Weil's Conjecture on Tamagawa Numbers (Lecture 1)

January 30, 2014

Let R be a commutative ring and let V be an R-module. A *quadratic form* on V is a map $q : V \to R$ satisfying the following conditions:

(a) The construction $(v, w) \mapsto q(v + w) - q(v) - q(w)$ determines an R-bilinear map $V \times V \to R$.

(b) For every element $\lambda \in R$ and every $v \in V$, we have $q(\lambda v) = \lambda^2 q(v)$.

A *quadratic space* over R is a pair (V, q), where V is a finitely generated projective R-module and q is a quadratic form on V.

One of the basic problems in the theory of quadratic forms can be formulated as follows:

Question 1. Let R be a commutative ring. Can one classify quadratic spaces over R (up to isomorphism)?

Example 2. Let V be a vector space over the field $\mathbf{R}$ of real numbers. Then any quadratic form $q : V \to \mathbf{R}$ can be diagonalized: that is, we can choose a basis $e_1, \ldots, e_n$ for V such that

$$q(\lambda_1 e_1 + \cdots + \lambda_n e_n) = \lambda_1^2 + \cdots + \lambda_a^2 - \lambda_{a+1}^2 - \cdots - \lambda_{a+b}^2$$

for some pair of nonnegative integers a, b with $a + b \leq n$. Moreover, the integers a and b depend only on the isomorphism class of the pair (V, q) (a theorem of Sylvester). In particular, if we assume that q is nondegenerate (in other words, that $a + b = n$), then the isomorphism class (V, q) is completely determined by the dimension n of the vector space V and the difference $a - b$, which is called the *signature* of the quadratic form q.

Example 3. Let $\mathbf{Q}$ denote the field of rational numbers. There is a complete classification of quadratic spaces over $\mathbf{Q}$, due to Minkowski (later generalized by Hasse to the case of an arbitrary number field). Minkowski's result is highly nontrivial, and represents one of the great triumphs in the arithmetic theory of quadratic forms: we refer the reader to [5] for a detailed and readable account.

Let us now specialize to the case $R = \mathbf{Z}$. We will refer to quadratic spaces (V, q) over $\mathbf{Z}$ as *even lattices*. The classification of even lattices up to isomorphism is generally regarded as an intractable problem (see Remark 17 below). Let us therefore focus on the following variant of Question 1:

Question 4. Let (V, q) and (V', q') be even lattices. Is there an effective procedure for determining whether or not (V, q) and (V', q') are isomorphic?

Let (V, q) be a quadratic space over a commutative ring R, and suppose we are given a ring homomorphism $\phi : R \to S$. We let V_S denote the tensor product $S \otimes_R V$. An elementary calculation shows that there is a unique quadratic form $q_S : V_S \to S$ for which the diagram

$$\begin{array}{ccc} V & \xrightarrow{q} & R \\ \downarrow & & \downarrow \phi \\ V_S & \xrightarrow{q_S} & S \end{array}$$

is commutative. The construction $(V, q) \mapsto (V_S, q_S)$ carries quadratic spaces over R to quadratic spaces over S; we refer to (V_S, q_S) as the *extension of scalars* of (V, q). If (V, q) and (V', q') are isomorphic quadratic spaces over R, then extension of scalars yields isomorphic quadratic spaces (V_S, q_S) and (V'_S, q'_S) over S. Consequently, if we understand the classification of quadratic spaces over S and can tell that (V_S, q_S) and (V'_S, q'_S) are *not* isomorphic, it follows that (V, q) and (V', q') are not isomorphic.

Example 5. Let $q : \mathbf{Z} \to \mathbf{Z}$ be the quadratic form given by $q(n) = n^2$. Then the even lattices $(\mathbf{Z}, q)$ and $(\mathbf{Z}, -q)$ cannot be isomorphic, because they are not isomorphic after extension of scalars to $\mathbf{R}$: the quadratic space $(\mathbf{R}, q_{\mathbf{R}})$ has signature 1, while $(\mathbf{R}, -q_{\mathbf{R}})$ has signature -1.

