The Geometry of Numbers

Rahbar Virk
Department of Mathematics
University of Wisconsin
Madison, WI 53706
virk@math.wisc.edu

March 3, 2007

Introduction

Plato said *God is a geometer*. Jacobi changed this to *God is an arithmetician*. Then came Kronecker and fashioned the memorable expression, *God created the natural numbers, and all the rest is the work of man* [Burton]. These words may sometimes give us the impression that geometry and number theory are disparate fields, on the contrary, some of the most powerful methods in arithmetic rely on geometric results. One such result is Minkowski's Convex Body Theorem. In this paper we will outline a proof of this result and indicate how it has applications to number theory. Specifically we will give a short proof of Fermat's Four Squares problem using Minkowski's Theorem and also outline the theorem's applications to algebraic number theory.

(Note: the proofs presented here follow the outlines in [Stewart], we fill in additional details when neccessary.)

Lattices

Let $e_1, \ldots, e_m$ be a linearly independent set of vectors in $\mathbb{R}^n$. The additive subgroup of $(\mathbb{R}^n, +)$ generated by $e_1, \ldots, e_m$ is called a *lattice of dimension m, generated by $e_1, \ldots, e_m$*. Note that a lattice of dimension m is a free abelian group of rank m. If L is a lattice generated by $\{e_1, \ldots, e_m\}$ we define the *fundamental domain* T to consist of all elements $\sum a_i e_i \, (a_i \in \mathbb{R})$ for which $0 \leq a_i < 1$, notice that this depends on the choice of generators.

Let $\mathbf{S}$ denote the set of all complex numbers of modulus 1, under multiplication $\mathbf{S}$ is a group and is called the *circle group*. Let $\mathbf{T}^n$ denote the direct product of n copies of $\mathbf{S}$, and call this the *n-dimensional torus*.

Theorem 1. *If L is an n-dimensional lattice in $\mathbb{R}^n$ then $\mathbb{R}^n/L$ is isomorphic to the n-dimensional torus $\mathbf{T}^n$*

Proof. Let $\{e_1, \ldots, e_n\}$ be the generators for L. Now $\{e_1, \ldots, e_n\}$ is a $\mathbb{R}$-basis for $\mathbb{R}^n$. Define $\phi : \mathbb{R}^n \to \mathbf{T}^n$ by

$$\phi(a_1 e_1 + \cdots + a_n e_n) = (e^{2\pi i a_1}, \ldots, e^{2\pi i a_n})$$

Now ϕ is an onto homomorphism with kernel of L, hence by the group isomorphism theorems the result follows. □

Note that when we restrict the theorem to the one dimensional case and the the lattice to $\mathbb{Z}$ we get that the quotient group $\mathbb{R}/\mathbb{Z}$ is isomorphic to the circle group $\mathbf{S}$.

Also note that the map ϕ as defined in the previous theorem, when restricted to the fundamental domain T, yields a bijection $T \to \mathbf{T}^n$.

The *volume* $v(X)$ of a subset $X \subseteq \mathbb{R}^n$ is defined as the value of the multiple integral

$$\int_X dx_1 \dots dx_n$$

where $(x_1, \dots, x_n)$ are cartesian coordinates. Note that the volume only exists when the integral does.
Let $L \subseteq \mathbb{R}^n$ be a lattice of dimension n, so that $\mathbb{R}^n/L \cong \mathbf{T}^n$. Let T be a fundamental domain of L. We previously noted the existence of a bijection

$$\phi : T \to \mathbf{T}^n$$

For any subset X of T define the *volume* $v(X)$ by

$$v(X) = v(\phi^{-1}(X))$$

which exists if and only if $\phi^{-1}(X)$ has a volume in $\mathbb{R}^n$.

Theorem 2. *Let $\gamma : \mathbb{R}^n \to \mathbf{T}^n$ be the natural homomorphism with kernel L. If X is a bounded subset of $\mathbb{R}^n$ and $v(X)$ exists, and if $v(\gamma(X)) \neq v(X)$, then $\gamma|_X$ (γ restricted to X) is not injective.*

Proof. Assume $\gamma|_X$ is injective. Now X, being bounded, intersects only a finite number of the sets $T + l$, for T a fundamental domain and $l \in L$. Put

$$X_l = X \cap (T + l)$$

Then we have

$$X = X_{l_1} \cup \dots \cup X_{l_n}$$

For each l_i define

$$Y_{l_i} = X_{l_i} - l_i$$

so that $Y_{l_i} \subseteq T$. We claim that the Y_{l_i} are disjoint. Since $\gamma(x - l_i) = \gamma(x)$ for all $x \in \mathbb{R}^n$ this follows from the assumed injectivity of γ. Now

$$v(X_{l_i}) = v(Y_{l_i})$$

for all i. Also

$$\gamma(X_{l_i}) = \phi(Y_{l_i})$$

where ϕ is the bijection $T \to \mathbf{T}^n$. Now we compute:

$$\begin{aligned} v(\gamma(X)) &= v(\gamma(\cup X_{l_i})) \\ &= v(\cup Y_{l_i}) \\ &= \sum v(Y_{l_i}) \qquad \text{by disjointness} \\ &= \sum v(X_{l_i}) \\ &= v(X) \end{aligned}$$

which is a contradiction. □

Minkowski's Theorem

A subset $X \subseteq \mathbb{R}^n$ is *convex* if whenever $x, y \in X$ then all points on the straight line segment joining x to y also lie in X. Equivalently, X is convex if, whenever $x, y \in X$, the point

$$\lambda x + (1 - \lambda)y$$

belongs to X for all real λ, $0 \leq \lambda \leq 1$. A subset $X \subseteq \mathbb{R}^n$ is *(centrally) symmetric* if $x \in X$ implies $-x \in X$, i.e X is invariant under reflection in the origin.

Theorem 3 (Minkowski's Theorem)**.** *Let L be an n-dimensional lattice in $\mathbb{R}^n$ with fundamental domain T, and let X be a bounded symmetric convex subset of $\mathbb{R}^n$. If*

$$v(X) > 2^n v(T)$$

then X contains a non-zero point of L.

Proof. Double the size of L to obtain a lattice $2L$ with fundamental domain $2T$ of volume $2^n v(T)$ (note that this is equivalent to shrinking X linearly by a half, and hence reducing its volume by a factor of 2^n). Consider the torus

$$\mathbf{T}^n = \mathbb{R}^n / 2L$$

By definition of volume

$$v(\mathbf{T}^n) = v(2T) = 2^n v(T)$$

Now the natural map $\gamma : \mathbb{R}^n \to \mathbf{T}^n$ cannot preserve the volume of X since this is strictly larger than $v(\mathbf{T}^n)$: since $\gamma(X) \subseteq \mathbf{T}^n$ we have that

$$v(\gamma(X)) \leq v(\mathbf{T}^n) = 2^n v(\mathbf{T}) < v(X)$$

It follows by Theorem 2 that $\gamma|_X$ is not injective. Hence there exist $x_1 \neq x_2$, $x_1, x_2 \in X$, such that

$$\gamma(x_1) = \gamma(x_2) \tag{1}$$

or equivalently

$$x_1 - x_2 \in 2L$$

But $x_2 \in X$, so $-x_2 \in X$ by symmetry; and now by convexity

$$\frac{1}{2}(x_1) + \frac{1}{2}(-x_2) \in X$$

or

$$\frac{1}{2}(x_1 - x_2) \in X$$

But by Equation 1 we already have that

$$\frac{1}{2}(x_1 - x_2) \in L$$

□

We have mentioned earlier that the fundamental domain of a lattice is dependant on the choice of basis, however, the volumes of all these distinct fundamental domains are equal. We now prove this and give a nice expression for the volume of the fundamental domain.

Lemma 4. *Let L be an n-dimensional lattice in $\mathbf{R}^n$ with basis $\{e_1, \ldots, e_n\}$. Suppose*

$$e_i = (a_{1i}, \ldots, a_{ni})$$

Then the volume of the fundamental domain T of L defined by this basis

$$v(T) = |det(a_{ij})|$$

Proof. We have that

$$v(T) = \int_T dx_1 \ldots dx_n$$

Define new variables by

$$x_i = \sum_j a_{ij} y_j$$

The Jacobian of this transformation is equal to $det(a_{ij})$, and T is the set of points $\sum a_{ij} y_i$ with $0 \leq y_i < 1$. By the transformation formula for multiple integrals [Apostol] we have that

$$\begin{aligned} v(T) &= \int_T |det(a_{ij})| dy_1 \ldots dy_n \\ &= |det(a_{ij}) \int_0^1 dy_1 \ldots dy_n \\ &= |det(a_{ij})| \end{aligned}$$

□

Corollary 5. *The volumes of the distinct fundamental domains of a lattice are all equal*

Proof. From the theory of free abelian groups we know that bases of a lattice (a free abelian group) are related by a unimodular matrix, so the result follows on applying the previous theorem. For further details see [Stewart] □

Corollary 6. *Let L be an n-dimensional lattice in $\mathbf{R}^n$, with basis $\{e_1, \ldots, e_n\}$ and*

$$e_i = (a_{1i}, \ldots, a_{ni})$$

where each $a_{ij} \in \mathbb{Z}$, then the volume of the fundamental domain T is given by

$$v(T) = |\mathbb{Z}^n / L|$$

Proof. Again from the theory of free abelian groups we have that

$$|\mathbb{Z}^n / L| = |det(a_{ij})|$$

where $\{e_1, \ldots, e_n\}$ is a basis for L and

$$e_i = (a_{1i}, \ldots, a_{ni})$$

For further details see [Stewart] □

The Four Squares Theorem

We now give a traditional application of Minkowski's theorem to giving a short and elegant proof of Fermat's Four Squares Theorem.

