The Riemann Zeta Club

Topic 2: Number Theory

Dr J Frost (jfrost@tiffin.kingston.sch.uk)

www.drfrostmaths.com

Last modified: 27th January 2017

Topic 2: Number Theory

Part 1 – Introduction

a. Some History

b. Divisibility Tricks

c. Coprimality

d. Breaking down divisibility problems

Part 2 – Factors and Divisibility

a. Using the prime factorisation

- i. Nearest cube/square
- ii. Number of zeros
- iii. Number of factors

b. Factors in an equality

c. Consecutive integers

Topic 2: Number Theory

Part 3 – Diophantine Equations

a. Factors in an equality (revisited)

b. Dealing with divisions

c. Restricting integer solutions

Part 4 – Modular Arithmetic

a. Introduction

b. Using laws of modular arithmetic

c. Useful properties of square numbers

c. Multiples and residues

d. Playing with different moduli

Topic 2: Number Theory

Part 5 – Digit Problems

a. Reasoning about last digit

b. Representing algebraically

Part 6 – Rationality

Part 7 – ‘Epilogue’

Topic 2 – Number Theory

Part 1: Introduction

What is Number Theory?

Number Theory is a field concerned with integers (and fractions), such as the properties of primes, integer solutions to equations, or proving the irrationality of π/e/surds.

How many zeros does 50! have? What is its last non-zero digit?

How many factors does 1000^{1000} have?

Are there any integer solutions to $a^3 + b^3 = c^3$?

Prove that the only non-trivial integer solutions to $\mathbf{a^b = b^a}$ is {2,4}

Who are the big wigs?

Euclid (300BC)

Better known for his work in geometry, but proved there are **infinitely many primes**. **Euclid's Algorithm** is used to find the Greatest Common Divisor of two numbers.

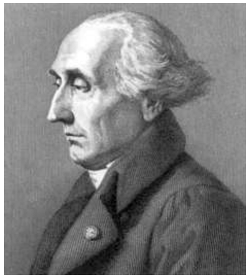
Fermat (1601-1665)

Most famous for posing "**Fermat's Last Theorem**", i.e. That $a^n + b^n = c^n$ has no integer solutions for a, b and c when $n > 2$. Also famous for **Fermat's Little Theorem** (which we'll see), and had an interest in '**perfect numbers**' (numbers whose factors, excluding itself, add up to itself).

Euler (1707-1783)

Considered the founder of 'analytic number theory'. This included various properties regarding the **distribution of prime numbers**. He proved various statements by Fermat (including proving there are no integer solutions to $a^4 + b^4 = c^2$). Most famous for '**Euler's Number**', or 'e' for short and Euler's identity, $e^{\pi i} = -1$.

Who are the big wigs?



Lagrange (1736-1813)

Proved a number of Euler's/Fermat's theorems, including proving that "**every number is the sum of four squares**" (the Four Square Theorem).

Dirichlet (1805-1859)

Substantial work on analytic number theory. e.g. **Dirichlet's Prime Number Theorem:** "All arithmetic sequences, where the initial term and the common difference are coprime, contain an infinite number of prime numbers."

Riemann (1826-1866)

The "one hit wonder" of Number Theory. His only paper in the field "On the number of primes less than a given magnitude" looked at the density of primes (i.e. how common) amongst integers. Led to the yet unsolved "**Riemann Hypothesis**", which attracts a $1m prize.

Who are the big wigs?

Andrew Wiles (1953-)

He broke international headlines when he **proved Fermat's Last Theorem** in 1995. Nuf' said.

Is 1 a prime number?

Vote No

Vote Yes

Euclid’s **Fundamental Theorem of Arithmetic**, also known as the **Unique Factorisation Theorem**, states that all positive integers are uniquely expressed as the product of primes.

Assume that 1 is a prime.
Then all other numbers can be expressed as a product of primes in multiple ways: e.g. $4 = 2 \times 2 \times 1$, but also $4 = 2 \times 2 \times 1 \times 1$, and $4 = 2 \times 2 \times 1 \times 1 \times 1$, and so on.
Thus the Fundamental Theorem of Arithmetic would be violated were 1 a prime.

http://primes.utm.edu/notes/faq/one.html provides some other reasons.

(Note also that 0 is neither considered to be ‘positive’ nor ‘negative’. Thus the ‘positive integers’ start from 1)

Divisibility Tricks

How can we tell if a number is divisible by...

2	?
3	?
4	?
5	?
6	?
7	?
8	?
9	?
10	?
11	?
12	?

