Using Mass Formulas to Enumerate Definite Quadratic Forms of Class Number One:

An (integer-valued) <u>quadratic</u> <u>form</u>

$$Q(\vec{x}) = \sum_{1\le i\le j\le n} c_{ij} x_i x_j$$

is a homogeneous polynomial of degree 2 in n variables with coefficients $c_{ij} \in \mathbb{Z}$.

We can also express $Q(\vec{x})$ as a symmetric (Hessian) matrix

$$A = (a_{ij}) = \left(\frac{\partial}{\partial x_i}\frac{\partial}{\partial x_j} Q(\vec{x})\right) \in \mathrm{Sym}_n(\mathbb{Z})$$

with even diagonal entries.

<u>Ex:</u> $Q(\vec{x}) = x^2 + xy + y^2$

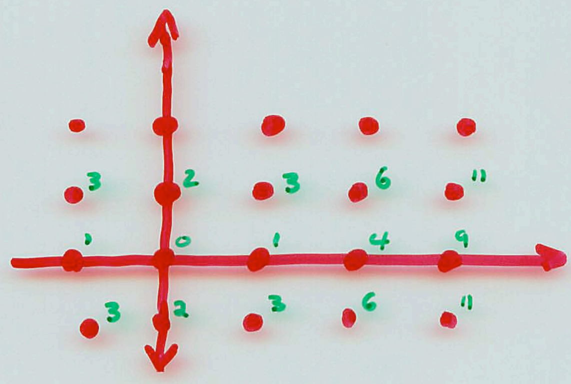
<u>Hessian</u> Gram

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \xrightarrow{\cdot\, 1/2} \begin{bmatrix} 1 & 1/2 \\ 1/2 & 1 \end{bmatrix}$$

$\in \mathrm{Sym}_n(\mathbb{Z})$

We can also think of Q as describing a lattice $L = \mathbb{Z}^n$ in a fixed quadratic vector space $(V, Q) = (\mathbb{Q}^n, Q)$.

Ex: $L = \mathbb{Z}^2 \subseteq (\mathbb{Q}^2, x^2 + 2y^2)$



For any ring R, we can consider $Q(\vec{x})$ as a quadratic form over R by considering its coefficient $c_{ij} \in R$.

In the lattice perspective this corresponds to considering the "lattice" $L \otimes_{\mathbb{Z}} R$ in the quadratic space $(\mathbb{Q} \otimes_{\mathbb{Z}} R, Q)$.

Equivalence of Quadratic Forms:

We say that two quadratic forms Q and Q' are <u>equivalent</u> <u>over R</u> and write $Q \sim_R Q'$ if there is some invertible R-linear change of variables $T \in GL_n(R)$ so that $Q'(\vec{x}') = Q(T\vec{x})$ as quadratic forms over R.

<u>Ex:</u> $(x')^2 + (y')^2 \sim_{\mathbb{Z}} x^2 + (x+y)^2 = 2x^2 + xy + y^2$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \vec{x} \longmapsto \begin{bmatrix} x \\ x+y \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \vec{x} =: \vec{x}' = \begin{bmatrix} x' \\ y' \end{bmatrix}$$

$$\begin{tikzcd} X \arrow[rr, "T"] \arrow[dr, "Q"'] & & X' \arrow[dl, "Q'"] \\ & R & \end{tikzcd}$$

$Q =$ pullback of Q' under T.

<u>Ex:</u> $x^2 + y^2 \sim_{\mathbb{F}_7} x^2 + (3y)^2 = x^2 + 2y^2$

From the matrix perspective we have $A' = {}^tTAT$, but on lattices we're forgetting about the basis.

Given a quadratic form Q, we define the <u>class of Q</u> to be the set of all $Q' \sim_{\mathbb{Z}} Q$ and the <u>genus of Q</u> (denoted $\mathrm{Gen}(Q)$) as the set of all Q' which are everywhere locally equivalent to Q, meaning that

Equivalently $Q' \sim_{\mathbb{Z}_v} Q$ for all places v of $\mathbb{Q}$.

