LATTICE FUN

OLGA RADKO MATH CIRCLE
ADVANCED 3
MARCH 7, 2021

Orchard in full bloom
Apples litter the damp ground
Sunrise come and gone

1. Introduction

Everybody loves whole numbers. Seriously, what's better than a nice integer? This is why number theory often deals with integer solutions. For example, Fermat's Last Theorem says that there are no non-trivial integer solutions to $a^n + b^n = c^n$ for $n > 2$. Consider the case where $n = 3$. The set of solutions to $x^3 + y^3 = z^3$ is a 2-dimensional surface in $\mathbb{R}^3$. Fermat's Last Theorem is a statement about this surface's (and other surfaces' for different values of n) avoidance of the integer points in $\mathbb{R}^3$. Take your favorite number theoretic result and turn it geometric! In this handout we will develop some tools to solve problems of this form (not FLT), granted they satisfy some extra conditions. One such problem will be Lagrange's four-square theorem, which states that every nonnegative integer can be written as the sum of four squares.

Definition 1. The **integer lattice** $\mathbb{Z}^n$ in $\mathbb{R}^n$ is the set of points with integer coordinates. Written as a set, $\mathbb{Z}^n = \{(a_1, a_2, \ldots, a_n) | a_i \in \mathbb{Z}\}$. We call each point in the lattice a **lattice point**.

The most common example is the integer lattice $\mathbb{Z}^2$ in $\mathbb{R}^2$. This is the set of points in the plane with integer coordinates.

Problem 1. Draw the integer lattice $\mathbb{Z}^2$.

We say that a set of vectors $\{v_1, v_2, \ldots, v_n\}$ **generates** $\mathbb{Z}^n$ if every lattice point can be written uniquely as $a_1 v_1 + \cdots + a_n v_n$ where the coefficients a_i are integers.

Problem 2. Find a set of vectors which generate the integer lattice $\mathbb{Z}^n$. Make sure your set has as few vectors as possible, this will ensure uniqueness.

Definition 2. We call the parallelepiped spanned by a generating set of $\mathbb{Z}^n$ the **fundamental region** of the lattice.

While the region itself might depend on the choice of generating set, the volume does not.

Problem 3. Draw a picture of the fundamental region of $\mathbb{Z}^3$. What is its volume?

2. Minkowski's Theorem

Many problems in number theory boil down to finding integer solutions to a problem which can be extended over $\mathbb{R}^n$. Our goal in this section is to develop some tools to prove existence of integer solutions inside a set of general (real-valued) solutions.

Theorem 1. (Blichfeldt) Let $X \subset \mathbb{R}^n$ be a set of finite volume. If $Vol(X) > 1$, then X contains two points which differ by an element of $\mathbb{Z}^n$. That is, there exist $x, y \in X$ such that $x - y \in \mathbb{Z}^n$.

Blichfeldt's theorem says that if a set X is large enough (volume-wise), then it can be translated in the plane to contain two integer points.

Let us first prove the theorem for $\mathbb{Z}^2 \subset \mathbb{R}^2$.

Problem 4. Prove Blichfeldt's theorem for $\mathbb{Z}^2$ by covering X with translates of the fundamental region and superimposing the regions on top of each other.

Problem 5. Does your proof of Blichfeldt's theorem for $\mathbb{Z}^2$ extend to a proof of Blichfeldt's for $\mathbb{Z}^n$?

Problem 6. Let $X \subset \mathbb{R}^n$ be a set of volume k. What is the maximum number of integer points we can guarantee to be in X after a possible translation?

We now know that with a large enough region and the freedom to move it around in the plane, we can guarantee integer solutions. However, our problems are often sensitive to translations and depend on a rigid set of solutions. The following theorem removes translations but introduces additional structure on the region we are concerned with. Specifically, we consider convex sets which are symmetric with respect to the origin.

Definition 3. A set $X \subset \mathbb{R}^n$ is **convex** if the line segment connecting any two points in X lies entirely in X.

Problem 7. Prove that if X is convex, then the midpoint of any two points in X is also in X.

Definition 4. A set $X \subset \mathbb{R}^n$ is **symmetric with respect to the origin** if for all $x \in X$, $-x$ is also in X.

This might remind you of the definition for odd functions.

Problem 8. The graph of a function $f : X \to Y$ is the set $graph(f) = \{(x, f(x)) | x \in X\} \subset X \times Y$. Convince yourself that this agrees with our notion of the graph of a function from $\mathbb{R}$ to $\mathbb{R}$. Prove that the graph of an odd function $f : X \to Y$ is a set which is symmetric with respect to the origin.

Now we are ready to state Minkowski's theorem.

Theorem 2. (Minkowski) Every convex set in $\mathbb{R}^n$ which is symmetric with respect to the origin and which has volume greater than 2^n contains a non-zero integer point.

