Minkowski's Convex Body Theorem

by Isabelle Bensimon

Project for MA341: Appreciation of Number Theory

Boston University, Summer Term 2009

Instructor: Kalin Kostadinov

Minkowski's Convex Body Theorem

In 1891, mathematician Hermann Minkowski (1864-1909) gave a lecture in Halle, Germany, where he introduced the lattice as the collection of points with integer coordinates in the coordinate system with perpendicular axes. This talk indicated his shift in focus from solving problems in Number Theory with geometric intuition towards "Geometrie der Zahlen," or, "the Geometry of Numbers." He defined this term to mean geometrical investigations of the lattice and associated bodies.

In an 1893 paper, Minkowski presents a theorem which defines parameters for the volume of a certain body in order for that body to contain a lattice point in the rectangular Euclidean coordinate system. He begins his paper, "In Number Theory, as in all other fields of analysis, the inspiration often comes from geometrical considerations even though at the end maybe only the analytical verification is shown." Indeed, from Minkowski's "geometrical considerations" a generation of new mathematical knowledge was derived. In essence, Minkowski laid the foundation for the modern theory of convexity.

Minkowski's Convex Body Theorem for n=2:

Let L be a lattice in $\Re^2$, where $L= \{mv_1 + nv_2 \mid m, n \in Z\}$ and v_1, v_2 are independent vectors. Let $\triangle$ be the area of a fundamental parallelogram for L. Let Ω be a convex body with $\text{Area}(\Omega) > 4\triangle$. Then Ω contains points of the lattice L other than the origin.

Before proving his extraordinary theorem, however, it is necessary to define certain terms. A subset $\Omega \subset \Re^n$ is convex if for all pairs of points $P, Q \in \Omega$, the entire line segment PQ is contained in Ω, where $PQ= \{(1-t)P + tQ \mid 0 \leq t \leq 1\}$. Furthermore, a

subset $\Omega \subset \Re^n$ is centrally symmetric if for every point $Q \in \Re^n$ contained in Ω, $-Q \in \Omega$, where -Q is the reflection of Q through the origin.

A convex body is a nonempty, bounded, centrally symmetric convex set. For example:

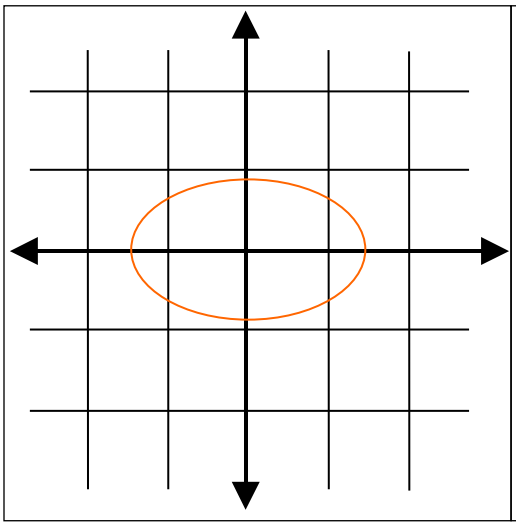


Figure 1

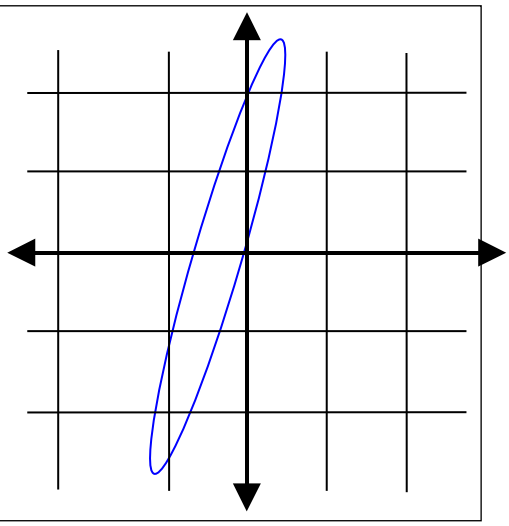


Figure 2

The following is not a convex body:

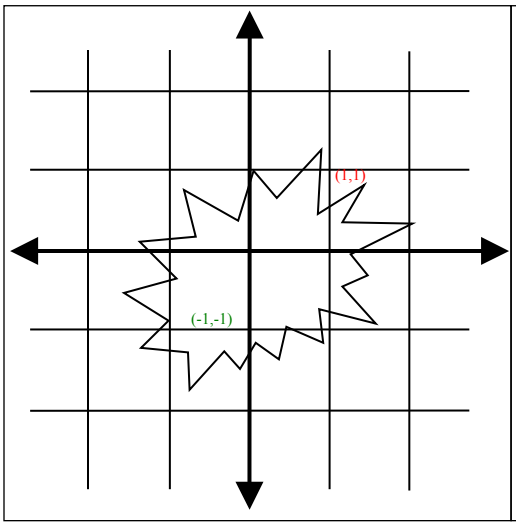


Figure 3: Not centrally symmetric

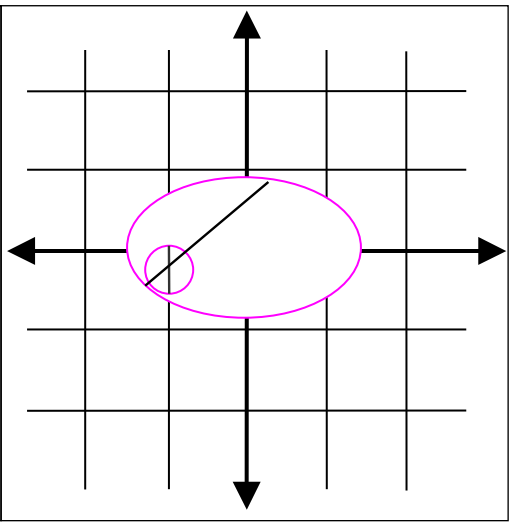


Figure 4: The entire line segment $PQ \notin \Omega$

Finally, we are ready to state, and offer one proof of, Minkowski's theorem.

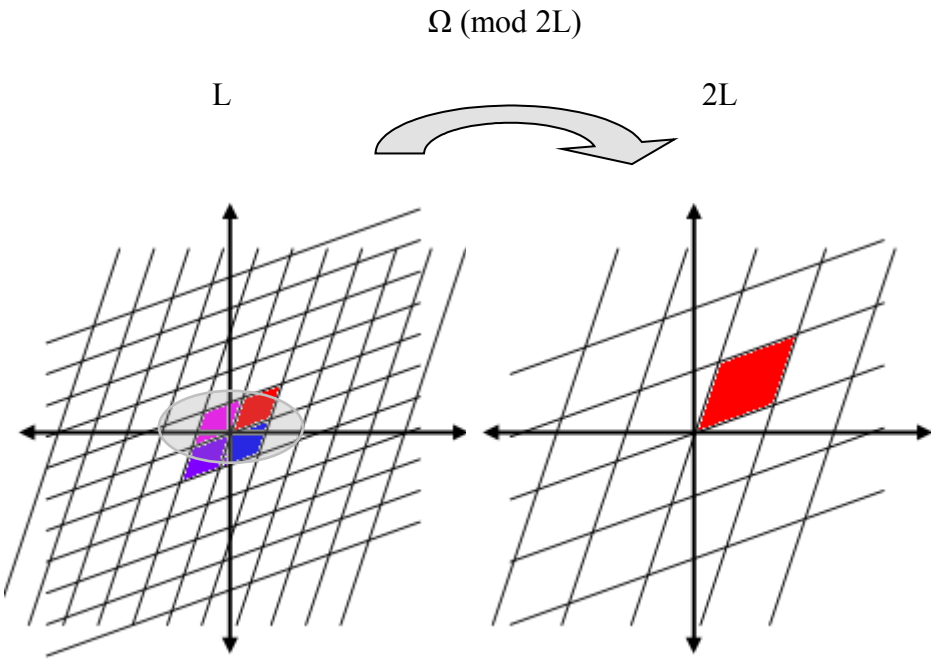
Proof of Minkowski's Convex Body Theorem for n=2:

Since Ω is a bounded region of the plane, and since the 2L lattice defines a "tiling" of the plane using non-overlapping parallelograms, then Ω can be split up into a finite set of non-overlapping regions ($\Omega_1, \Omega_2, \Omega_3, \ldots, \Omega_n$) that are each defined by the 2L parallelogram which they overlap, and that together make up Ω. Under a (mod 2L) mapping, we are translating these n regions into F, the fundamental parallelogram of the 2L lattice, without in any way changing their size or shape. Therefore the n translated regions ($\Omega F_1, \Omega F_2, \Omega F_3, \ldots, \Omega F_n$) each have the same area as the original untranslated regions (i.e. $\text{Area}(\Omega_1)=\text{Area}(\Omega F_1)$, etc).

As a result, the sum of the areas of $\Omega F_1, \Omega F_2, \ldots, \Omega F_n$ is equal to the sum of the areas of $\Omega_1, \Omega_2, \ldots, \Omega_n$ which itself equals the area of Ω.