- $Q' \sim_{\mathbb{Z}_p} Q$ for all primes $p \in \mathbb{N}$
- $Q' \sim_{\mathbb{R}} Q$

<u>Thrm (Siegel)</u>: There are only finitely many classes in $\mathrm{Gen}(Q)$.

We denote by $h(Q)$ the number of classes in $\mathrm{Gen}(Q)$, called the <u>class number of Q</u>.

Local and Global Representations:

We say that Q (globally) represents $m \in \mathbb{Z}$ if $\exists\, \vec{x} \in \mathbb{Z}^n$ so that $Q(\vec{x}) = m$, and say that Q locally represents m if $\exists\, \vec{x}_v \in \mathbb{Z}_v^n$ so that $Q(\vec{x}_v) = m$ for all places v of $\mathbb{Q}$.

Let $r_Q(m) := \#\{\vec{x} \in \mathbb{Z}^n \mid Q(\vec{x}) = m\}$.

For Q (positive) definite we see that $r_Q(m) < \infty \quad \forall m \in \mathbb{Z}$.

In this case we can define the theta series of Q by

$$\Theta_Q(z) := \sum_{m \geq 0} r_Q(m)\, e^{2\pi i m z}.$$

This is a modular form.

$\in M_{n/2}(N, \chi)$.

Genus and Class Invariants:

① $Q' \in \mathrm{Gen}(Q) \overset{\text{Hasse-Minkowski}}{\Longrightarrow} (V, Q) \sim_{\mathbb{Q}} (V, Q')$

So all rational invariants are also genus invariants.

Ex: $\det(Q) \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, Hasse Invariants $c_p \in \{\pm 1\}$, signature $\in \mathbb{Z}$.

② $Q' \in \mathrm{Gen}(Q) \Rightarrow \det(A) = \det(A') \in \mathbb{Z}$

Since $A' = {}^tT_v A T_v$

$\Rightarrow \det(A') = \det(T_v)^2 \cdot \det(A)$

But $\det(T_v) \in \mathbb{Z}_v^\times$

$\Rightarrow \det(A)$ and $\det(A') \in \mathbb{Z}$ have the same p-divisibility and the same sign.

$\Rightarrow \det(A) = \det(A')$.

③ $Q \sim_{\mathbb{Z}} Q' \Longrightarrow r_Q(m) = r_{Q'}(m) \quad \forall m \in \mathbb{Z}$

$\Longrightarrow \Theta_Q(z) = \Theta_{Q'}(z)$.

Consequences of $h(Q) = 1$:

- Q locally represents m

  $\Rightarrow$ Q represents m (globally)

- $\Theta_Q(z)$ is an Eisenstein series

- The circle method gives an exact formula for $r_Q(m)$

- There is a "simple" formula for $r_Q(m)$ as a sum over divisors of m.

  Ex: $Q = x^2 + y^2 + z^2 + w^2$

  $$\Rightarrow r_Q(m) = 8 \cdot \sum_{\substack{0<d \mid m \\ 4 \nmid d}} d$$

- The adelic "symmetric space"

  $$\left| O_Q(\mathbb{Q}) \backslash O_Q(\mathbb{A}_{\mathbb{Q}}^{\times}) / \mathrm{Stab}_{\mathbb{A}}(L) \right| = 1.$$

This is like $h \cong SL_2(\mathbb{Z}) \backslash SL_2(\mathbb{R}) / SO_2(\mathbb{R})$.

How many (classes of) primitive, definite quadratic forms have class number one?

Magnus $\Rightarrow$ only finitely many in $n \geq 3$ variables, and need $n \leq 35$.

(1937 by Mass Formula)

Watson $\Rightarrow$ need $n \leq 10$, and lists most of them for each $2 < n \leq 10$.

(1960's + 70's by reducing to "maximal" lattices)

Gerstein $\Rightarrow$ $n \geq 16t + 5 \Rightarrow h(Q) \geq p(t)$ for any totally real F, so need $n \leq 36$.

(1972 by modular lattices)

Pfeuffer $\Rightarrow$ Only finitely many Q over all totally real number fields!