Example 6. Let $q, q' : \mathbf{Z}^2 \to \mathbf{Z}$ be the quadratic forms given by

$$q(m, n) = m^2 + n^2 \qquad q'(m, n) = m^2 + 3n^2.$$

Then $(\mathbf{Z}^2, q)$ and $(\mathbf{Z}^2, q')$ become isomorphic after extension of scalars to $\mathbf{R}$ (since both quadratic forms are positive-definite). However, the quadratic spaces $(\mathbf{Z}^2, q)$ and $(\mathbf{Z}^2, q')$ are not isomorphic, since they are not isomorphic after extension of scalars to the field $\mathbf{F}_3 = \mathbf{Z}/3\mathbf{Z}$ (the quadratic form $q_{\mathbf{F}_3}$ is nondegenerate, but $q'_{\mathbf{F}_3}$ is degenerate).

Using variants of the arguments provided in Examples 5 and 6, one can produce many examples of even lattices (V, q) and (V', q') that cannot be isomorphic: for example, by arranging that q and q' have different signatures (after extension of scalars to $\mathbf{R}$) or have nonisomorphic reductions modulo n for some integer $n > 0$ (which can be tested by a finite calculation). This motivates the following definition:

Definition 7. Let (V, q) and (V', q') be positive-definite even lattices. We say that (V, q) and (V', q') *of the same genus* if (V, q) and (V', q') are isomorphic after extension of scalars to $\mathbf{Z}/n\mathbf{Z}$, for every positive integer n (in particular, this implies that V and V' are free abelian groups of the same rank).

Remark 8. One can also define study genera of lattices which are neither even nor positive definite, but we will restrict our attention to the situation of Definition 7 to simply the exposition.

More informally, we say that two even lattices (V, q) and (V', q') are of the same genus if we cannot distinguish between them using variations on Example 5 or 6. It is clear that isomorphic even lattices are of the same genus, but the converse is generally false. However, the problem of classifying even lattices within a genus has a great deal of structure. One can show that there are only finitely many isomorphism classes of even lattices in the same genus as (V, q). Moreover, the celebrated *Smith-Minkowski-Siegel mass formula* allows us to say exactly how many (at least when counted with multiplicity).

Notation 9. Let (V, q) be a quadratic space over a commutative ring R. We let $\mathrm{O}_q(R)$ denote the automorphism group of (V, q): that is, the group of R-module isomorphisms $\alpha : V \to V$ such that $q = q \circ \alpha$. We will refer to $\mathrm{O}_q(R)$ as the *orthogonal group* of the quadratic space (V, q). More generally, if $\phi : R \to S$ is a map of commutative rings, we let $\mathrm{O}_q(S)$ denote the automorphism group of the quadratic space (V_S, q_S) over S obtained from (V, q) by extension of scalars to S.

Example 10. Suppose q is a positive-definite quadratic form on an real vector space V of dimension n. Then $\mathrm{O}_q(\mathbf{R})$ can be identified with the usual orthogonal group $\mathrm{O}(n)$. In particular, $\mathrm{O}_q(\mathbf{R})$ is a compact Lie group of dimension $\frac{n^2-n}{2}$.

Example 11. Let (V, q) be a positive-definite even lattice. For every integer d, the group $\mathrm{O}_q(\mathbf{Z})$ acts by permutations on the set $V_{\leq d} = \{v \in V : q(v) \leq d\}$. Since q is positive-definite, each of the sets $V_{\leq d}$ is finite. Moreover, for $d \gg 0$, the action of $\mathrm{O}_q(\mathbf{Z})$ on $V_{\leq d}$ is faithful (since an automorphism of V is determined by its action on a finite generating set for V). It follows that $\mathrm{O}_q(\mathbf{Z})$ is a finite group.

Let (V, q) be a positive-definite even lattice. The mass formula gives an explicit formula for the sum $\sum_{(V', q')} \frac{1}{|\mathrm{O}_{q'}(\mathbf{Z})|}$, where the sum is taken over all isomorphism classes of even lattices (V', q') in the genus of (V, q). The explicit formula is rather complicated in general, depending on the reduction of (V, q) modulo p for various primes p. For simplicity, we will restrict our attention to the simplest possible case.

Definition 12. Let (V, q) be an even lattice. We will say that (V, q) is *unimodular* if the bilinear form $b(v, w) = q(v + w) - q(v) - q(w)$ induces an isomorphism of V with its dual $\mathrm{Hom}(V, \mathbf{Z})$.

