Chapel Hill Math Circle Exit Ticket:
November 23, 2024: Sums of Squares

Please remove this sheet, complete it, and return it before the end of our session.

- Did you find today's topic interesting?
- Was the this topic appropriately challenging relative to your background? That is, was the topic neither too elementary nor inaccessibly advanced?
- How could we improve this worksheet for future sessions?
- What did you enjoy about today's topic?
- What did you find particularly challenging?
- Was there anything you thought was too difficult?
- Was there anything you thought was too easy?
- Are there any topics you would be interested in seeing us cover in the future?

Sums of Squares

Abstract

In Chapel Hill Math Circle's session of October 26, 2024 for the advanced group, we explored *Pythagorean triples*: positive integer solutions (a, b, c) such that $a^2 + b^2 = c^2$. In this session, we consider which positive integers n are expressible in the form $a^2 + b^2$, where a and b are integers. Our starting point is taking positive primes p, and determining when we can express p as a sum of two squares. To do so, in Sections 2–4 we introduce techniques using the *geometry of numbers*. Generalizing these geometric techniques to four dimensions will enable us to prove *Lagrange's Four-Square Theorem*: every nonnegative integer n is expressible as the sum of four perfect squares.

Background needed: Prerequisites basic algebra and geometry. We will use some number theory, such as properties of *prime numbers* and *modular arithmetic*, especially modulo a prime p. For our geometry of numbers section, we shall explore regions that are *symmetric with respect to a point* and introduce properties of the *determinant* of 2×2 and 4×4 *matrices*, especially relating such determinants to areas and volumes of 2- and 4-dimensional parallelipipeds.

Note: Like most Chapel Hill Math Circle worksheets, this document shall be archived at chapelhillmathcircle.org. You can presently find CHMC's archives—and for *all* groups' worksheets, not just those for the advanced group—by navigating to the "Calendar" tab or page, selecting the relevant academic term, then finding the clickable links for each worksheet (where available). Blue text in this document, including in the References, typically provides a clickable link to an external website.

Contents

0 Warmup

As prerequisites for this session, it will help to answer the following first. You do *not* need to know these answers already, and many questions will be revisited later in the worksheet.

0.1 Let S be a region in the plane. If P is a point, what does it mean to say that S is *symmetric with respect to P*? In particular, what does it mean for S to be symmetric with respect to the origin, $(0,0)$?

0.2 Let

$$M := \begin{bmatrix} a & c \\ b & d \end{bmatrix} \tag{0.0.1}$$

be a 2×2 matrix. What is the *determinant* of M, denoted $\det M$? Can you extend this definition for 2×2 matrices to 3×3 and 4×4 matrices?

0.3 Let a, b, m be integers. What does it mean to say that *a is congruent to b modulo m*, denoted $a \equiv b \pmod{m}$?

0.4 Let p be an integer. What does it mean for p to be a *prime number*?

0.5 Let S be a subset of the plane, $\mathbb{R}^2$. What does it mean to say that S is *convex*?

0.6 Let C be a circle of radius R. What is the area of C as a function of R?

0.7 Let $P := (p_1, p_2)$ and $Q := (q_1, q_2)$ be points in the plane. What are the coordinates for M, the midpoint of $\overline{PQ}$?

Can you generalize this result to higher dimensions? For example, if our points lie in n-dimensional space, $\mathbb{R}^n$, and we have $P := (p_1, p_2, \ldots, p_n)$, $Q := (q_1, q_2, \ldots, q_n)$, then what are the n-dimensional coordinates for the midpoint of $\overline{PQ}$?

0.8 In the plane $\mathbb{R}^2$, what are vectors? How do we add and subtract vectors? How do we multiply vectors by a scalar? Your answer may be geometric and conceptual, algebraic, or both.

Can you generalize this to 3-dimensional space, $\mathbb{R}^3$? What about n-dimensional space, $\mathbb{R}^n$?

1 Number Theory Preliminaries

1.1 Discussion

We begin with some concepts from number theory that will later be useful for our purposes.

Let's begin with some very basic notation:

Notation. The sets below are denoted as follows:

1.1 The set of all *integers*, denoted $\mathbb{Z}$, is the set $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

1.2 The set of all *real numbers* is denoted $\mathbb{R}$.

1.3 If n is a positive integer, then $\mathbb{R}^n$ denotes *n-dimensional space* over the reals. An element of $\mathbb{R}^n$ is an n-tuple of the form $(x_1, x_2, \ldots, x_n)$, where each x_i is a real number.

Next, we introduce the following fundamental definitions, most of which should be familiar to those who have been to math circle before:

Definition 1.1.1. Let $a, b \in \mathbb{Z}$. We say *a divides b*, denoted $a \mid b$, if and only if there exists some $n \in \mathbb{Z}$ such that $an = b$. Equivalently, a is a *divisor* of b, and b is a *multiple* of a.

Definition 1.1.2. Let $a, b, m \in \mathbb{Z}$. Then a is *congruent to b modulo m*, denoted $a \equiv b \pmod{m}$, if and only if $m \mid a - b$.

Remark. Intuitively, $a \equiv b \pmod{m}$ if and only if a and b have the same remainder upon being divided by m. Congruence modulo m is also an *equivalence relation*. Further, in practice we are typically interested only in the case where $m \geq 2$, even though this definition makes sense for all integers m.

Definition 1.1.3. Let p be an integer. Then p is *prime number* (or simply *prime*) if and only if whenever $p = ab$ for some integers a, b, then either $a = \pm 1$ or $b = \pm 1$.

The following results, which we present without proof, are indispensable properties of primes:

Proposition 1.1.4. *Let p be a prime. If a is an integer such that $p \nmid a$, then there exists an integer b such that $ab \equiv 1 \pmod{p}$.*

That is, when a is not divisible by a prime p, a has a multiplicative inverse mod p.

Proposition 1.1.5. *Let p be a prime integer. If a, b are integers and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Equivalently, if p is prime and $ab \equiv 0 \pmod{p}$, then either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

1.2 Exercises

1.2.1 For each pair of integers (a, p) below, p is prime. Compute the remainder upon dividing a^{p-1} by p. That is, "compute"[1] $a^{p-1} \pmod{p}$ in the sense of finding its remainder upon dividing by p.

(a) $p := 5$, $a := 3$.

(b) $p := 7$, $a := 3$.

(c) $p := 13$, $a := 2$.

(d) $p := 11$, $a := 22$.

(e) $p := 173$, $a := 172$.

Hint: There is an observation that can *dramatically* simplify your computations.

(f) Combining your results from Exercise #1.2.1(a)–1.2.1(e), can you formulate a conjecture? If so, can you prove it?

[1] Saying that we are "computing $a^{p-1} \pmod{p}$" is technically incorrect, given Definition 1.1.2, since congruence indicates a *relation* rather than an *operation*. Even so, I hope it is clear what it intended by this *abuse of language*.

1.2.2 For the following, each p is a prime number. Simplify $(p-1)! \pmod{p}$, where $(p-1)!$ denotes $(p-1)$ *factorial*:

$$(p-1)! := 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1).$$

(a) $p := 3$.