(1978-9 by Mass Formula)

Mass Formulas:

Assuming Q is definite, we define

$$\mathrm{Mass}^+(Q) := \sum_{Q' \in \mathrm{Gen}(Q)} \frac{1}{\#\mathrm{Aut}^+(Q')} \in \mathbb{Q}_{>0}$$

$$= 2 \cdot \prod_v \beta_v(Q)^{-1}$$

where the local density $\beta_v(Q)$ is defined by

$$\beta_v(Q) := \frac{1}{2} \lim_{\substack{U \supseteq \{Q\} \\ \text{open} \\ U \to \{Q\}}} \frac{\mathrm{vol}(Q^{-1}(U))}{\mathrm{vol}(U)}$$

where $Q \longleftrightarrow A \in \mathrm{Sym}_n(\mathbb{Z})$ defines

$$\begin{aligned} M_n(\mathbb{R}) &\xrightarrow{Q} \mathrm{Sym}_n(\mathbb{R}) \\ X &\longmapsto {}^tXAX . \end{aligned}$$

For $v = p$ prime, we can write the local density more simply as

$$\beta_p(Q) = \frac{1}{2} \cdot \lim_{\alpha \to \infty} \frac{\#\{X \in M_n(\mathbb{Z}/p^\alpha\mathbb{Z}) \mid {}^tXAX = A\}}{p^{\frac{n(n-1)}{2} \cdot \alpha}}$$

which can be computed at all but finitely many places by Hensel's Lemma, and if $p \nmid 2 \cdot \det(A)$ then the limit stabilizes at $\alpha = 1$.

$$\Rightarrow \beta_p(Q) = \frac{\# O_Q^+(\mathbb{F}_p)}{p^{\frac{n(n-1)}{2}}}$$

This tells us that the infinite product for $\mathrm{Mass}^+(Q)$ is generically a product like

Since over $\mathbb{F}_p$ there is only one orthogonal group if n is odd, but two if n is even.

$$\zeta(2) \cdot \zeta(4) \cdot \cdots \cdot \zeta(n-1) \quad \text{if } n \text{ is odd,}$$

$$\zeta(2) \cdot \zeta(4) \cdot \cdots \cdot \zeta(n-2)\, L(n/2, \chi) \quad \text{if } n \text{ is even,}$$

where χ is some quadratic character determined by $\det(A)$.

Explicit Mass Formula "Highlights":

- Local densities for $p > 2$ (Pall, '65) and for $p = 2$ (Watson, '76) $/\mathbb{Q}$ in terms of local Jordan form.

- Conway + Sloane, '88 give a correct unproven formula for all local densities, differing from Watson's $/\mathbb{Q}$

- Shimura gives an explicit formula for maximal lattices over totally real fields F ('99)

- Gan–Hanke–Yu give an extended formula for definite maximal lattices $/F$ (also for Hermitian forms!). ('01)

Ex: $Q = x^2 + y^2 + z^2 \Rightarrow n = 3$

$$\mathrm{Mass}^+(Q) \overset{\text{G-H-Y}}{=} \frac{1}{2^{\frac{n-1}{2}} \cdot d} \cdot |\zeta_F(-1)| \cdot \tau(O_F^+(Q)) \cdot \prod_{p \in S'} \lambda_p$$

where

$$\lambda_p := \begin{cases} \frac{p-1}{2} & \text{if aniso. } \dim(V_p) = 3 \\ \frac{p+1}{2} & \text{if aniso. } \dim(V_p) = 1 \end{cases}$$

and $S' := \left\{ \text{primes } p \text{ s.t. } p \mid \det(Q) \text{ or aniso. } \dim(V_p) = 3 \right\}$

$$\Rightarrow S' = \{2\} \quad \text{and} \quad \lambda_2 = \frac{2-1}{2} = \frac{1}{2}$$

$$\Rightarrow \mathrm{Mass}^+(Q) = \frac{1}{2} \cdot \left| \frac{-1}{12} \right| \cdot 2 \cdot \frac{1}{2}$$

$$= \frac{1}{24}$$

Check: $\#\mathrm{Aut}^+(Q) = \frac{1}{2} \cdot 2^n \cdot n!$

$$= \frac{1}{2} \cdot 48 = 24.$$

This proves that $h(Q) = 1$, or checks the mass formula if we knew this independently.