Remark 13. Let (V, q) be a positive-definite even lattice. The condition that (V, q) be unimodular depends only on the reduction of q modulo p for all primes p. In particular, if (V, q) is unimodular and (V', q') is in the genus of (V, q), then (V', q') is also unimodular. In fact, the converse also holds: any two unimodular even lattices of the same rank are of the same genus (though this is not obvious from the definitions).

Remark 14. The condition that an even lattice (V, q) be unimodular is very strong: for example, if q is positive-definite, it implies that the rank of V is divisible by 8.

Theorem 15 (Mass Formula: Unimodular Case)**.** *Let n be an integer which is a positive multiple of 8. Then*

$$\sum_{(V,q)} \frac{1}{|\mathrm{O}_q(\mathbf{Z})|} = \frac{\Gamma(\frac{1}{2})\Gamma(\frac{2}{2})\cdots\Gamma(\frac{n}{2})\zeta(2)\zeta(4)\cdots\zeta(n-4)\zeta(n-2)\zeta(\frac{n}{2})}{2^{n-1}\pi^{n(n+1)/4}}$$
$$= \frac{B_{n/4}}{n} \prod_{1 \le j < n/2} \frac{B_j}{4j}.$$

Here ζ denotes the Riemann zeta function, B_j denotes the jth Bernoulli number, and the sum is taken over all isomorphism classes of positive-definite even unimodular lattices (V, q) of rank n.

Example 16. Let $n = 8$. The right hand side of the mass formula evaluates to $\frac{1}{696729600}$. The integer $696729600 = 2^{14}3^5 5^2 7$ is the order of the Weyl group of the exceptional Lie group E_8, which is also the automorphism group of the root lattice of E_8 (which is an even unimodular lattice). Consequently, the fraction $\frac{1}{696729600}$ also appears as one of the summands on the left hand side of the mass formula. It follows from Theorem 15 that no other terms appear on the left hand side: that is, the root lattice of E_8 is the *unique* positive-definite even unimodular lattice of rank 8, up to isomorphism.

Remark 17. Theorem 15 allows us to count the number of positive-definite even unimodular lattices of a given rank with multiplicity, where a lattice (V, q) is counted with multiplicity $\frac{1}{|\mathrm{O}_q(\mathbf{Z})|}$. If the rank of V is positive, then $\mathrm{O}_q(\mathbf{Z})$ has order at least 2 (since $\mathrm{O}_q(\mathbf{Z})$ contains the group $\langle \pm 1 \rangle$), so that the left hand side of Theorem 15 is at most $\frac{C}{2}$, where C is the number of isomorphism classes of positive-definite even unimodular lattices. In particular, Theorem 15 gives an inequality

$$C \geq \frac{\Gamma(\frac{1}{2})\Gamma(\frac{2}{2})\cdots\Gamma(\frac{n}{2})\zeta(2)\zeta(4)\cdots\zeta(n-4)\zeta(n-2)\zeta(\frac{n}{2})}{2^{n-2}\pi^{n(n+1)/4}}.$$

The right hand side of this inequality grows very quickly with n. For example, when $n = 32$, we can deduce the existence of more than eighty million pairwise nonisomorphic (positive-definite) even unimodular lattices of rank n.

We now describe a reformulation of Theorem 15, following ideas of Tamagawa and Weil. Suppose we are given a positive-definite even lattice (V, q), and that we wish to classify other even lattices of the same genus. If (V', q') is a lattice in the genus of (V, q), then for every positive integer n we can choose an isomorphism $\alpha_n : V/nV \simeq V'/nV'$ which is compatible with the quadratic forms q and q'. Using a compactness argument (or some variant of Hensel's lemma) we can assume without loss of generality that the isomorphisms $\{\alpha_n\}_{n>0}$ are compatible with one another: that is, that the diagrams

$$\begin{array}{ccc} V/nV & \xrightarrow{\alpha_n} & V'/nV' \\ \downarrow & & \downarrow \\ V/mV & \xrightarrow{\alpha_m} & V'/mV' \end{array}$$

commute whenever m divides n. In this case, the data of the family $\{\alpha_n\}$ is equivalent to the data of a single isomorphism $\alpha : \widehat{\mathbf{Z}} \otimes_{\mathbf{Z}} V \to \widehat{\mathbf{Z}} \otimes_{\mathbf{Z}} V'$, where $\widehat{\mathbf{Z}} \simeq \varprojlim_{n>0} \mathbf{Z}/n\mathbf{Z}$ denotes the profinite completion of the ring $\mathbf{Z}$.