(b) $p := 5$.

(c) $p := 7$.

(d) $p := 11$.

(e) Say instead that n is a *composite* integer rather than prime. Can you simplify $(n-1)! \pmod{n}$?

(f) Based on the examples above, can you formulate a conjecture?

1.2.3 Let p be a positive prime. Prove that if a, b are integers such that $a^2 \equiv b^2 \pmod{p}$, then either $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$.

Note: This result fails for composite moduli. For example, we have $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$, but, for example, $1 \not\equiv \pm 5 \pmod{8}$.

1.2.4 Let p be a positive prime. As a function of p, how many distinct perfect squares are there modulo p? How many distinct *nonzero* perfect squares are there mod p? You will likely want to take the case $p = 2$ separately.

Hint: If p is an odd positive prime, then I claim there are $\frac{p-1}{2}$ distinct nonzero perfect squares mod p, and $\frac{p+1}{2}$ total distinct perfect squares mod p. Can you explain why? Consider the result from Exercise #1.2.3.

1.2.5 Let p be a positive prime. Prove that there exist integers r, s such that

$$r^2 + s^2 + 1 \equiv 0 \pmod{p}. \tag{1.2.1}$$

Hint: For an odd positive prime, by Exercise #1.2.4, there are $\frac{p+1}{2}$ total distinct perfect squares mod p. Consider the sets

$$R := \{r^2 \pmod{p} : r \text{ is an integer}\}$$
$$S := \{-1 - s^2 \pmod{p} : s \text{ is an integer}\}.$$

By a counting argument, can you show that, mod p, some integer lies in both R and S? If so, what can you conclude?

Note: This result will be used in Section 4.

1.2.6 One of our primary goals for this session is to determine, with proof, which positive primes p are expressible as the sum of two perfect squares. To gain some relevant background, complete Table 1.2.1.

What patterns do you notice? Do you have any conjectures? Can you prove them?

1.2.7 Motivated by Exercise #1.2.2, we have the following.

Theorem 1.2.1 (Wilson's Theorem)**.** *Let p be a positive prime. Then*

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \equiv -1 \pmod{p}. \tag{1.2.2}$$

Conversely, if n is a composite positive integer, then $(n-1)! \equiv 0 \pmod{n}$.

Can you explain why the prime $p = 2$ is an exception

Hint: For the prime case, recalling Proposition 1.1.4: the integers $1, 2, \ldots, p-1$ each have multiplicative inverses mod p. Can you pair up each such integer with its multiplicative inverse? If so, will this simplify computing the product $(p-1)! \pmod{p}$?

1.2.8 The following theorem is enormously helpful:

Theorem 1.2.2 (Fermat's Little Theorem)**.** *Let a, p be integers, where p is prime and $p \nmid a$. Then*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1.2.3}$$

p	$p \pmod 4$	$p = a^2 + b^2$?	-1 a perfect square (mod p)?
2	2	YES: $1^2 + 1^2$	YES: $1^2 \equiv -1 \pmod 2$
3	3	NO	NO
5	1	YES: $1^2 + 2^2$	YES: $2^2 \equiv 3^2 \equiv -1 \pmod 5$
7	3	NO	NO
11	3	NO	NO
13			
17			
19			
23			
29			
31			
37			
41			
43			
47			
53			
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Table 1.2.1: Exercise #1.2.6: For positive primes p, compare $p \pmod 4$ to the solvability of $a^2 + b^2 = p$ over the integers and whether -1 is a perfect square modulo p.

Prove Fermat's Little Theorem.

Hint: Let a be an integer such that $a \not\equiv 0 \pmod p$. First, show that the sets

$$\{1, 2, 3, \dots, p-1\} \text{ and } \{a \cdot 1, a \cdot 2, a \cdot 3, \dots a \cdot (p-1)\}$$

are the same mod p, up to reordering. What happens if you multiply all the elements of each set, then reduce mod p?

Remark. Fermat's Little Theorem should not be confused with *Fermat's Last Theorem*. The latter states that if n is a positive integer with $n \geq 3$, then the equation $x^n + y^n = z^n$ has no solutions (x, y, z) over the integers unless at least one of x, y, and z is zero.

1.2.9 The following theorem will be central to our proof in Section 3. As such, please feel free to use this result even if you are unable to prove it.

Theorem 1.2.3. *Let p be a positive prime. If $p \equiv 1 \pmod 4$, then there exists an integer a such that*

$$a^2 \equiv -1 \pmod p. \tag{1.2.4}$$

That is, if p is a positive prime with $p \equiv 1 \pmod 4$, then there is a "square root of $-1 \pmod p$".

Hint: By Wilson's Theorem, $(p-1)! \equiv -1 \pmod p$. Write $(p-1)!$ as

$$(p-1)! = \left(1 \cdot 2 \cdot \dots \cdot \frac{p-3}{2} \cdot \frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2} \cdot \frac{p+3}{2} \cdot \dots \cdot (p-2) \cdot (p-1)\right).$$

Modulo p, we have

$$\begin{aligned} 1 &\equiv -(p-1) \pmod p \\ 2 &\equiv -(p-2) \pmod p \\ 3 &\equiv -(p-3) \pmod p \\ &\vdots \qquad \vdots \\ \frac{p-3}{2} &\equiv -\frac{p+3}{2} \pmod p \\ \frac{p-1}{2} &\equiv -\frac{p+1}{2} \pmod p. \end{aligned}$$

Using this, and the hypothesis that $p \equiv 1 \pmod 4$, show that if

$$a := \left(\frac{p-1}{2}\right)!,$$

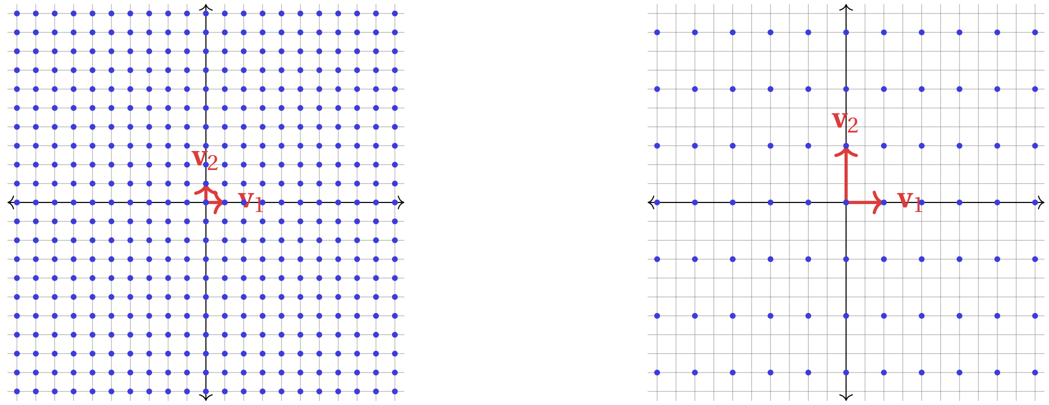
then $a^2 \equiv -1 \pmod p$.

