Mass formula for non-Desarguesian planes

and a characteristic class for unimodular lattices, part I.

Alfred Rheinhold Weiss, John Atwell Moody

I. Introduction.

When we speak of projective planes, we will mean *combinatorial* projective planes. This is in the sense that it is currently beyond computer calculation to know whether it is possible to schedule students in classes with each student taking 13 classes of 13, with each pair of students having one class in common. Such a configuration cannot satisfy Pappus' and Desargues' theorems since there is no twelve-element field.

In earlier collaborations we proved that existence of a $1+n+n^2$-element projective plane is equivalent to embedding the root lattice $\sqrt{n}A_{n^2+n}$ into A_{n^2+n} in such a way that the induced action on the finite cyclic quotient group $\widehat{A_{n^2+n}}/A_{n^2+n} \cong \mathbb{Z}/((1+n+n^2)\mathbb{Z})$ is multiplication by $n+1$. The discriminant of $\widehat{A_{n^2+n}}/A_{n^2+n} \otimes \mathbb{Z}/n\mathbb{Z}$ is $1+n+n^2 \equiv 1 \; mod \; n$ and the embedding provides an isotropic subgroup of order $n^{\frac{n^2+n}{2}}$. The number-theoretic Bruck-Ryser condition on the number n is exactly the condition for a quadratic form over $\mathbb{Z}/(n\mathbb{Z})$ of discriminant 1 and dimension $\frac{n^2+n}{2}$ to have such an isotropic subgroup. When the multiplicity of a prime p in n is odd there is a nondegenerate form over $\mathbb{F}_p$ on the middle layer, when also $\frac{n^2+n}{2}$ is odd, the hyperbolic form has discriminant -1 while there is a form of dimension 2 and discriminant 1 with a nonzero isotropic vector if $-1 \; mod \; p$ is a square.

As a problem of Siegel theta series, on the other hand, this involves a symmetric matrix Ω with positive definite imaginary part; the axioms become a system of equations with one equation for each entry. We focus on specializations $\Omega = Qi$. The shift of emphasis attempts to be an allegory of the following practical observation: if a size two square matrix M has columns v, w then knowing the entries of M^tM requires knowing v^tw. But $MM^t = vv^t + ww^t$ is a sum of two parts, one completely independent of w and the other completely independent of v.

This leads to a particular calculation of what we call the 'mass' of the projective planes with $1 + n + n^2$ points as the minimum of the value of a particular coefficient of the theta series of an ordinary (positive definite rational integer) lattice of dimension N as we allow the lattice to vary.

We'll begin the analysis by describing the theta series of every unimodular (positive definite rational integral) lattice in terms of a 'characteristic polynomial' $c(M) \in \mathbb{Z}[C]$. Shimura's paper introducing half-integer modular forms appears not to have noticed that the level can be taken index three, not only level index six; rather than search the literature we make the simple improvement, and $c(M)$ is analogous to a Weierstrass polynomial. This gives an upper bound for $\mu(N)$ which is an equality if M is generic, not expected to be equality when M is unimodular, while our unimodular calculation surely can be extended later, by others perhaps, by using more of the geometric context.

All that is needed to construct $c(M)$ as it is, or let us call it $c(L)$ for a unimodular lattice L is the one series which we consider as a 'constant of nature,' $C + 24C^2 + 852C^3 + 35744C^4$.... which results by solving for q in the equation $C = \frac{1}{16}\lambda(q)(1 - \lambda(q))$. From the theta series of a formal difference $\theta([L] - [E])$ where E is the Euclidean lattice of the same rank, we evaluate the q-expansion at this 'constant of nature' series by the substitution

Corollary 12.

$$c(L) = \theta([L] - [E])(C + 24C^2 + 852C^3...) \in \mathbb{Z}[C]$$

with

$$\theta([L] - [E])(q) = \theta(L)(q)/\theta(E)(q)$$

.

Regardless of whether L may be even or odd (more correctly, even or general – there is no such thing as an odd lattice), the polynomial $c(L) \in \mathbb{Z}[C]$ then has degree at most $[N/8]$ where N is the dimension of L. The coefficients of $c(M)$ arising in this way from a change-of-coordinate automorphism in the q-expansions (C/q is a unit) give the direct formula for the number of elements of every length in a unimodular lattice of rank N in terms of the lengths of elements up

to $[\sqrt{N/8}]$. The polynomial $c(M)$, paired with the dimension N, gives a pair $(c(M), N)$ belonging to the image of the commutative group underlying a Witt ring W_0 with $\mathbb{Z}$-basis the indecomposable unimodular lattic isomorphism types, and there is an induced exact sequence of commutative groups

$$0 \to A \to W_0 \to \mathbb{Z}[[C]]^\times \times \mathbb{Z}$$

such that there is a unique largest ideal $K \subset W_0$ contained in A.

A modification where the kernel is K exactly involves including some functoriality, that is we need to apply the map $c \times rank : W_0 \to \mathbb{Z}[[C]]^\times \times \mathbb{Z}$ to a tensor product $L \otimes M$ and view M as a variable, so $c(L \otimes M)$ is a bilinear form on W_0 whose kernel is the ideal K and $c(L \otimes -)$ induces $W_0 \to (\mathbb{Z}[[C]]^\times \times \mathbb{Z})^{W_0}$ and in turn an embiedding $W_0/K \to (\mathbb{Z}^\times \times \mathbb{Z})^{W_0}$. Since K is an ideal the iamge has a ring structure with the multipication in W_0/K corresponding to a Witt operation in $(\mathbb{Z}[[C]]^\times)^{W_0}$ which distributes across multipication. One wonders whether two historical definitions of 'Witt ring' can be made to coincide. The relation with the Chern character in topology, coming from the big Witt Ring structure, might be related to the Witt structure of tensoring lattices.

Associated to each unimodular lattice of dimension N (we'll eventually apply this when the unimodlar lattice is a tensor product), is a map $\mathbb{P}^1 \to \overline{A}_N$ which we define as follows. Each element of $\mathbb{P}^1$ lifts to a point $\tau \in \mathbb{H}$ under the branched cover given by the action of the index-three subgroup of $PSl_2(\mathbb{Z})$ generated by S and T^2. Then if Q is the size N symmetric unimodular integer matrix associated to our lattice, we map each such τ to the class of $Q\tau$ in Siegel's upper half plane modulo the action of the corresponding subgroup of Siegel's modular group modulo $\{I, -I\}$. To show that the action is well-defined we need to consider $S(\tau) = \frac{-1}{\tau}$ and verify that $Q\frac{-1}{\tau}$ is in the same orbit as $Q\tau$. The block matrix $\begin{pmatrix} 0 & Q^{-1} \\ -Q & 0 \end{pmatrix}$ is integer symplectic and sends $Q\tau$ to $(0Q\tau + B)(CQ\tau + 0)^{-1}$ for $B = Q^{-1}$ and $C = -Q$ which is $Q^{-1}(-Q^2\tau)^{-1} = Q^{-1}\frac{-1}{\tau}$ and this describes the same point as $Q\frac{-1}{\tau}$ since Q and Q^{-1} define a pair of mutually dual lattices, equal because Q is unimodular. Therefore each unimodular lattice L has associated a rational curve in $\overline{A}_N$, a copy of $\mathbb{C} \cup \{\infty\}$, and the characteristic polynomial of L describes

the unique polynomial with constant coefficient 1 which has the zeroes with multiplicity agreeing with the intersection divisor of the theta divisor of $\overline{A_N}$ with the embedded rational curve.