By virtue of the Chinese remainder theorem, the ring $\widehat{\mathbf{Z}}$ can be identified with the product $\prod_p \mathbf{Z}_p$, where p ranges over all prime numbers and $\mathbf{Z}_p$ denotes the ring $\varprojlim \mathbf{Z}/p^k\mathbf{Z}$ of p-adic integers. It follows that (V, q) and (V', q') become isomorphic after extension of scalars to $\mathbf{Z}_p$, and therefore also after extension of scalars to the field $\mathbf{Q}_p = \mathbf{Z}_p[p^{-1}]$ of p-adic rational numbers. Since the lattices (V, q) and (V', q') are positive-definite and have the same rank, they also become isomorphic after extending scalars to the field of real numbers. It follows from Minkowski's classification that the quadratic spaces $(V_{\mathbf{Q}}, q_{\mathbf{Q}})$ and $(V'_{\mathbf{Q}}, q'_{\mathbf{Q}})$ are isomorphic (this is known as the *Hasse principle*: to show that quadratic spaces over $\mathbf{Q}$ are isomorphic, it suffices to show that they are isomorphic over every completion of $\mathbf{Q}$; see §3.3 of [5]). We may therefore choose an isomorphism $\beta : V_{\mathbf{Q}} \to V'_{\mathbf{Q}}$ which is compatible with the quadratic forms q and q'.

Let $\mathbf{A}_f$ denote the ring of *finite adeles*: that is, the tensor product $\widehat{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{Q}$. The isomorphism $\widehat{\mathbf{Z}} \simeq \prod_p \mathbf{Z}_p$ induces an injective map

$$\mathbf{A}_f \simeq \widehat{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{Q} \hookrightarrow \prod_p (\mathbf{Z}_p \otimes_{\mathbf{Z}} \mathbf{Q}) \simeq \prod_p \mathbf{Q}_p,$$

whose image is the *restricted product* $\prod_p^{\mathrm{res}} \mathbf{Q}_p \subseteq \prod_p \mathbf{Q}_p$: that is, the subset consisting of those elements $\{x_p\}$ of the product $\prod_p \mathbf{Q}_p$ such that $x_p \in \mathbf{Z}_p$ for all but finitely many prime numbers p. The quadratic spaces (V, q) and (V', q') become isomorphic after extension of scalars to $\mathbf{A}_f$ in two different ways: via the isomorphism α which is defined over $\widehat{\mathbf{Z}}$, and via the isomorphism β which is defined over $\mathbf{Q}$. Consequently, the composition $\beta^{-1} \circ \alpha$ can be regarded as an element of $\mathrm{O}_q(\mathbf{A}_f)$. This element depends not only the quadratic space (V', q'), but also on our chosen isomorphisms α and β. However, any other isomorphism between $(V_{\widehat{\mathbf{Z}}}, q_{\widehat{\mathbf{Z}}})$ and $(V'_{\widehat{\mathbf{Z}}}, q'_{\widehat{\mathbf{Z}}})$ can be written in the form $\alpha \circ \gamma$, where $\gamma \in \mathrm{O}_q(\widehat{\mathbf{Z}})$. Similarly, the isomorphism β is well-defined up to right multiplication by elements of $\mathrm{O}_q(\mathbf{Q})$. Consequently, the composition $\beta^{-1} \circ \alpha$ is really well-defined as an element of the set of double cosets

$$\mathrm{O}_q(\mathbf{Q}) \backslash \mathrm{O}_q(\mathbf{A}_f) / \mathrm{O}_q(\widehat{\mathbf{Z}}).$$

Let us denote this double coset by $[V', q']$.

