Primes

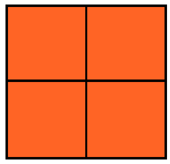
Why are many mathematicians obsessed with prime numbers?

Prime numbers are the building blocks of all the numbers – Gauss proved around 1800 that all numbers can be written as a unique product of primes. But there is no simple formula that can tell us the n^{th} prime, or whether a given number is prime. The most important unsolved problem in Pure Mathematics, the Riemann Hypothesis, concerns the distribution of the primes.

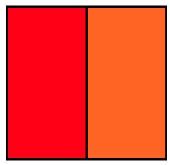
These pages are designed to be a gentle introduction to visualizing prime numbers, for students of any age.

Numbers as shapes

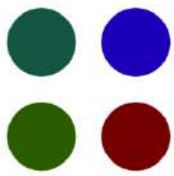
What shape is a number? For example, what shape is the number 4? Some people (mathematicians) might visualize the number 4 as a square.



Or you could picture it like this, made up of two 2s:



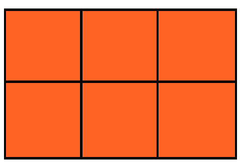
You might have used blobs like this:

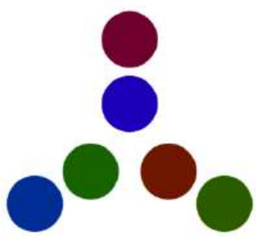


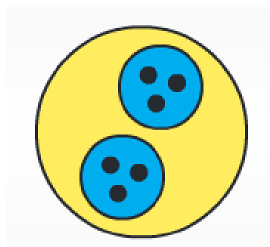
Here is an image of 4 from the online applet **primitives**: http://www.ptolemy.co.uk/project/primitives.

Why do you think it is represented this way?

Here are some representations of the number **6**:



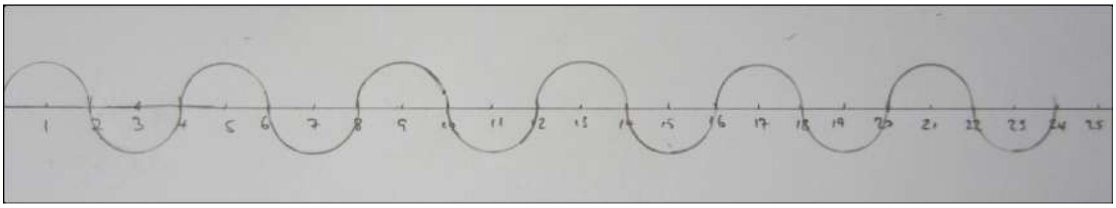




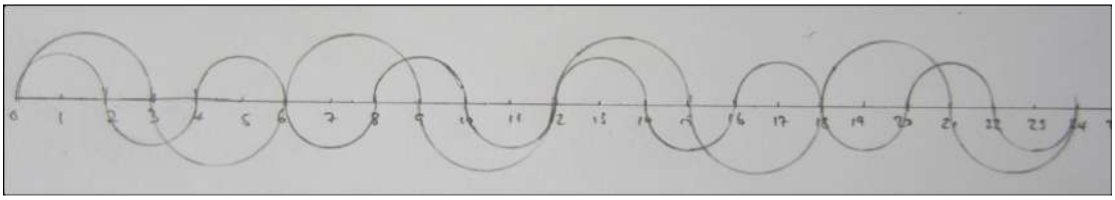
Draw some other numbers as shapes like this.

Prime curves

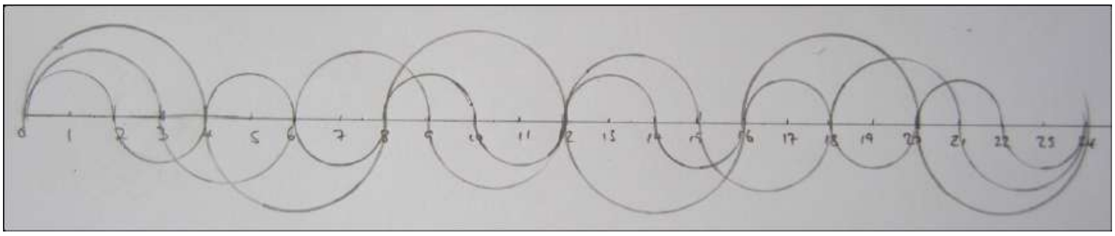
Here is an image of the 2x table drawn as a curve through the number line:



When we add the 3x table, we get:

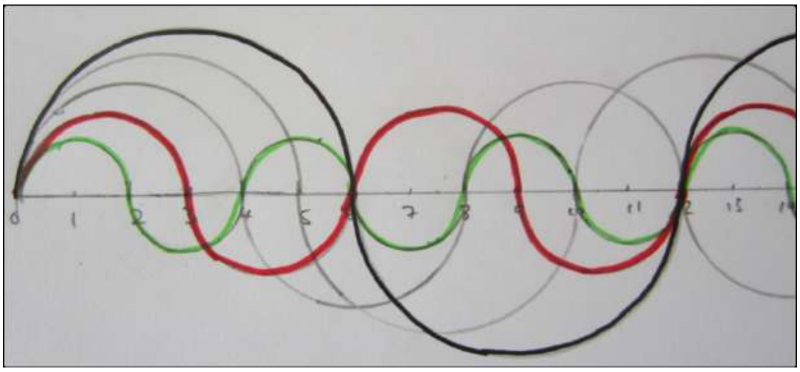


Notice how some numbers (such as 6) have been crossed twice. Now let’s add the 4x table:



What can you say about the numbers that haven’t been crossed yet? How many times will these numbers be crossed if we keep going?

When you have drawn more (all) curves, pick a number and highlight all the curves that go through it, like this one for 6:



What can you say about the number of curves through different numbers?

This was inspired by this online applet: http://www.jasondavies.com/primos/

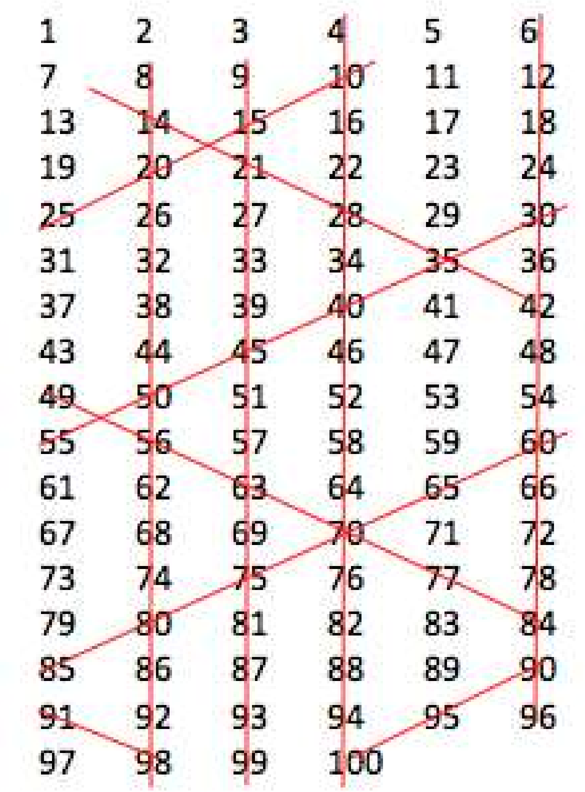
Finding primes

It is not easy to find out if a number is prime; you have to divide it by all the numbers up to its square root and see if any of them divide into it. Or alternatively you can look on the web.

You will have heard of the Sieve of Eratosthenes before; this gives a systematic way of finding the primes by crossing out all the numbers that are in all n times tables (apart from n itself).

Even this is a bit dull, but here is a nice way of doing it for numbers up to 100:

Put all the numbers in a grid like this and cross out times tables with lines like this:



What can you say about prime numbers by looking at this grid?

The twin prime conjecture says that there are an infinite number of primes that are 2 apart (such as 5 and 7). Why does this suggest this might be the case?

A prime triple is three primes that are 2 apart, such as 3, 5 and 7. What does this picture tell us about other triple primes?

Prime sequences

Linear (arithmetic) sequences are sequences that go up by the same amount each time, such as 5, 9, 13, 17, 21, …

You may have noticed that this sequence contains a lot of primes. If you carry on this sequence, can you estimate roughly what percentage of it are primes? Conversely, roughly how many of the primes are in this sequence?

Find some other linear sequences that contain a lot of primes (hint: look at the previous section!).

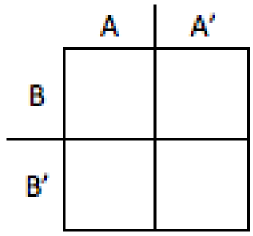
The sequence above has 2 primes in a row (13 and 17). Does this sequence ever have more than 2 primes in a row?

Can you find a sequence with 3 primes in a row? Or more?

Prime Karnaugh maps

If you have read the section on Boole, you will know all about Karnaugh maps.