Notation

This means “2 divides 8”.

$$2 \mid 8$$

This means “2 does not divide 9”.

$$2 \nmid 9$$

n is divisible by 5.

$$5 \mid n$$

n is a factor of 15.

$$n \mid 15$$

Notation

This is NOT a coordinate! It means "the **Greatest Common Divisor** of 15 and 10".

$$(15,10) = 5$$

The **Lowest Common Multiple** of 6 and 8.

$$LCM(6,8) = 24$$

True or false

If $3|n$ and $5|n$, then is it the case that $15|n$?

False

True

If $4|n$ and $6|n$, then is it the case that $24|n$?

False

True

Take 12 for example. It’s divisible by 4 and 6, but not by 24.

In general, if a number is divisible by *a* and b, then the largest number it’s guaranteed to be divisible by the **Lowest Common Multiple** of *a* and *b*. LCM(4,6) = 12.

Coprime

If two numbers a and b share no common factors, then the numbers are said to be **coprime** or **relatively prime**. The following then follows:

$$LCM(a,b) = \ ab$$

$$(a,b) = 1$$

Coprime?

2 and 3?	No	True
5 and 6?	No	True
10 and 15?	No	True

Breaking down divisibility problems

We can also say that opposite:

If we want to show a number is divisible by 15:

?

But be careful. This only works if the two numbers are coprime:

If we want to show a number is divisible by 8:

...we can just show it’s divisible by 4 and 2?

?

Breaking down divisibility problems

Key point: If we're trying to show a number is divisible by some large number, we can break down the problem – if the number we're dividing by, n, has factors a, b such that $n = ab$ and a and b are coprime, then we show that n is divisible by a and divisible by b. Similarly, if $n = abc$ and a, b, and c are all coprime, we show it's divisible by a, b and c.

If we want to show a number is divisible by 24:

We can show it's divisible by ?

(Note, 2 and 12 wouldn't be allowed because they're not coprime. That same applies for 4 and 6)

Which means we'd have to show the number has the following properties:

1.
2.

?

Breaking down divisibility problems

[Hamilton 2006 Q1] Find the smallest positive integer which consists only of 0s and 1s, and which is divisible by 12.

Answer: ?

A number divisible by 12 must be divisible by 3 and 4. If divisible by 4, the last two digits are divisible by 4, so most digits must be 0.

If divisible be three, the number of 1s must be a multiple of 3. For the smallest number, we have exactly 3 ones.

Breaking down divisibility problems

Explain why **k and $k + 1$ are coprime** for any positive integer k.

Answer:

?

The same reasoning underpins Euclid's proof that there are infinitely many primes. Suppose we have a list of all known primes: $p_1, p_2, \ldots, p_n$. Then consider one more than their product, $p_1 p_2 \ldots p_n + 1$. This new value will always give a remainder of 1 when we divide by any of the primes p_1 to p_n. If it's not divisible by any of them, either the new number is prime, or it is a composite number whose prime factors are new primes. Either way, we can indefinitely generate new prime numbers.

Coprime

If k is odd, will $k-1$ and $k+1$ be coprime?

Answer:

?

If k is even, will $k-1$ and $k+1$ be coprime?

Answer:

?

These are two very useful facts that I've seen come up in a lot of problems. We'll appreciate their use more later:

1. **k and $k+1$ are coprime for any positive integer k.**
2. **$k-1$ and $k+1$ are coprime if k is even.**

Topic 2 – Number Theory

Part 2: Factors and Divisibility

Using the prime factorisation

Finding the prime factorisation of a number has a number of useful consequences.

$$360 = \boxed{?}$$

We'll explore a number of these uses...

Using the prime factorisation

Handy Use 1: Smallest multiple that's a square or cube number?

$$360 = 2^3 \times 3^2 \times 5$$

Smallest multiple of 360 that's a perfect square = ?

If the powers of each prime factor are even, then the number is a square number (known also as a "perfect square"). For example $2^4 \times 3^2 \times 5^2 = (2^2 \times 3 \times 5)^2$. So the smallest number we need to multiply by to get a square is $2 \times 5 = 10$, as we'll then have even powers.

Using the prime factorisation

Handy Use 1: Smallest multiple that's a square or cube number?

$$360 = 2^3 \times 3^2 \times 5$$

Smallest multiple of 360 that's a cube = ?

If the powers of each prime factor are multiples of three, then the number is a cube number.

For example $2^3 \times 3^6 \times 5^3 = (2 \times 3^2 \times 5)^3$. So the smallest number we need to multiply by to get a square is $3 \times 5^2 = 75$.