It is not difficult to show that the construction $(V', q') \mapsto [V', q']$ induces a bijection from the set of isomorphism classes of even lattices (V', q') in the genus of (V, q) with the set $\mathrm{O}_q(\mathbf{Q}) \backslash \mathrm{O}_q(\mathbf{A}_f) / \mathrm{O}_q(\widehat{\mathbf{Z}})$ (the inverse of this construction is given by the procedure of *regluing*, which we will discuss in the next lecture). Moreover, if $\gamma \in \mathrm{O}_q(\mathbf{A}_f)$ is a representative of the double coset $[V', q']$, then the group $\mathrm{O}_{q'}(\mathbf{Z})$ is isomorphic to the intersection

$$\mathrm{O}_q(\widehat{\mathbf{Z}}) \cap \gamma^{-1} \mathrm{O}_q(\mathbf{Q}) \gamma.$$

Consequently, the left hand side of the mass formula can be written as a sum

$$\sum_{\gamma} \frac{1}{|\mathrm{O}_q(\widehat{\mathbf{Z}}) \cap \gamma^{-1} \mathrm{O}_q(\mathbf{Q}) \gamma|}, \tag{1}$$

where γ ranges over a set of double coset representatives.

At this point, it will be technically convenient to introduce two modifications of the calculation we are carrying out. For every commutative ring R, let $\mathrm{SO}_q(R)$ denote the subgroup of $\mathrm{O}_q(R)$ consisting of those automorhisms of (V_R, q_R) which have determinant 1 (if R is an integral domain, this is a subgroup of index at most 2). Let us instead attempt to compute the sum

$$\sum_{\gamma} \frac{1}{|\mathrm{SO}_q(\widehat{\mathbf{Z}}) \cap \gamma^{-1} \mathrm{SO}_q(\mathbf{Q}) \gamma|}, \tag{2}$$

where γ runs over a set of representatives for the collection of double cosets

$$X = \mathrm{SO}_q(\mathbf{Q}) \backslash \mathrm{SO}_q(\mathbf{A}_f) / \mathrm{SO}_q(\widehat{\mathbf{Z}}).$$

If q is unimodular, expression (2) differs from the expression (1) by an overall factor of 2 (in general, the expressions differ by a power of 2).

Remark 18. Fix an orientation of the $\mathbf{Z}$-module V (that is, a generator of the top exterior power of V). Quantity (2) can be written as a sum $\sum \frac{1}{|\operatorname{SO}_{q'}(\mathbf{Z})|}$, where the sum is indexed by all isomorphism classes of *oriented* even unimodular positive-definite lattices (V', q') which are isomorphic to (V, q) as *oriented* quadratic spaces after extension of scalars to $\mathbf{Z}/n\mathbf{Z}$, for every integer $n > 0$.

Let $\mathbf{A}$ denote the ring of *adeles*: that is, the ring $\mathbf{A}_f \times \mathbf{R}$. Then we can identify X with the collection of double cosets $\operatorname{SO}_q(\mathbf{Q})\backslash \operatorname{SO}_q(\mathbf{A})/\operatorname{SO}_q(\widehat{\mathbf{Z}} \times \mathbf{R})$. The virtue of this maneuver is that $\mathbf{A}$ has the structure of a locally compact commutative ring containing $\mathbf{Q}$ as a *discrete* subring. Consequently, $\operatorname{SO}_q(\mathbf{A})$ is a locally compact topological group which contains $\operatorname{SO}_q(\mathbf{Q})$ as a discrete subgroup and $\operatorname{SO}_q(\widehat{\mathbf{Z}} \times \mathbf{R})$ as a compact open subgroup.

Let μ be a Haar measure on the group $\operatorname{SO}_q(\mathbf{A})$. One can show that the group $\operatorname{SO}_q(\mathbf{A})$ is unimodular: that is, the measure μ is invariant under both right and left translations. In particular, μ determines a measure on the quotient $\operatorname{SO}_q(\mathbf{Q})\backslash \operatorname{SO}_q(\mathbf{A})$, which is invariant under the right action of $\operatorname{SO}_q(\widehat{\mathbf{Z}} \times \mathbf{R})$. We will abuse notation by denoting this measure also by μ. Write $\operatorname{SO}_q(\mathbf{Q})\backslash \operatorname{SO}_q(\mathbf{A})$ as a union of orbits $\bigcup_{x\in X} O_x$ for the action of the group $\operatorname{SO}_q(\widehat{\mathbf{Z}} \times \mathbf{R})$. If $x \in X$ is a double coset represented by an element $\gamma \in \operatorname{SO}_q(\mathbf{A})$, then we can identify the orbit O_x with the quotient of $\operatorname{SO}_q(\widehat{\mathbf{Z}} \times \mathbf{R})$ by the finite subgroup $\operatorname{SO}_q(\widehat{\mathbf{Z}} \times \mathbf{R}) \cap \gamma^{-1} \operatorname{SO}_q(\mathbf{Q})\gamma$. We therefore have