If not, here’s a quick introduction. Karnaugh maps are like Venn diagrams; they show intersections between sets. Members of both sets A and B it would go in the top left corner. Members of set A but not B (B’) would go in the bottom left corner.

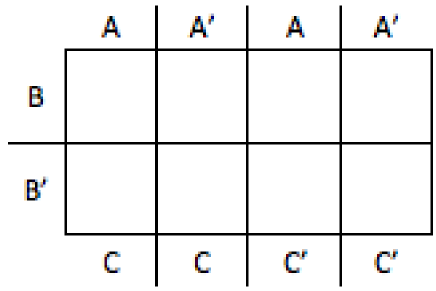


If A is the set of all even numbers and B is the set of all multiples of 3, where would you put the numbers 1 to 10 in this Karnaugh map?

Can you say anything about the types of numbers in each box?

Here is a 3-set Karnaugh map.

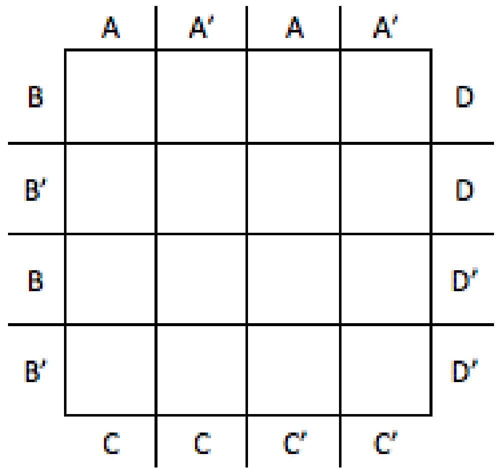
If C is the set of all multiples of 5, where would the numbers 1 to 15 go?



Let’s go crazy and make a 4-set Karnaugh map

Put the numbers 1 to 30 on this map, where:

A = multiples of 2
B = multiples of 3
C = multiples of 5
D = multiples of 7



What do you notice about numbers in different boxes?

What if you keep going past 30?

Can you draw a 5-set Karnaugh map?

Try all these activities on a Venn diagram. Which do you prefer?

Prime spiral

You may have seen the Ulam spiral (on the right) before.

Continue the spiral, then circle all the prime numbers. What do you notice? Why do you think this is?

Why have I started at 41 instead of 1? Explore spirals starting with different numbers.

						83
66	65	64	63	62	61	82
67	50	49	48	47	60	81
68	51	42	41	46	59	80
69	52	43	44	45	58	79
70	53	54	55	56	57	78
71	72	73	74	75	76	77

Here is something you may not have seen called the *Klauber triangle*, named after Laurence Klauber, an American expert in rattlesnakes:

					1					
				2	3	4				
			5	6	7	8	9			
		10	11	12	13	14	15	16		
	17	18	19	20	21	22	23	24	25	
26	27	28	29	30	31	32	33	34	35	36

Continue the triangle and circle the primes. Any interesting patterns?

If you read the section on *Babbage*, you will know a bit about prime generating functions. What are the functions that generate the most primes in this triangle?

What happens if you start the Klauber triangle with different numbers at the top, like maybe 41?

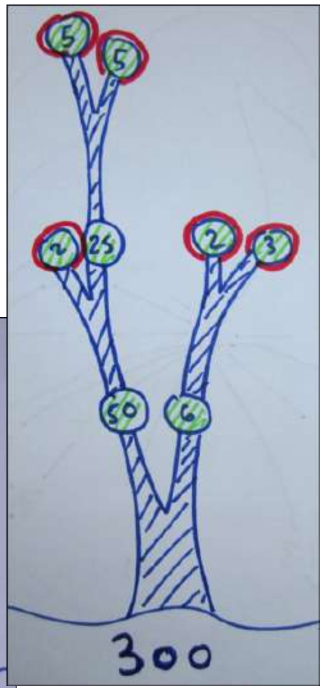
Prime games

Prime Nim (Shannon's Nim): Play *Nim* (see the section on *Fibonacci*) with one pile of counters, where you can only take a prime number of counters - but let's include 1 as a prime to make things simpler.

What are the safe positions for this game? Extend this to more than one pile. What if we do not include 1 as a prime?

Last prime: Two players alternatively hold up any number of fingers from one to five. The cumulative total is noted down. The object is to keep the total prime. The first player unable to raise the total to a higher prime is the loser. If you play first, how many fingers should you hold up?

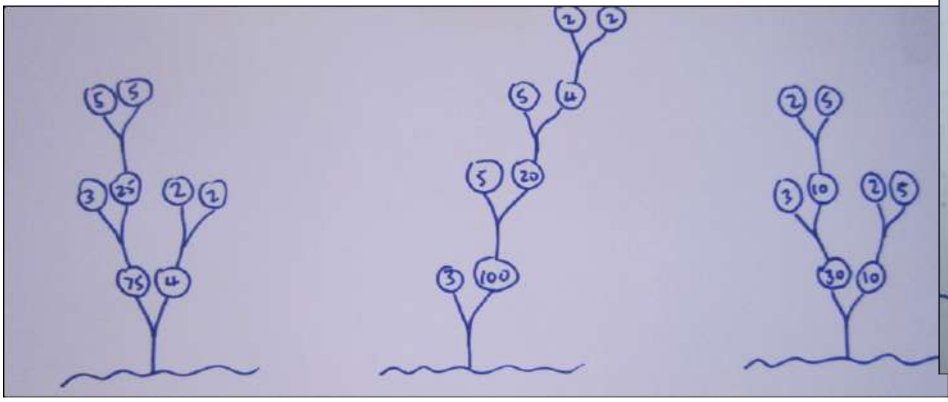
Play this again but with both hands (10 fingers). What should you start with this time?



Prime factors

Usually prime factors are found using a factor tree.

Here are lots of different ways of factorizing 300:



However you do it, they all come up with the same answer 300 = 2 x 2 x 3 x 5 x 5.

But did you also notice that:

- They all have 4 pairs of factors too?

- There is one even pair of factors in each and one pair of factors divisible by 5. (In the third one above, the even pair is also the pair that is divisible by 5).

- The rest of the pairs are relatively prime.

Can you explain any of these facts? Investigate similar facts for other prime factorizations.

Uniqueness

Have you ever thought about the uniqueness of prime factorization?

To prove that the prime factors of a number are unique, we need something called *Euclid's Lemma*, which says that if a prime p divides a composite number r x s, then either p divides r or p divides s. Try this out for yourself.

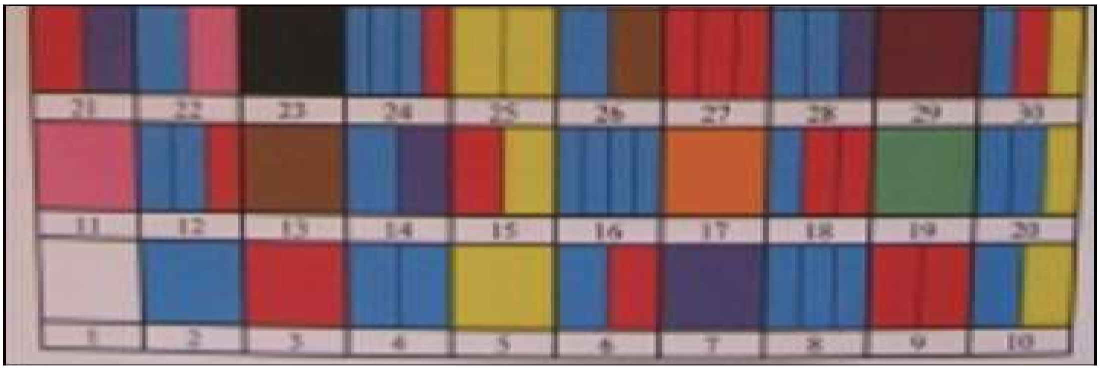
Suppose there were two different prime factorizations of 300. We know one factorization is 2.2.3.5.5; the other one could either have 5 different factors, or a different number of factors altogether.

Let the other factorization be *p.q.r.s.t.u….* for some other primes *p*, *q*, *r*, … How can you use Euclid's Lemma to prove that the factorization 2.2.3.5.5 is unique?

Prime clothing

There are numerous items of clothing on the internet that have mathematical designs. I particularly like this prime factorization jumper created by Sondra Eklund:

Can you see how it works? If you can't quite work it out, here's the pattern with the first few numbers on it:



Can you spot any patterns in the columns or diagonals of this pattern?

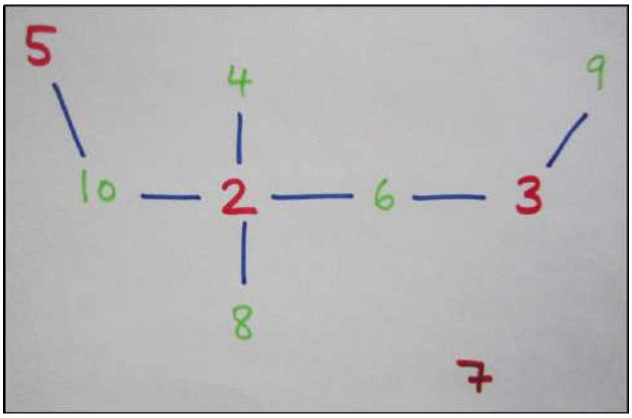
Can you create your own prime factorization pattern?