2 The Geometry of Numbers

2.1 Discussion

In this section, we introduce techniques from the *geometry of numbers*. Useful references include Chapter 22 of [6], [2], and [3].

Throughout, $\mathbb{R}^n$ denotes n-dimensional space, and $\mathbb{Z}^n$ denotes the set of all n-tuples $(a_1, a_2, \dots, a_n)$ where all coordinates are *integers*. A point in $\mathbb{R}^n$ will typically be denoted in boldface, like $\mathbf{v}$, while ordinary numbers will be typeset in the usual way, like a or x.



(a) $\Lambda := \mathbb{Z}^2$, generated by $\mathbf{v}_1 = (1,0)$, $\mathbf{v}_2 = (0,1)$.

(b) Λ generated by $\mathbf{v}_1 = (2,0)$, $\mathbf{v}_2 = (0,3)$.

Figure 2.1.1: Simple examples of lattices in the plane.

Definition 2.1.1. Let $B := \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$ be a set of n vectors in $\mathbb{Z}^n$, meaning all the coordinates for each $\mathbf{v}_j$ are integers. The *lattice* Λ *generated by* B is the set of all points $\mathbf{v}$ of the form

$$\mathbf{w} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n, \tag{2.1.1}$$

where each scalar coefficient a_j is an integer

This definition will become easier to understand when consider examples like those in Figures 2.1.1–2.1.2.

Remark. This is *not* the standard definition of a lattice. It will suffice for our purposes, though, and it is also considerably simpler to use for our purposes.

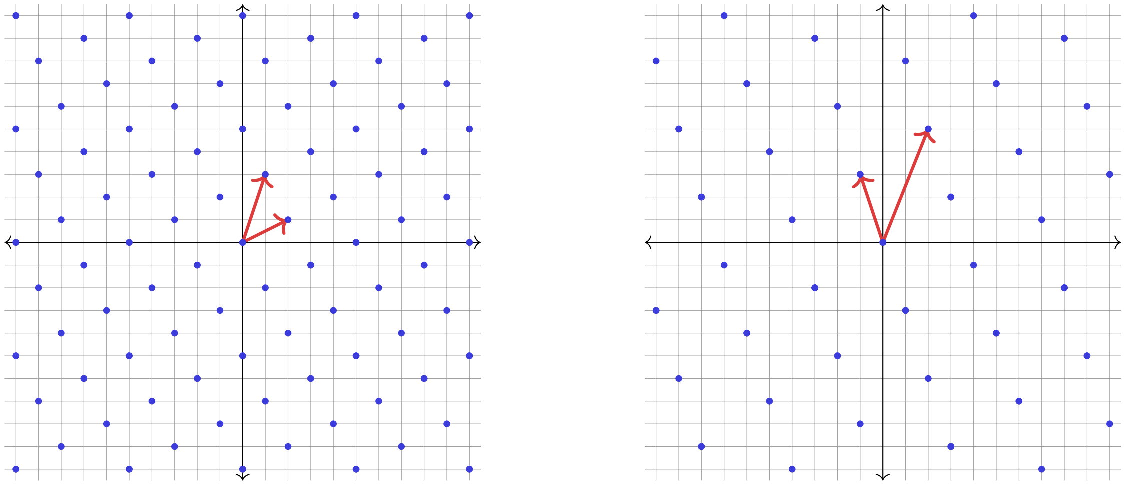
Definition 2.1.2. Let $B := \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ generate an n-dimensional lattice Λ. Then the *fundamental parallelepiped* of Λ with respect to B is the set $P(B) := \{t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n : 0 \le t_1, \ldots, t_n < 1\}$. The *fundamental domain* of Λ relative to B is the set $D(B) := \{t_1\mathbf{v}_1 + \cdots + t_n\mathbf{v}_n : -1 \le t_1, \ldots, t_n < 1\}$.

Remark. See Figure2.1.4 for examples.

Also, note that the fundamental parallelepiped and fundamental domain depend on the generating set B for our lattice Λ, not just the lattice Λ alone.

Proposition 2.1.3. *If* $\mathbf{v}_1 := (a,b), \mathbf{v}_2 := (c,d) \in \mathbb{R}^2$, *then the area enclosed by the parallelogram* P *determined by* $\mathbf{v}_1$ *and* $\mathbf{v}_2$ *is*

$$|\det(\mathbf{v}_1, \mathbf{v}_2)| := \left|\det \begin{bmatrix} a & c \\ b & d \end{bmatrix}\right| = |ad - bc|. \tag{2.1.2}$$



(a) Λ generated by $\mathbf{v}_1 = (2,1)$, $\mathbf{v}_2 = (1,3)$.

(b) Λ generated by $\mathbf{v}_1 = (2,5)$, $\mathbf{v}_2 = (-1,3)$.

Figure 2.1.2: More examples of lattices in the plane.

Notation: If $B := \{\mathbf{v}_1, \mathbf{v}_2\}$, then $\text{Area}(B) := |\det(\mathbf{v}_1, \mathbf{v}_2)|$. In general, $\text{Area}(B)$ is independent of the generating set B, depending only on the lattice Λ. See Figure 2.1.5 for an example.

Lemma 2.1.4 (Blichfeldt's Lemma in the Plane)**.** *Let* $B := \{\mathbf{v}_1, \mathbf{v}_2\}$ *generate a lattice* Λ *in the plane* $\mathbb{R}^2$*. If* S *is any bounded subset of* $\mathbb{R}^2$ *such that* $\text{Area}(S) > 4\,\text{Area}(B)$*, then there exist* distinct $\mathbf{v}, \mathbf{w} \in S$ *such that* $\mathbf{v} - \mathbf{w} \in 2\Lambda$*. (That is, there exist two points in* S *whose difference is* twice *a lattice point in* Λ*.)*

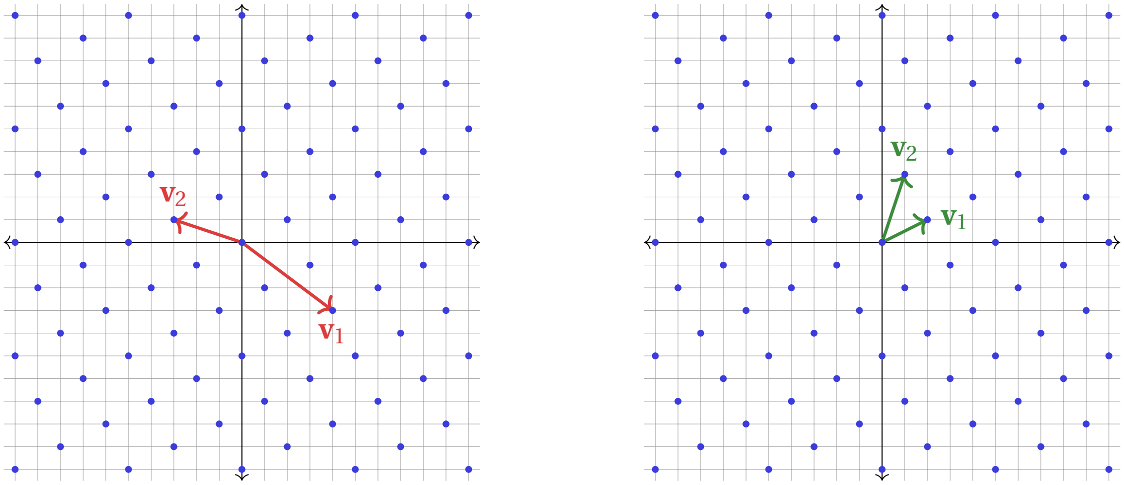
Equivalently, if S *is a bounded subset of* $\mathbb{R}^2$ *such that* $\text{Area}(S) > \text{Area}(B)$*, then* S *must contain two distinct points whose difference lies in* Λ*.*

Since a proof of this lemma is a bit too complicated to outline in the exercises, we present it here.