$$\sum_{\gamma} \frac{1}{|\operatorname{SO}_q(\widehat{\mathbf{Z}} \times \mathbf{R}) \cap \gamma^{-1} \operatorname{SO}_q(\mathbf{Q})\gamma|} = \sum_{x\in X} \frac{\mu(O_x)}{\mu(\operatorname{SO}_q(\widehat{\mathbf{Z}} \times \mathbf{R}))} \tag{3}$$

$$= \frac{\mu(\operatorname{SO}_q(\mathbf{Q})\backslash \operatorname{SO}_q(\mathbf{A}))}{\mu(\operatorname{SO}_q(\widehat{\mathbf{Z}} \times \mathbf{R}))}. \tag{4}$$

Of course, the Haar measure μ on $\operatorname{SO}_q(\mathbf{A})$ is only well-defined up to scalar multiplication. Rescaling the measure μ has no effect on the left hand side of the preceding equation, since μ appears in both the numerator and the denominator of the right hand side. However, it is possible to say more: it turns out that there is a canonical normalization of the Haar measure, known as *Tamagawa measure*.

Construction 19. Let G be a connected semisimple algebraic group of dimension d over the field $\mathbf{Q}$ of rational numbers. Let Ω denote the collection of all left invariant d-forms on G, so that Ω is a 1-dimensional vector space over $\mathbf{Q}$. Choose a nonzero element $\omega \in \Omega$.

The vector ω determines a left-invariant differential form of top degree on the smooth manifold $G(\mathbf{R})$, which in turn determines a Haar measure $\mu_{\mathbf{R},\omega}$ on $G(\mathbf{R})$. For every prime number p, an analogous construction yields a measure $\mu_{\mathbf{Q}_p,\omega}$ on the p-adic analytic manifold $G(\mathbf{Q}_p)$. One can show that the product of these measures determines a measure μ_{Tam} on the restricted product

$$G(\mathbf{R}) \times \prod_p^{\mathrm{res}} G(\mathbf{Q}_p) \simeq G(\mathbf{A}).$$

Let λ be a nonzero rational number. Then an elementary calculation gives

$$\mu_{\mathbf{R},\lambda\omega} = |\lambda|\mu_{\mathbf{R},\omega} \qquad \mu_{\mathbf{Q}_p,\lambda\omega} = |\lambda|_p\mu_{\mathbf{Q}_p,\omega};$$

here $|\lambda|_p$ denotes the p-adic absolute value of λ. Combining this with the product formula $\prod_p |\lambda|_p = \frac{1}{|\lambda|}$, we deduce that μ_{Tam} is independent of the choice of nonzero element $\omega \in \Omega$. We will refer to μ_{Tam} as the *Tamagawa measure* of the algebraic group G.

If (Λ, q) is a positive-definite even lattice, then the restriction of the functor $R \mapsto \operatorname{SO}_q(R)$ to $\mathbf{Q}$-algebras can be regarded as a semisimple algebraic group over $\mathbf{Q}$. We may therefore apply Construction 19 to obtain a canonical measure μ_{Tam} on the group $\mathrm{SO}_q(\mathbf{A})$. We may therefore specialize equation (4) to obtain an equality

$$\sum_{\gamma} \frac{1}{|\,\mathrm{SO}_{q'}(\mathbf{Z})|} \quad = \quad \frac{\mu_{\mathrm{Tam}}(\mathrm{SO}_q(\mathbf{Q})\backslash \mathrm{SO}_q(\mathbf{A}))}{\mu_{\mathrm{Tam}}(\mathrm{SO}_q(\widehat{\mathbf{Z}} \times \mathbf{R}))}, \tag{5}$$

where it makes sense to evaluate the numerator and the denominator of the right hand side independently.