Using the prime factorisation

Handy Use 2: Number of zeros on the end?

$$2^7 \times 3^2 \times 5^4$$

Q1) How many zeros does this number have on the end?

?

Q2) What's the last non-zero digit?

?

Using the prime factorisation

Handy Use 2: Number of zeros on the end?

What is the highest power of 10 that's a factor of:

50!

?

1000!

?

Using the prime factorisation

Handy Use 2: Number of zeros on the end?

What is the highest power of 10 that's a factor of:

In general, $n!$

?

Using the prime factorisation

[SMC 2005 Q24] For how many positive integer values of k less than 50 is it impossible to find a value of n such that $n!$ ends in exactly k zeros?

A: 0

B: 5

C: 8

D: 9

E: 10

When $n!$ is written in full, the number of zeros at the end of the number is equal to the power of 5 when $n!$ is written as the product of prime factors. We see that 24! ends in 4 zeros as 5, 10, 15 and 20 all contribute one 5 when 24! is written as the product of prime factors, but 25! ends in 6 zeros because 25 = 5 × 5 and hence contributes two 5s. So there is no value of n for which $n!$ ends in 5 zeros. Similarly, there is no value of n for which $n!$ ends in 11 zeros since 49! ends in 10 zeros and 50! ends in 12 zeros. The full set of values of k less than 50 for which it is impossible to find a value of n such that $n!$ ends in k zeros is 5, 11, 17, 23, 29, 30 (since 124! ends in 28 zeros and 125! ends in 31 zeros), 36, 42, 48.

Using the prime factorisation

Handy Use 3: Number of factors?

$$72576 = 2^7 \times 3^4 \times 7$$

A factor can combine any number of these prime factors together. e.g. $2^2 \times 5$, or none of them (giving a factor of 1).

We can use between 0 and 7 of the 2s to make a factor. That's 8 possibilities.

Similarly, we can have between 0 and 4 threes. That's 5 possibilities.

And we can either have the 7 or not in our factor. That's 2 possibilities.

So there's $8 \times 5 \times 2 = 80$ factors

Using the prime factorisation

Handy Use 3: Number of factors?

$$a^q \times b^r \times c^s$$

In general, we can add 1 to each of the indices, and multiply these together to get the number of factors. So above, there would be $(q+1)(r+1)(s+1)$ factors.

Using the prime factorisation

Handy Use 3: Number of factors?

How many factors do the following have?

50? =

?

10^{100}?

?

200? =

?

2003^{2003}? (Note: 2003 is prime)

?

Using the prime factorisation

Question: How many multiples of 2013 have 2013 factors?

A: 0

B: 1

C: 3

D: 6

E: Infinitely many

Hint: $2013 = 3 \times 11 \times 61$
Use the 'number of factors' theorem backwards: If there are 2013 factors, what could the powers be in the prime factorisation?

Solution: Firstly note that any multiple of 2013 must have at least powers of 3, 11 and 61 in its prime factorisation (with powers at least 1). If there are 2013 factors, then the product of one more than each of the powers in the prime factorisation is 2013. e.g. We could have $3^2 \times 11^{10} \times 61^{60}$, since $(2+1)(10+1)(60+1) = 2013$. There's $3! = 6$ ways we could arrange these three powers, which all give multiples of 2013. Our multiple of 2013 can't introduce any new factors in its prime factorisation, because the number of factors 2013 only has three prime factors, and thus can't be split into more than three indices.

Int Kangaroo

Pink

Grey

Factors in an equality

We can reason about factors on each side of an equality.

What do we know about n and k?

$$3n = 8k$$

Answer:

?

Factors in an equality

In general, if we know some property of a number, it can sometimes help to replace that number with an expression that represents that property.

This skill becomes hugely important when considering integer solutions for equations.

$\boldsymbol{n}$ **is even:**	**Let** $\boldsymbol{n = 2k}$ **for some integer** $\boldsymbol{k}$
$\boldsymbol{n}$ **is odd:**	**Let** $\boldsymbol{n =}$?
$\boldsymbol{n}$ **is a multiple of 9:**	**Let** $\boldsymbol{n =}$?
$\boldsymbol{n}$ **only has prime factors of 3:**	**Let** $\boldsymbol{n =}$?
$\boldsymbol{n}$ **is an odd square number:**	?

Factors in an equality

Question: Show that $\boldsymbol{2^n = n^3}$ has no integer solution for n.

Answer:

?

Factors in an equality

Question: If $3n^2 = k(k+1)$, then what can we say about k and $k+1$? *(Recall: k and $k+1$ are coprime)*

Answer:

?