We know that F is tiled by exactly 4 parallelograms of the L lattice and therefore has area $4\triangle$. Since $\text{Area}(\Omega) > 4\triangle$, $\text{Area}(\Omega) > \triangle^{2,}$ where $\triangle^2$ is the area of the fundamental parallelogram for 2L. Since $\Omega F_1, \Omega F_2, \ldots, \Omega F_n$ all fit within F but together have greater area than F, then at least two of them must overlap, arbitrarily ΩF_i and ΩF_j. Since this overlap has non-zero area, it contains an infinite set of points, and *each* point in that overlap is the common "(mod 2L)" mapping of one point in Ω_i and one point in Ω_j. We know those two points to be distinct points in Ω since $\Omega_1, \Omega_2, \Omega_3, \ldots, \Omega_n$ are non-overlapping.

Therefore, for distinct points $p_1, p_2 \in \Omega$, $p_1 \equiv p_2 \pmod{2L}$.



Pictured above, the fundamental parallelogram is shaded in red for both L and 2L. Clearly, $4\triangle = \triangle_2$ where $\triangle_2$ is the area of the fundamental parallelogram for 2L.

If $p_1 \equiv p_2 \pmod{2L}$, algebraically, this means that if $p_1 = a_1v_1 + b_1v_2$ and $p_2 = a_2v_1 + b_2v_2$, then $a_1 \equiv a_2 \pmod 2$ and $b_1 \equiv b_2 \pmod 2$. Thus, $(a_1 - a_2) \equiv 0 \pmod 2$ and $(b_1 - b_2) \equiv 0 \pmod 2$, and therefore are both even. This means that the point $(p_1 - p_2)$, which is equal to $(a_1 - a_2)v_1 + (b_1 - b_2)v_2$ is an element of the 2L lattice, and is non-zero since p_1 and p_2 are distinct. In other words, there exists a point p_3 in the lattice L such that $p_1 - p_2 = 2p_3$.

Since a convex body is centrally symmetric, if $p_2 \in \Omega$, then $-p_2 \in \Omega$. In addition, since for points p_1, $-p_2$, the entire line segment $p_1(-p_2) \in \Omega$, for $t = ½$, the point $q = (1-½)p_1 + (½)(-p2) = ½p_1 - ½p2 = (p_1-p2)/2$. Since p1 and p2 are distinct, $q \neq 0$.

Finally, as $p_1 \equiv p_2 \pmod{2L}$, $p_1 - p_2 \in 2L$, and thus $q \in L$!

The convex body theorem has a number of implications for Number Theory. For one, Minkowski's theorem introduces an alternative way to prove that primes of the form

p=4k+1 can be written as the sums of two squares.

Theorem: Every prime $p \equiv 1 \pmod 4$ is a sum of two squares.

Proof:

Choose $a \in \mathbb{Z}$ such that $a^2 \equiv -1 \pmod p$ for p-prime. -1 is a quadratic residue modulo p iff $p \equiv 1 \pmod 4$[1]. Let L be a lattice in $\Re^2$, where $L = \{mv_1 + nv_2 \mid m, n \in \mathbb{Z}\}$ and v1= (a,1) and v2= (p,0). The area of a fundamental parallelogram of L is given by $\triangle$, which has a base of length p and height of length 1. Therefore $\triangle$ = base x height = p.

Let $(x, y) = mv_1 + nv_2$ for some $m, n \in \mathbb{Z}$, i.e. (x, y) is a point on our lattice L. From our definition of the vectors v_1 and v_2, x = ma + p and y = m, and thus $x^2 + y^2 = (ma + p)^2 + m^2 = m^2a^2 + 2map + p^2 + m^2 = m^2(a^2+1) + 2map + p^2$. 2map and p^2 are both congruent to 0 modulo p, therefore $m^2(a^2+1) + 2map + p^2 \equiv m^2(a^2+1) \pmod p$. By our choice of a, $a^2 + 1 \equiv 0 \pmod p$, and thus $m^2(a^2 + 1) \equiv 0 \pmod p$.

Let Ω be a circle centrally symmetric about the origin with radius $(2p)^{1/2}$. Ω is given by $\{(x, y) \in \Re \mid x^2 + y^2 < 2p\}$. The area of Ω is given by $2\pi p$, which is greater than $4p = 4\triangle$. Therefore, by Minkowski's theorem Ω contains an lattice, or integral, point other than the origin, arbitrarily given by (j, b). As (j, b) is a lattice point, $j^2 + b^2 \equiv 0 \pmod p$. Also as $(j, b) \in \Omega \setminus (0,0)$, $j^2 + b^2 < 2p$. Since at least one of a and b is nonzero, j^2+b^2 is greater than 0. As $0 < j^2 + b^2 < 2p$, for $j^2 + b^2$ to be congruent to 0 modulo p, $j^2 + b^2$ must be equal to p. Therefore every prime $p \equiv 1 \pmod 4$ is a sum of two squares!

