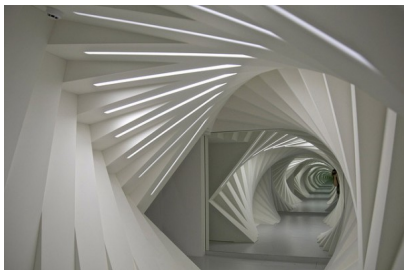


# Counting and Sizes of Infinity

Dr Lynne Walling

University of Bristol



Welcome to **Mathematics** at the **University of Bristol**, where our **teaching** is informed by our **research**.

I am a **number theorist**, which means that in my research I study questions primarily about the **integers**, which are

$$\dots, -3, -2, -1, 0, 1, 2, 3, \dots$$

**Number theorists** love to **count**. For instance, a classical question in number theory is:

*Given a positive integer  $t$ , how many ways can we write  $t$  as a sum of squares?*

For example, using 4 squares, we have:

$$\begin{aligned}10 &= 1^2 + 1^2 + 2^2 + 2^2 \\ &= 0^2 + 0^2 + 1^2 + 3^2,\end{aligned}$$

and

$$\begin{aligned}27 &= 0^2 + 1^2 + 1^2 + 5^2 \\ &= 1^2 + 1^2 + 3^2 + 4^2 \\ &= 0^2 + 3^2 + 3^2 + 3^2.\end{aligned}$$

*Note that for  $x \neq 0$ , we can replace  $x^2$  by  $(-x)^2$  and have another solution. For instance,  $10 = (-1)^2 + 1^2 + (-2)^2 + 2^2$ .*

**Generalising this question:** How many ways can we write an integer  $t$  as a sum of  $k$  squares?

For instance, how many integer solutions do we have to the equation

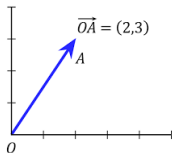
$$12,345 = x_1^2 + x_2^2 + x_3^2 + \cdots + x_{99}^2?$$

Instead of proceeding *case by case*, I want to count in an **intelligent** way, solving all cases at once.

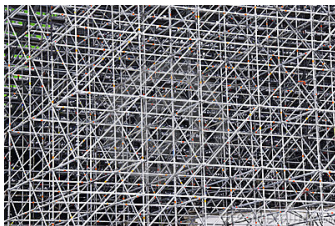
To do this, I use *mathematical structures* to **model** the information I want to count, *functions* to **encode** these counts, and then again use *mathematical structures* as well as **symmetry** to **decipher** these counts.

**STRUCTURE:** With  $x_1, x_2, \dots, x_k$  integers, I think of  $(x_1, x_2, \dots, x_k)$  as a vector in a *lattice*, sitting inside a  $k$ -dimensional space.

2-dimensions:



3-dimensions:



I can capture **geometry** by defining a *dot product* of vectors:

For **Euclidean** geometry, I set

$$(x_1, x_2, \dots, x_k) \cdot (y_1, y_2, \dots, y_k) = x_1y_1 + x_2y_2 + \dots + x_ky_k.$$

Then in the standard Euclidean geometry,

$$(x_1, x_2, \dots, x_k) \cdot (x_1, x_2, \dots, x_k) = x_1^2 + x_2^2 + \dots + x_k^2$$

is (the square of) the **length** of the vector  $(x_1, x_2, \dots, x_k)$ , and this vector is perpendicular to the vector  $(y_1, y_2, \dots, y_k)$  exactly when

$$(x_1, x_2, \dots, x_k) \cdot (y_1, y_2, \dots, y_k) = 0.$$

So my original question can be rephrased: *Given an integer  $t$ , how many vectors in the lattice have (squared) length  $t$ ?*

**GENERALISING:** There are other **geometries** I can capture on this  $k$ -dimensional space, by redefining the **dot product**.