Factor maps

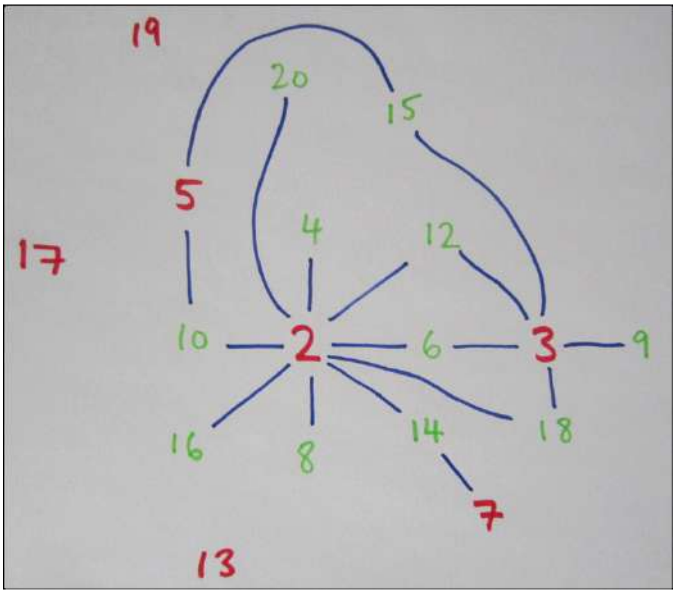
In the picture on the right, the prime (red) numbers are joined to non-primes (green) if they are a factor.

This is a tree in the mathematical sense of the word (no loops).

Will it always be possible to join the numbers using a tree?



If you keep going, you realize that this can't be possible (why?):



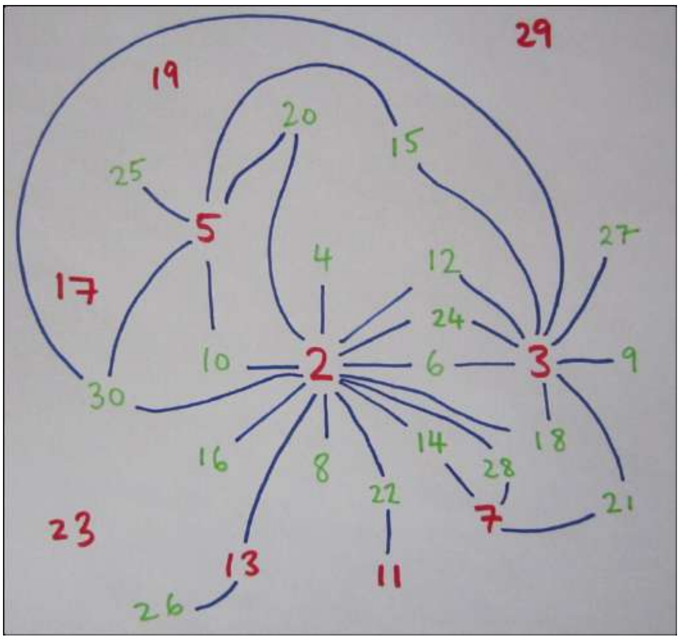
There is a loop 2-6-3-12.

But will it be possible to keep joining the numbers in this way without crossing the lines over (i.e. a *planar* graph)?

Here is as far as I got (up to 30). The graph is still planar – can this keep going forever?

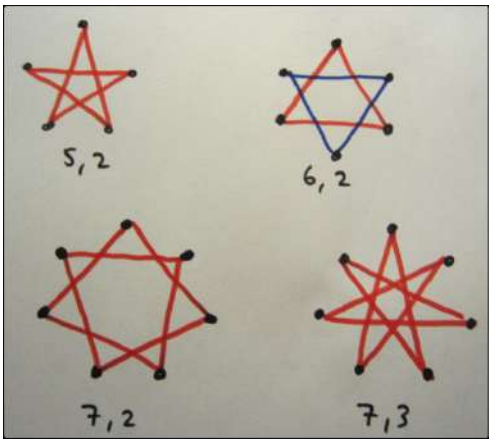
Is there a particular way you have to draw it to keep it planar?

Explore for yourself!



Prime stars

You have probably made some star doodles at some point. If you haven't, draw some dots (roughly) evenly round a circle and join them missing a few each time. Here are a few:



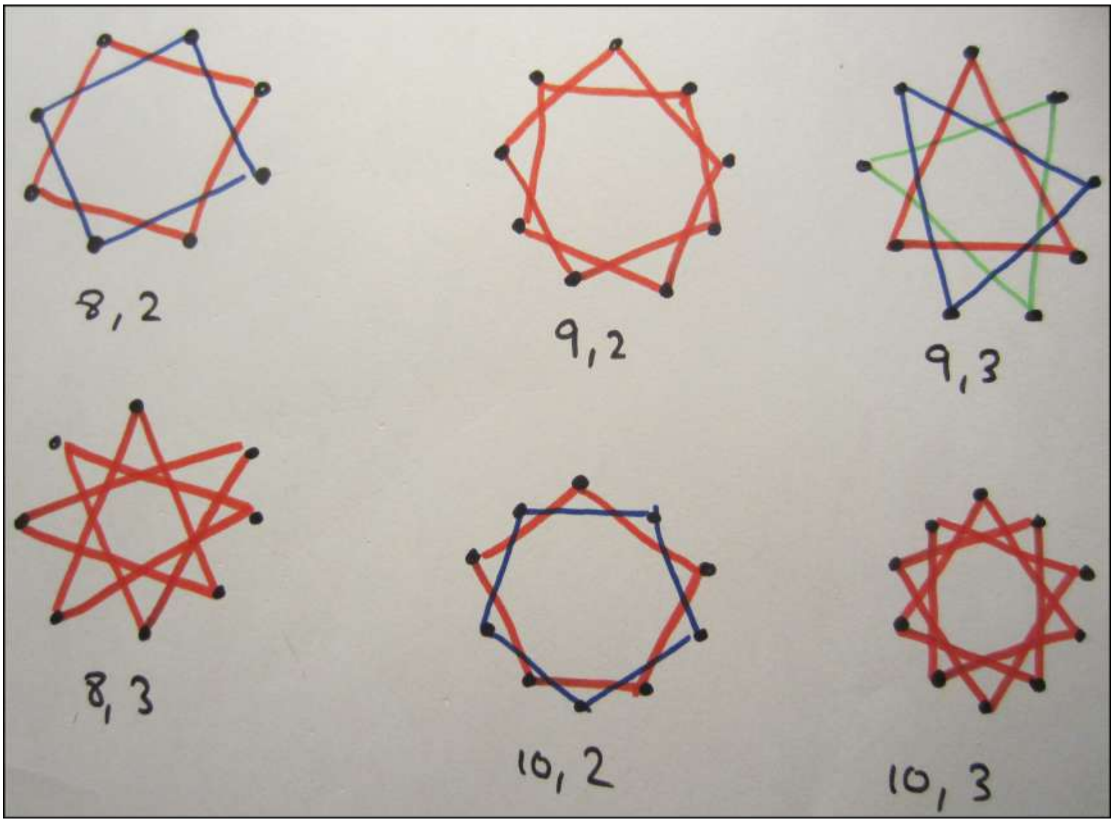
The first number is the number of dots and the second number is how many missed each time.

Which ones make good stars? Well, they're all good, but my favourite are the ones that go back to the start without taking pen from paper.

Find some other stars that can go back to the start without taking pen from paper.

What can you say about the ones that go back to the start?

I was thinking it was something to do with the first number being prime (5 and 7 here), so I drew a few more:



As you can see, it is not as simple as the first number being a prime number, as (8,3) and (10,3) both work.

So what *is* it about?

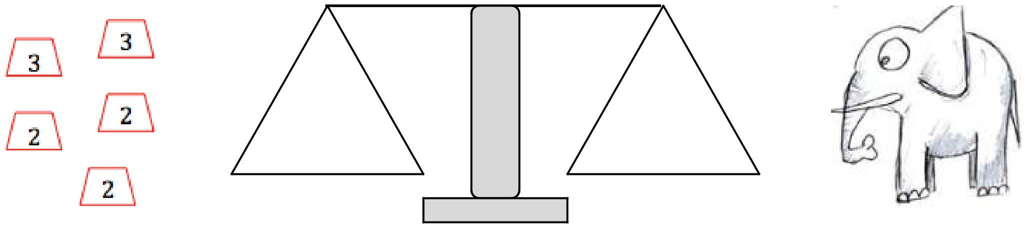
Greatest common divisors

You have to learn about these at school (sometimes called Highest Common Factors), but what's the big deal with them?

