Day 1: 2-D Lattices and Bases

We're going to start by just playing around with lattices to get a feel for how they work. Go to the "lattice player" `https://stanford.edu/~jonlove/mc20/lattice-play.html`.

Definitions

You will see two pink vectors labeled **u** and **v**.[a] As long as they don't lie on the same line, they form a **lattice basis**.

The gray points are obtained by taking $m\mathbf{u} + n\mathbf{v}$ for various integers m and n. These are called **lattice points** or **lattice vectors**. The set of all of these points is "**the lattice generated by the basis** $\{\mathbf{u}, \mathbf{v}\}$."

The pink parallelogram is called the **fundamental parallelogram of the basis** $\{\mathbf{u}, \mathbf{v}\}$. It conatins every point in the interior, as well as every point on the edge connecting O to **u**, and every point on the edge connecting O to **v**. It does *not* contain the points on the other two edges.

[a] I will use bold lowercase letters for vectors, italic lowercase letters for numbers.

Explore the following questions in breakout rooms. (You can take turns sharing your screen, or one of you can share your screen and the others can use annotations to discuss.)

Exploration 1

Move **u** and **v** around. Make observations about how the fundamental parallelogram changes, and how the lattice changes. Can you find **u** and **v** very long, but generating a nonzero lattice vector which is very short? Can you find a basis with a really funky stretched out fundamental parallelogram, but which generates a nice, even lattice?

Exploration 2

"The entire plane is a jigsaw puzzle, where each puzzle piece is an identical copy of the fundamental parallelogram."
First try to understand this visually, then prove Proposition 3. Make sure everyone in your group is satisfied; even if you figure it out, explaining your ideas clearly is a skill worth practicing! (Hint: the hard part is making the definitions precise.)

Proposition 3

Suppose $\mathbf{u}$ and $\mathbf{v}$ are linearly independent vectors in $\mathbb{R}^2$. Prove that every point in the plane can be written uniquely in the form $\mathbf{l}+\mathbf{p}$, where $\mathbf{l}$ is in the lattice generated by $\mathbf{u}$ and $\mathbf{v}$, and $\mathbf{p}$ is in the fundamental parallelogram of $\mathbf{u}$ and $\mathbf{v}$.

Definition

The **standard lattice** or **integer lattice** is the set of points

$$\mathbb{Z}^2 := \{(m,n) \mid m,n \in \mathbb{Z}\}.$$

For example, if $\mathbf{p} = (1,0)$ and $\mathbf{q} = (0,1)$, then $\{\mathbf{p},\mathbf{q}\}$ generates $\mathbb{Z}^2$.

Exploration 4

Find as many different choices of $\mathbf{u}$ and $\mathbf{v}$ as possible that generate $\mathbb{Z}^2$. (For example, what happens if you set $\mathbf{u} = (5,2)$ and $\mathbf{v} = (2,1)$?) Come up with a hypothesis for a criterion that determines whether a basis generates $\mathbb{Z}^2$.

Exploration 5

Now let's start to use the green and blue sliders! Choose a basis $\mathbf{u}$ and $\mathbf{v}$ that generates $\mathbb{Z}^2$ (from Exploration 4), and look for integers a, b, c, and d such that $a\mathbf{u}+b\mathbf{v} = (1,0)$ and $c\mathbf{u}+d\mathbf{v} = (0,1)$. Repeat with different choices of $\{\mathbf{u},\mathbf{v}\}$, and try to predict what a,b,c,d will work in each case.

Exploration 6

What algebraic relationships must be satisfied by the variables a,b,c,d and the components of $\mathbf{u}$ and $\mathbf{v}$ in order to guarantee that $a\mathbf{u}+b\mathbf{v} = (1,0)$ and $c\mathbf{u}+d\mathbf{v} = (0,1)$? Can you express these relationships in a single equation?

Exploration 7

Generalize your results to other lattices. That is, suppose a lattice is generated by a basis $\{\mathbf{u}, \mathbf{v}\}$, and the same lattice is also generated by $\{\mathbf{p}, \mathbf{q}\}$ (the previous explorations were considering the special case $\mathbf{p} = (1, 0)$ and $\mathbf{q} = (0, 1)$). What relationship must be satisfied by $\mathbf{u}, \mathbf{v}, \mathbf{p}, \mathbf{q}$?
(Hint: each basis appears in the lattice generated by the other)

Guiding question going forward:

Given a basis, what are the shortest vectors
in the lattice generated by this basis?

For some bases (like $\{(1, 0),\ (0, 1)\}$) this is easy, but it's not always so straightforward.

Exploration 8

What makes the basis $\{(1, 0),\ (0, 1)\}$ so easy to work with? Are there other bases for which it's easy to identify the short lattice vectors?

Optional Exploration: Lattice Points and Polygons

Exploration 9

Prove Theorem 10 and its corollary below. For the theorem, start with easy cases and build your way up to more complicated ones.

Theorem 10 (Pick's Theorem)

If the vertices of a polygon lie on a lattice $\mathcal{L}$ in $\mathbb{R}^2$, then the area of the polygon is

$$\left(i + \frac{b}{2} - 1\right) f,$$

where

- i is the number of points in $\mathcal{L}$ in the interior of the polygon,
- b is the number of points in $\mathcal{L}$ on the boundary of the polygon, and
- f is the area of the fundamental parallelogram of $\mathcal{L}$.

Corollary 11

Let S be any bounded convex subset of $\mathbb{R}^2$, and $\mathcal{L}$ be any lattice. Then the number of lattice points in S is at most

$$\frac{\text{Area}(S)}{f} + \frac{\text{Perimeter}(S)}{2\ell} + 1,$$

where f is the area of the fundamental parallelogram of $\mathcal{L}$, and ℓ is the length of the shortest nonzero vector in $\mathcal{L}$.
(You may use the following fact without proof: if A and B are convex subsets of $\mathbb{R}^2$ and A is contained in B, then the perimeter of A is at most the perimeter of B.)

Exploration 12

Explain why each of the three individual terms in Corollary 11 are necessary. That is, if you remove any individual term from the sum, describe a set S that would contain more lattice points than the modified sum would predict.

Exploration 13

Does a version of Pick's Theorem hold in 3 dimensions?