Arithmetic Bounds when $n=3$:

Since n is odd, the classes and proper classes coincide. So

$$h(Q) = 1 \Rightarrow \mathrm{Mass}^+(Q) = \frac{1}{\#\mathrm{Aut}^+(Q)} \in \frac{1}{\mathbb{Z}}$$

$$\Rightarrow \frac{1}{12} \cdot \prod_{p \in S'} \frac{p \pm 1}{2} \in \frac{1}{\mathbb{N}}.$$

However the factor $\lambda_p = \frac{p \pm 1}{2} \in \mathbb{Z}$ if $p > 2$, and λ_p will contain some (odd) prime factors that are not killed by the remaining product if $p \in S$ is very large.

$$\Rightarrow \frac{p \pm 1}{2} < 24$$

$$\Rightarrow p \pm 1 < 48$$

$$\Rightarrow p < 49 \quad \text{for all } p \mid \det(Q)$$

So there are finitely many ternary quadratic spaces (V, Q) with a class #1 max'l lattice!

Basic Strategy:

1. Enumerate quadratic spaces (V, Q) which could support a maximal lattice L of class number one.
2. Construct a maximal lattice on each (V, Q).
3. Check if $h(L) = 1$ by testing Mass v.s. #Aut.
4. Enumerate all possible non-maximal local lattice types on (V, Q) satisfying the mass eligibility test. ($\mathrm{Mass}^+ \in \frac{1}{\mathbb{N}}$ or $\mathrm{Mass}^+ \leq 1$)

Finding a Maximal Lattice:

1. Compute elementary divisors of $L^\#/L$ (w.r.t. $A \in \mathrm{Sym}_n(\mathbb{Z})$).
2. Find a "Watson" super lattice containing L, so the elementary divisors of $L^\#/L$ are square-free.
3. Look for totally isotropic subspaces of $L^\#/L$ over $\mathbb{F}_p$ for all $p \mid \#(L^\#/L)$.
4. Use 2-neighbors to find an even lattice, which corresponds to a quadratic form.

Outline of Computational Tools:

Quadratic Spaces:

→ Constructive Hasse-Minkowski/$\mathbb{Q}$

→ Maximal lattice finding.

→ Local invariants (std ⟷ GHY)

→ Local tests (aniso dim + invs/$\mathbb{Q}_p$)

Square Classes:

→ Over local + global fields

→ Hilbert Symbol

→ Weak approx. for local-global/$\mathbb{Q}$

Quadratic Forms:

→ Neighbor method for finding all classes in Gen(Q)

→ Spinor Genera in Gen(Q)

→ Automorphism finding

Also, CS + GHY mass formulas and special values of $\zeta(s)$ + $L(s,\chi)$

Computational Challenges:

→ Dealing with non-free lattices over # fields F with $h(F) > 1$.

→ Computing local masses at $\mathfrak{p} | 2$ when 2 is ramified.

→ Local-Global for $(V, Q) / F$

→ Maximal lattice finding ($\mathfrak{p} | 2$ - neighbors)

→ Exact special values of $\zeta_F(m)$ and $L_F(m, \chi)$.

→ Enumeration of totally real F with bounded root disc.

(Voight)

Future Directions:

Finding totally definite class number one forms for other groups!

Adelic Interpretations:

① $\tau(G_F \backslash G_{\mathbb{A}}) = \#$ ← known

$\Longleftrightarrow$ Mass Formula

② $G_F \backslash G_{\mathbb{A}} / K \xleftrightarrow{1-1}$ Classes in a Genus of "objects".

<u>Ex</u>: $G = U_{2n}(H) \rightsquigarrow$ Hermitian forms H of class #1.

$G = G_2 \xrightarrow{?}$ Octonion orders of type #1.

$G = F_4 \xrightarrow{?}$ Freudenthal orders of type #1.

$G = O_n(Q) \longrightarrow$ Quadratic forms Q of class #1.

Interpreting Classes in a Genus:

$G =$ linear algebraic gp acting as isometries on $(V, \varphi)/F$.

$(L, \varphi) \subseteq$

Extra algebraic structure

Global field

Lattice with extra structure induced from (V, φ)

$G_{\mathbb{A}} :=$ adelization of G

$:= \prod_v{}' G_v$ with all but finitely many components stabilizing (L, φ).