Diophantine equations

They are important in the theory of *Diophantine equations*, which is concerned with finding **integer** solutions to equations of the form $ax + by = c$.

But before that, a classic puzzle: How can you weigh any object (that weighs a whole number of kilograms) on a pair of balancing scales with a (infinite) set of 2kg and 3kg weights? What if the elephant weighed 1kg?



Solved it? If the elephant weighed 1kg, this is the same as trying to find two integers x and y that solve $2x + 3y = 1$? Can you solve this? How many different solutions can you find?

Now suppose we had 2kg and 4kg weights instead; can we weigh any elephant now? Which elephants can we not weigh? Can you weigh a 1kg elephant? Try solving $2x + 4y = 1$. How many different (integer) solutions can you find?

You may have realized that the second one is not solvable, but why not?

Can you tell by looking at these Diophantine equations if they will have solutions?

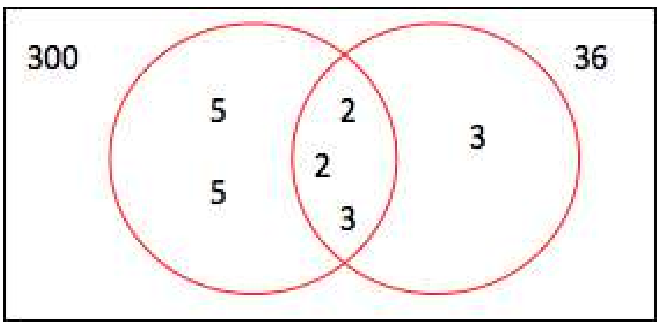
(a) $2x + 3y = 2$ (b) $3x + 6y = 99$ (c) $4x + 6y = 99$

Finding GCDs

How do we find GCDs? What is the GCD of (say) 300 and 36? One method you may have seen is to use prime factorization:

Find 300 = 2.2.3.5.5 and 36 = 2.2.3.3, then put these factors in a Venn diagrams like this.

The GCD is the product of the factor in the middle, which here is 2.2.3 = 12.



A nice by-product of this method is that you get the Lowest Common Multiple (LCM) for free! If you take the product of all the numbers in the Venn diagram you get the LCM, so here it is 2.2.3.3.5.5.

What are the drawbacks of this method? Try it for two larger numbers like 3108 and 5291.

And finally, this method suggests that the GCD and LCM are closely connected – can you see how?

Euclid's algorithm

Another method, which is more suitable for larger numbers, is *Euclid's algorithm*, which basically uses the division algorithm.

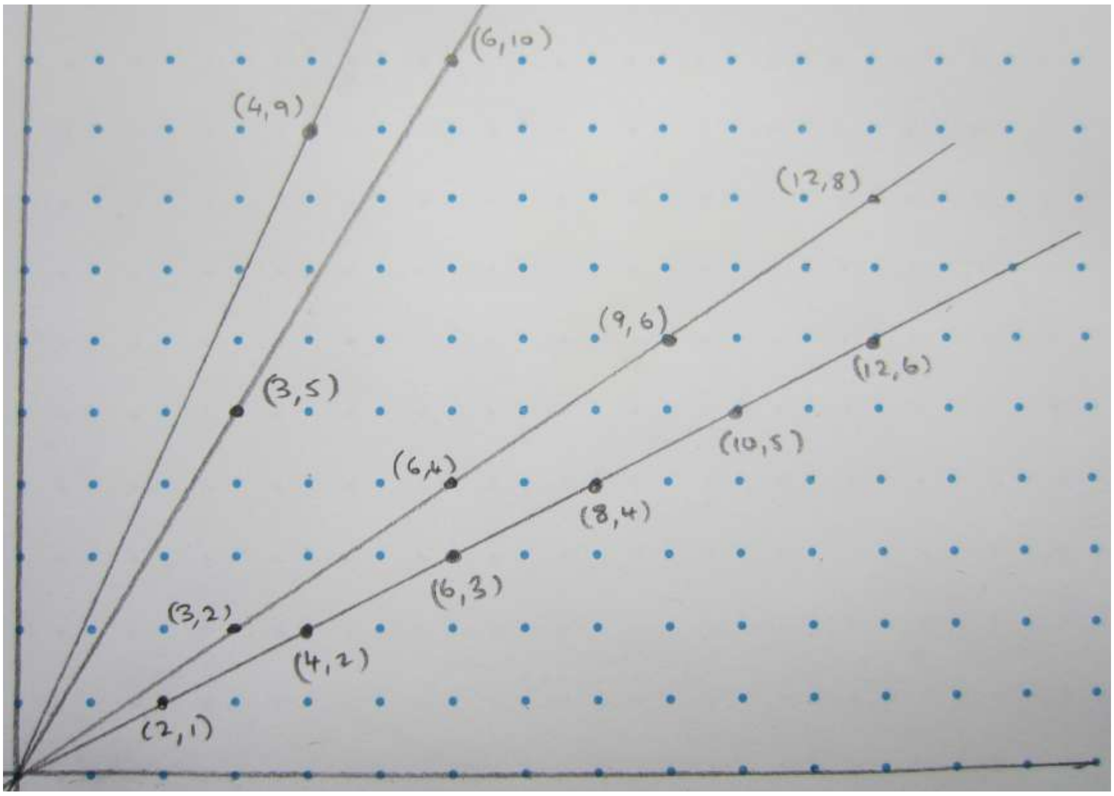
Here is the algorithm used to find the GCD of 300 and 36:

300 = 8 x 36 + **12**
36 = 3 x 12 + 0

The answer is the last non-zero remainder, which is 12. Can you see how (and why) it works? Try it with some larger numbers (like 3108 and 5291) to get an idea of what is going on.

Line segments

Look at these lines. How is the number of lattice points (integer co-ordinates) connected to GCD?



Relatively prime fractions

Here's a little starter: You probably know that to reduce a fraction to its simplest form you must divide numerator and denominator by their greatest common divisor. Can you make 15 fractions from the numbers 1 to 30 such that all are in their simplest form?

Now, here's a more interesting investigation:

Choose a number n. I am going to choose 4. Now find all pairs of relatively prime numbers that are less than or equal to n.

So I have pairs (1,2) (1,3) (1,4) (2,3) and (3,4).

Now discard those pairs with a pair **sum** less than or equal n.

So I discard (1,2) and (1,3).

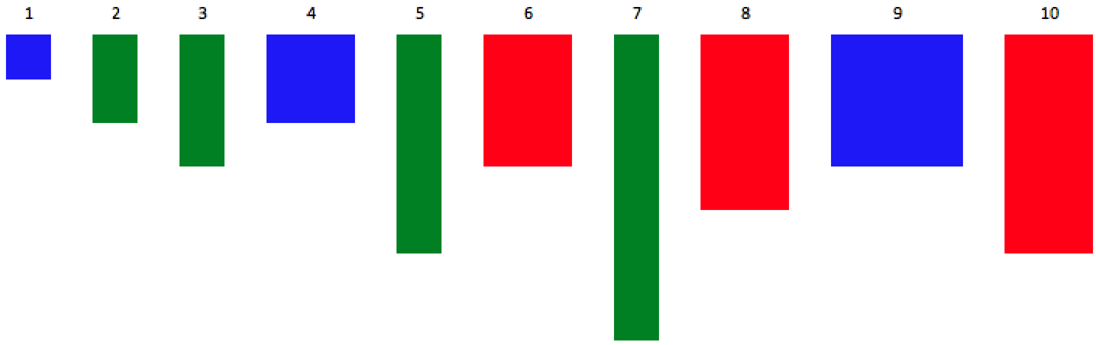
I am left with (1,4) (2,3) and (3,4).

Now work out: $\frac{1}{1\times 4}+\frac{1}{2\times 3}+\frac{1}{3\times 4}=\frac{1}{4}+\frac{1}{6}+\frac{1}{12}=\frac{1}{2}$

Try this for other numbers n. What do you notice? Can you explain what is happening?