For instance, in 2-dimensional space, I can define

$$(x_1, x_2) \cdot (y_1, y_2) = 3x_1y_1 + x_1y_2 + x_2y_1 + 5x_2y_2,$$

corresponding to the vector  $(x_1, x_2)$  having (squared) length

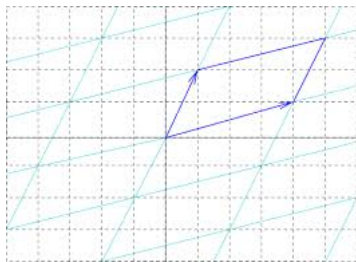
$$(x_1, x_2) \cdot (x_1, x_2) = 3x_1^2 + 2x_1x_2 + 5x_2^2.$$

So in *this* geometry, the (squared) length of the vector  $(1, 0)$  is 3, the (squared) length of the vector  $(-1, 3)$  is 42, and these vectors are perpendicular as

$$(1, 0) \cdot (-1, 3) = -3 + 3 + 0 + 0 = 0.$$

**GENERALISING FURTHER:** Instead of just looking at each vector singly, I could take a *sublattice* and look at the geometry it inherits.

*Example of a sublattice of the standard 2-dimensional lattice:*



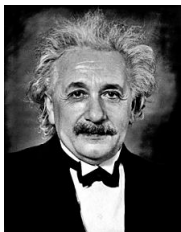
Then I can ask: *Given an  $n$ -dimensional geometry  $T$ , how many  $n$ -dimensional sublattices of our  $k$ -dimensional lattice have their geometry described by  $T$ ?*

**MORAL:** **Mathematical structure** and **symmetry** are beautiful things, and **functions** are our friends!



In the 1st year course *Foundations and Proof*, we explore **SIZES OF INFINITY**.

Let's ask first: **Does infinity exist?**



Albert Einstein, 1879 – 1955

*Two things are infinite: the universe and human stupidity; and I'm not sure about the universe.*

*Everything that can be counted does not necessarily count; everything that counts cannot necessarily be counted.*

We use the numbers  $1, 2, 3, 4, 5, \dots$  to count, so we sometimes call these the *counting numbers*, or more formally, the *positive integers*.

We use  $\mathbb{Z}_+$  to denote the set (that is, the collection) of all the positive integers, of which there are **infinitely** many.

We say that a set  $X$  is *countable* if there is a one-to-one correspondence between the elements of  $X$  and the elements of  $\mathbb{Z}_+$ , and when there is we write

$$|X| = |\mathbb{Z}_+|.$$

(So we think of  $|\mathbb{Z}_+|$  as capturing the “size” of the set of positive integers.)

**Is every infinite set countable?**

First, we note that every **infinite** set  $X$  contains a countable subset.

*Intuitively:* Suppose  $X$  is an infinite set. Choose  $a_1$  from  $X$ .

Next, choose  $a_2$  from  $X$  so that  $a_2 \neq a_1$  (possible since  $X$  is infinite).

Then, choose  $a_3$  from  $X$  so that  $a_3 \neq a_1$  and  $a_3 \neq a_2$ .

Continue... We get a subset  $A = \{a_1, a_2, a_3, \dots\}$  of  $X$  with  $|A| = |\mathbb{Z}_+|$ .

**WARNING!** The argument above is *inductive*, meaning that it describes an *algorithm*, which in our lifetime we can only apply finitely many times. So to make this argument **rigorous** one needs to use the technique of *Transfinite Induction*, or *The Axiom of Countable Choice*, or ...

**Conclusion:**  $|\mathbb{Z}_+|$  is the “smallest magnitude of infinity”.

Thus there must be as many **even positive integers** as there are **positive integers** (since the set of **even positive integers** is **infinite** and is **contained in** the set of **positive integers**).

Here is a one-to-one correspondence between the **positive integers** and the **even positive integers**:

positive integers  $\leftrightarrow$  even positive integers

$$1 \leftrightarrow 2$$

$$2 \leftrightarrow 4$$

$$3 \leftrightarrow 6$$

$\vdots$

$$n \leftrightarrow 2n$$

$\vdots$

Now consider  $\mathbb{Z}_+ \times \mathbb{Z}_+$ , the set of ordered pairs of positive integers. Surely there are **more** of these than there are positive integers...  
**or are there?**

**Claim:**  $|\mathbb{Z}_+ \times \mathbb{Z}_+| = |\mathbb{Z}_+|$ .

To prove this, we need to set up a one-to-one correspondence between the collection of ordered pairs of positive integers and the positive integers.