Proof. Consider the fundamental domain of Λ with respect to B, $D := D(B)$. Note that $\text{Area}(D) = 4\,\text{Area}(B)$. Tile the plane with pairwise disjoint copies of D, each translated parallel to the generating vectors in B: for every $j, k \in \mathbb{Z}$, set $D_{j,k} := D : 2j\mathbf{v}_1 + 2k\mathbf{v}_2$. (See Figure 2.1.6 for examples.) In particular, $D = D_{0,0}$.) Then the sets $D_{j,k}$ partition $\mathbb{R}^2$: every point in the plane lies in *precisely one* of the $D_{j,k}$. In particular, every point of our given set S must lie in some $D_{j,k}$.

First, note that every point (x, y) in S will lie in some unique parallelogram $D_{j,k}$ in our tiling. Map, via translations parallel to the $\mathbf{v}_j$, each point $x\mathbf{v}_1 + y\mathbf{v}_2 \in S$ to its unique counterpart in the fundamental domain D; see Figure 2.1.7 for an example, where the red points in S are translated into the blue fundamental domain D.

Since $\text{Area}(S) > 4\,\text{Area}(B)$, by a pigeonhole principle-like argument, there must be two *distinct* points $\mathbf{v}, \mathbf{w} \in S$ which map to the same point in D. By our construction of D and



(a) Λ is generated by $\mathbf{v}_1 = (4,-3)$, $\mathbf{v}_2 = (-3,1)$.

(b) Λ is also generated by $\mathbf{v}_1 = (2,1)$, $\mathbf{v}_2 = (1,3)$.

Figure 2.1.3: A lattice Λ generated by two different generating sets.

the map, two such points must differ by an element of 2Λ, as claimed. □

Theorem 2.1.5 (Minkowski's Theorem in the Plane)**.** *Let B generate Λ, a lattice in $\mathbb{R}^2$. If $S \subseteq \mathbb{R}^2$ is a bounded set such that*

(a) S is convex,

(I.e., for all $\mathbf{u}, \mathbf{v} \in S$, the entire line segment L with endpoints $\mathbf{u}$ and $\mathbf{v}$ lies in S: $\mathbf{u}, \mathbf{v} \in S$ implies $(1-t)\mathbf{u} + t\mathbf{v} \in S$ for all $t \in [0,1]$. In particular, the midpoint $\frac{1}{2}(\mathbf{u}+\mathbf{v}) \in S$.)

(b) S is symmetric about the origin

(I.e., for all $\mathbf{u} \in S$, $-\mathbf{u} \in S$), and

(c) S has area greater than $4\,\mathrm{Area}(B) = \mathrm{Area}(D)$,

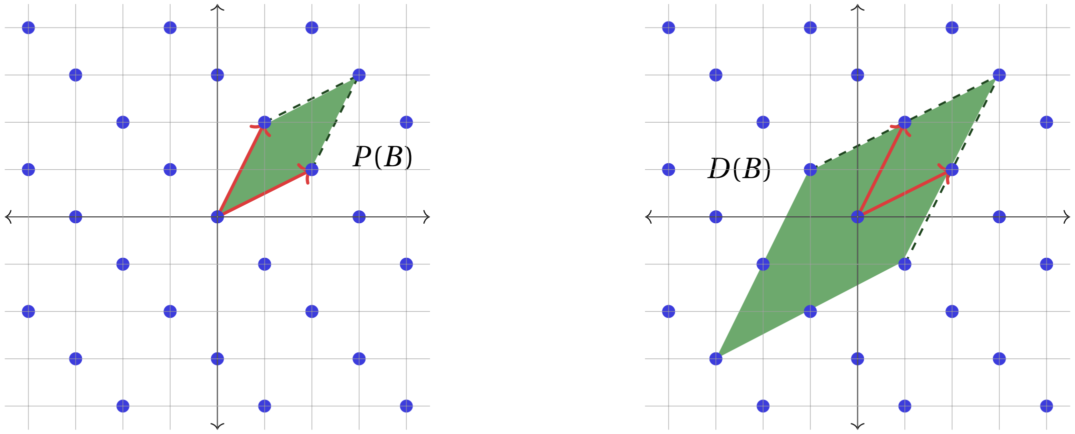
then S contains at least one point (x,y) such that $(x,y) \in \Lambda$ and $(x,y) \neq (0,0)$.

That is, if S satisfies conditions 2.1.5(a)–2.1.5(c), then S contains at least one nonzero *lattice point.*

In the exercises, we consider examples of sets S that satisfy precisely two of the conditions in Theorem 2.1.5, but which do not contain a nonzero lattice point.

The following suggests a general strategy for trying to apply Minkowski's Theorem to prove some desired result:

Strategy 2.1.6 (Strategy for using Minkowski's Theorem)**.** *Say you are trying to prove the existence of a mathematical object satisfying some particular property.*



(a) The fundamental parallelepipied $P(B)$ for lattice Λ generated by the red vectors.

(b) The fundamental domain $D(B)$, comprising four translations of $P(B)$.

Figure 2.1.4: The fundamental parallelepipied $P(B)$ and the fundamental domain $D(B)$.

(a) Choose a lattice Λ in $\mathbb{Z}^n$ generated by some generating subset B such that the points of Λ can be interpreted as having some desired condition.

(b) Select a suitable subset S of $\mathbb{R}^n$ satisfying the hypotheses of Minkowski's Theorem such that a nonzero point of Λ that also lies in S will have your desired property.

(c) Deduce from Minkowski's Theorem the existence of such a point.

(d) Conclude that an object with the proerties sought does indeed exist.

Let us revisit Strategy 2.1.6 in the context of the proof of our key result from Section 3. Let p be a positive prime with $p \equiv 1 \pmod 4$, and our goal is to show that p is expressible in the form $p = x^2 + y^2$, where x, y are integers.