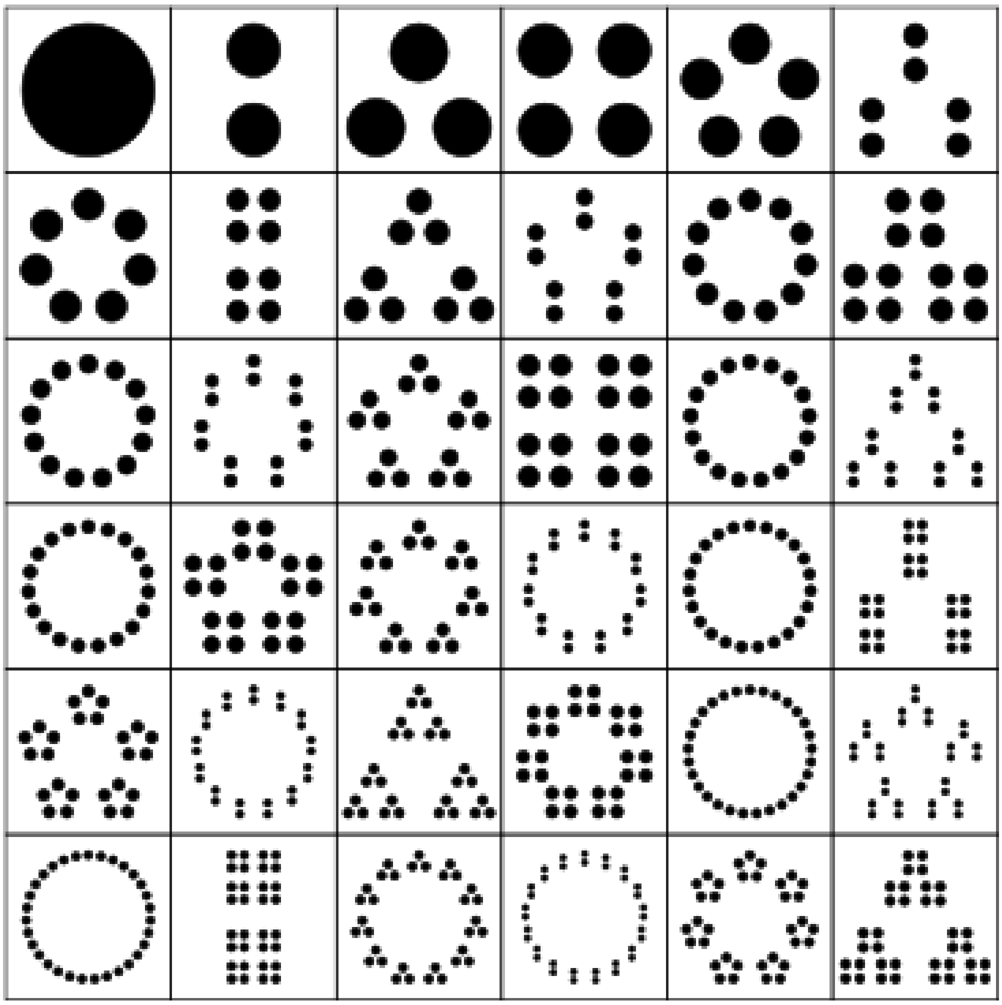
Notes on Numbers as Shapes

If we stick with squares and rectangles, then we get the following



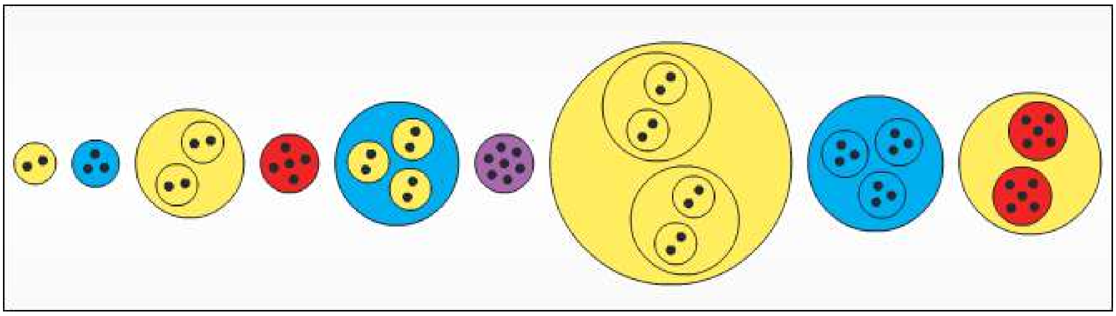
We can see the prime numbers as 1xp rectangles.

Using blobs, we could have something like this (taken from http://mathlesstraveled.com).



Notice how the primes appear as circles as they can not be grouped like the other numbers.

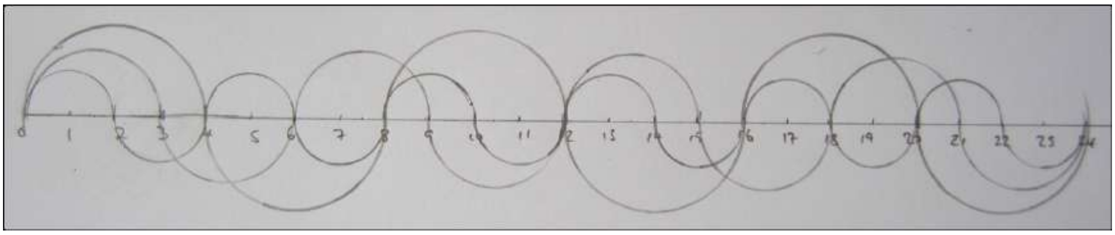
The first few primitives look like this:



These pictures give a beautiful way of showing prime factors; notice how the primes are colour coded.

Notes on Prime Curves

Here is the picture after 2, 3 and 4x tables. Of course, the numbers left over are the primes larger than 4.



If we carried on like this, and included the 1x table, then the primes would be crossed exactly twice (as they have two factors) and all other numbers would be crossed more than twice.

In fact, they would all be crossed an even number of times apart from the square numbers, as they have an odd number of factors.

Notes on Finding primes

Looking at the sieve, we can see that primes are all in the first and fifth columns (apart from 2 and 3).

Mathematically speaking, we would say that all primes greater than 3 are of the form 6k+1 or 6k-1, or that they are congruent to 1 or 5 (mod 6).

Of course, this has to be true, as numbers of the form 6k+2 and 6k-2 are divisible by 2, 6k+3 is divisible by 3 and 6k is divisible by 6.

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90
91	92	93	94	95	96
97	98	99	100		

This suggests that primes will pop up in ‘twins’, as they are either 6k+1 or 6k-1. It appears to be true that there are an infinite number of twin primes but no one has proved it yet.

The first prime triple is 3, 5, 7. But there are no more because that would mean we would have to have another prime in the third column (6k+3).

Notes on Prime Sequences

The linear sequence shown (with n^{th} term 4n+1) carries on like this 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, …

If we arrange the numbers in a grid like and highlight the primes we have:

1	**5**	**9**	**13**	**17**	**21**	**25**	**29**	**33**	**37**	**41**
2	6	10	14	18	22	26	30	34	38	42
3	7	11	15	19	23	27	31	35	39	43
4	8	12	16	20	24	28	32	36	40	44

It would appear that around half the numbers of the sequence are primes so far, but of course as we get further through the sequence, the frequency of primes will decrease as that is what primes do (this is called the *Prime Number Theorem*).

But they will never stop; just as there are an infinite number of primes, it was shown by *Dirichlet* that there are an infinite number of primes in the sequence 4n + 1 (and indeed any other linear sequence an + b where a and b are relatively prime).

It has also been shown that the sequence 4n+1 contains (asymptotically) half the primes, the other half being in 4n+3 (apart from 2 of course).

The sequence 4n+1 can only ever contain two primes in a row. To see why, consider two consecutive primes in this sequence; they must be of the form 6k+1 then 6k+5 (like 13 and 17) as they are 4 apart. But then the next number in this sequence will be 6k+9, which is not prime. The sequence 4n+3 starts with 3 primes in a row (3,7,11) but, for the same reasons, this never happens again.

From the previous section we know that two other linear sequences containing all the primes between them (apart from 2 and 3) are 6n+1 and 6n+5. The sequence 6n+5 starts with a run of 5 primes (5, 11, 17, 23, 29) but this is as good as it will ever get. Can you prove why? [Hint: use the sieve of Eratosthenes above, or use an algebraic argument as above for 4n+1.

Notes on Karnaugh Prime maps

Here is the 2-set Karnaugh map with numbers 1 to 10:

	A	A'
B	6	3,9
B'	2,4,8,10	1,5,7

The primes above 2 and 3 go in A'B'.

The powers of 2 go in the box AB' (apart from 10, which will leave this box as soon as we include the set of multiples of 5 – see below) and the powers of 3 are in A'B. The number with prime factors 2 and 3 (= 6) goes in AB.

Here is the 3-set Karnaugh map with numbers 1 to 15:

	A	A'	A	A'
B		15	6,12	3,9
B'	10	5	2,4,8,14	1,7,11,13
	C	C	C'	C'

Here is the 4-set Karnaugh map with numbers 1 to 30:

	A	A'	A	A'	
B				21	D
B'			14, 28	7	D
B	30	15	6, 12, 18, 24	3, 9, 27	D'
B'	10, 20	5, 25	2,4,8,16, 22, 26	1, 11, 13, 17, 19, 23, 29	D'
	C	C	C'	C'	

If we keep going, the first number in ABCD will be 2.3.5.7 = 210.

Suppose we drew a infinite-set Karnaugh map and each set was a multiple of the primes. What would go in each box then?

Notes on Prime Spiral

You will probably have noticed that most of the primes between 41 and 100 lay on the diagonal.