Divisibility with consecutive integers

Every other integer is divisible by 2.	1	**2**	3	**4**	5	**6**	7	**8**
Every third integer is divisible by 3.	1	2	**3**	4	5	**6**	7	8
Every fourth integer is divisible by 4.	1	2	3	**4**	5	6	7	**8**

An ‘obvious’ fact that can aid us in solving less than obvious problems!

Divisibility with consecutive integers

[SMC 2003 Q13] Which of the following is divisible by 3 for every whole number *x*?

A: $x^3 - x$

B: $x^3 - 1$

C: x^3

D: $x^3 + 1$

E: $x^3 + x$

Since $x^3 - x = x(x-1)(x+1)$, $x^3 - x$ is always the product of **three consecutive whole numbers** when x is a whole number. As one of these must be a multiple of 3, $x^3 - x$ will be divisible by 3. Alternatively, substituting 2 for x in the expressions in *B*,*C* and *E* and substituting 3 for x in the expression in results in *D* numbers which are not divisible by 3.

(Note: We'll revisit this problem later when we cover modulo arithmetic!)

Divisibility with consecutive integers

[BMO 2005/06 Q1] Let n be an integer greater than 6. Prove that if $n-1$ and $n+1$ are both prime, then $n^2(n^2+16)$ is divisible by 720.

?

Use what you know!

- ✓ If $n-1$ and $n+1$ are both prime, I can establish properties about n's divisibility.
- ✓ 720 has a factor of 5. What expression can I form that we know will be divisible by 5?

Topic 2 – Number Theory

Part 3: Diophantine Equations

What is a Diophantine Equation?

An equation for which we're looking for **integer** solutions.
Some well-known examples:

$$\boxed{x^n + y^n = z^n}$$

When n=2, solutions known as Pythagorean triples. No solutions when n>2 (by Fermat's Last Theorem).

$$\boxed{3x + 4y = 24}$$

Linear Diophantine Equation.

$$\boxed{\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}}$$

Erdos-Staus Conjecture states that 4/n can be expressed as the sum of three unit fractions (unproven).

$$\boxed{x^2 - ny^2 = 1}$$

Pell's Equation. Historical interest because it could be used to find approximations to square roots. e.g. If solutions found for $x^2 - 2y^2 = 1$, x/y gives an approximation for √2

Factors in an equality

To reason about factors in an equality, it often helps to get it into a form where each side is a product of expressions/values.

Example: How many positive integer solutions for the following?

$$(x-6)(y-10)=15$$

Answer: ?

The RHS is 15, so the multiplication on the LHS must be $1\times 15, 3\times 5, 5\times 3, 15\times 1, -1\times -15, -3\times -5$, etc. So for the first of these for example, $x-6=1$ and $y-10=15$, so $x=7$ and $y=25$. **Make sure you don't forget negative factors.**

Forming a Diophantine Equation

You should try to form an equation where you can reason about factors in this way!

[Hamilton 2011 Q3] A particular four-digit number N is such that:
(a) The sum of N and 74 is a square; and
(b) The difference between N and 15 is also a square.
What is the number N?

Step 1: Represent algebraically:

?

Step 2: Combine equations in some useful way.

?

Step 3: Reason about factors

?

Forming a Diophantine Equation

Aim to factorise your equation.

[BMO 2011/12 Q1] Find all positive values of n for which $n^2 + 20n + 11$ is a (perfect) square.

Hint: Perhaps complete the square?

?

Forming a Diophantine Equation

There's a variety of different strategies to factorise a Diophantine Equation.

[BMO 2012/13 Q4] Find all positive integers n such that $12n - 119$ and $75n - 539$ are both perfect squares.

Based on the strategy on the previous question, we might have tried one equation subtracting the other to get the difference of two squares:

$$12n - 119 = k^2 \quad (1)$$
$$75n - 539 = q^2 \quad (2)$$
$$(2) - (1): \quad 63n - 420 = (q + k)(q - k)$$

But this is a bad strategy, because unlike before, we haven't eliminated the variable on the LHS, and thus the above equation isn't particularly useful. How could we deal with just 2 variables?

?

Manipulating a Diophantine Equation

Aim to factorise your equation.

[Maclaurin 2008 Q3] Show that the following equation has no integer solutions:

$$\frac{1}{x}+\frac{1}{y}=\frac{5}{11}$$

Questions of this form are quite common, particularly in the Senior Maths Challenge/Olympiad. And the approach is always quite similar...