- Let a be a "square root of -1 mod p", with $a^2 \equiv -1 \pmod p$, and following Strategy 2.1.6(a), define Λ to be the lattice generated by $(p, 0)$ and $(a, 1)$. By our selection of a, every point (x, y) in Λ will satisfy $x^2 + y^2 \equiv 0 \pmod p$.
- Choose S to be the disc in the plane centered at the origin and with radius $R := \sqrt{2p}$. Note, in particular, that S is convex and symmetric about the origin. Further, by our choice of Λ and R, $\text{Area}(S) = 2\pi p > 4 \cdot \det \Lambda = 4p$, so the area hypothesis of Minkowski's Theorem also obtains.
- By Minkowski's Theorem, there exists a nonzero point (x, y) simultaneously in S and Λ.
- Since $(x, y) \in \Lambda$, $x^2 + y^2 \equiv 0 \pmod p$. Since $(x, y) \in S$, $x^2 + y^2 < 2p$.

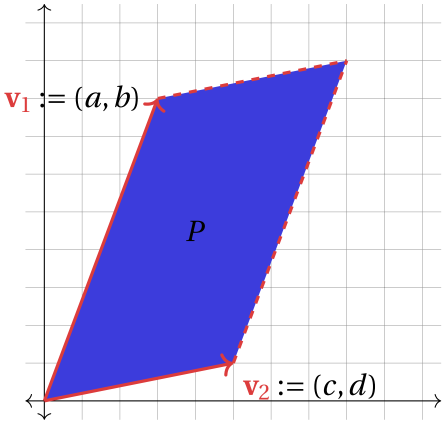


Figure 2.1.5: Illustrating Proposition 2.1.3: Area $P = |\det(\mathbf{v}_1, \mathbf{v}_2|)$.

- Combining these results, there exist integers x, y such that $x^2 + y^2 = p$, as desired.

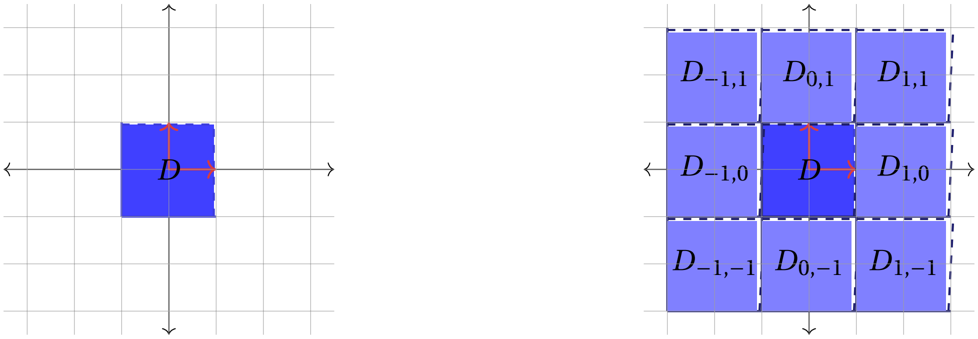
Remark. Our discussion above of Blichfeldt's Lemma and Minkowski's Theorem are special cases of a more general result, but that generality would come at the cost of digressions into highly technical matters irrelevant to our theme for this worksheet. The main technicalities we are bypassing concern (1) the technical definition of a lattice, something more general than what we need for our purposes, (2) delicate matters concerning area, volume, and higher-dimensional volume (since *nobody* wants a digression into *measure theory*), (3) concepts like *compactness*, which can relax the strict inequality in Blichfeldt's Lemma and Minkowski's Theorem to weak inequality (i.e., $\mathrm{Vol}(S) \geq 2^n$ rather than $\mathrm{Vol}(S) > 2^n$).

Many of these geometric techniques have wider applicability, too. Minkowski's Theorem can be used to prove *Minkowski's bound* for the *class number* of an *algebraic number field*. Minkowski's Theorem also provides a proof for *Dirichlet's Approximation Theorem* regarding simulaneous *Diophantine approximations*. Minkowski's Theorem also provides a solution to The Orchard Problem from pages 43–44 in Chapter 4 of [9]:

> A tree is planted at each lattice point in a circular orchard which has center at the origin and radius 50. (All trees are taken to be exact vertical cylinders of the same radius.) If the radius of the trees exceeds 1/50 of a unit, show that from the origin one is unable to see out of the orchard no matter in what direction he looks; show, however, that if the trees are shrunk to a radius less than $1/\sqrt{2501}$, one can see out if he looks in the right direction.

2.2 Exercises

2.2.1 For the following regions in the plane, which are symmetric about the origin? Which are convex? Which have areas greater than 4? Draw some pictures!



(a) The fundamental domain $D := [-1,1) \times [-1,1)$ for the lattice Λ generated by $(1,0)$ and $(0,1)$.

(b) Tiling the plane with translated copies of the fundamental domain.

Figure 2.1.6: Tiling the plane with translations $D_{i,j}$ of the fundamental domain $D := [-1,1) \times [-1,1)$. Each $D_{j,k}$ has center at $(2j, 2k)$.

(a) $x^2 + y^2 \leq 2$.

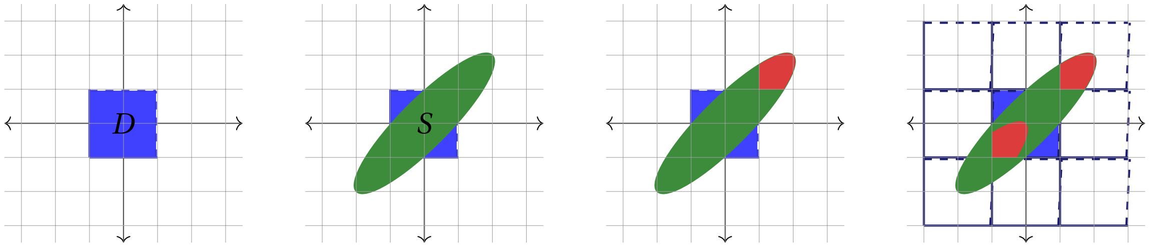
(b) $y \geq x^2$.

(c) $x^2 - y^2 \geq 1$.

(d) $(x-3)^2 + 9(y-4)^2 \leq 9$.

2.2.2 In the discussion following Proposition 2.1.3, we claimed that the area of a fundamental parallelogram depends only on the lattice Λ, not the generating set B. In Figure 2.1.3, we have two different generating sets for the same lattice: $\{(4,-3), (-3,1)\}$ for the first, and $\{(2,1), (1,3)\}$ for the latter. Verify that for each choice of generating set B, $\text{Area}(B)$ is identical.

2.2.3 Prove Proposition 2.1.3, at least for the parallelogram in Figure 2.1.5,



(a) The fundamental domain, $D := [-1,1) \times [-1,1)$.

(b) A region S such that Area(S) > Area(D).

(c) Identifying some points in $S \setminus D$: points in S lying outside the fundamental domain D.

(d) Translating the red points in $S \setminus D$ to the fundamental domain D.

Figure 2.1.7: Illustrating the proof of Blichfeldt's Lemma for the lattice $\Lambda = \mathbb{Z}^2$ generated by $(1,0)$ and $(0,1)$

2.2.4 Let Λ be the lattice $\mathbb{Z}^2$, generated by the vectors $(1,0)$ and $(0,1)$. For the following regions S, explain why each satisfies precisely two of the conditions in Theorem 2.1.5 and why each S contains no nonzero lattice points.