Apart, then, from the considerations of naturality there is the crucial question of genericity which we can focus on a bit more now, in the question to what extent does the whole theta divisor depend on its intersection with this countable collection of rational curves. A lattice which is not unimodular has complex scalar multiples by elements τ in the upper half-plane. An interlinked concept is that we should consider the lattice and its dual. For tensor products, we need make no distinction when L Is unimodular between an element of a tensor product $L \otimes M$ versus a linear map of the underlying abelian groups $L \to M$. Both the inclusion of naturality needed to reduce the subgroup A to an ideal, and the inclusion of genericity that will allow us to understand whether we can include non-unimodular lattices or even algebraic and non-rational lattices, both involve replacing unimodularity with the more general concept of duality.

Two paths towards explicating the mass of finite projective planes failing Desargues' or Pappus' axioms or other features if they had been of comparable cryptographic interest, then, are that there is an evident mass formula which works for any generic M, and a the Witt operation coming from tensor product which we will require a functorial approach, and everything reduces to a simple characteristic polynomial in the unimodular case when duality degenerates. Stepping back a bit, one should say, the reason there are finiteness theorems at all in modular forms is that projective varieties are algebraic; this in turn because Laurent series in C invariant under $C \mapsto \frac{1}{C}$ are finite; this principle applies most clearly in the unimodular case, we are considering extending the direct calculation of c to tensor products and to a Zariski closure.

II. Calculation of the mass of projective planes

Let $N = 1 + n + n^2$ and let o be the all-ones column vector of size N.

1. Definition. The *mass* $\mu(N)$ of the projective planes with N points is the sum of $1/Aut(P)$ where P runs over representative of the isomorphism types of combinatorial projective planes with N points.

2. Notation For a size N square real matrix M let $Q = M^t M$ be the associated symmetric matrix. We will say Q is of *rational integral type* if the entries are rational integers or rational half-integers and the diagonal entries are integers. We define the real number $d(M) = n.trace(Q) + o^t Q o$ with n such that $N = 1+n+n^2$, and let $L \subset \mathbb{R}^N$ be the integer span of the columns of M. When we speak of the magnitude of an element of L we are referring to the Euclidean magnitude in R^N.

3. Theorem. $\mu(N)$ is equal to the $\frac{1}{2^N N!^2}$ times the minimum over square size N real matrices M of the number of ways of writing the number $d(M)$ as the sum of squared magnitude of N elements in the lattice L which is the integer span of the columns of M.

Proof. The minimum is achieved when the entries are linearly independent over $\mathbb{Q}$. Then the squared magnitudes of N elements adding to $d(M)$ decomposes into of N^2 equations saying that after possibly negating each element, the integer coefficient sequences describing these elements of L comprise the incidence matrix of a combinatorial projective plane. The number of such tuples is $2^N N!^2$ times the number of projective planes with a total ordering chosen for both points and lines. The stabilizer of an isomorphism type under permuting points and lines is the automorphism group hence the mass $\mu(N)$ is the reciprocal of this number added once for each such tuple of elements of the lattice.

In complete detail, choose for each i a linear combination of the columns of M with coefficients $v_{1,i}, ...v_{N,i}$ (which we might obtain by applying the matrix M to that column in the usual way); and if we denote the column as v_i its squared magnitude is $(Mv_i)^t Mv_i = v_i^t Q v_i$. If Q has just the (j, j) entry equal to 1 and the rest zero,

then $trace(Q) = 1$ and the entries of Q sum to 1, while the squared magnitude of the i'th vector is $v_{j,i}^2$ giving $\sum_i v_{j,i}^2 = n \cdot 1 + 1 = (n+1)$ for every j. If instead every entry of Q is taken to be 1, the sum of the squared magnitudes is $\sum_i (\sum_j v_{j,i})^2$ which is to equal $trace(Q) + o^t Q o = n + (1+n+n^2)^2 = (n+1)^2(1+n+n^2)$. If for any one value of i, the absolute value $|\sum_j v_{j,i})|$ were less than $(n+1)$ surely its square would be less than $(n+1)^2$ and there would need to be a different index i' such that $(\sum_j v_{j,i'})^2$ is larger. Then $|\sum_j v_{j,i'}| > n+1 = \sum_j v_{j,i'}^2$. Now one asks, how can a sum of numbers be strictly decreased in magnitude by squaring each number; it cannot. Thus for all i, $|\sum_j v_{j,i}| = n+1 = \sum_j v_{j,i}^2$. This means all $v_{j,i} \in \{-1, 0, 1\}$ and for each i exactly $n+1$ of the $v_{j,i}$ are not zero, and these are all either equal to 1 or equal to -1. There are 2^N solutions for each basic solution in which all $v_{j,i} \in \{0, 1\}$ by multiplying all $v_{j,i}$ by 1 or -1 for all j, for each fixed i. From now on we will only consider such basic solutions with positve entries. Looking at a basic solution, we consider the case when Q has just a pair of nonzero off-diagonal entries in rows a, b. We have $trace(Q) = 0$, $oQo^t = 2$ and $\sum_i v_{a,i} v_{b,i} + v_{b,i} v_{a,i} = 2$, meaning $\sum_i v_{a,i} v_{v,i} = 1$. The rule from before when $j = a$ and $j = b$ gives $\sum_i v_{a,i}^2 = n+1 = \sum_i v_{b_i}^2$ and when we revisit these knowing all $v_{j,i} \in \{0, 1\}$ it tells us that if we assembled the $v_{j,i}$ into a matrix, each row now would have $n+1$ entries of 1 and the rest zero, while the fact $\sum_i v_{a,i} v_{b,i} = 1$ tells us that the rows have one entry of 1 in common exactly. Therefore the rows satisfy the axioms of a projective plane and it follows easily now that the columns also do.

4. Remark. The minimum is achieved generically, thus it is achieved for our (positive definite) matrices arbitrarily close to any particular integer matrix. It is also achieved for a (large) nonempty set of matrices M such that additionally Q is rational integral type, thus

5. Corollary. Writing $q = e^{i\pi\tau}$ we have that $\mu(N)$ occurs as the minimum value, as M ranges even with the restriction that $Q = M^t M$ is rational integral type, of the coefficient of $q^{i\pi d(M)\tau}$ in the q expansion of $\frac{1}{2^N N!^2}\theta(M,\tau)^N$ where $\theta(M,\tau) = \sum_{v \in L} e^{i\pi|v|^2\tau}$.

The significance of M having 'rational integral type' is that it is equivalent to the exponents in the q expansion of $\theta(M)$ being whole

numbers. A more usual, and stronger, condition is that M is (rational) 'integral' which is equivalent to all entries of $Q = M^t M$ itself being whole numbers. These definitions and properties are actually properties of Q or even L and do not depend on the choice of M however we find it helpful to visualize columns of a particular matrix M in $\mathbb{R}^N$.