Minkowski's theorem tells us that for a large enough and well-structured set, we are guaranteed a non-trivial lattice point.

Problem 9. Let K be our set satisfying the conditions of Minkowski's theorem. Shrink each coordinate of $\mathbb{R}^n$ by a factor of 2 to get a new set, call it $K' := \frac{1}{2}K$.

1. What is the volume of K' in relation to that of K?
2. Prove that the sum of any two points in K' sits in K. (Hint: Convexity might be useful)
3. Apply Blichfeldt's theorem to K' to prove Minkowski's theorem. (Hint: Symmetry with respect to the origin might be useful)

3. Applications

Let's take a look at some problems for which we can use Minkowski's theorem!

3.1. **Polya's Orchard Problem.**

Orchard in full bloom
Apples litter the damp ground
Sunrise come and gone

It's spring time; the birds are singing and the flowers are blooming. What a time. Picture this: You are standing in the center of a circular orchard of integer radius R. The trees were planted at the integer lattice points and have each grown to have the same radius r. If the radius is small enough, you will have a clear line-of-sight through the orchard in some direction. If the radius is too large, there is no line-of-sight through the orchard no matter the direction. The following figure is an example, feel free to color it in with whatever type of trees you would like.

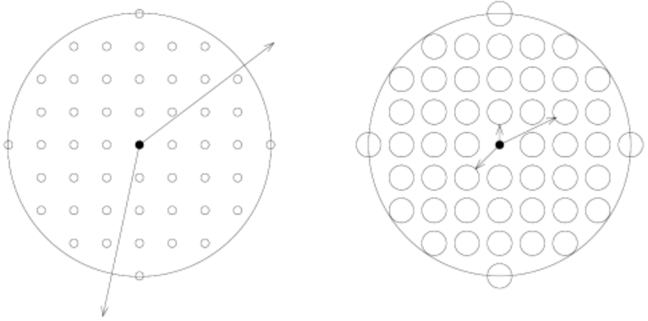

Figure 1. Two orchards of radius 4.

Problem 10. Show that if $r < \frac{1}{\sqrt{R^2+1}}$, then there is a clear line-of-sight. (Hint: Take a look at the ray through the point $(R, 1)$ and calculate the distance from the closest integer points to the ray)

Problem 11. Prove that if $r > \frac{1}{R}$, then there is no line-of-sight through the orchard. If you'd like, you can use the following steps:

(1) Show that if $r \geq 1$, then there is no line-of-sight.
(2) Now suppose $r < 1$ and $r > \frac{1}{R}$. Then $R \geq 2$. Choose a potential line-of-sight, say it passes through a point P on the circle. Thicken this line-of-sight equally on both sides into a rectangle of width $2r$ tangent to P and $-P$. From here, use Minkowski's to get a contradiction. (Don't forget to rule out any lattice points that sit outside the orchard but inside the rectangle.)

Any interest in counting the number of trees in the orchard? If so, google "the Gauss circle problem". If orchards are not your slice of fruit, maybe rational approximations are your cup of tea.

Problem 12. Prove that there exists a rational approximation of $\sqrt{3}$ within 10^{-3} with denominator at most 501. Come up with an upper bound for the smallest denominator of a ϵ-close rational approximation of any irrational number $\alpha > 0$. Your bound can have some dependence on α and should get smaller as α gets larger.

3.2. **Detour: General Lattices.** In this section we will extend our notion of an integer lattice and prove generalizations of our main theorems. This will be very useful for our next application.

Definition 5. Let $v_1, \ldots, v_n$ be a set of n vectors in $\mathbb{R}^n$. We say that $\{v_1, \ldots, v_n\}$ is a **basis** for $\mathbb{R}^n$ if every vector $v \in \mathbb{R}^n$ can be written as $c_1v_1 + c_2v_2 + \cdots + c_nv_n$ for some coefficients $c_i \in \mathbb{R}$.

Now that we have the notion of a basis, we are ready to define the general lattice.

Definition 6. Given a basis $\{v_1, \dots, v_n\}$ of $\mathbb{R}^n$, we construct a **lattice** Λ generated by the basis. More concretely, $\Lambda = \{a_1 v_1 + \cdots + a_n v_n | a_i \in \mathbb{Z}\}$. Note that the coefficients in this definition are integers, not real numbers.

Problem 13. Draw the lattice in $\mathbb{R}^2$ generated by the vectors $(2, 1), (0, 2)$.

We define the fundamental region of a general lattice similarly to that of the integer lattice. The fundamental region of a lattice Λ is the parallelepiped spanned by its generating set of vectors. Once again, the volume of the fundamental region depends only on the lattice and not on the choice of basis.

Definition 7. A map $T : \Lambda_1 \to \Lambda_2$ between two lattices in $\mathbb{R}^n$ is called **linear** if $T(v+w) = T(v)+T(w)$ for all $v, w \in \Lambda_1$ and $T(cv) = cT(v)$ for all $c \in \mathbb{Z}, v \in \Lambda_1$. A linear map is said to respect the addition and scalar multiplication of the lattices.

