

Integer Lattices in a Linear Algebra Course

Pallavi Jayawant (Bates College), Dan Schaal (South Dakota State University), Jim Seibert (Regis University), Jessica Sidman (Mount Holyoke College), Kevin Woods (University of California, Berkeley)

Abstract

This is designed to be a module in a Linear Algebra course. The basic question we will explore is, “When can every d -dimensional integer vector be written as sums and differences of a given set of vectors?” A more formal way to say this (though you probably won’t phrase it like this to your class) is, “When does a set of vectors generate the lattice \mathbb{Z}^d ?” Some of the linear algebra concepts that we will use are determinants, inverses, bases, and solving simultaneous equations. This module would also fit in nicely in a beginning number theory class (exploring gcd and the Euclidean algorithm) or an abstract algebra class (delving into the theory of modules over a Principal Ideal Domain; in fact, this module would make a nice introduction to that subject).

Introduction and Goals

This module explores the question, “When can every d -dimensional integer vector be written as sums and differences of a given set of vectors?” Besides being a fun glimpse of some discrete math and geometry, it is a nice application of several core ideas of linear algebra, including determinants, inverses, bases, and solving simultaneous equations.

A couple of places you might want to insert this module into a linear algebra class are soon after the idea of the inverse is developed or when discussing how to solve simultaneous equations using matrices. The lesson plan will lead you through an interactive session and will encourage student experimentation. Exercises (with answers) follow the lesson plan. You might want to work through some of them in class by inserting and discussing them at the appropriate point of the lecture. Otherwise, you can give the ones you like to students as homework.

This module would also work very well in a number theory or an abstract algebra course. We will parenthetically note some ideas for these classes.

Beginnings: two integers in one dimension

Start with a question: “What integers can be written as sums and differences of 5 and 7?” Give the students a couple of examples:

$$12 = 5 + 7 \text{ and } 3 = 5 + 5 - 7.$$

Ask them to decide if 19 can be (answer: yes, $19 = 5 + 7 + 7$) and if 2 can be ($2 = 7 - 5$). How about 1? ($1 = 5 + 5 + 5 - 7 - 7 = 3 \cdot 5 - 2 \cdot 7$... say this aloud “three fives minus two sevens.”)

Ask for any guesses about which integers can be written as sums and differences of 5 and 7. Show them how to get every integer: for example, if we want to write 200 with fives and sevens take the equation

$$1 = 3 \cdot 5 - 2 \cdot 7$$

and multiply by 200 to get

$$200 = 200 \cdot 3 \cdot 5 - 200 \cdot 2 \cdot 7 = 600 \cdot 5 - 400 \cdot 7$$

(read aloud as “two hundred is six hundred fives minus four hundred sevens”).

Now do another example: “Can every integer be written as sums and differences of 4 and 6?” Get them to realize that you can only get even numbers when you take sums and differences. Make sure it is clearly stated that the problem is that the common factor of 2 cannot be gotten rid of. What about “9 and 12?” (Same problem, a common factor of 3.)

Ask for them to guess the answer to, “If we are given two numbers (like 5 and 7 or like 4 and 6) how can we tell whether every integer can be written as sums and differences of two numbers?” Answer: when they have no common factor. Unfortunately, there’s probably not enough time to prove this in a linear algebra class, but perhaps assign an exercise or two where they physically work it out for some other examples.

(In a number theory class, on the other hand, this should definitely be proven if it hasn’t already. The key is to use the Euclidean algorithm.)

(In an abstract algebra class, you might also want to prove this, because it is the starting point for the greatest common divisor of two elements of a PID.)

Two vectors in two dimensions

Ask, “Can every integer vector be written as sums and differences of $\begin{bmatrix} 3 \\ 2 \end{bmatrix}$ and $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$?”

Ask them to decide if $\begin{bmatrix} 7 \\ 4 \end{bmatrix}$ can be ($\begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \end{bmatrix} + 2 \begin{bmatrix} 2 \\ 1 \end{bmatrix}$).

How about $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ($\begin{bmatrix} 1 \\ 0 \end{bmatrix} = 2 \begin{bmatrix} 2 \\ 1 \end{bmatrix} - \begin{bmatrix} 3 \\ 2 \end{bmatrix}$)?