III. Half-integer weight

Some discussions of half-integer weight such as Shimura's first paper focus on $\Gamma_0(4)$ which becomes $\Gamma(2)$ if we use the Jacobi definition of $\theta(\tau)$, without the extra factor of 2; while the most useful cocycle extends rather to the larger index three subgroup H of the modular group containing both $\Gamma(2)$ and the element S; rather than get involved with invariants of various smaller subgroups one can work equivariantly for the action of this group H on the full ring of entire holomorphic functions $\mathbb{H} \to \mathbb{C}$.

The group $PSl_2(\mathbb{Z})$ acts on $\mathbb{H}$ of course, and it acts on the Riemann sphere where the action is determined by its permutation of $0, 1, \infty$. The λ function $\mathbb{H} \to \mathbb{P}^1$ is equivariant for this action, so it is compatible with the group homomorphism $PSl_2(\mathbb{Z}) \to Sl_2(\mathbb{F}_2) = S_3$.

The only cocycle that is needed will be a cocycle with values in the entire holomorphic functions on $\mathbb{H}$, but it does not extend meaningfully to the whole group $PSl_2(\mathbb{Z})$, rather only on the index-three subgroup which I call H, which is the inverse image of the cyclic group $\{1, S\}$ under reduction modulo two.

The extension is split, the same group $\{1, S\}$ can be interpreted as a subgroup of $PSl_2(\mathbb{Z})$.

The subgroup H of index three is generated by T^2, S and the cocycle c sends T^2 to the identity and both S to $1/\sqrt{i\tau}$, the entire holomorphic function on H where the branch of square root is chosen so the value at i is 1.

The non-extendability of the cocycle is very important and it explains the only reason anyone ever needed to use any congruence subgroups.

The invariants of the group action of H twisted by c and its positive powers (composing c with the i'th power map on functions) describe a graded ring; its labelling half-integers (instead of using the actual power of c is now only a historic artefact.

Knowing the 'graded truncation' to degrees an integer multiple of

the whole number 2 gives enough information to show that the theta series of any unimodular integral (positive definite) lattice can be expressed as a power of the theta series of $\mathbb{Z}$ itself times what is a priori a rational polynomial in $C = \frac{1}{16}\lambda(1-\lambda)$. The terms of degree a whole multiple of two in the H invariants for the twisted action is a polynomial algebra with a generator in degree two and a generator in degree four and we will take care of both odd integer and half-integer parts and the degree-two generator all by passing modulo isomorphism types of Euclidean lattices.

Let $S, T \in PSl_2(\mathbb{Z})$ be the matrices $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ considered modulo $\{I, -I\}$. The group acts on the entire holomorphic functions $\mathbb{H} \to \mathbb{C}$ where $\mathbb{H}$ is the upper half plane; if we let τ be the coordinate coming from the standard embedding of the upper half plane within the plane, the action is given

$$({}^S f)(\tau) = f(\frac{-1}{\tau})$$

$$({}^T f)(\tau) = f(\tau + 1).$$

We verify that this is a legitimate action by checking that the action of $(TS)^3$ on the identity function τ sends τ to $\frac{-1}{\frac{-1}{\tau+1}+1}$ which evaluates to τ.

Next we pass to the subgroup $H \subset PSL_2(\mathbb{Z})$ which is the group of elements which reduce modulo 2 to one of the two permutation matrices. The generators of H are S, TST^{-1} and T^2, and by restriction the subgroup H continues to act on our function space.

We create the modified action of H by choosing a function $c(g)$ for $g \in H$ by the rule

$${}^g f(\tau) = c(g) f({}^g \tau)$$

The result is a group action if and only if the function c from H to the ring of entire functions on $\mathbb{H}$ satisfies the cocycle rule $c(gh) =^g c(h)c(g)$. Our group H maps onto the order-two cyclic group generated by S with kernel the normal subgroup known as $\Gamma(2)$ freely generated by T^2 and ST^2S. The rules

$$c(TST^{-1}) = c(S) = \frac{1}{\sqrt{-i\tau}}, \quad c(T^2) = 1$$

uniquely define a cocycle. It cannot be considered a 'pullback' from the cyclic group of order two because the original action does not descend, even while it is determined by its values at these three elements. Note for example $c(ST) =^S c(T)c(S) = 1 \cdot c(S) = c(s)$ while $c(TS) =^T c(S)c(T) =^T c(S)$ is $\frac{-1}{-i(\tau+1)}$. Here by $\sqrt{-i\tau}$ we refer to the square root branch such that $1 = \sqrt{-i\tau}$ when $\tau = i$. The only relation we need to check is

$$^S c(S)c(S) =^S (\frac{1}{\sqrt{i\tau}})\frac{1}{\sqrt{i\tau}}$$

$$= \frac{1}{\sqrt{\frac{-i}{\tau}}}\frac{1}{\sqrt{i\tau}} = 1$$

which does hold due to our choice of branch for the square root function.

There are also the powers of c where we write $c^i(g) = c(g)^i$. The direct sum of the invariant holomorphic functions for all the (positive) powers of c comprise a graded ring, it is conventional to let the invariants for the action using c^i be given degree $\frac{i}{2}$; of course the notation exists for historical reasons. The invariants of degree a whole even number for the normal index two subgroup $\Gamma(2)$ are very well-known, they comprise a polynomial algebra generated by what we shall call $x = \theta(\tau)^4$ and $y = \theta(\tau+1)^4$. The invariants of H on this whole-number-even degree subring are the same as the invariants of the cyclic group action of S on the same ring. It fixes x and sends y to

$$-\tau^{-2}\theta(1-\frac{1}{\tau})^4$$

In terms of the two-variable theta function $\theta(z,\tau) = \sum e^{i\pi n^2\tau+2i\pi nz}$ the Jacobi sum identity says $\theta(0,\tau)^4 = \theta(1/2,\tau)^4 + e^{i\pi\tau}\theta(\tau/2,\tau)^4$. Each value of the two-variable theta function in the Jacobi formula can be rewritten in terms of the single variable function $\theta(\tau) = \theta(0,\tau)$, as

$$\theta(1/2,\tau) = \theta(1+\tau)$$

$$e^{i\pi\tau/4}\theta(\tau/2,\tau) = (i\tau)^{-1/2}\theta(1-\frac{1}{\tau}).$$

For the first equation both sides represent different expressions for the same sum, the sum over integers n of the quantity $e^{i\pi n^2\tau+i\pi n}$

(which also happens to be the alternating sum of the $e^{i\pi n^2\tau}$). For the second equation, the left side is the sum over integers n of $e^{i\pi\tau\ (n^2+n+1)}$. Since $e^{i\pi/4}\tau^{-1/2} = \frac{1}{\sqrt{-i\tau}}$ the right side is the transform of $\theta(\tau)$ using the action of S and the cocycle c. Taking fourth powers and substituting we see

$$\theta(\tau)^4 = \theta(1+\tau)^4 + (-\tau^{-2})\theta(1-1/\tau)$$

$$= \theta(1+\tau)^4 +^S \theta(1+\tau)^4.$$

From this

$$^S\theta(1+\tau)^4 = \theta(\tau)^4 - \theta(1+\tau)^4$$

Remembering that we are writing $x = \theta(\tau)^4$ and $y = \theta(1+\tau)^4$ and that $^Sx = x$ this gives $^Sy = x - y$ and $^S\lambda = 1 - \frac{^Sy}{x} = 1 - \frac{x-y}{x} = \frac{y}{x} = 1 - \lambda$. As S sends the ideal points 1 to -1 in the upper half plane which both map to $[y : x] = [1 : 0]$ the point at infinity, while λ by $^S\lambda = 1 - \lambda$ makes λ S-equivariant. More generally λ is equivariant for the action of $PSl_2(\mathbb{Z})$ on $\mathbb{H}$ inducing the action on $\mathbb{P}^1$ preserving $\{0, 1, \infty\}$ for which $\Gamma(2)$ is the stabilizer of λ. Now from the rules $^Sx = x$, $^sy = (x - y)$ we see also that