Now $G_{\mathbb{A}}$ acts on lattices in (V, φ) by a local non-archimedean action

$$\begin{array}{ccc} g_{\mathbb{A}} : L & \dashrightarrow & L' \\ \updownarrow & & \updownarrow \\ (L_{\mathfrak{p}}) & \longmapsto & (g_{\mathfrak{p}} L_{\mathfrak{p}}) \end{array}$$

$g_{\mathbb{A}} = (g_v)$.

Then the $G_{\mathbb{A}}$-orbit of L is the set of lattices in (V, φ) which are locally isomorphic to (L, φ).

We call this the <u>genus</u> of (L, φ).

Let $K := \mathrm{Stab}_{\mathbb{A}}(L, \varphi) \subseteq G_{\mathbb{A}}$ be the adelic stabilizer of (L, φ). Then

$$G_{\mathbb{A}}/K \xleftrightarrow{\;1\text{-}1\;} \text{Genus of } L$$

$$G_F \backslash G_{\mathbb{A}}/K \xleftrightarrow{\;1\text{-}1\;} \text{Classes in the Genus of } L$$

$$\underbrace{\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot}_{\text{Finite set of points}} \quad \Longleftarrow \quad \text{Finitely many by reduction theory}$$

<u>Question:</u> When is there just one pt?

<u>Claim/Conj:</u> There are only finitely many such K over all totally real number fields F.

We consider only totally real F since we want G_v to be compact at all archimedean places.

Tamagawa Numbers and Mass Formulas:

$G =$ connected semi-simple linear algebraic group $/F$

$$\tau(G) := \mathrm{vol}\,(G_F \backslash G_{\mathbb{A}}) := \int_{G_F \backslash G_{\mathbb{A}}} d\mu_{\mathbb{A}}$$

Tamagawa number

To define $\mu_{\mathbb{A}}$ on $G_{\mathbb{A}}$ we choose a set of local Haar measures μ_v on F_v, and choose any top-degree (left) invariant non-vanishing differential "volume" form ω on G/F.

This gives a measure $\mu_{\mathbb{A}}$ on $G_{\mathbb{A}}$

$$\mu_{\mathbb{A}}(U) := \int_{U \subseteq G_{\mathbb{A}}} |\omega|_{\mathbb{A}} \cdot \prod_v d\mu_v$$

Tamagawa measure

independent of ω which is (left) $G_{\mathbb{A}}$-inv.

$\Longrightarrow$ Measure on $G_F \backslash G_{\mathbb{A}}$.

To derive a mass formula from a known Tamagawa number, write

$$G_{\mathbb{A}} = \coprod_{i=1}^{r} G_F\, a_i\, K \quad , \quad K = \mathrm{Stab}_{\mathbb{A}}(L)$$

Assume K is cpt.

$$\Rightarrow \tau(G) = \mathrm{vol}\,(G_F \backslash G_{\mathbb{A}})$$

$$= \coprod_{i=1}^{r} \mathrm{vol}\,(G_F \backslash G_F a_i K)$$

$$= \coprod_{i=1}^{r} \mathrm{vol}\,(G_F \backslash G_F a_i K a_i^{-1})$$

$$= \coprod_{i=1}^{r} \mathrm{vol}\,\big(\underbrace{(G_F \cap a_i K a_i^{-1})}_{Aut^{+}(L_i)\ <\ \infty} \backslash a K a^{-1}\big)$$