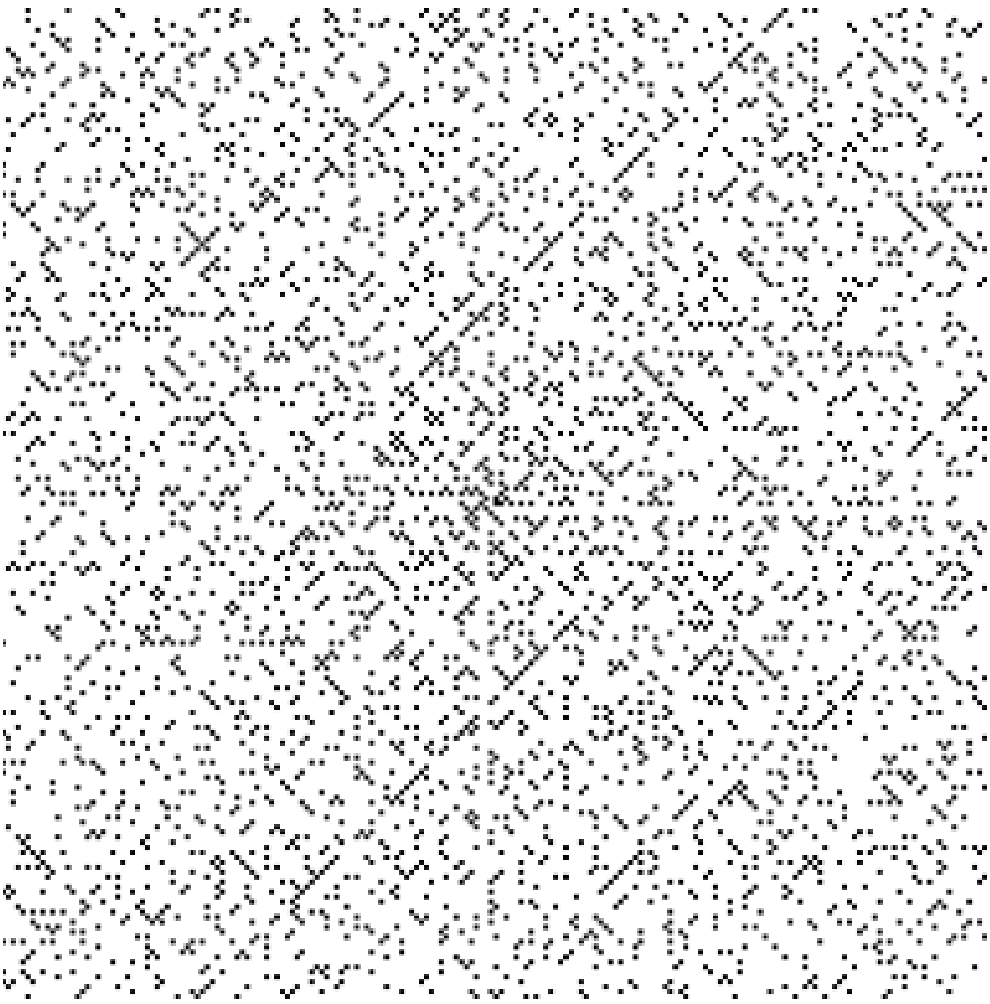
This is just the output of Euler's prime generating function $n^2 + n + 41$.

This prime diagonal will keep going until n=39 which gives the prime 1601. The next number on the diagonal 1681 is composite (= 41 x 41).

Another interesting number to put in the middle is 17. Try it!

				100	99	98	97
77	76	75	74	73	72	71	96
78	57	56	55	54	53	70	95
79	58	45	44	43	52	69	94
80	59	46	41	42	51	68	93
81	60	47	48	49	50	67	92
82	61	62	63	64	65	66	91
83	84	85	86	87	88	89	90

Here is an image of the Ulam spiral (with central number 1) showing where the primes occur:



Notice how many of the primes seem to lie on diagonals.

Here is the Klauber triangle with the primes in red:

					1					
				2	3	4				
			5	6	7	8	9			
		10	11	12	13	14	15	16		
	17	18	19	20	21	22	23	24	25	
26	27	28	29	30	31	32	33	34	35	36

Notice how primes seem to appear in columns; the column starting with 5 looks promising as a prime generating function.

What function is it? Let's extend the columns upwards to create a rectangle like this

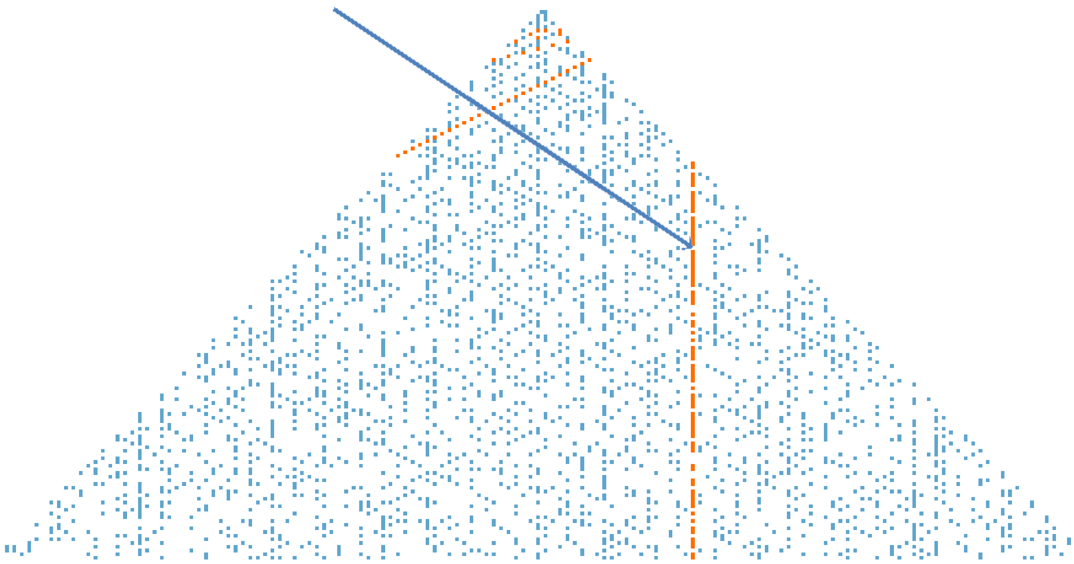
-4	-3	-2	**-1**	0	1	2	3	4	5	6
-2	-1	0	**1**	2	3	4	5	6	7	8
2	3	4	**5**	6	7	8	9	10	11	12
8	9	10	**11**	12	13	14	15	16	17	18
16	17	18	**19**	20	21	22	23	24	25	26
26	27	28	**29**	30	31	32	33	34	35	36

If the top row is the 0th term of the sequence, then the column that started with 5 (in **bold**), is the function $n^2 + n - 1$.

For how long does this sequence continue to generate primes? Well, the next one is 41 (prime) but then the next one is 55 (composite).

As we move to the right the sequences are all one higher than before. So the middle column is the function $n^2 + n + 1$ which does quite well.

Of course, if we keep going along we'll eventually get to Euler's function; here is an larger image of Klauber's triangle showing where primes occur; note Euler's function shown as a vertical red line:



Notes on Prime Nim

The only way to discover how to win at these Nim games is to play them.

One pile, 1 included: Trivially, if we start with an prime number of counters, player 1 wins straight away.

If we don't start with a prime number of counters, a few games reveal that we are trying to get to the safe position of 4 counters, from which our opponent must take 1, 2 or 3 leaving us with a win.

We can do this as player 1 by getting the safe position of a multiple of 4 on each go (by taking 1, 2 or 3) unless we *start* on a multiple of 4 in which case player 2 would win by the same strategy.

Three piles, 1 included:

In normal Nim we aim to get to safe positions by analyzing the binary digits of each pile and getting an even number of each binary digit.

For example, with 1, 5 and 10 counters (say) we have binary digits:

	8	**4**	**2**	**1**
1=	0	0	0	1
5=	0	1	0	1
10 =	1	0	1	0

Now there are an odd number of binary digits in the columns 2, 4 and 8. So as player 1 we can move to a safe position by taking 6 counters from the pile with 10 in, to give:

	8	**4**	**2**	**1**
1=	0	0	0	1
5=	0	1	0	1
4 =	0	1	0	0

Now there is an even number of binary digits in each column and we will win from here.

In Prime Nim, we can simplify the game by only considering the remainder of each pile on division by 4, as we can always reduce piles by 4 by taking 1, 2 or 3 counters.

So in the case of 1, 5 and 10 counters, we can simplify these to remainders 1, 1 and 2. Now it is clear that we should take 2 from the large pile to get to the safe position of an even number of binary digits.
One pile, 1 ***not*** *included*: This game is much more difficult to analyze! Because we can no longer take 1, we can't use the multiple of 4 strategy.

Playing the games a few times we realize that sometimes we will get to positions where 1 counter is left. I suppose we should then change the rules to say the last person who can take *any* counters is the winner (so leaving your opponent with 1 counter constitutes a win). So if we are on 4 (say), a winning move is to take 3.