6. Theorem. The terms of weight a whole multiple of two in the ring of half-integer modular forms for the cocycle c is the same as the ring of ordinary modular forms of weight a whole multiple of two for the index three subgroup $H \subset PSl_2(\mathbb{Z})$. The group H is generated by $\Gamma(2)$ and the element S, and the ring of modular forms of degree a whole multiple of two and level H is freely generated by the following elements of weight 2 and 4:

$$\theta(\tau)^4$$

$$\theta(\tau)^4\theta(1+\tau)^4 - \theta(1+\tau)^8$$

IV. Relation with modular forms of lattices.

Let M be a real square matrix of size N with nonzero determinant and L the column span of M in Euclidean space $\mathbb{R}^N$.

Proposition 7. $\theta(M, \frac{-1}{\tau}) = (-i\tau)^{N/2}(\frac{1}{det(M)})\theta(M', \tau)$ where $M' = (M^t)^{-1}$.

Proof. The dual basis of $\mathbb{R}^N$ to the columns of M is the columns of M' and this is the standard Poisson summation argument.

We write $\theta(\tau)$ for $\theta(M, \tau)$ when M is the size-one identity (this is the classical theta function which Jacobi had denoted θ_3).

8. Corollary. If $Q = M^t M$ is rational integral of determinant 1 (so L is what is called a 'unimodular lattice') then $\theta(M, \frac{-1}{\tau}) = (-i\tau)^{N/2}\theta(M, \tau)$ and is therefore an element in our ring of modular forms invariant for the twisted action of H.

Proof. To say M and M' have the same column span (image) is to say $M'^{-1}M$ is invertible with integer entries, and $M'^{-1}M = M^t M = Q$.

Thus

9. Lemma. Let $e, f \in \{0, 1, 2, 3\}$ such that $e \equiv -N \ mod\ 4$ and $f \equiv -N^2 \ mod\ 4$. For M as above

i) There is a unique polynomial $P(X, Y)$ with rational coefficients which has degree $\frac{1}{4}(N + e)$ if we assign X to degree 1 and Y to degree 2, such that $\theta(\tau)^e\theta(M, \tau) = P(\theta(\tau)^4, \theta(\tau)^4\theta(1 + \tau) - \theta(1 + \tau)^8)$.

ii) Writing λ for the modular lambda function (of τ) we have $\theta(M, \tau) = \theta(\tau)^{N+e}P(1, \lambda(1 - \lambda))$. hence

$$\frac{1}{2^N N!^2}\theta(M, \tau)^N = \frac{1}{2^N N!^2}\theta(\tau)^{N(N+e)}P(1, \lambda(1 - \lambda))^N.$$

iii) The coefficient of $e^{i\pi\tau\ d(M)}$ in the q expansion of this function an upper bound for the mass $\mu(N)$ which is equal to the stable part of the coefficient which remains while M is perturbed

transcendentally (without preserving for example its determinant).

We will simplify the analysis in terms of a single variable polynomial and the rank in a later section. The number $d(M)$, the sum of the squared lengths of the columns of M added to the squared length of the column sum, always exceeds N. The Bruck-Ryser condition (which can be proved by considering lattices modulo n^2) gives arbitrarily large values of n such that there is no projective plane with $1+n+n^2$ points. There must be an associated lattice realizing this bound. We can always choose M so that one column is minimal length. Therefore a lattice realizing the bound in the cases when $\mu(N) = 0$ cannot have an increasing sequence of coefficients of its theta series.

10. Remark. Rains and Sloane proved that once $N \geq 24$ a unimodular lattice has a point of squared norm less than or equal to $2[N/24]+2$. Therefore for a unimodular lattice we can always choose M to have a column of squared length $\leq 2[N/24] + 2$.

V. Remarks and caution about Riemann theta relations

By choosing perpendicular elements $f_1, ..., f_N \in L$ spanning a sublattice of finite index, with coset representatives a_α, we can write $\theta(M,\tau)$ in terms of the two-variable theta function $\theta(z,\tau) = \sum_{n=-\infty}^{\infty} e^{i\pi n^2\tau + 2i\pi nz}$ as a sum with terms indexed by α, with each term being a sum over the corresponding coset. We obtain

$$\theta(M,\tau) = \sum_\alpha e^{i\pi\tau|a_\alpha|^2} \prod_i \theta(\langle e_\alpha, f_i\rangle\tau, |f_i|^2\tau)$$

corresponding with the expression $|a_\alpha + \sum n_i f_i|^2 = |a_\alpha|^2 + 2\sum n_i\langle f_i,\ a_\alpha\rangle + \sum n_i^2 |f_i|^2$

For $\theta(M,\tau)^N$ instead of only taking the N'th power of this, we can also use a finite index sublattice of $L^{\oplus N}$ which needn't respect the direct sum decomposition.

This formula can be used to calculate the theta series of a tensor product and in principle can answer the question whether the group theoretic kernel in W_0 is an ideal. In any case in a later section we define a possibly smaller subgroup which is guaranteed to be an ideal and give a different formula for the theta series of a tensor product.

VI. A 'characteristic class' and big Witt vectors

The rational functions which we considered can be viewed as elememnts of the polynomial ring in one variable, let us call it $C = \frac{1}{16}\lambda(1-\lambda)$ and for each lattice of rank N with $e \in \{0,1,2,3\}$ such that $e \equiv -N \ mod\ 4$ we obtain a polynomial with $\mathbb{Q}$-entries of degree at most $\frac{N+e}{8}$ in the variable C. This is because for M unimodular of rank N such that $Q = M^tM$ is rational integral $\theta(M,\tau)\theta(\tau)^e = P(X,Y)$ with P homogeneous of degree $\frac{N+e}{4}$ if we give $X = \theta(\tau)^4$ degree one and $Y = \theta(\tau)^4\theta(1+\tau)^4 - \theta(1+\tau)^8$ degree two. Then $P(1, Y/X^2)$ becomes an ordinary polynomial in C which we will call $c(M)$. The highest power of C that occurs when the polynomial $c(M)$ is simplified equals the highest power of Y that can actually occur in P, this is the whole number $\frac{N+e-4}{8}$ if $N+e \equiv 4 \ mod\ 8$ and $\frac{N+e}{8}$ if $N+e \equiv 0 \ mod\ 8$.

The theta function of a direct sum of lattices is the product of the theta functions of the lattices, and the same is true for the characteristic polynomials in C, with now any Euclidean lattice contributing the trivial factor of 1.