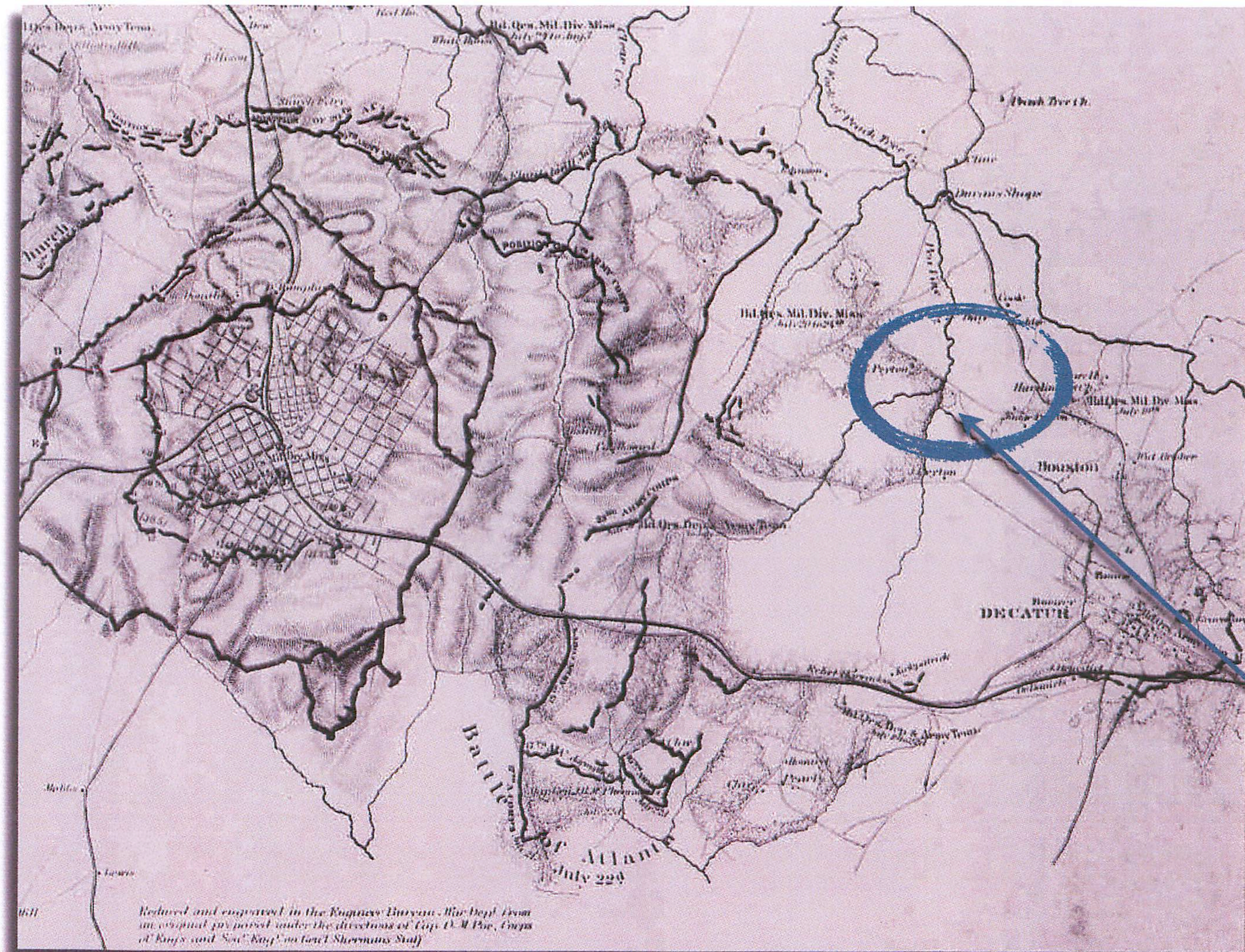
$$= \mathrm{vol}\,(a K a^{-1}) \cdot \sum_{i=1}^{r} \frac{1}{\# Aut^{+}(L_i)}$$

$$= \mathrm{vol}\,(K) \cdot \sum_{i=1}^{r} \frac{1}{\# Aut^{+}(L_i)}$$

$$\Rightarrow \sum_{i=1}^{r} \frac{1}{\# Aut^{+}(L_i)} = \tau(G) \cdot \mathrm{vol}(K)^{-1}$$

$$= 2 \cdot \prod_{v} \mathrm{vol}\,(K_v)^{-1}$$

$$= 2 \prod_{v} \beta_v(Q)^{-1}.$$



4pm
Doug Ulmer (Georgia Tech)
Constructing elliptic curves of high rank over function fields

5:15pm
Jonathan Hanke (Athens)
Using mass formulas to enumerate definite quadratic forms of class number one

at the Emory University
Math & Science Center W201

Athens-Atlanta Number Theory Seminar

Tuesday, October 20, 2009