In order to prove Minkowski's theorem for n-dimensions, it is necessary to present certain properties.

[1] Proof omitted.

Properties of Dilates:

- Ω is nonempty iff $r\Omega$ is nonempty.
- Ω is bounded iff $r\Omega$ is bounded.
- Ω is convex iff $r\Omega$ is convex.
- Ω is centrally symmetric iff $r\Omega$ is centrally symmetric.

Therefore if $\Omega \subset \Re^n$ is a convex body of volume V, then for $r \in +\Re$, $r\Omega$ is a convex body of volume $r^n \text{Vol}(\Omega)$. Here, we define $\text{Vol}(r\Omega) = r^n \text{Vol}(\Omega)$.

Minkowski's Convex Body Theorem: Suppose $\Omega \subset \Re^n$ is a convex body with $\text{Vol}(\Omega) > 2^n$. Then there exist integers $x_1,\ldots,x_n$, not all zero, such that $P=(x_1,\ldots,x_n) \in \Omega$.

Proof of Minkowski's Convex Body Theorem:

Since $\frac{1}{2} \in +\Re$, for a convex body Ω, $\frac{1}{2}\Omega$ is also a convex body. Therefore the $\text{Vol}(\frac{1}{2}\Omega) = (\frac{1}{2})^n \text{Vol}(\Omega)$. As $\text{Vol}(\Omega) > 2^n$, $\text{Vol}(\frac{1}{2}\Omega) > 1$.

Ω contains a non-zero integral point $P_0 \in Z^n$ iff $\frac{1}{2}\Omega$ contains a non-zero point Q_0 such that $2Q_0 \in Z^n$. Therefore to prove that a convex body with $\text{Vol}(\Omega) > 2^n$ contains a non-zero integral point, I will show that $\text{Vol}(\Omega) > 1$ contains a non-zero half-integral point (a point Q_0 such that $2Q_0 \in Z^n$):

For $\text{Vol}(\Omega) > 1$, if Ω contains P and Q, then $-Q \in \Omega$ as Ω is centrally symmetric. Since Ω is convex, the entire line segment P(-Q) is contained in Ω. For $t = \frac{1}{2}$, this includes the point $R = \frac{1}{2}P + \frac{1}{2}(-Q) = \frac{1}{2}P - \frac{1}{2}Q$.

For a positive integer r, let L(r) be the number of 1/r lattice points contained in Ω. In other words, points P such that $rP \in Z^n$.

As $\lim_{r\to\infty} \frac{L(r)}{r^n \mathrm{Vol}(\Omega)} = 1$, by Gauss' Circle Problem, $\lim_{r\to\infty} \frac{L(r)}{r^n} = \mathrm{Vol}(\Omega)$.

Since the $\mathrm{Vol}(\Omega) > 1$, $L(r) > r^n$ as r increases. As $|Z/rZ|^n = r^n < L(r)$, by the pigeonhole principle there exists unique integral points $P= (x_1,\ldots,x_n)$ and $Q=(y_1,\ldots,y_n)$ such that $(1/r)P$ and $(1/r)Q$ are contained in Ω and $x_i \equiv y_i \pmod r$ for all $i=1,\ldots,n$.

For these points, $R=\frac{1}{2}(1/r)P - \frac{1}{2}(1/r)Q = \frac{1}{2}((x_1- y_1)/r,\ldots, (x_n- y_n)/r) = \frac{1}{2}((P-Q)/r))$.

As $(x_1- y_1)/r,\ldots, (x_n- y_n)/r \in Z^n$, $(P-Q)/r) \in Z^n$.

Therefore, $R=\frac{1}{2}((P-Q)/r))$ is a half-integral point lying in Ω. Therefore a convex body with $\mathrm{Vol}(\Omega) > 2^n$ contains a non-zero integral point.

Sources

- Jacques Bensimon
- Minkowski Seminar by Alvaro Lozano-Robledo, former PhD student at Boston University: http://math.bu.edu/people/alozano/seminar/minkowski.pdf
- *A Theorem of Minkowski; The Four Squares Theorem* by Pete L. Clark
- From measuring took to geometrical object: Minkowski's development of the concept of convex bodies by Tinne Hoff Kjeldsen