We might call the element $c(M) \in \mathbb{Q}[C]$ coming from a unimodular lattice of integral type spanned over $\mathbb{Z}$ by the columns of M its 'characteristic polynomial', it is reminiscent of a total Chern class. The leading coefficient in the q-expansion of C is 0 if we scale by a factor of 16 so let's define $C = \frac{1}{16}\lambda(1-\lambda) = \frac{1}{16}(16q - 128q^2...)(1 - 16q + 128q^2...)$ so for unimodular lattices of rational integral type and rank N less than 16 the only possible 'characteristic polynomial' is $a_0 + a_1C$ and $\theta(M,\tau) = \theta(\tau)^N(a_0 + a_1C)$ The numbers a_0 and a_1 in this case are just the first two coefficients in the q expansion of the polynomial $c(M) \in \mathbb{Q}[C]$ upon setting C to $\frac{1}{16}\lambda(1-\lambda)$.

We can prove that always $c(M) \in \mathbb{Z}[C]$ and summarize and justify what we have said,

11. Theorem. Any unimodular lattice (even or odd), spanned in Euclidean space by the columns of a matrix M, has an associated 'characteristic polynomial' in one variable $c(M) \in \mathbb{Z}[C]$. It is unaffected by direct sum with any Euclidean lattice, and for a lattice of dimension N the degree in C of $c(M)$ is at most $N/8$. The theta

series $\theta(M,\tau)$ is determined by its 'characteristic polynomial' $c(M)$ by replacing C by $\frac{1}{16}\lambda(1-\lambda)$ and multiplying by $\theta(\tau)^N$ leading to the simple formula

$$\theta(M,\tau) = c(M)(\frac{1}{16}\lambda(\tau)(1-\lambda(\tau)))\theta(\tau)^N.$$

where $C(M)(\frac{1}{16}\lambda(\tau)(1-\lambda(\tau))$ means the polynomial $C(M) \in \mathbb{Z}[C]$ with C evaluated at (=substituted for) the series $\frac{1}{16}\lambda(\tau)(1-\lambda(\tau)) \in \mathbb{Z}[[q]]$. The subgroup of $\mathbb{Z}[C]$ spanned as a group under addition by the $c(M)$ is a subring. All $c(M)$ have leading coefficient in the q expansion equal to 1. In this ring a direct sum of lattices corresponds to the product of their characteristic polynomials.

Proof. The only thing mentioned that was not already proved is that the rational coefficients of every $c(M) \in \mathbb{Q}[C]$ in the unimodular case are ordinary integers. The proof is similar to the observataion that Weirstrass polynomials have integer coefficients in the integral setting, write $u = \frac{C}{q}$ and consider the q-expansion of $\frac{\theta(M,\tau)}{\theta^N} \in \mathbb{Z}[q]$. It belongs to $\mathbb{Z}[uq]$ and the magic which is created by the theory of half-integer modular forms means that it is a polynomial in uq. That is to say, the sequence of coefficients of the polynomial $c(M)$ is the 'uq' expansion of $\frac{\theta(M,\tau)}{\theta^N}$ which not only has integer coefficients but happens to have only finitely may nonzero coefficients. Moreover the coefficients are $1, a_1, a_2, ...a_{[N/8]}$ are just simple transforms of the number of lattice elements of length $0, 1, \sqrt{2}, \sqrt{3}, ..., \sqrt{[N/8]}$

There is nothing mysterious about the needed unit u which induces the automorphism of $\mathbb{Z}[q]$ by substituting qu for q, which is the main step in transformation we've described of the infinite sequence of numbers of elements of each squared length into the finite sequence of coefficients of the characteristic polynomial. The unit $u \in \mathbb{Z}[[q]]$ is explicitly

$$u = \frac{(\sum_{n=-\infty}^{\infty}(-q)^{n^2})^4)\frac{1}{16q}((\sum_{n=-\infty}^{\infty}q^{n^2})^4 - (\sum_{n=-\infty}^{\infty}(-q)^{n^2})^4)}{(\sum_{n=-\infty}^{\infty}q^{n^2})^8}$$

where n ranges over all integers (including negative and zero) in each sum.

12. Corollary. In the positive-definite unimodular setting, once the number of lattice elemnts up to length $\sqrt{[N/8]}$ are written down, the number of lattice elements of all lengths are given by a direct formula (inverse the change-of-coordinate automorphism $\mathbb{Z}[[q]] \to \mathbb{Z}[[[uq]])$ The characteristic element $c(M)$ in $\mathbb{Z}[C]$ expressed in the variable C is given by

$$c(M) = \theta(M)(v^{-1}C) \sum_{j=0}^{\infty} (1 - (\sum_{n=-\infty}^{\infty} (v^{-1}C)^{n^2})^N)^j \in \mathbb{Z}[C]$$

where v is the unit $\phi(u) \in \mathbb{Z}[[C]]$ obtained by applying to the unit u pictured above (but with q replaced by C) the unique automorphism ϕ of $\mathbb{Z}[[C]]$ such that $\phi(uC) = C$.

Thus, in N dimensions the number of elements in a unimodular lattice of dimension N which have distance from the origin less than or equal to $\sqrt{[N/8]}$ determine the number of elements of every other distance from the origin.

The proof is this: start with the original equation involving the unit above $c(M)(qu) = \theta(M)(q)/\theta(q)^N$. It holds q replaced everywhere, including in the expression for u, with a formal variable C. Then $c(M)(Cu) = \theta(M)(C)/\theta(C)^N$. Finally apply ϕ and Cu becomes C on one side of the equation while C becomes $v^{-1}C$ on the other.

Incidentally, there is just one such unit $v \in \mathbb{Z}[[C]]$. If it could be written down once it will never need to be calculated ever again, it has infinitely many terms (like the difficulty with the digits of a constant of nature such as π), it cannot actually be written down once, but its definition can. The series for v begins $v = 1 - 24q - 276q^2 - 8672q^3 - 344658q^4 - 15390480q^5 - 737293560q^6 - 37026698304q^7 - 1923581395371q^8$... and when we invert, replace q by C and multiply by C we find

$$v^{-1}C = C + 24C^2 + 852C^3 + 35744C^4 + 1645794C^5 + 80415216C^6 + 4094489992C^7 + 214888573248C^8 + 11542515402255C^9 + 631467591804472C^{10}... \quad (1)$$

Also, on the right side, the factor following $\theta(M)(v^{-1}C)$ is nothing but a series expansion of the N'th power of the q-expansion of $\theta(\tau)^{-1}$ with q replaced by $v^{-1}C$. It is probably better to write the formula

$$c(M) = \theta(M)(v^{-1}C)\theta(v^{-1}C)^{-N}$$

and now the second factor is the $(1-2(v^{-1}C)+4(v^{-1}C)^2-8(v^{-1}C)^3+14(v^{-1}C)^4-24(v^{-1}C)^5+40(v^{-1}C)^6-64(v^{-1}C)^7+100(v^{-1}C)^8-154(v^{-1}C)^9+232(v^{-1}C)^{10}...)^N$ where one merely substitutes in the permanently fixed series for $v^{-1}C$ just above, which, also, come to think of it, we can do once and for all, giving

$$\text{second factor } = (1-2C-44C^2-1520C^3-62930C^4-2875004C^5-139754312C^6 \\ -7089934304C^7-371085722540C^8-19890542685160C^9-1262935183608944C^{10}...)^N \quad (2)$$

and this is a once-for-all calculation.