Step 1: It's usually a good strategy in algebra to get rid of fractions: so multiply through by the dominators.

?

Manipulating a Diophantine Equation

Aim to factorise your equation.

$$11x + 11y = 5xy$$

Step 2: Try to get the equation in the form $(ax - b)(ay - c) = d$

This is a bit on the fiddly side but becomes easier with practice.
Note that $\boldsymbol{(x+1)(y+1) = xy + x + y + 1}$
Similarly $(\boldsymbol{ax} - \boldsymbol{b})(\boldsymbol{ay} - \boldsymbol{c}) = a^2\boldsymbol{xy} - ac\boldsymbol{x} - ab\boldsymbol{y} + b^2$

So initially put the equation in the form $5xy – 11x – 11y = 0$
Looking at the form above, it would seem to help to multiply by the coefficient of xy (i.e. 5), giving $\boldsymbol{25xy – 55x – 55y = 0}$
This allows us to factorise as (5x – 11)(5y – 11) – 121 = 0.
The "-121" is because we want to 'cancel out' the +121 the results from the expansion of (5x – 11)(5y – 11).

So $\boldsymbol{(5x – 11)(5y – 11) \;=\; 121}$

Manipulating a Diophantine Equation

Aim to factorise your equation.

$$(5x - 11)(5y - 11) = 121$$

Step 3: Now consider possible factor pairs of the RHS as before.

Since the RHS is $121 = 11^2$, then the left hand brackets must be 1×121 or 11×11 or 121×1 or -1×-121, etc. (don't forget the negative values!)

If $5x - 11 = 1$, then x is not an integer.
If $5x - 11 = 11$, then x is not an integer.
If $5x - 11 = -1$, then $x = 2$, but $5y - 11 = -121$, where y is not an integer.
(And for the remaining three cases, there is no pair of positive integer solutions for x and y)

Manipulating a Diophantine Equation

Let's practice! Put in the form $(ax-b)(ay-c)=d$

Use the 4 from $4xy$

-5 and -7 swap positions.

(-5) x (-7)

$$\frac{7}{x}+\frac{5}{y}=4 \Rightarrow \mathbf{4xy-5x-7y=0} \Rightarrow \mathbf{(4x-7)(4y-5)=35}$$

$$\frac{1}{x}+\frac{1}{y}=1 \Rightarrow \boxed{?} \Rightarrow \boxed{?}$$

$$\frac{3}{x}+\frac{3}{y}=2 \Rightarrow \boxed{?} \Rightarrow \boxed{?}$$

(Source: **SMC**)

$$\frac{1}{x}+\frac{2}{y}=\frac{3}{19} \Rightarrow \boxed{?} \Rightarrow \boxed{?}$$

In general, this technique is helpful whenever we have a mixture of variables both individually and as their product, e.g. x, y and xy, and we wish to factorise to aid us in some way..

Now for each of these, try to find integer solutions for x and y! (if any)

Dealing with divisions

Suppose you are determining possible values of a variable in a division, **aim to get the variable in the denominator only.**

Example: How many positive integer solutions for n given that the following is also an integer:

$$\frac{n}{100-n}$$

?

Dealing with divisions

In a division, sometimes we can analyse how we can modify the dividend so that it becomes divisible by the divisor.

[SMC 2005 Q21] What is the sum of the values of n for which both n and $\frac{n^2-9}{n-1}$ are integers?

A: -8

B: -4

C: 0

D: 4

E: 8

Note that $n^2 - 1$ is divisible by $n - 1$. Thus:

$\frac{n^2-9}{n-1} = \frac{n^2-1}{n-1} - \frac{8}{n-1} = n + 1 - \frac{8}{n-1}$. So $n - 1$ must divide 8.

The possible values of $n - 1$ are −8, −4, −2, −1, 1, 2, 4, 8, so n is −7, −3, −1, 0, 2, 3, 5, 9. The sum of these values is 8.

(*Note that the sum of the 8 values of* $n - 1$ *is clearly 0, so the sum of the 8 values of* n *is 8.*)

Dealing with surd expressions

For Diophantine Equations involving surds, remember that the contents of the surd must be a square number. Square each side of the equation.

[SMC 2000 Q24] How many pairs of positive integers x, y satisfy the equation: $\sqrt{x} - \sqrt{17} = \sqrt{y}$.

A: 0

B: 1

C: 2

D: 17

E: ∞

Squaring both sides:

$$x - 2\sqrt{17x} + 17 = y$$

If y is an integer, then $\sqrt{17x}$ must be an integer. This will be the case when $x = 17k^2$ for any positive integer k (except 1, because then y would be 0). But there's infinitely many choices for k, thus there's infinitely many solutions for x, y.