How about $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ ($\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 2 \begin{bmatrix} 3 \\ 2 \end{bmatrix} - 3 \begin{bmatrix} 2 \\ 1 \end{bmatrix}$)?

Argue as before that we can write any integer in this way, for example

$$\begin{aligned} \begin{bmatrix} 200 \\ 300 \end{bmatrix} &= 200 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + 300 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &= 200 \cdot (2 \begin{bmatrix} 2 \\ 1 \end{bmatrix} - \begin{bmatrix} 3 \\ 2 \end{bmatrix}) + 300 \cdot (2 \begin{bmatrix} 3 \\ 2 \end{bmatrix} - 3 \begin{bmatrix} 2 \\ 1 \end{bmatrix}) \\ &= -500 \begin{bmatrix} 2 \\ 1 \end{bmatrix} + 400 \begin{bmatrix} 3 \\ 2 \end{bmatrix}. \end{aligned}$$

Now ask, “Can every integer vector be written as sums and differences of $\begin{bmatrix} 3 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$?”

Can $\begin{bmatrix} 2 \\ 0 \end{bmatrix}$ ($\begin{bmatrix} 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix} - \begin{bmatrix} 1 \\ 1 \end{bmatrix}$)?

How about $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$? Have them try for a minute to find an answer (there isn't one).

Guide them to seeing why you can't do it: Tell them that we want to find integers a and b such that

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = a \begin{bmatrix} 3 \\ 1 \end{bmatrix} + b \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

(where a or b being negative would mean subtracting that many of the vector). Ask them if we could do it if a and b were allowed to be any real number (answer: yes, because $\begin{bmatrix} 3 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ form a basis of \mathbb{R}^2). Figure out what a and b would have to be using your favorite method of solving simultaneous equations (if this method is to write it as a matrix equation, then you're a step ahead of the game; if it's not, then we'll do that in a minute anyway). Answer: $a = \frac{1}{2}$ and $b = -\frac{1}{2}$. Ask them if any other a and b might work (answer: no, because the system of equations is nonsingular, or because $\begin{bmatrix} 3 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ form a basis). Conclude that $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ cannot be written as sums and differences of $\begin{bmatrix} 3 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$."

(Exercise 5 would be a great one to do in class if you have time. You could assign one vector to each student to see if it can be written as sums and differences, and then plot the answer on the board. Have them check more than 12 vectors if desired, but make sure that the fraction in part c will still work out.)

Doing it with matrices

If you haven't already, show them how to see this using matrices:

$$\begin{aligned} \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= a \begin{bmatrix} 3 \\ 1 \end{bmatrix} + b \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \end{aligned}$$

Multiply both sides by

$$\begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix}^{-1} = \frac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 3 \end{bmatrix}$$

(note that it's this $\frac{1}{\det} = \frac{1}{2}$ that is introducing ugly fractions that we don't want) to get the answer,

$$\begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}.$$

Go back to the first example with $\begin{bmatrix} 3 \\ 2 \end{bmatrix}$ and $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$ and do the same thing to show how we could have answered it:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

and multiply both sides by

$$\begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}^{-1} = \frac{1}{-1} \begin{bmatrix} 1 & -2 \\ -2 & 3 \end{bmatrix}$$

to get the answer

$$\begin{bmatrix} -1 \\ 2 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}.$$

Notice that $\det = -1$ made things work out nicely

Ask them to say in general, "If we are given two 2-dimensional vectors, how can we tell if every integer vector can be written as sums and differences them?" (answer: if the matrix you get by putting the two vectors side by side has determinant ± 1).

We're done!

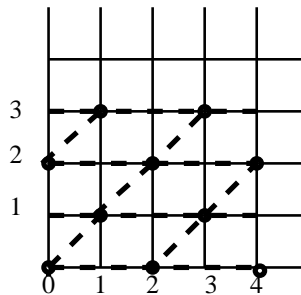
(In an abstract algebra class, work through Exercise 6. Depending on the level, you can say that you'll eventually prove it. The proof is from the theory of modules over a PID, where in this case, we are looking at modules over \mathbb{Z} . Basically, you find the Smith normal form for the lattice/module generated by your vectors. The Smith normal form will tell you whether the vectors generate the full \mathbb{Z}^d lattice. In particular, it is the full \mathbb{Z}^d lattice if the greatest common divisor of all of the $d \times d$ maximal minors of the matrix given by putting the vectors side by side is one.)