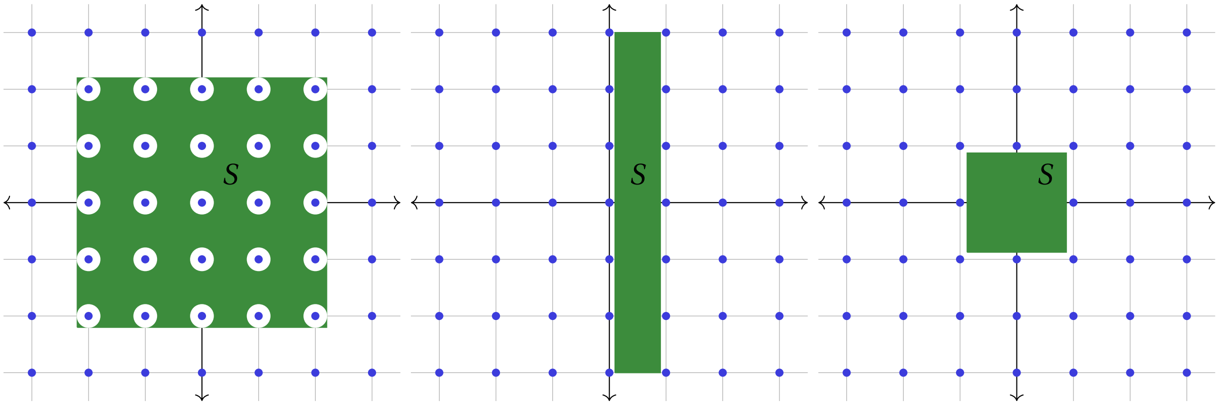
(a) S from Figure 2.2.1a.

(b) S from Figure 2.2.1b

(c) S from Figure 2.2.1c.

2.2.5 Prove Theorem 2.1.5, Minkowski's Theorem in the Plane.

Hint: By Exercise 2.2.4, you will need to use each condition in Minkowski's Theorem in your proof. Lemma 2.1.4, Blichfeldt's Lemma in the Plane, will be invaluable.



(a) Which condition in Theorem 2.1.5 does this S fail to satisfy?

(b) Which condition in Theorem 2.1.5 does this S fail to satisfy?

(c) Which condition in Theorem 2.1.5 does this S fail to satisfy?

Figure 2.2.1: Examples of regions S satisfying precisely two conditions in Theorem 2.1.5.

3 Using the Geometry of Numbers: Primes as the Sum of Two Squares

3.1 Discussion

Our goal is to prove the following theorem geometrically:

Theorem 3.1.1. *Let p be a positive prime. If $p \equiv 1 \pmod 4$, then there are integers x, y such that*

$$p = x^2 + y^2. \tag{3.1.1}$$

That is, any positive prime $p \equiv 1 \pmod 4$ is expressible as the sum of two perfect squares.

In light of Strategy 2.1.6, our aim is to construct a lattice Λ with generating set B and a set S in the plane such that a nonzero point $(x, y) \in \Lambda \cap S$ will be such that $x^2 + y^2 = p$. For background, recall in particular Theorem 1.2.3: if p is a positive prime with $p \equiv 1 \pmod 4$, then -1 is a perfect square mod p. If a is an integer such that $a^2 \equiv -1 \pmod p$, then set

$$\mathbf{v}_1 := (p, 0) \tag{3.1.2}$$

$$\mathbf{v}_2 := (a, 1), \tag{3.1.3}$$

and let Λ be the lattice generated by $\mathbf{v}_1$ and $\mathbf{v}_2$.

3.2 Exercises

3.2.1 For the following primes p, consider the following lattices Λ generated by $\mathbf{v}_1 := (p, 0)$ and $\mathbf{v}_2 := (a, 1)$, where a is an integer satisfying $a^2 \equiv -1 \pmod p$.

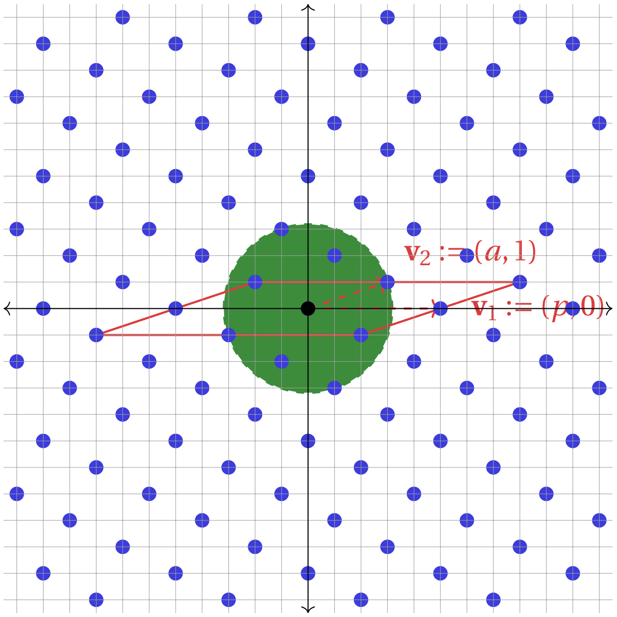


Figure 3.2.1: For $p := 5$ and $a := 3$ with $a^2 \equiv -1 \pmod{p}$, consider Λ generated by $\mathbf{v}_1 := (p,0)$ and $\mathbf{v}_2 := (a,1)$. Further, consider the open disc $x^2 + y^2 < 2p$, and show it contains a *nonzero* lattice point in Λ.

For each, verify that the open disc with center $(0,0)$ and of radius $\sqrt{2p}$ contains a *nonzero* point in the lattice.

Remark. To draw these, it may help to know that $\sqrt{2\cdot 5} = \sqrt{10} \approx 3.162$, $\sqrt{2\cdot 13} = \sqrt{26} \approx 5.099$, and $\sqrt{2\cdot 17} = \sqrt{34} \approx 5.83$. Can you draw your own lattices and circles for different primes p with $p \equiv 1 \pmod{4}$?

(a) $p = 5$: $\mathbf{v}_1 := (5,0)$, $\mathbf{v}_2 := (a,1) = (3,1)$, as in Figure 3.2.1.

(b) $p = 13$: $\mathbf{v}_1 := (13,0)$, $\mathbf{v}_2 := (a,1) = (5,1)$, as in Figure 3.2.2.

(c) $p = 13$: $\mathbf{v}_1 := (13,0)$, $\mathbf{v}_2 := (a,1) = (8,1)$., as in Figure 3.2.3.

Note: Compare Figures 3.2.2–3.2.3. These are different lattices, using different square roots of $-1 \pmod{p}$, and they identified different solutions to $x^2 + y^2 = p = 13$.