Restricting integer solutions

When you have to find all integer solutions to some equation, there's usually some way to round down your search.

[Cayley 2011 Q5] Solve the equation $5a - ab = 9b^2$, where a and b are **positive integers**.

Answer: ?

Hint: What do we know about the RHS of the equation?
What do this then tell us about $5a$ and ab?

$9b^2 \geq 0$, therefore $ab \leq 5a$. And since a is positive, then dividing both sides by a gives us $b \leq 5$.
This means we only need to try $b = 1$, 2, 3, 4 and 5!

If we sub in b = 1, we get 4a = 9, for which there's no integer solution.
Continuing with possible b, we eventually find all our solutions.

In general, look out for things that are squared, as we know their value must be at least 0 (nonnegative).

Diophantine Equation Summary

1 Try to get whatever equation you have as a **product** on each side, so that you can reason about the factors. e.g. $(x+10)(x-6)=100$

2 You can occasionally use the **difference of two squares** to factorise. e.g:

$$10^3x+x+1=k^2$$
$$\rightarrow \quad 10^3x+x=k^2-1$$
$$=1001x=(k+1)(k-1)$$

3 To factorise, you might need to think backwards to determine what could expand to get the terms you have. e.g. If you have x, y and xy in your expression, then $(x+1)(y+1)$ would expand to give all 3 of these.

In some contexts you can **complete the square**.

4 Once factorised, you need to consider possibilities for the factors on each side. Don't forget **negative factors**.

5 You can use number theory knowledge to round down what factors could be.

e.g. If you have k^2, then prime factors in k come in pairs.

e.g. If you have two factors that are consecutive, they are coprime and thus share no factors.

Topic 2 – Number Theory

Part 4: Modular Arithmetic

What the devil is it?

On a digital clock, were we to specify the hour as “27”, what we’d actually mean is 3 in the morning.

These hours are the same in “**modulo 24 arithmetic**”, i.e. our numbers are limited to 0 to 23, after which they loop back round.

$$27 \equiv 3 \pmod{24}$$

We’d say “**27 is congruent to 3 modulo/mod 24**”

What the devil is it?

Numbers in modulo k arithmetic are all equivalent to numbers in the range 0 to $k-1$, where they then repeat.

0, 1, 2, 3, 4, 5, 6, 7, ... ≡ 0, 1, 2, 0, 1, 2, 0, 1, ... (mod 3)

This operator usually means ‘equivalent’, and in this context more specifically means ‘congruent’.

We can use modulo arithmetic to represent the **remainder** (also known as the **residue**) when we divide by some number.

$$4 \equiv 1\ (mod\ 3) \qquad 15 \equiv 3\ (mod\ 4)$$

$$-1 \equiv 4\ (mod\ 5)$$

What the devil is it?

How would we represent $3|x$?

?

How would we represent “x is one less than a multiple of 5”.

?

Properties of Modular Arithmetic

Addition works just as if it was a normal equality.

If $4 \equiv 1 \pmod{3}$ then $4 + 5 \equiv 1 + 5 \pmod{3}$

Multiplication also works.

If $4 \equiv 1 \pmod{3}$ then $8 \equiv 2 \pmod{3}$

Exponentiation also works (this one we'll use a lot!).

If $5 \equiv 2 \pmod{3}$ then $5^k \equiv 2^k \pmod{3}$ for any k

Quickfire Examples

Given that $73 \equiv 1 \ (mod\ 4)$
Then $146 \equiv \boxed{?} (mod\ 4)$

Given that $107 \equiv 3 \ (mod\ 13)$
Then $110 \equiv \boxed{?} (mod\ 13)$

Given that $17 \equiv 1 \ (mod\ 16)$
Then $17^{100} \equiv \boxed{?} \ (mod\ 16)$

Given that $17 \equiv 2 \ (mod\ 15)$
Then $170 \equiv \boxed{?} \ (mod\ 15)$

Properties of Modular Arithmetic

Multiplication also works.

If $a \equiv b \ (mod\ c)$, then $ka \equiv kb \ (mod\ c)$
e.g. If $4 \equiv 1 \ (mod\ 3)$, then $8 \equiv 2 \ (mod\ 3)$

But is the converse always true?
i.e. If $ka \equiv kb \ (mod\ c)$, then is $a \equiv b \ (mod\ c)$?
If not, can you think of a counterexample?

?

