{R}}$ be the space of left invariant top forms on $SO_q(\mathbb{R})$. This is a vector space over the real numbers, and is one dimensional over them. Any non-zero vector gives you a left invariant measure on this group. In fact, we can say a little bit more. This group is not just any compact Lie group. It's the solution in $GL_n(\mathbb{R})$ to a set of equations. Those equations make sense over the rational numbers, since that is where q is defined. So then this has the structure of an algebraic group over $\mathbb{Q}$ and belongs to algebraic geometry. So inside of it is $V_{\mathbb{Q}}$, the space of algebraic invariant top forms defined over $\mathbb{Q}$. Any nonzero element of this one dimensional $\mathbb{Q}$-vector space gives you a Haar measure. What about the factor $SO_q(\mathbb{A}^{fin})$? This is essentially a product of $SO_q(\mathbb{Q}_p)$ (the restricted product). This is a p-adic analytic Lie group. There's a space $V_{\mathbb{Q}_p}$, a one dimensional vector

space over $\mathbb{Q}_p$ of left invariant top forms on $SO_Q(\mathbb{Q}_p)$. This contains a subspace of rational top forms $V_{\mathbb{Q}}$, which is one dimensional over the rational numbers. They're the same algebraic group. If you choose a nonzero vector in $V_{\mathbb{Q}}$, it gives you a Haar measure everywhere. The idea is to choose $\omega \in V_{\mathbb{Q}}$ and multiply all these measures together. We hope that gives a measure on $SO_q(\mathbb{A})$. This would not converge with the orthogonal group.

What happens when you multiply ω by -5? It gets multiplied by 5 on the real side. For every prime p, you are talking about the p-adic absolute value. So that's $\frac{1}{5}$ on $SO_q(\mathbb{Q}_5)$ and 1 at every other prime. This measure, μ_{Tam}, is the Tamagawa measure.