A grid of the ordered pairs of positive integers

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: ONE

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: TWO

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	



## Counting: **THREE**

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: **FOUR**

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: **FIVE**

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: **SIX**

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
<b>(3, 1)</b>	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: SEVEN

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: **EIGHT**

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: **NINE**

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: **TEN**

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
<b>(4, 1)</b>	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	



## Counting: **ELEVEN**

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: **TWELVE**

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: THIRTEEN

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: **FOURTEEN**

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	<b>(4, 2)</b>	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

## Counting: **FIFTEEN**

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
<b>(5, 1)</b>	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

**Formula?** Note that we have been counting along successive cross-diagonals.

(1, 1)	(1, 2)	(1, 3)	(1, 4)	(1, 5)	...
(2, 1)	(2, 2)	(2, 3)	(2, 4)	(2, 5)	...
(3, 1)	(3, 2)	(3, 3)	(3, 4)	(3, 5)	...
(4, 1)	(4, 2)	(4, 3)	(4, 4)	(4, 5)	...
(5, 1)	(5, 2)	(5, 3)	(5, 4)	(5, 5)	...
⋮	⋮	⋮	⋮	⋮	

(3, 2) is the 3rd pair on the 4th cross-diagonal.

On the first 3 cross-diagonals, there are  $1 + 2 + 3 = 6$  pairs.

So the pair (3, 2) is the  $3 + 6$ th pair that we count.

*More generally,  $(m, n)$  is the  $m + \frac{(m+n-2)(m+n-1)}{2}$ th pair that we count.*

We can use this to show that there are as many **positive integers** as there are **positive rational numbers** (which are all numbers of the form  $\frac{m}{n}$  where  $m$  and  $n$  are positive integers).

Each positive rational number can be written **uniquely** as  $\frac{m}{n}$  where  $m$  and  $n$  are positive integers with  $\text{hcf}(m, n) = 1$ .

So we can identify the set of **positive rational numbers** with a **subset** of  $\mathbb{Z}_+ \times \mathbb{Z}_+$ , the set of **ordered pairs of positive integers**:  $\frac{m}{n} \leftrightarrow (m, n)$ .

Hence with  $\mathbb{Q}_+$  denoting the set of **positive rational numbers**, we have

$$|\mathbb{Q}_+| \leq |\mathbb{Z}_+ \times \mathbb{Z}_+| = |\mathbb{Z}_+|.$$

But we also know that each **positive integer** is a **positive rational number**, so

$$|\mathbb{Z}_+| \leq |\mathbb{Q}_+|.$$

Thus  $|\mathbb{Q}_+| = |\mathbb{Z}_+|$ .

Are all infinite sets countable, meaning the same “size” as  $\mathbb{Z}_+$ ?

No!

We can show that there are more **real** numbers in the interval between 0 and 1 than there are **positive integers**.

To do this, we argue by **contradiction**: We assume there **are** as many positive integers as there are real numbers between 0 and 1, and we then derive a **contradiction**.

**Technical fact:** Each real number has a **unique** decimal expansion, **provided** we not use any decimal expansion that ends in all 9's.

*Using geometric progressions, we can show that  $0.99999\dots = 1$ , so for instance,  $0.356799999\dots = 0.35680000\dots$*



**Suppose** that the real numbers between 0 and 1 are **countable**, meaning that they are in one-to-one correspondence with the positive integers. Then we can **enumerate** these real numbers as

$$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \dots$$

Each of these has a decimal expansion. For instance,

$$\alpha_1 = 0.a_{1,1}a_{1,2}a_{1,3}a_{1,4}a_{1,5}\dots$$

where each  $a_{1,j}$  is a digit in the decimal expansion of  $\alpha_1$ .

(So  $a_{1,j} = 0, 1, 2, 3, 4, 5, 6, 7, 8, \text{ or } 9$ .)