Theorem 7. *Every positive integer n is expressible as the sum of four squares.*

Proof. (Note: throughout this proof we assume p is an odd prime as $2 = 1^2 + 1^2 + 0 + 0$) We claim that the congruence

$$u^2 + v^2 + 1 \equiv 0 \pmod{p}$$

has a solution u, v in the integers. This is because both u^2 and $-1 - v^2$ take on $(p+1)/2$ values as u, v run through $0, \ldots, p-1$;So we have some u, v that satisfy

$$u^2 + v^2 + 1 \equiv 0 \pmod{p}$$

Consider the lattice L in $\mathbb{R}^4$ consisting of $(a, b, c, d) \subseteq \mathbb{Z}^4$ such that

$$c \equiv ua + vb, \qquad d \equiv ub - va \pmod{p}$$

It is easy to verify that the fundamental domain has volume p^2 Now a 4-dimensional sphere, center the origin, has volume $\frac{\pi r^4}{2}$, and if we choose to make r^2 say $1.9p$, then this is greater than $16p^2$. So applying Minkowski's Theorem there exists a non-zero lattice point (a,b,c,d) in this 4-sphere, so:

$$a^2 + b^2 + c^2 + d^2 \leq r^2 = 1.9p < 2p$$

Now modulo p, we have

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &\equiv a^2 + b^2 + (ua + vb)^2 + (ub - va)^2 \\ &\equiv a^2 + b^2 + u^2a^2 + v^2b^2 + 2uavb + u^2b^2 + v^2a^2 - 2ubva \\ &\equiv (a^2 + b^2)(1 + u^2 + v^2) \\ &\equiv 0 \end{aligned}$$

Thus, as $0 \neq a^2 + b^2 + c^2 + d^2 < 2p$ we have that:

$$a^2 + b^2 + c^2 + d^2 = p$$

So we have the required result for all primes, now using the fundamental theorem of arithmetic and the following identity due to Euler:

$$\begin{aligned} & (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) \\ = \; & (aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2 \\ + \; & (aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2 \end{aligned}$$

we have that the result holds for all positive integers. □

Minkowski's Theorem and the Theory of Algebraic Numbers

In this section we assume that the reader has a working knowledge some familiarity with algebraic number theory. Full details can be found in [Stewart], [Lang] and [Hardy and Wright].

Quoting [Stewart]: 'Algebraic Number Theory' can be read in two distinct ways. One is the theory of numbers viewed algebraically, the other is the study of algebraic numbers. Both apply here. The focus of algebraic number theory is to extend the properties of the natural numbers to more general number structures: algebraic number fields, and their rings of algebraic integers. These structures have most of the standard properties that we associate with ordinary whole numbers, but some subtle properties sometimes fail to generalize. One particular property that fails to generalize and can be problematic is that of unique factorization.

The notion of prime in the regular whole numbers can be viewed as two different ideas. First is the notion of being 'irreducible' in the sense that a prime has no factors other than 1 and itself. The second being that if p is a factor of a product ab then it must be a factor of either a or b. It turns out that in certain number fields these ideas do not concide. In an integral domain a prime is always irreducible but the reverse is not always true, as a result unique factorization into irreducibles breaks down. The factorization of ideals in such rings turns out to be more satisfactory: every ideal is a unique product of prime ideals. The extent to which factorization in these rings is not unique can be 'measured' by the group of ideal classes (fractional ideals modulo principal ones). This group of ideal classes is called the *class group* and its order: called the *class number* turns out to be of crucial importance in the theory of numbers and many deep and delicate results are related to its arithmetic properties. For instance unique factorization holds in a ring of integers if and only if the class number is 1. In general the larger the class number the more 'non-unique' the factorization.

Due to length restrictions on this paper we cannot go into full explanations but the following are two important results on the class group that utilize Minkowski's Theorem. For full details we again refer the reader to [Stewart], [Lang] and [Hardy and Wright].

Theorem 8. *The class group of number field is a finite abelian group. The class number h is finite.*

Theorem 9. *Every non-zero ideal of the ring of integers is equivalent to an ideal whose norm is* $\leq (\frac{2}{\pi})^t \sqrt{|\Delta|}$.

References

[Hardy and Wright] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*, Oxford University Press, 1954.

[Stewart] I. Stewart, D. Tall. *Algebraic Number Theory and Fermat's Last Theorem*, A.K. Peters 2002.

[Hilbert] D. Hilbert. *Geometry and the Imagination*, Chelsea Pub. NY 1952.

[Burton] D. Burton. *Elementary Number Theory*, C. Brown 1989.

[Apostol] T.M. Apostol. *Mathematical Analysis*, Addison-Wesley, Reading MA 1957.

[Lang] S. Lang. *Algebraic Number Theory*, Addison-Wesley, Reading MA 1970.