The safe positions I have found so far are 9, 10, 18, 24, 30, …

Example: 9 is safe because your opponent can only take 2 (leaving 7), 3 (leaving 6 which is a winning position), 5 (leaving 4 which is a winning position) or 7 (leaving 2).

It might seem safe positions have something to do with multiples of 6, but not all of them are; for example 42 isn't safe because your opponent could take 23 leaving you with 9 which is a safe (losing) position.

So it seems that there is no simple formula for safe positions in this game, which is probably to be expected if we are dealing with primes!

Three piles, 1 not included: Help!

Notes on Last Prime

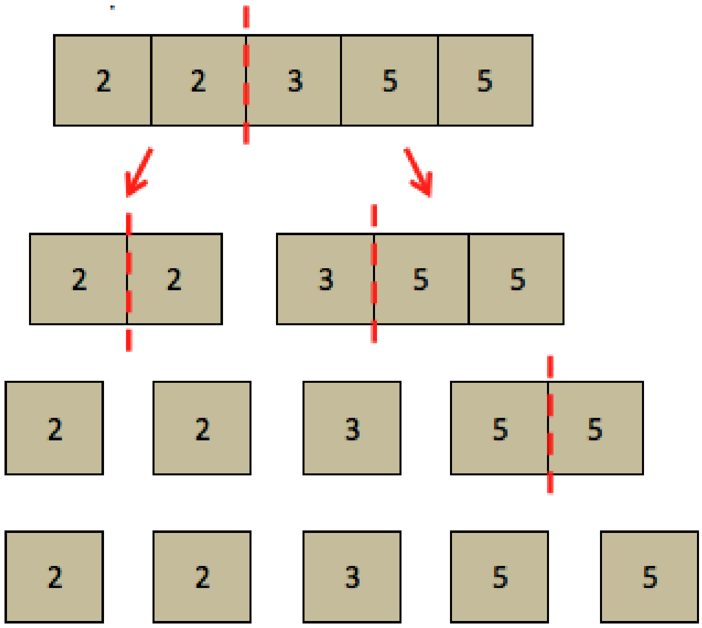
This is really a Nim-like game in disguise.

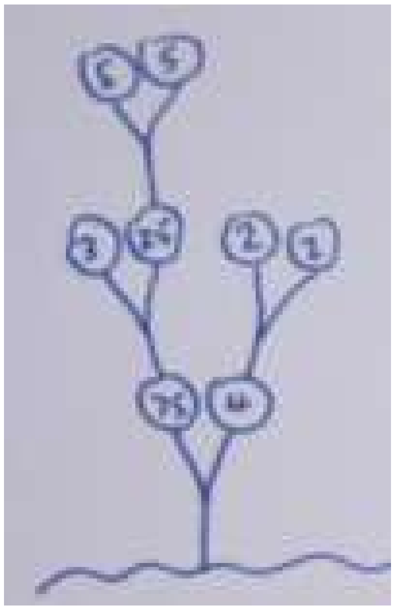
1 hand: You should hold up 5 fingers on your first go. Then the game is fixed to follow this pattern: 5, 7, 11, 13, 17 and then there is a gap of 6 to the next prime so player 1 is the winner.

2 hands: This follows a similar principle but is just a bit longer. The first primes that are more than 10 apart are 113 and 127. So you are aiming to be the first to 113. Working backwards, you can create safe positions: 113, 101, 89, 73, 61, 47, 31, 19 and so you should start with 7 fingers.

Notes on prime factors

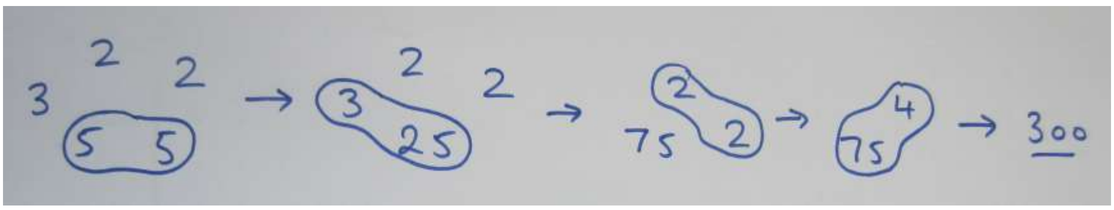
Why do all the factorizations of 300 have 4 pairs of factors? One way of looking at this is to think of the prime factors as squares of chocolate that we are going to snap off into single blocks. Moving along a branch of the factor tree is like snapping the bar of chocolate along a line. So the factorization of 300 on the right below could be represented by breaking a chocolate bar like this:





We will always need 4 breaks to break this chocolate bar into single squares. In general we will need n-1 breaks to break up a chocolate bar with n squares (see the game *Choco Choice* in the section on *Parity*).

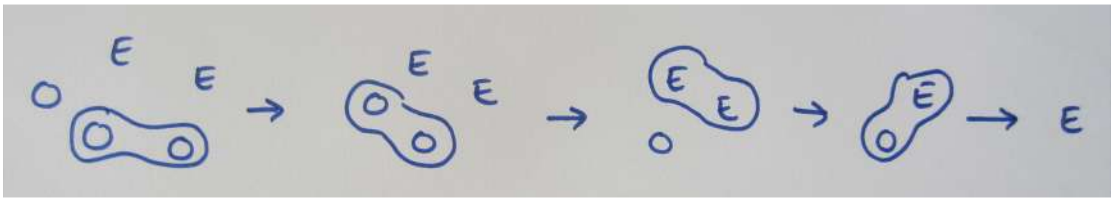
Another way of thinking about this is join pairs of prime factors together (reversing the factorizing process) to make composites like this:



Then we can see that there must be four pairings to get 5 numbers to 1.

Why is there one even pair of factors in all factorizations of 300?

If we look at the even and odd factors in the above diagram, we can see that pairing two odds created another odd and we pair an odd and even, we create another even; in each case the number of evens does not change. If we pair two evens then we reduce the number of evens by one. So as there is only two even prime factors in 300, we can only have one even pairing; as soon as we pair them (whenever we do it) we only have one even left.



Generally, pairing two even numbers reduces the evens by one, so if we have n even factors we will have n-1 even pairs.

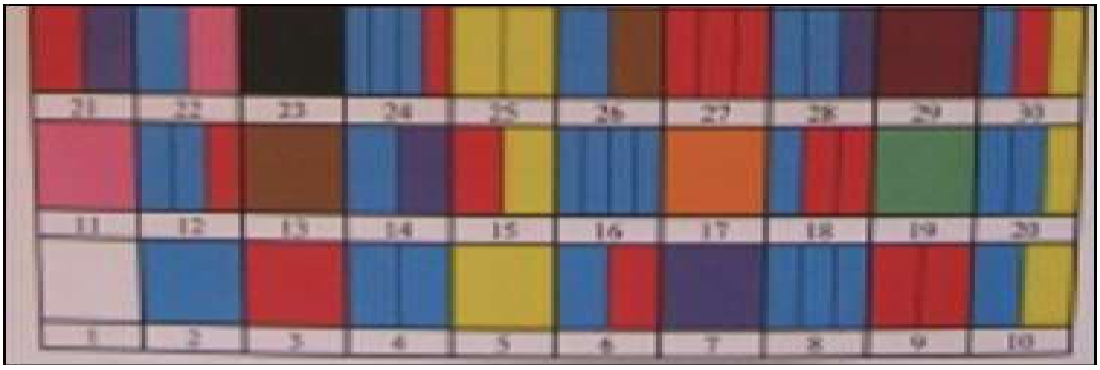
This is also the case with the multiples of 5. So for 300 we have one even pair, one multiple of 5 pair, and the rest are relatively prime as they are contain combinations of different factors.

Uniqueness

Suppose there are two different prime factorizations of 300. One is 2.2.3.5.5, the other is *p.q.r.s.t.u*.... for some other primes *p*, *q*, *r*, ...

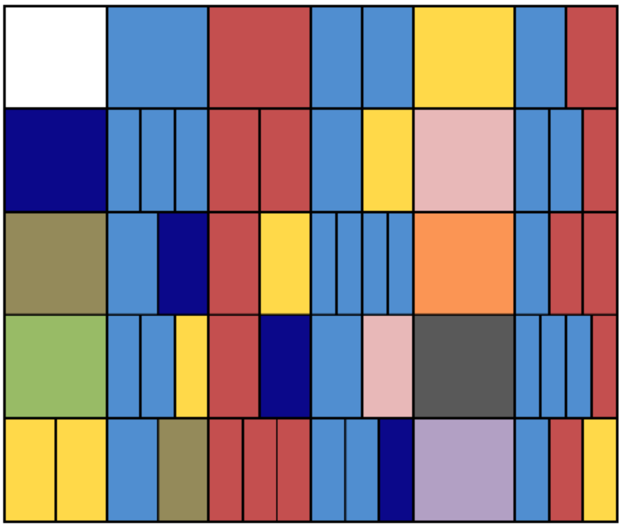
By repeated applications of Euclid's Lemma, the prime p must divide one of the factors 2, 3 or 5, in which case it must ***be*** one of 2, 3 or 5. If we carry on this logic, the other factors q, r, etc. must also be one of each of the other factors of 2.2.3.5.5 and so all prime factorizations are unique.