We create a grid of these numbers with their decimal expansions:

$$\alpha_1 = 0.a_{1,1}a_{1,2}a_{1,3}a_{1,4}a_{1,5} \cdots$$

$$\alpha_2 = 0.a_{2,1}a_{2,2}a_{2,3}a_{2,4}a_{2,5} \cdots$$

$$\alpha_3 = 0.a_{3,1}a_{3,2}a_{3,3}a_{3,4}a_{3,5} \cdots$$

$$\alpha_4 = 0.a_{4,1}a_{4,2}a_{4,3}a_{4,4}a_{4,5} \cdots$$

$$\alpha_5 = 0.a_{5,1}a_{5,2}a_{5,3}a_{5,4}a_{5,5} \cdots$$

$\vdots$

Now we construct another real number  $\beta$  between 0 and 1 that is **not** in the list  $\alpha_1, \alpha_2, \alpha_3, \dots$ :

We look at the “diagonal” of our grid of decimal expansions:

$$\alpha_1 = 0.a_{1,1}a_{1,2}a_{1,3}a_{1,4}a_{1,5}\cdots$$

$$\alpha_2 = 0.a_{2,1}a_{2,2}a_{2,3}a_{2,4}a_{2,5}\cdots$$

$$\alpha_3 = 0.a_{3,1}a_{3,2}a_{3,3}a_{3,4}a_{3,5}\cdots$$

$$\alpha_4 = 0.a_{4,1}a_{4,2}a_{4,3}a_{4,4}a_{4,5}\cdots$$

$$\alpha_5 = 0.a_{5,1}a_{5,2}a_{5,3}a_{5,4}a_{5,5}\cdots$$

$\vdots$

We set  $\beta = 0.b_1b_2b_3b_4b_5\cdots$  where

$$b_i = \begin{cases} 1 & \text{if } a_{i,i} \neq 1, \\ 2 & \text{if } a_{i,i} = 1. \end{cases}$$

We know that  $\beta$  is **not** equal to any  $\alpha_i$  since the  $i$ th digit in the decimal expansion of  $\beta$  is not equal to the  $i$ th digit in the decimal expansion of  $\alpha_i$ .

This is our **contradiction**:

We *assumed* that the set of real numbers between 0 and 1 was **countable**, meaning that we could enumerate all of them as  $\alpha_1, \alpha_2, \alpha_3, \dots$ , and then we *constructed* a real number  $\beta$  between 0 and 1 that is not in this list.

Hence it **cannot** be the case that the set of **real** numbers between 0 and 1 is **countable**.

Thus the **magnitude** of the set of real numbers between 0 and 1 is **larger** than that of the positive integers.

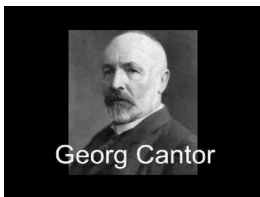
Mathematicians have **proved** that there is a one-to-one correspondence between **all** real numbers, and those between 0 and 1 (we will prove this). (So in some sense, the magnitude of the **unit interval** is the same as the magnitude of the **real line**.)

Mathematicians have also proved that there are magnitudes of infinity **larger** than that of the real line (we will prove this).

**Unknown:** Is there a magnitude of infinity **between** that of the positive integers and that of the real numbers?



*Infinity is a dreadfully poor place.  
They can never manage to make ends meet.*  
– Norton Just, *The Phantom Tollbooth*



Georg Cantor, 1845 – 1918

Cantor introduced and studied these notions of **magnitudes of infinity**, which he believed came directly from God.

Although Cantor's work is now fundamental in mathematics, initially there were mathematicians and philosophers who objected vehemently to Cantor's claims and methods of argument, calling him a *scientific charlatan* and a *corrupter of youth*, whose work was *laughable, wrong* and *contradicted the uniqueness of the absolute infinity in the nature of God*.



Bertrand Russell, 1872 – 1970

Another significant outcome of Cantor's work was the discovery of certain **paradoxes**, exemplifying that not everything one can think to write down gives an **unambiguous** definition, and in particular, that one needs to be careful when defining a **set**.

For instance, in 1901 Russell presented the following:  
Suppose there is a set  $R$  consisting of all sets that do not contain themselves as elements.

**But then we have an unresolvable paradox:**

If  $R \notin R$  then  $R \in R$ , and if  $R \in R$  then  $R \notin R$ .

A variation of this paradox is the following:

## A PARADOX:

The barber is the man in town who shaves all the men who do not shave themselves.



*Who shaves the barber?*