(In a number theory course, you should also work through Exercise 6, since gcd comes up again.)

Exercises

- Find two different ways to write 1 as sums and differences of 3 and 5.
(Possible answer: $1 = 2 \cdot 3 - 5$ and $1 = 2 \cdot 5 - 3 \cdot 3$.)
 - How can you write 0 as sums and differences of 3 and 5?
(Possible answer: $0 = 5 \cdot 3 - 3 \cdot 5$, "five threes minus three fives.")
 - Use part b to show how to find an infinite number of different ways to write 1 as sums and differences of 3 and 5.
(Possible answer: For any k , multiply the equation $0 = 5 \cdot 3 - 3 \cdot 5$ by k and add to $1 = 2 \cdot 3 - 5$ to get $1 = (5k + 2) \cdot 3 - (3k + 1) \cdot 5$. This gives a different way to write 1 for each k .)
- Can every integer be written as sums and differences of 3 and 7? Explain.
(Answer: yes. $\gcd(3, 7) = 1$, or notice $1 = 7 - 2 \cdot 3$ and so for any n , $n = n \cdot 7 - 2n \cdot 3$.)
 - What integers can be written as *sums* (no subtracting allowed!) of 3 and 7? (Hint: infinitely many integers can be)
(Answer: 3, 6, 7, 9, 10, 12, 13, 14, ... and everything else after that. Once we know 12, 13, and 14 can be written, we can add 3 to these to get 15, 16, and 17, add 3 again to get 18, 19, and 20, and so on. You probably want to ignore the subtlety that 0 is the "empty sum" of 3 and 7.)
- Show how to write 1 as sums and differences of 6, 10, and 15. Show that any integer can be written as sums and differences of 6, 10, and 15.
(Possible answer: $1 = 6 + 10 - 15$. Then for any n , $n = n \cdot 6 + n \cdot 10 - n \cdot 15$.)

- (b) Can every integer be written as sums and differences of 6 and 10? of 6 and 15? of 10 and 15? Explain.
(Answer: no to all three. In all cases there is a common factor.)
- (c) Can every integer be written as sums and differences of 6, 10, and 14? Why or why not?
(Answer: no. sums and differences can only give you even numbers, since all three numbers are even.)
- (d) How do you think that you can decide, given three integers, whether every integer can be written as sums and differences of these three?
(Answer: you can do it if and only if the three integers do not have a common factor except 1.)
- (e) How do you think that you can decide, given any number of integers, whether every integer can be written as sums and differences of these given integers?
(Answer: same thing. You can do it if and only if the integers have no common factor except 1.)
4. (a) Can all integer vectors be written as sums and differences of $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 17 \\ 1 \end{bmatrix}$? Explain.
(Answer: yes. Because $\det \begin{bmatrix} 1 & 17 \\ 0 & 1 \end{bmatrix} = 1$.)
- (b) Show how to make an infinite number of pairs of vectors in \mathbb{R}^2 such that, for each pair, all integer vectors can be written as sums and differences of those two vectors.
(Possible answer: For any k , $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $\begin{bmatrix} k \\ 1 \end{bmatrix}$ work, because $\det \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} = 1$.)
5. (a) For all integer vectors $\begin{bmatrix} x \\ y \end{bmatrix}$ with $1 \leq x \leq 4$ and $1 \leq y \leq 3$ (i.e., $\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \end{bmatrix}, \dots, \begin{bmatrix} 4 \\ 3 \end{bmatrix}$), decide whether $\begin{bmatrix} x \\ y \end{bmatrix}$ can be written as sums and differences of $\begin{bmatrix} 3 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$.
(Answer: $\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 3 \end{bmatrix}$, and $\begin{bmatrix} 4 \\ 2 \end{bmatrix}$ can be.)
- (b) Plot on graph paper the $\begin{bmatrix} x \\ y \end{bmatrix}$ that can be written in such a way. Notice any patterns?
(Answer: see picture.)



The points form “diamonds.”)

- (c) What fraction of the 12 integer vectors $\begin{bmatrix} x \\ y \end{bmatrix}$ with $1 \leq x \leq 4$ and $1 \leq y \leq 3$ can be written in such a way?
(Answer: $\frac{6}{12} = \frac{1}{2}$.)