Notes on prime clothing



You can see that each prime factor has a colour code (2 = blue, 3 = red, etc.) so each square shows which prime factors, and how many of them, occur in each prime factorization.

If we put them in 6 columns we get:

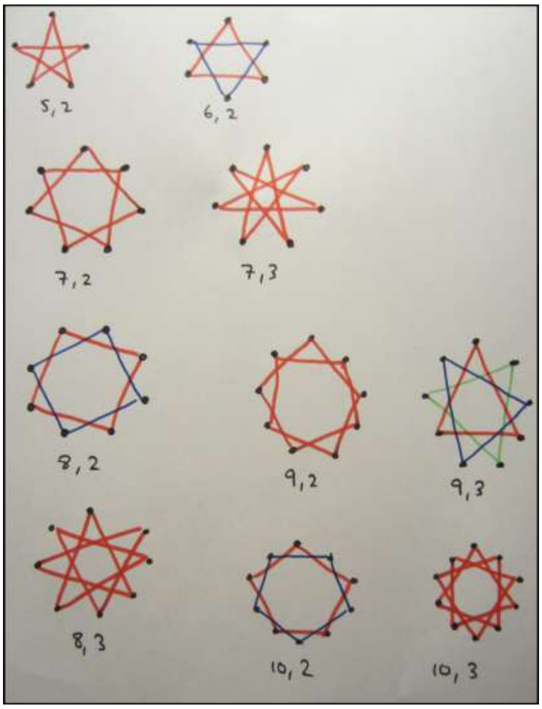


You can clearly see the primes in columns 1 and 5.

We can also see the multiples of 2 and 3 in columns and multiples of 5 and 7 in the diagonals.

Here is another t-shirt that is interesting!

Notes on prime stars



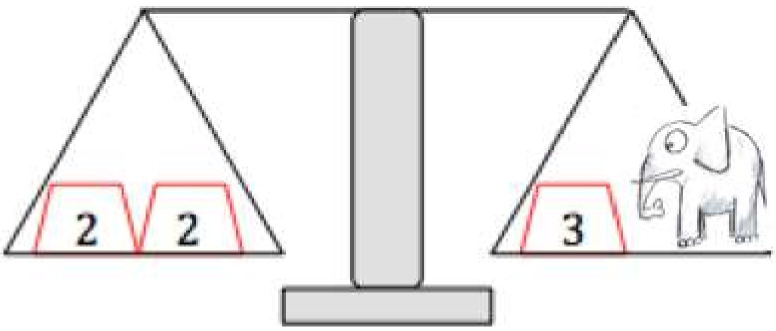
If the number of dots and the size of jump are relatively prime, we get a star that can be drawn without taking pen from paper.

Generally, the number of stars we get is the *greatest common divisor* of the two numbers. So if they are relatively prime, the gcd is 1, and we get a star that can be drawn without taking the pen from paper.

We can see that for gcd(9,3) = 3, and we get 3 separate stars.

Notes on greatest common divisors

We can weigh the 1kg elephant like this:



This means that we can any integer-weight elephant by putting on multiples of 2kg and 3kg weights. For example, we could weigh a 100kg elephant with 200 x 2kg weights on the left pan, and 100 x 3kg weights on the right pan.

So to work out the weight of any elephant (x kg), we just place weights in the ratio 2:1 as shown until we get a balance.

So one solution to the equation $2x + 3y = 1$ is **x = 2, y = -1**, but there are infinitely many others (such as x=5, y=-3).

Also we can solve **any** equation of the form $2x + 3y = c$ with **x = 2c, y = -c**.

You may have realized there are no integer solutions to the equation $2x + 4y = 1$. Substituting different values of x and y into the expression $2x + 4y$, we soon realize that we can only generate even numbers.

Why? Substituting values for x and y into expression $mx + ny$, we can only generate multiples of $\gcd(m,n)$. So if m and n are relatively prime (as in our first example with m=2, n=3) then we have gcd = 1 and we can generate any multiple of this i.e. *any integer*.

Based on this we can work out if there are solutions to the following Diophantine equations:

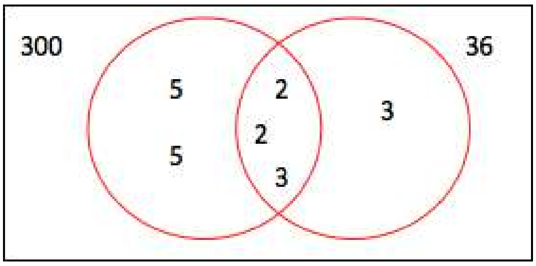
(a) $2x + 3y = 2$ has (infinite) solutions as gcd(2,3) = 1

(b) $3x + 6y = 99$ has (infinite) solutions as 99 is a multiple of gcd(3,6) = 3

(c) $4x + 6y = 99$ has no solutions as 99 is not a multiple of gcd(4,6) = 2

Finding GCDs

The Venn diagram method is good for small numbers; we would not want to use it for large numbers as the prime factorization takes a long time.



Using the example shown, 300 = 2.2.3.5.5 and 36 = 2.2.3.3 and we have that GCD = 2.2.3 and LCM = 2.2.3.3.5.5.

How are these connected? Well, if we do GCD x LCM we get 2.2.2.2.3.3.3.5.5 which is the same as 300 x 36. This is indeed always the case, so we have the rule:

$$lcm(a,b) \times \gcd(a,b) = a \times b$$

This gives us a handy way of finding the LCM if we know the GCD (and vice versa).

One thing we can conclude from this is that if two numbers are relatively prime, then gcd(a,b) = 1 and then we have $lcm(a,b) = a \times b$.

Euclid's algorithm

Here is Euclid's algorithm to find *gcd(5291,3108)*:

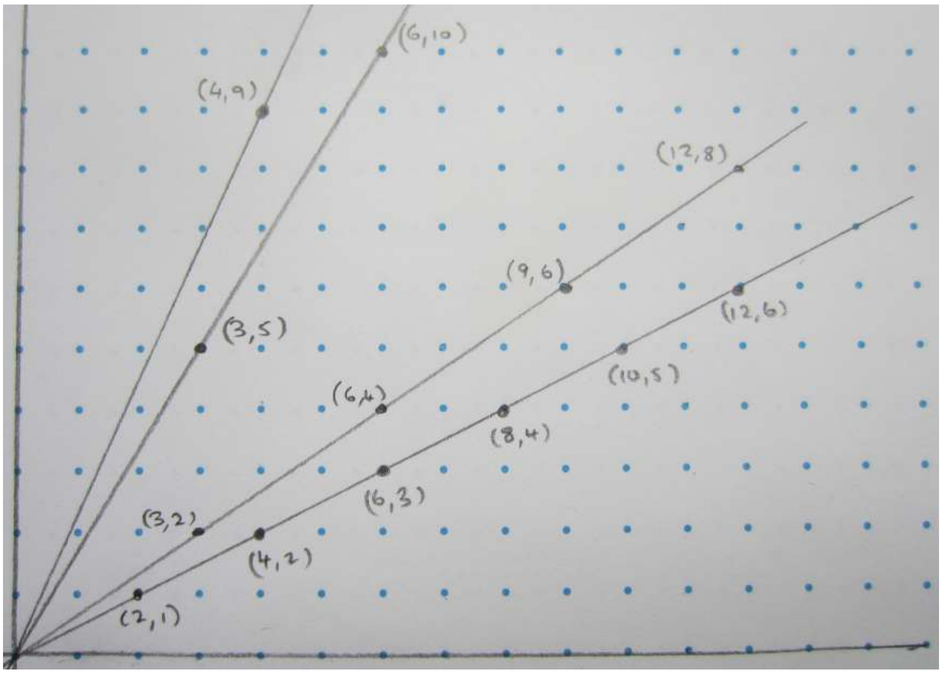
5291 = 1 x 3108 + 2183
3108 = 1 x 2183 + 925
2183 = 2 x 925 + 333
925 = 2 x 333 + 259
333 = 1 x 259 + 74
259 = 3 x 74 + **37**
74 = 2 x 37 + 0

The last non-zero remainder is 37, and this is the greatest common divisor of 5291 and 3108.

We can get an idea of how it works by 'undoing' the calculation from the bottom up.

From the bottom line, we can see that gcd(74,37) = 37. Now, moving one line up, as 37 is the gcd of 37 and 74, it must also be the gcd of 259. We can carry on moving up the calculation like this until we can conclude that 37 is the gcd of 5291 and 3108.

Line segments



If you pick a co-ordinate on one of the lines, say (12,8), and go along its line starting at the origin, we pass through 4 lattice points (integer co-ordinates).

This corresponds to the fact that the greatest common divisor of 12 and 8 is 4. This works for any lattice point.

Notes on Relatively prime fractions

It turns out that the answer is always ½, but why?