We should really stress this, that the two series above are universal; the same two series work together for every unimodular lattice.

It seems like we have constructed (more likely begun learning known things) some sort of racing car, almost, and one cannot wait to see if this really works.

Let's try this for the odd indecomposable twelve dimensional lattice L from the oeis database with $\theta(M) = 1+0q+264q^2+2048q^3+7944q^4+24576q^5+64416q^6+135168q^7+253704q^8+475136q^9+825264q^{10}$, we replace q by series (1) which is $C+24C^2+852C^3...$, then multiply by the second factor which is the series (2) with the exponent chosen as $N=12$ giving $c(M)$ as $1-24C+0C^2+0C^3+0C^4+0C^5+0C^6....$ Since all but two coefficients have simplified to zero, this is equal to the polynomial $1-24C \in \mathbb{Z}[[C]]$, and now that single degree-one characteristic polynomial, taken together with the rank 12, determines the theta series, it is merely the adjusted theta series of Euclidean space $(1-24C)\theta(\tau)^{12}$ upon setting $C = \frac{1}{16}\lambda(\tau)(1-\lambda(\tau))$.

It really will be true that even though the formula above is the expression of a power series in $\mathbb{Z}[[C]]$, once we replace q with C in the formula for v and substitute into the formula for $c(M)$, the unimodularity condition implies that the coefficients in $c(M)$ of of all powers of C higher than $N/8$ are zero and there is no need to caluculate them; or we can replace every q expansion here by its Taylor polynomial up to that degree (in this example, degree one) and ignore higher terms. One has a finite polynomial expression for $c(M)(C)$ in starting from only the truncated theta series of the lattice, which is the finite generating series for the number of lattice elements of length $1, \sqrt{2}, \sqrt{3}, ... \sqrt{[N/8]}$.

In the example, this means that, since all the subsequent coefficients in $1-24C$ cancel to zero we could have erased all but the first two terms of the original theta series leaving $1+0q$ ignoring anything of higher degree to find $c(M)=1-24C$; from this and the dimension the full theta series of the lattice reappears including all the higher terms $+264q^2+2048q^3+7944q^4+..$

That is to say, once $c(M)$ is written down using elements of norm no larger than $\sqrt{[N/8]}$ one can substitute $c(M)$ and N into the formula of the previous theorem to obtain the full theta series.

For another example, just from knowing the E_8 lattice is eight dimensional unimodular and has no element of length 1 its theta series begins $1+0q$ giving $c(M)=1-16C$ exactly (using just terms of degree zero and one in (1) and (2)). Then $\theta(E_8,\tau)=(1-16C)\theta(\tau)^8$ with $\theta(\tau)=(1+2q+2q^4...)$ and $1-16C=1-16^q+384q^2-4800q^3+41984q^4-290016q^5+1688064q^6-8612736q^7+39542784q^8...$ giving full expansion of the product $\theta(E_8)=1+240q^2+2160q^4+6720q^6+17520q^8...$

Calculations we find online use the fact that E_8 happens to be an even lattice, its theta series we see only now has no odd powers of q so is invariant for $q\mapsto -q$ and is hence invariant for the full modular group. We have instead used Theorem 11 relying on half-integer modular forms and the cocycle c which work for both even and odd unimodular lattices; the fact E_8 happens to be even arrives in our conclusions, not our hypotheses, we do not need to assume it anywhere. Even while 1 and $c(E_8)$ generate the polynomial ring $\mathbb{Q}[C]$ over Q there is more information when we work integrally and even more if we instead work integral-multiplicatively.

Wikipedia's table has three unimodular lattices of lattice of dimension 12, there must be one besides $\mathbb{Z}^{12}$ or $E_8\oplus\mathbb{Z}^4$. and that it has no element of length 1. We could have replaced its theta series with 1 in the formula for the characteristic polynomial, we still would have obtained $1-24C$ and hence its full theta series just from that one fact

$$(1-24C)\theta^{12}=1+0q+264q^2+2048q^3+7944q^5....$$

Comparing the new rank twelve lattice with E_8 and the Euclidean lattice, The new characteristic polynomial is a rational linear combination of the earlier two, which are 1 and $1-16C$, but remember: direct sum of lattices represents addition in W_0 but it agrees with multiplication, not addition, of theta series.

For further examples, we've coded the relevant functions in javascript at https://spectrograph.uk/modular.html. if you enter a command like $extend([1,3,5],35)$ it will write down the series whose coefficients are the only possibilities for number of elements of each squared length in a positive definite unimodular lattice of rank 35 assuming the sequence starts $1,3,5,0,0..$ The javascript answers $1+3q+5q^2+401142q^5+22277394q^6...$ and you can set the number of terms by writing for example $trunc = 15$. Or, to calculate the characteristic polynomial of the Leech lattice you can say $char(Leech,24)$ and it answers $1-48C+48C^2-4096C^3$. To do the same calculation stepwise, you get the same answer from $substitute(divide(Leech,pow(theta(),24)),qprime())$, here qrime() just always returns our 'constant of nature' series. We also could have just defined Leech to be $polyTimes(pow(theta(),24),substitute([1,-48,48,-4096],C()))$ or using the function that does this as in $unimod([1,-48,48,-4096])$. (Caution, if you copy a minus sign from here it will paste a double minus sign –).

As an example of an (inefficient) upper bound for the mass of projective planes with $1+3+3^2=13$ points, we use the lattice $E_8\oplus\mathbb{Z}^5$. The matrix Q has trace $5+18$ and sum of entries $5+6$ so $d(M)=3{\cdot}23{+}11=80$ and the 80'th coefficient of $\frac{1}{2^{13}\ 13!^2}(1-16C)\theta^5$ $=\frac{1}{317651255653438586880000}(1-16C)\theta^5$ is an upper bound for the mass of combinatorial 13-element projective planes.

As we've said already, the upper bound matches the precise mass if we allow either transcendental deformations of M or allow the ratios among the absolute values of its entries to tend to $\{0,\infty\}$. We do not expect that it would acheived if we let the lattice range over rank 13 unimodular lattices considering Remark 10; for $N=1+n+n^2$ we are counting lattice elements with the same squared norm as n times the sum of the squared norms of the generators of a fundamental parallelpiped, N in number, plus the squared norm of their sum, while for every $N\geq 24$ Rains and Sloane found nonzero lattice

elements of squared norm less than or equal to $[N/24] + 2$.

Thus the structure integrally of the Witt group of lattices is thus more interesting than the nearly unrelated $\mathbb{Q}$-span of the theta series. The abelian group in $\mathbb{Z}[[C]]^\times \times \mathbb{Z}$ spanned by the characteristic polynomials $c(M)$ paired with the ranks N to give $(c(M), N)$ is a ring because products of generators come from direct sums of lattices, and we've mentioned that the image of W_0 in $Hom(W_0, \mathbb{Z}[[C]]^\times \times \mathbb{Z})$ inherits a Witt ring structure which should be related to a big Witt vector structure on $\mathbb{Z}[[C]]$.

In Reddit posts students say, if multiplication is repeated addition and exponentiation is repeated multiplication, what comes next? In fact exponentiation is where the train goes off track. One possibility of a binary operation after addition and multiplication ought to be $a * b = a^{log(b)}$ which happens to be commutative, $a * b = a^{log(b)} = e^{log(a)log(b)} = b^{log(a)} = b * a$.