Properties of Modular Arithmetic

Another common misconception (according to a BMO veteran) is that if:

$$a \equiv c \ \ (mod\ n) \text{ and } b \equiv d\ (mod\ n)$$

then:

$$a^b \equiv c^d\ (mod\ n)$$

This is <u>not</u> in general true!

I’ll leave it as an exercise to find a counterexample…

Using Laws of Modular Arithmetic

Often, it helps to consider all the possible residues.

Question: Show that the arithmetic sequence 2, 5, 8, 11, ... does not contain a square number.

?

Using laws of Modular Arithmetic

[SMC 2005 Q14] A square number is divided by 6. Which of the following could not be the remainder?

A: 0

B: 1

C: 2

D: 3

E: 4

When divided by 6, a whole number leaves remainder 0, 1, 2, 3, 4 or 5. So the possible remainders when a square number is divided by 6 are the remainders when 0, 1, 4, 9, 16 and 25 are divided by 6. These are 0, 1, 4, 3, 4 and 1 respectively, so a square number cannot leave remainder 2 (or remainder 5) when divided by 6..

Using laws of Modular Arithmetic

Problem Revisited!
Which of the following is divisible by 3 for every whole number x? *(Now answer using modular arithmetic)*

A: $x^3 - x$

B: $x^3 - 1$

C: x^3

D: $x^3 + 1$

E: $x^3 + x$

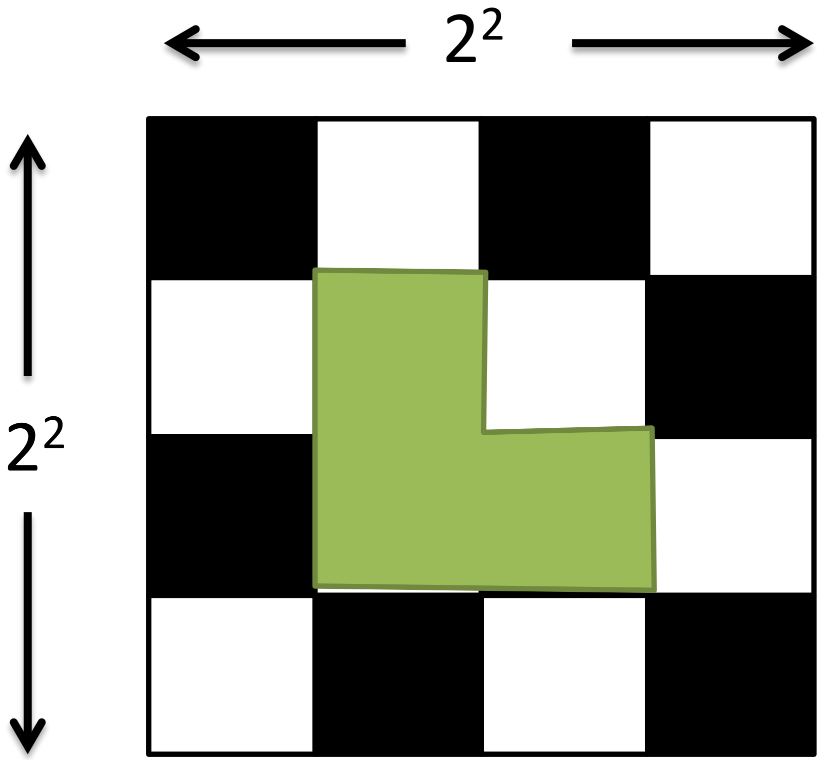
If for the natural numbers. $x \equiv 0{,}1{,}2\ (mod\ 3)$ then:

$$x^3 \equiv 0{,}1{,}8 \equiv 0{,}1{,}2\ (mod\ 3)$$

Then $x^3 - x \equiv 0 - 1, 1 - 1, 2 - 2 \equiv 0{,}0{,}0\ (mod\ 3)$
i.e. For all numbers of x, $x^3 - x$ gives us a remainder of 0 when dividing by 3.

Using laws of Modular Arithmetic

Source: Frosty Special



A square chessboard of sides 2^n (for any n) is tiled with L-shapes, each of 3 squares, such that tiles don't overlap.
Show that you will always have 1 square on the chessboard left untiled.

?

Using laws of Modular Arithmetic

[BMO 1999/2000 Q2] Show that, for every positive integer n, $121^n - 25^n + 1900^n - (-4)^n$is divisible by 2000.

Hint: 2000 = 2^4 x 5^3, thus the only two coprime factors are 16 and 125.

?

Useful properties of square numbers

We’ve so far seen that it can sometimes be useful to consider the possible residues of a square number to eliminate possibilities (as we’ll see for an upcoming example).