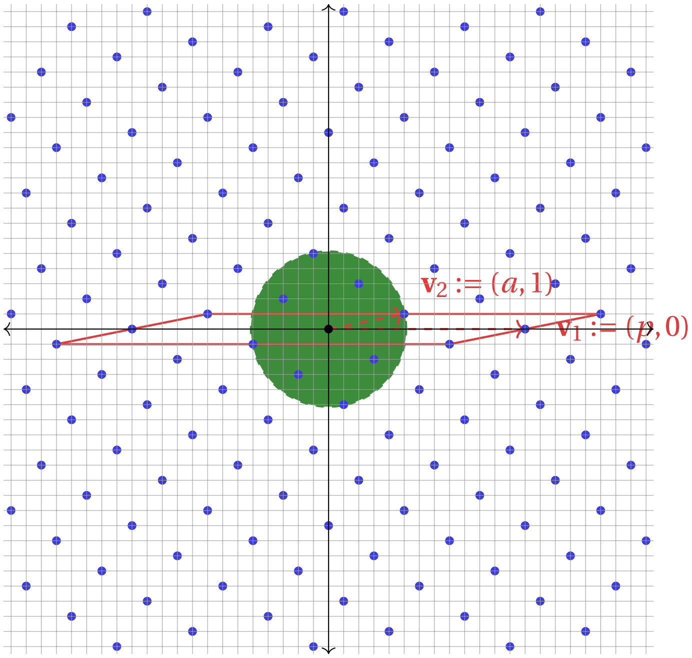


Figure 3.2.2: For $p := 13$ and $a := 5$ with $a^2 \equiv -1 \pmod{p}$, consider Λ generated by $\mathbf{v}_1 := (p,0)$ and $\mathbf{v}_2 := (a,1)$. Further, consider the open disc $x^2 + y^2 < 2p$, and show it contains a *nonzero* lattice point in Λ.

(d) $p = 17$: $\mathbf{v}_1 := (17,0)$, $\mathbf{v}_2 := (a,1) = (4,1)$, as in Figure 3.2.4.

3.2.2 Let S the open disc $x^2 + y^2 < 2p$ centered at the origin and of radius $\sqrt{2p}$. Show that S satisfies the three criteria in Minkowski's Theorem, relative to the lattice Λ generated by $(p,0)$ and $(a,1)$, where $a^2 \equiv -1 \pmod{p}$.

3.2.3 For Λ as above, show that for all $(x,y) \in \Lambda$, $x^2 + y^2 \equiv 0 \pmod{p}$.

Hint: Any such (x,y) is of the form $c(p,0) + d(a,1)$, where c, d are integers.

3.2.4 For any nonzero $(x,y) \in \Lambda \cap S$, show that $x^2 + y^2 = p$.

That is, the nonzero lattice point in S produces a solution, completing the proof of Theorem 3.1.1.

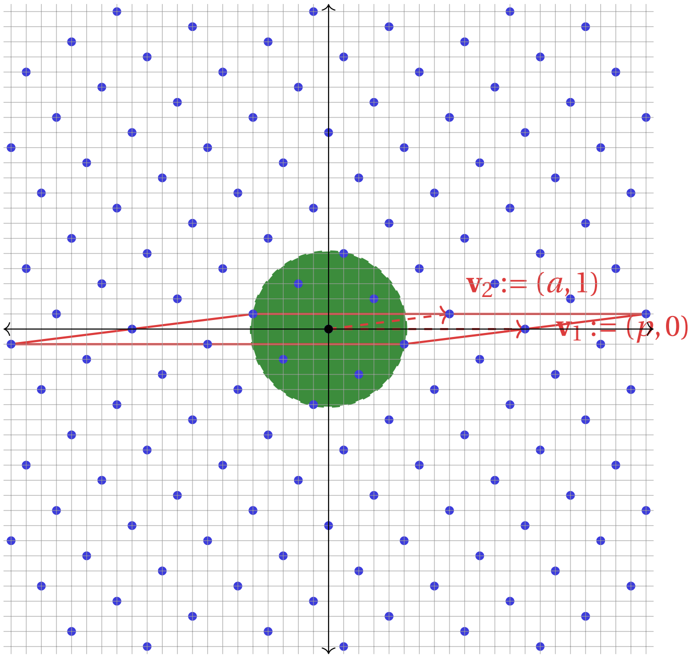


Figure 3.2.3: For $p := 13$ and $a := 8$ with $a^2 \equiv -1 \pmod{p}$, consider Λ generated by $\mathbf{v}_1 := (p, 0)$ and $\mathbf{v}_2 := (a, 1)$. Further, consider the open disc $x^2 + y^2 < 2p$, and show it contains a *nonzero* lattice point in Λ.

3.2.5 **Challenging:** Let p be a positive prime such $p \equiv 1$ or $9 \pmod{20}$. You may accept (without proof) that for such primes p, -5 is a perfect square mod p, meaning there exists some integer a such that $a^2 \equiv -5 \pmod{p}$.

Modify the proof above to prove that there are integers x, y such that

$$p = x^2 + 5y^2. \tag{3.2.1}$$

Hint: To apply Minkowski's Theorem, you need a lattice generated by some set B, and a set S.

Note: This exercise is adapted from the proof of Proposition 13 in [7].

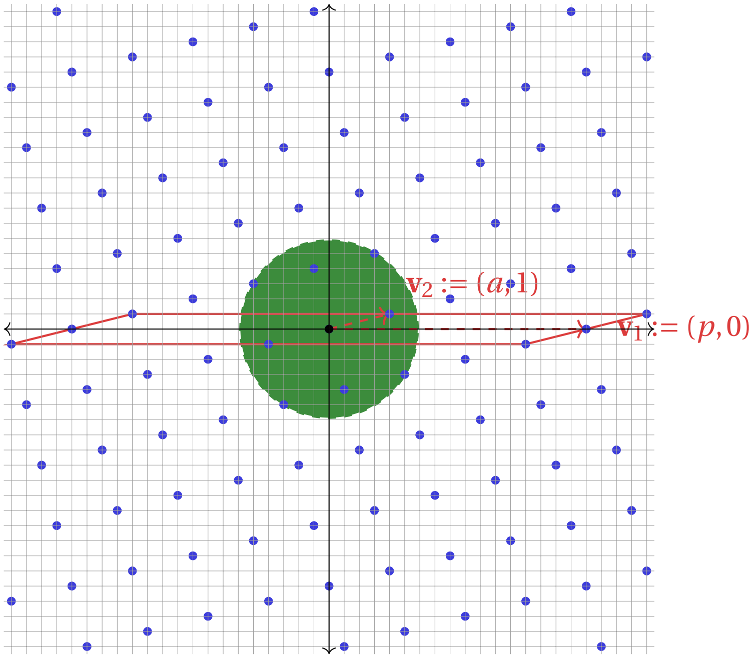


Figure 3.2.4: For $p := 17$ and $a := 4$ with $a^2 \equiv -1 \pmod p$, consider Λ generated by $\mathbf{v}_1 := (p,0)$ and $\mathbf{v}_2 := (a,1)$. Further, consider the open disc $x^2 + y^2 < 2p$, and show it contains a *nonzero* lattice point in Λ.