In a ring of big Witt vectors we allow more general choices. For an illustrative example which is not directly relevant, we can define the *Chern character* $ch(f)$ of a polynomial $f \in \mathbb{Q}[C]$ with $f(0) = 1$. First define ch as a function acting on elements $f \in \mathbb{C}[T]$ such that $f(0) = 1$, characterised by two axioms not very different than the axioms of the logarithm map, that that $ch(fg) = ch(f) + ch(g)$ and for any complex scalar v one has $ch(1 + vC) = e^{vC}$. The restriction of ch to $\mathbb{Q}[[C]]$ takes values in $\mathbb{Q}[[C]]$ and the Witt product $f * g$ is defined to be $ch^{-1}(ch(f)ch(g))$. As we mentioned, this particular Witt structure is not compatible with the map $c : W_0 \to \mathbb{Z}[[C]]^\times \times \mathbb{Z}$.

A completely different, third big Witt structure comes from doing the same thing but with the q-expansions – replacing C by its q-expansion rather than working directly with C.

Being able to use the case when N is odd as we can in defining the characteristic polynomial does matter as our calculation of the mass of combinatorial projective planes with N points depends on one coefficient of $\frac{1}{2^N N!^2}\theta(M, \tau)$ when N, the size of M, is odd, and the particular coefficient of $q^{d(M)}$ (recall $d(M) = trace(Q) + o^t Q o$ and $Q = M^t M$) is an upper bound for the mass of projective planes with

N points which known to be the precise upper bound, in the sense that the minimum value is the precise mass, if we allow transcendental deformations of M or, I believe, remove the unimodularity assumption. But the point is, for N even we already know that there are no combinatorial projective planes with N points.

As we observed in the introduction, the polynomial $c(L)$ for each unimodular lattice L is the unique polynomial with constant coefficient 1 whose roots with multiplicity define the divisor in $\mathbb{C} \subset \mathbb{C} \cup \{\infty\} = \mathbb{P}^1 \subset \overline{A}_N$ where the rational curve corresponding to L meets the theta divisor in $\overline{A}_N$. There is a rank N vector bundle on A_N which is not a trivial bundle even while it describes the fixed constant complex vector space spanned by each lattice, the columns of each matrix Ω with positive definite imaginary part, equivalently the real vector space spanned by those columns together with the columns of the identity matrix (which when we reduce modulo these additively give us an algebraic torus of dimension N). The Euler derivation of this vector bundle is a vector field on the universal cover of each abelian variety. We shall have to think carefully of why this vector-field which is not translation invariant has a leaf which covers all but one point of a Riemann sphere in the moduli space.

VII q'-expansions

An H-invariant holomorphic function $\mathbb{H} \to \mathbb{C}$ for a positive power of the cocycle c because it is $\Gamma(2)$ invariant for the same cocycle has an expansion as a power series in q where $q = e^{i\pi\tau}$ and also a power series expansion in $q' = e^{i\pi\frac{-1}{\tau}}$ and $q'' = e^{i\pi(\tau+1)}$. We have always brought calculations into the case when the power of c is a multiple of 4 and the case of c^4 is useful to look at. The differential form $(\sum_{n=-\infty}^{\infty} q^{n^2})^4 d\ log\ q$ is the same as the differential form $(\sum_{n=-\infty}^{\infty} q'^{n^2})^4 d\ log\ q'$. The residue of the first when $q = 0$ must be 1 and the residue of the second when $q' = 0$ must be -1 The two fourth power in the firt expression tends to 1 as $q \to 0$ and in the other tends to 1 as $q' \to 0$. In this sense it seems legal to speak of 'the q-expansion' without worrying whether we are using the variable q or q', or considering the cusp at 0 or at $i\infty$. In this sense the ring of big Witt vectors will be the same regardless of choosing q or q'.

It is a worry whether the transform by STS^{-1} can really be expressed in terms of T^2 and S. From the relation $STSTST = 1$ we have $STS = (TST)^{-1} = TST$ and multiplying by $(T^2)^{-1}$ we get TST^{-1} which is in our group H so STS and therefore ST and STS^{-1} belongs. The transform by T^2 does not even change q. Perhaps there is no need to worry about q'' since its cusp cannnot be transformed to the others using elements of $H \subset PSl_2(\mathbb{Z})$. That is to say, one could write out the theta series of a lattice using q'' as a variable, and there might be difficulties interpreting the ring of big Witt vectors among series in q'' whose initial term is 1, but this seems not to be possibly a serious worry.

VIII. The bilinear form on W_0.

By Eichler's theorem every positive definite lattice decomposes uniquely into a direct sum of indecomposable lattices so the Witt ring W_0 has canonical additive enerators. Its addition comes from direct sum and multiplication from tensor product. For each M the element $c(M) \in \mathbb{Z}[C]$ only depends on the underlying element $w \in W$ and induces a group homomorphism $c : W_0 \to \mathbb{Z}[[C]]^\times$ The rank homomorphism $W_0 \to \mathbb{Z}$ defines a second one; and the homomorphism they define together is an abelian group map $W_0 \to \mathbb{Z}[[C]]^\times \times \mathbb{Z}$. The kernel A is the additive subgroup of W_0 comprising formal differences $w - w'$ represented by lattices W, W' with the same rank and theta series. As always for an abelian subgroup of a ring, there is a unique maximal element K among the ideals of W_0 contained in A.

For $v, w \in W_0$ we may define $\langle v, w\rangle = \theta(L \otimes M, \tau)$ where L, M are lattices repreenting v, w. This defines a bilinear form, and a map of commutative groups $W_0 \otimes W_0 \to \mathbb{Z}[[C]]^\times \times \mathbb{Z}$.

13. Lemma. The isotropy subgroup of the bilinear form is the unique largest ideal of W_0 contaied in A.

Proof. The isotrpy subgroup is the set of formal differences $[L]-[L']$ where $\theta(L \otimes M, \tau) = \theta(L' \otimes M, \tau)$ for all M. Multiplying such a formal difference by a class $[N]$ gives $[L \otimes N] - [L' \otimes N]$ we apply associativity of tensor product $(L \otimes N) \otimes M \cong L \otimes (N \otimes M)$ and also for L'.

Now we can improve the analytic map, we obtain

$$W_0 \to (\mathbb{Z}[[C]]^\times \times \mathbb{Z})^{W_0}$$

where the codomain the set of abelian group maps $W_0 \to \mathbb{Z}[[C]]^\times \times \mathbb{Z}$.

14. Corollary. The image W of W_0 under the improved map has a well-defined Witt operation, which can be interpreted as a Chern character theory, correctly distributing over multiplication.

IX. Relation with existing Witt rings

The invariant $c(M)$ is quite literally a divisor on $\mathbb{P}^1$ already, the element $\frac{1}{16}\lambda(1-\lambda)$ is a rational function with two zeros and one double pole (more symmetrically, a branched cover with ramification indices $1, 1, 2$) and the theory of the Chern character applies directly and there is a Witt ring. Also the theta series of a lattice is always a specialization of the Siegel theta series, it already comes from the theta divisor on the moduli of abelian varieties, where again there is a Witt ring. Thirdly, a positive definite rational integer lattice can be interpreted as the structure on the first integer homology (which is also the fundamental group) and its dual the first cohomology of a real torus coming from choosing a flat Riemannian metric, and there is a more general theory of the arithmetic of counting geodesics.