Remark 20. The construction $R \mapsto \mathrm{O}_q(R)$ also determines a semisimple algebraic group over $\mathbf{Q}$. However, this group is not connected, and the infinite product $\prod_p \mu_{\mathbf{Q}_p,\omega}$ does not converge to a measure on the restricted product $\prod_p^{\mathrm{res}} \mathrm{O}_q(\mathbf{Q}_p) = \mathrm{O}_q(\mathbf{A}_f)$. This is the reason for preferring to work with the group SO_q in place of O_q.

Remark 21. The numerator on the right hand side of (5) is called the *Tamagawa number* of the algebraic group SO_q. More generally, if G is a connected semisimple algebraic group over $\mathbf{Q}$, we define the *Tamagawa number* of G to be the measure $\mu(G(\mathbf{Q})\backslash G(\mathbf{A}))$.

The denominator on the right hand side of (5) is computable: if we choose a differential form ω as in Construction 19, it is given by the product

$$\mu_{\mathbf{R},\omega}(\mathrm{SO}_q(\mathbf{R})) \prod_p \mu_{\mathbf{Q}_p,\omega}(\mathrm{SO}_q(\mathbf{Z}_p)).$$

The first term is the volume of a compact Lie group, and the second term is a product of local factors which are related to counting problems over finite rings. Carrying out these calculations leads to a very pretty reformulation of Theorem 15:

Theorem 22 (Mass Formula, Adelic Formulation)**.** *Let (V, q) be a nondegenerate quadratic space over $\mathbf{Q}$. Then $\mu_{\mathrm{Tam}}(\mathrm{SO}_q(\mathbf{Q})\backslash \mathrm{SO}_q(\mathbf{A})) = 2$.*

The appearance of the number 2 in the statement of Theorem 22 results from the fact that the algebraic group SO_q is not simply-connected. Let Spin_q denote the (2-fold) universal cover of SO_q, so that Spin_q is a simply-connected semisimple algebraic group over $\mathbf{Q}$. We then have the following more basic statement:

Theorem 23. *Let (V, q) be a positive-definite quadratic space over $\mathbf{Q}$. Then*

$$\mu_{\mathrm{Tam}}(\mathrm{Spin}_q(\mathbf{Q})\backslash \mathrm{Spin}_q(\mathbf{A})) = 1.$$

Remark 24. For a deduction of Theorem 22 from Theorem 23, see [4].

Theorem 23 motivates the following:

Conjecture 25 (Weil's Conjecture on Tamagawa Numbers)**.** Let G be a simply-connected semisimple algebraic group over $\mathbf{Q}$. Then $\mu_{\mathrm{Tam}}(G(\mathbf{Q})\backslash G(\mathbf{A})) = 1$.

Conjecture 25 was proven by Weil in a number of special cases. The general case was proven by Langlands in the case of a split group ([3]), by Lai in the case of a quasi-split group ([2]), and by Kottwitz for arbitrary simply connected algebraic groups satisfying the Hasse principle ([1]; this is now known to be all simply-connected semisimple algebraic groups over $\mathbf{Q}$, by work of Chernousov).

Our goal in this course is to prove an analogue of Conjecture 25 in which $\mathbf{Q}$ has been replaced by global field of positive characterstic. We will review the formulation (and interpretation) of this conjecture in the next lecture.

References

[1] Kottwitz, R. E. *Tamagawa numbers.* Annals of Mathematics 127 (3), 1988, 629-646.

[2] Lai, K.F. *Tamagawa number of reductive algebraic groups.* Compositio Mathematica 41 (2) 153-188, 1980.

[3] Langlands, R. P. *The volume of the fundamental domain for some arithmetical subgroups of Chevallaey groups.* In *Algebraic Groups and Discontinuous subgroups*, Proc. Sympos. Pure Math., IX, Providence, R.I., 1966.

[4] Ono, Takashi. *On the relative theory of Tamagawa numbers.* Annals of Mathematics 78: 47-73, 1963.

[5] Serre, J. P. *A Course in Arithmetic.* Springer-Verlag, 1973.

[6] Tamagawa, T. *Adèles.* In *Algebraic Groups and Dicsontinuous Subgroups*, Proc. Sympos. Pure Math., IX, Providence, R.I., 1966.

[7] Weil, André. *Adeles and algebraic groups.* Progress in Mathematics, 23, 1982.