4 The Geometry of Numbers and Lagrange's Four-Square Theorem

4.1 Discussion

Our goal in this section is to generalize results from Sections 2–3 to four dimensions to prove the following:

Theorem 4.1.1 (Lagrange's Four-Square Theorem)**.** *Let $n \geq 0$ be a nonnegative integer. Then there exist integers w, x, y, and z such that*

$$w^2 + x^2 + y^2 + z^2 = n. \tag{4.1.1}$$

That is, any nonnegative integer is expressible as the sum of four perfect squares (where $0 = 0^2$ is included as a perfect square).

Lemma 4.1.2 (Blichfeldt's Lemma in n-Dimensional Space)**.** *Let $B := \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ generate a lattice $\Lambda \subset \mathbb{R}^2$. If S is any bounded subset of $\mathbb{R}^n$ such that* $\mathrm{Vol}(S) > 2^n \mathrm{Vol}(B)$*, then there exist* distinct $\mathbf{v}, \mathbf{w} \in S$ *such that* $\mathbf{v} - \mathbf{w} \in 2\Lambda$*. (That is, there exist two points in S whose difference is* twice *a lattice point in Λ.)*

Equivalently, if S is a bounded subset of $\mathbb{R}^n$ such that $\mathrm{Vol}(S) > \mathrm{Vol}(B)$*, then S must contain two distinct points whose difference lies in Λ.*

Theorem 4.1.3 (Minkowski's Theorem in n-Dimensional Space)**.** *If $\Lambda \subseteq \mathbb{R}^n$ is an n-dimensional lattice given by generating set $B := \{\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n\}$, and $S \subseteq \mathbb{R}^n$ is a bounded set such that*

(a) S is convex,

(b) S is symmetric about the origin, and

(c) S has n-dimensional volume greater than $2^n\,\mathrm{Vol}(B)$,

then S contains a point $(x, y) \in S \cap \Lambda$ such that $(x, y) \neq (0, 0)$.

That is, any such S satisfying 4.1.3(a)–4.1.3(c) contains a nonzero *lattice point of Λ.*

The proofs of the more general Blichfeldt's Lemma and Minkowski's Theorem are analogous to those for the versions in the plane. The main difference is that we'll have additional factors of 2 in the volume condition depending on our dimension. For example, in the plane, we have $4 = 2^2$ *quadrants*, but in 3-space we have $2^3 = 8$ *octants*.

To generalize our two-square theorem from Section 3 to higher dimensions, we must also know the folling 4-dimensional formulas for area, which we assert without proof.

Proposition 4.1.4. *If $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_n \in \mathbb{R}^n$, then the n-dimensional volume enclosed by the parallelepiped determined by $\mathbf{v}_1, \cdots, \mathbf{v}_n$ is*

$$\left|\det\begin{pmatrix} | & | & & | \\ \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_n \\ | & | & & | \end{pmatrix}\right|. \tag{4.1.2}$$

Proposition 4.1.5. *In 4-dimensional space $\mathbb{R}^4$, the 4-dimensional volume of a hypersphere sphere of radius R is*

$$\frac{\pi^2}{2}R^4. \tag{4.1.3}$$

Finally, using Exercise #1.2.5, we construct a lattice Λ generated by the set B containing the vectors:

$$\mathbf{v}_1 := (p, 0, 0, 0) \tag{4.1.4}$$
$$\mathbf{v}_2 := (0, p, 0, 0) \tag{4.1.5}$$
$$\mathbf{v}_3 := (r, s, 1, 0) \tag{4.1.6}$$
$$\mathbf{v}_4 := (s, -r, 0, 1). \tag{4.1.7}$$

In particular, for this generating set, we have $\mathrm{Vol}(B) = p^2$, by Proposition 4.1.4.

Remark. Many of you have requested topics concerning 4-dimensional geometry, so I hope this unexpected application of higher-dimensional geometry—and to number theory, of all topics!—piques your interest. For another interesting application of 4-dimensional geometry, see [1]. Like that video's creator, though, I can't offer much help in trying to visualize how to "see" the geometry of 4-dimensional space, but that may not prevent you from appreciating how to use higher dimensional spaces.

4.2 Exercises

4.2.1 Prove the following:

Lemma 4.2.1. *Let $a, b \in \mathbb{Z}$ be expressible as sums of squares of four perfect squares, with $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$ integers such that*

$$\begin{aligned} a &= x_1^2 + x_2^2 + x_3^2 + x_4^2, \text{ and} \\ b &= y_1^2 + y_2^2 + y_3^2 + y_4^2, \end{aligned}$$

Then

$$\begin{aligned} (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\ (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2 \\ + (x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3)^2 \\ + (x_1 y_3 - x_2 y_4 - x_3 y_1 + x_4 y_2)^2 \\ + (x_1 y_4 + x_2 y_3 - x_3 y_2 - x_4 y_1)^2. \end{aligned}$$

That is, if a, b are integers that are sums of four squares, so is the product ab.

Note: This identity may be motivated by properties of *quaternions*, a type of 4-dimensional number system.

4.2.2 Show that if Lagrange's Theorem holds for every prime p, then Lagrange's Theorem hold for every nonnegative integer n.

4.2.3 Let p be a positive prime. Using an argument analogous to our proof of Theorem 3.1.1 in Section 3, prove that there exist four integers w, x, y, z such that $w^2 + x^2 + y^2 + z^2 = p$.

References

[1] 3Blue1Brown. Why 4d geometry makes me sad. https://www.youtube.com/watch?v=piJkuavhV50, November 8, 2024.

[2] Pete L. Clark. Geometry of numbers with applications to number theory. http://alpha.math.uga.edu/~pete/geometryofnumbers.pdf, 2011–2012. online: retrieved November 18, 2024.

[3] Keith Conrad. Sums of two squares and lattices. https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Picksumofsq.pdf. online: retrieved November 19, 2024.

[4] Keith Conrad. When is -1 a square modulo primes? https://kconrad.math.uconn.edu/blurbs/ugradnumthy/minus1squaremodp.pdf. online: retrieved November 21, 2024.

[5] Euler's Basement. What's the geometry of numbers? - Minkowski's theorem #SoME2. https://www.youtube.com/watch?v=RquUIXUMLcc, August 14, 2022.

[6] Jay R. Goldman. *The Queen of Mathematics: A Historically Motivated Guide to Number Theory*. CRC Press, 6000 Broken Sound Parkway, NW, Suite 100, Boca Raton, FL 33487, CRC Press reprint edition, 2010.

[7] Thomas R. Hagedorn. Primes of the form $x^2 + ny^2$ and the geometry of (convenient) numbers. https://hagedorn.pages.tcnj.edu/files/2022/08/Geometry-of-Convenient-Numbers.pdf, August 2022. online: retrieved November 19, 2024.

[8] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, Walton Street, Oxford OX2 6DP, fifth edition, 1979.

[9] Ross Honsberger. *Mathematical Gems I*, volume 1 of *Dolciani Mathematical Expositions*. The Mathematical Association of America, 1973.

[10] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, second edition edition, 1990.

[11] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, Inc., New York, fifth edition, 1991.

[12] Hao Xing. Minkowski's theorems and applications. https://www.youtube.com/playlist?list=PLHvJR_m56rsVOocyLOcUCJ4r_ZTyjNtSb, February 1, 2021 through February 7, 2021.