Problem 14. Prove that a convex region remains convex after applying any linear map.

Definition 8. A linear map $T : \Lambda_1 \to \Lambda_2$ is an **isomorphism** if it is also a bijection.

Problem 15. Given a lattice $\Lambda \subset \mathbb{R}^n$ generated by $\{v_1, v_2, \dots v_n\}$, construct an isomorphism $T : \mathbb{Z}^n \to \Lambda$. That is, construct an invertible linear map from the set of vectors with integer coordinates to the set of lattice points which respects addition and scalar multiplication. (Hint: Look at the definition of Λ as a set.)

This isomorphism can be extended to an isomorphism $\tilde{T} : \mathbb{R}^n \to \mathbb{R}^n$ by allowing real-valued coefficients instead of just integers. Given a region $X \subset \mathbb{R}^n$, we can look at its image under this map. The following definition gives us the relationship between the volume of a region and the volume of its image.

Definition 9. Given a linear isomorphism $F : \mathbb{R}^n \to \mathbb{R}^n$, the absolute value of its **determinant**, $|\det F|$, is the volume scaling factor of the map. That is, if a region $D \subset R^n$ has volume k, then its image $F(D)$ has volume $k \cdot |\det F|$.

Problem 16. What is $|\det \tilde{T}|$? (Hint: Look at the fundamental regions of both lattices)

From now on we refer to $|\det \tilde{T}|$ as $\det \Lambda$ since it is a property of the lattice and not our choice of isomorphism.

When faced with a problem involving lattices, we can often solve the problem in our integer lattice $\mathbb{Z}^n$ and then apply it to our general lattice Λ using the isomorphism. The only thing we have to keep track of is the scaling factor.

Problem 17. Generalize Blichfeldt's theorem to any lattice and prove your result. (Hint: Use the inverse of our map $\tilde{T}$ to map the region into the plane with the integer lattice, then map back at the end. Make sure to keep track of the volume scaling factors)

Problem 18. How would you extend Minkowski's theorem to other lattices? Prove your extension! (Hint: Use the lattice isomorphism constructed previously).

3.3. **Lagrange's Four Square Theorem.** Everybody's heard of Fermat's sum of two squares theorem, but would you like to know what's twice as good? That's right, Lagrange's **four** square theorem.

Theorem 3. (Lagrange) Every nonnegative integer n can be written as the sum of four squares.

We will prove this theorem in steps. First, we introduce the quaternions.

Definition 10. The **quaternions** are the set of $\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} | a, b, c, d \in \mathbb{R}\}$ equipped with multiplication given by distributivity with $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ and $\mathbf{ij} = \mathbf{k}$.

We will be interested in the subset where the coefficients a, b, c, d are integers. This is equipped with a **norm** function $N : \mathbb{H} \to \mathbb{Z}^+$ given by $N(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = a^2 + b^2 + c^2 + d^2$. **Fun fact:** We have that for two quaternions α, β, $N(\alpha\beta) = N(\alpha)N(\beta)$.

Problem 19. (1) Show that if two nonnegative integers can be written as the sum of four squares, then so can their product. (Hint: Use our norm function on the quaternions)
(2) Explain why this implies that we can reduce the theorem to proving any prime number can be written as the sum of four squares.
(3) Reduce further to odd primes by proving it for $n = 2$.

Recall a result from quadratic reciprocity: There are $\frac{p+1}{2}$ quadratic residues $\mod p$. That is, there are $\frac{p+1}{2}$ values $\mod p$ that can be written as the square of another integer.

Problem 20. Use the above fact to show that there exist α, β such that $\alpha^2 + \beta^2 + 1 \equiv 0 \mod p$. (Hint: It might be useful to look at this as $\alpha^2 \equiv -1 - \beta^2 \mod p$ and count the number of distinct element on both sides.)

Fix α, β from the problem above. Consider the lattice Λ generated by $\{(p, 0, 0, 0), (0, p, 0, 0), (\alpha, \beta, 1, 0), (\beta, -\alpha, 0, 1)\}$

Problem 21. Show that $\det \Lambda = p^2$. (This requires taking determinants in the linear algebra sense, don't worry if you haven't seen it).

Take the open ball of radius $\sqrt{2p}$ in $\mathbb{R}^4$. The volume of this ball is $2\pi^2 p^2$ (4-dimensional volume formula).

Problem 22. (1) Apply Minkowski's theorem to get a lattice point inside the ball.
(2) Show that the sum of the squares of the coordinates in the lattice point is divisible by p.
(3) Prove that p is the sum of four squares.

You may also enjoy this proof of Lagrange's Four-Square Theorem, written without any words with more than 4 letters: `https://web.stanford.edu/~yuvalwig/math/teaching/TheBarn.pdf`