X. Where are we now?

Up to now when the columns of a matrix M spans a lattice, we've written $\theta(M,\tau)$ for the theta series of the lattice, even while it only depends on $Q = M^tM$.

Important additional notation.

Now we will change notation, or, allow conflicting notation, that we will allow ourselves to write $\theta(Q,\tau) = \sum_v e^{\imath\pi v^t Q v}$ where v runs over integer column vectors of the appropriate size. This is what we had previously called M^tM.

Let's define a two-variable theta series depending on square matrices A, B which need not have the same size

$$\theta(A,B) = \sum_M e^{i\pi\ trace(M^tAMB)}$$

where M ranges over integer matrices of the appropriate size. One can take one of A, B to be real and the other negative definite where, in the special case they do have the same size, it agrees with the Siegel theta series. for convergence, as a formal series it is symmetric

$$\theta(A,B) = \theta(B,A).$$

The following proposition is notation for the theta series of a tensor product

15. Proposition. If A, B are integer matrices then $\theta(A\otimes B,\tau) = \theta(A^t, B\tau)$.

Proof.

$$\theta(A^t,B\tau) = \sum_M e^{i\pi\tau\ trace(M^tA^tMB)} = \sum_{i,j,k,\ell} e^{i\pi\tau\ m_{j,i}a_{k,j}m_{k,\ell}b_{\ell,i}}$$

$$= \sum_{i,j,k,\ell} e^{i\pi\tau\ m_{j,i}(a_{k,j}b_{\ell,i})m_{k,\ell}}$$

$$= \sum_{i,j,k,\ell} e^{i\pi\tau\ m_{k,\ell}(a\otimes b)_{(k,\ell),(j,i)}m_{j,i}}$$

If we take B symmetric real positive definite then $\theta(B^t\tau, A) = \theta(A, B^t\tau) = \theta(A, B\tau)$ which is the Siegel theta series for a period matrix A and the complex matrix $B\tau$ with positive definite imaginary part.

Thus

16. Corollary. The theta series of the tensor product of the positive definite latticess spanned by the columns of M, V is what we are now calling $\theta(M^tM, V^tV\tau)$, it is the Siegel theta series associated with the period lattice spanned by the columns of M evaluated at the point of Siegel half space consisting of the complex matrix $V^tV\tau$ with positive definite imaginary part.

The theta series of a tensor product of lattices is not mysterious anymore. It is a specialization of the Siegel theta function.

To understand tensor products of unimodular lattices with other lattices, we shall merely have to repeat the foregoing theory of half-integer modular forms in the more general Siegel setting.

The Siegel theory has some built-in asymmetry, where one lattice is considered to describe a point in half-space while the other describes periods of an abelian variety, and some needless symmetry where the size of A and B must be equal. There is perhaps no harm in considering a pair of abelian varieties and it is no longer seeming ridiculous to think that the Witt theory which we seek may relate to the existing theory of characteristic classes in cohomology or sections of vector bundles in algebraic geometry.

Also, switching the tenssor factors allows that we might study non-unimodular lattices through how they behave under tensor product with those which are unimodular. It is reminiscent of the comment in the introduction that when M is a square size two integer matrix with columns u, v the product M^tM has entries like u^tv while the product MM^t is a sum of two non-interacting parts vv^t and uu^t

Also, the more functorial version of theta series we were mentiioning perhaps earlier, $\theta(L \otimes (-), \tau)$ which are functions assigning to any

other lattice L' the element $c(L \otimes M) \in \mathbb{Z}[[C]]^\times \times \mathbb{Z}$ are really nothing new, just an updated or more functorial way of understanding the Siegel theta series. And the ideal $K \subset W_0$ which we found earlier just comprises the set of formal differencese $[L] - [L']$ of unimodular lattices whose Siegel modular forms agree on the subvariety comprising scalar multiples of real positive definite matrices by scalars in the one-dimensional upper-half plane.

X. Conclusion.

It not likely in the unimodular rational integral type context where the modular forms technique applies directly, even for large N, that $\mu(N)$ should actually equal to the minimum value of the coefficient of $e^{i\pi\tau\ d(M)}$ or merely an upper bound. This is because forcing Q to be integral removes any possibility of transcendental genericity, and including the further condition $det(M) = det(Q) = 1$ does not allow the ratios among entries of Q to have magnitudes tending to $\{0, \infty\}$. That is to say, it is not yet known whether a transcendental deformation is needed to split off the meaningful stable part of the coefficient.

Although the direct combinatorics of the projective planes question is beyond computer calculation even in cases like $n = 12$ currently, we have defined the mass of projective planes with N points which is zero if and only if there are no combinatorial projective planes (not even those allowed to fail Pappus' and Desargues' conditions) with N points, and we have identified the mass as the minimum value as M ranges of a particular coefficient of a power series (q-expansion) which we have described in general terms, and shown when M is unimodular and $Q = M^t M$ is rational integral type, the series is a power of the classical theta function times the integer polynomial $c(M)$.

The homomorphism c from the underlying additive group of W_0 to $\mathbb{Z}[[C]]^\times \times \mathbb{Z}$ sends the class of each actual unimodular lattice to a polynomial, the 'characteristic polynomial' $c(w) \in \mathbb{Z}[C]$ determined by the number of lattice elements of length up to $[\sqrt{N/8}]$ where N is the dimension, paired with its dimension N.

We also gave the explicit coset formula for the θ series of a lattice given a finite index lattice spanned by perpendicular elements, in terms of the two-valued theta functions and only the coset representatives and lengths of the basic elements. And we gave direct formulas for the theta series in terms of the characteristic polynomial $c(M)$ and for the characteristic polynomial in terms of the number of lattice elements of distance up to $\sqrt{\ [N/8]\ }$ from one fixed origin.

While the additive span of the $c(M)$ in $\mathbb{Z}[C]$ is a ring, the multiplicative 'span' of the $c(M)$ in $\mathbb{Z}[C]^\times \times \mathbb{Z}$, coming as it does from all unimodular lattices is the one relevant to the problem of piecing together the axioms of a combinatorial projective plane from the disparate information coming from each particular choice of M, as we have outlined, and which may or may not require even more genericity than requiring M to be positive unimodular. The kernel A of $W_0 \to \mathbb{Z}[[C]]^\times \times \mathbb{Z}$ is a subgroup and the largest ideal K in A is the kernel of $W_0 \to Hom(W_0, \mathbb{Z}[[C]]^\times \times \mathbb{Z})$ which must then admit a theory of Chern characters. For $d(M) = N\ trace(M) + o^t M o \in \mathbb{Z}$ the coefficient of $q^{d(M)}$ in $c(M)\theta^N$ is an upper bound of the mass of projective planes with N points. That is to say each unimodular lattice of dimension N provides very explicit upper bound for the mass of projective planes with N points in terms of the characteristic polynomial, but we do not know if the minimum over unimodular lattices is the precise mass. It will certainly be possible to extend the detailed calculation beyond the unimodlar case and there, generically in M, the inequality is shown by us to be an equality which calculates the precise mass in principle but less explicitly.