- (d) In general, what fraction of integer vectors do you think can be written as sums and differences of two given vectors in \mathbb{R}^2 ? (Hint: look at the determinant of $\begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix}$ and compare to part c)

(Answer: $\frac{1}{|\det M|}$, where M is the matrix formed by putting the two vectors side by side.)

6. (a) Show that $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ can be written as sums and differences of $\begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 3 \\ 2 \end{bmatrix}$, and $\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$.

(Answer: $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} - \begin{bmatrix} 0 \\ 3 \\ 2 \end{bmatrix}$.)

- (b) Can every integer vector be written in such a way? Explain.
(Quick answer: yes. Do the same thing we did in 2 dimensions. Since $\det = 1$, the process will work.)
- (c) Given three integer vectors in \mathbb{R}^3 , how can we tell whether every integer vector can be written as sums and differences of these three? Explain. (Hint: generalize from two vectors in \mathbb{R}^2)
(Answer: if and only if the matrix formed by putting the three vectors side by side has determinant ± 1 . This works for the same reasons as the two dimensional case.)
- (d) Given n integer vectors in \mathbb{R}^n , how can we tell whether every integer vector can be written as sums and differences of them?
(Same answer.)

7. (a) Show that $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ can be written as sums and differences of $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$, $\begin{bmatrix} 1 \\ 3 \end{bmatrix}$, and $\begin{bmatrix} 0 \\ 2 \end{bmatrix}$. Show that $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ can also. Explain how to write any integer vector in such a way.

(Possible answer: $\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 2 \end{bmatrix} - \begin{bmatrix} 1 \\ 3 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix} + 3 \begin{bmatrix} 0 \\ 2 \end{bmatrix} - 2 \begin{bmatrix} 1 \\ 3 \end{bmatrix}$. Then we have

$$\begin{aligned} \begin{bmatrix} a \\ b \end{bmatrix} &= a \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ &= a \left(\begin{bmatrix} 2 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 2 \end{bmatrix} - \begin{bmatrix} 1 \\ 3 \end{bmatrix} \right) + b \left(\begin{bmatrix} 2 \\ 1 \end{bmatrix} + 3 \begin{bmatrix} 0 \\ 2 \end{bmatrix} - 2 \begin{bmatrix} 1 \\ 3 \end{bmatrix} \right) \\ &= (a+b) \begin{bmatrix} 2 \\ 1 \end{bmatrix} + (a+3b) \begin{bmatrix} 0 \\ 2 \end{bmatrix} - (a+2b) \begin{bmatrix} 1 \\ 3 \end{bmatrix}. \end{aligned}$$

- (b) Can every integer vector be written as sums and differences of $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 3 \end{bmatrix}$? of $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$

and $\begin{bmatrix} 0 \\ 2 \end{bmatrix}$? of $\begin{bmatrix} 1 \\ 3 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ 2 \end{bmatrix}$? Explain using determinants.

(Answer: no to all three. The determinants are, respectively 5, 4, and 2.)

- (c) Can every integer vector be written as sums and differences of $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$, $\begin{bmatrix} 4 \\ 3 \end{bmatrix}$, and $\begin{bmatrix} 6 \\ 0 \end{bmatrix}$?

Why or why not?

(Answer: no. Since all of the first coordinates are even, the first coordinate of all sums and differences will be even.)

- (d) Can every integer vector be written as sums and differences of $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 4 \\ 3 \end{bmatrix}$? of $\begin{bmatrix} 2 \\ 1 \end{bmatrix}$

and $\begin{bmatrix} 6 \\ 0 \end{bmatrix}$? of $\begin{bmatrix} 4 \\ 3 \end{bmatrix}$ and $\begin{bmatrix} 6 \\ 0 \end{bmatrix}$? Explain using determinants.

(Answer: no to all three. The determinants are, respectively, 2, -6, and -18.)

- (e) How do you think we can decide, given three integer vectors in \mathbb{R}^2 , whether every integer vector can be written as sums and differences of these three? (Hint: examine the determinants that you computed in parts b and d, and combine with ideas from our examination of two integers (like 5 and 7) in one dimension.)

(Answer: if and only if you take the determinants of the three matrices formed by taking any two of the three vectors and putting them side by side, and the three determinants have no common factor.)