There’s other handy properties to add to our ‘toolkit’:

Prove that if that if a square number is **even**, then it’s divisible by 4.

?

Prove that if a square number is **odd**, then it’s **one more than a multiple of 8**.

?

Another problem revisited…

Question: If $3n^2 = k(k+1)$, then what can we say about k and $k+1$? *(Recall: k and $k+1$ are coprime)*

We previously established that either k is a square and $k+1$ is three times a square, or vice versa. We can eliminate one of these cases using modular arithmetic.

Case 1: $k = a^2$ and $k+1 = 3b^2$ →

?

Key Point: Modular Arithmetic can be useful to reason about what numbers can and can't be.

Multiples and Residues

Suppose we’re working in modulo 7 arithmetic, and that we start with a number 3, and find successive multiples:

$$\mathbf{3, 6, 9, 12, 15, 18, 21}$$

$$\equiv \mathbf{3, 6, 2, 5, 1, 4, 0 \ (mod\ 7)}$$

Notice that we get all possible remainders/residues. Under what conditions do you think this happens?

?

We can see that because the last residue is 0, **this number will be divisible by 7**.
i.e. Every 7th number will be divisible by 7 under the above conditions.

Multiples and Residues

[BMO 2004/05 Q4] Determine the least possible value of the largest term in an arithmetic progression of seven distinct primes..

Hint: If a is the first value and d is the difference, what properties must d have to avoid being divisible by something?

?

BMO

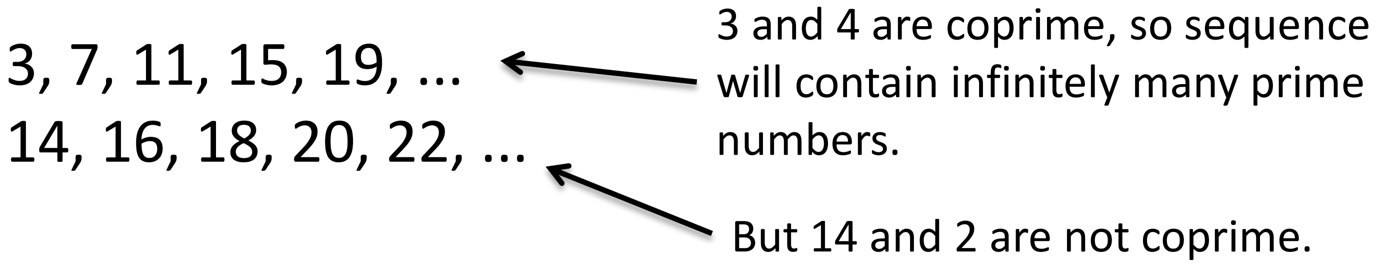
Round 2

Round 1

Multiples and Residues

A bit of extra context for this problem:

In the introduction, we saw **Dirichlet's Prime Number Theorem:** "All arithmetic sequences, where the initial term and the common difference are coprime, contain an infinite number of prime numbers."



3, 7, 11, 15, 19, ...

14, 16, 18, 20, 22, ...

3 and 4 are coprime, so sequence will contain infinitely many prime numbers.

But 14 and 2 are not coprime.

As recently as 2004, it was proven that the sequence of prime numbers contains an arbitrarily long arithmetic progression. i.e. We can find an arithmetic sequence of any length. (This is now known as the **Green-Tao Theorem**)
e.g. 3, 5, 7 and 47, 53, 59 are prime arithmetic sequences of length 3.

The theorem however only proves their existence; it doesn't provide a method to find a sequence of a given length. The longest sequence found so far is of length 26.

Dealing with remainders

If x divided by y gives a remainder of z, then $x - z$ is divisible by y.

For example, consider that 53 divided by 10 gives a remainder of 3.
Then obviously 53 – 3 = 50 is divisible by 10.

[Kangaroo Pink 2012 Q7] When 144 is divided by the positive integer n, the remainder is 11. When 220 is divided by the positive integer n, the remainder is also 11. What is the value of n?

A: 11

B: 15

C: 17

D: 19

E: 38

By our above rule, n divides 144 – 11 = 133 and 220 – 11 = 209.
133 = 19 x 7 and 209 = 19 x 11
So both are divisible by 19.

Negative remainders

Sometimes it can be more convenient to put our remainder as a negative number for purposes of manipulation.

For example, if the remainder when we divide a number by 3 is 2, then we could also say this remainder is -1 because they are congruent.
By laws of modular arithmetic, $2^n \equiv (-1)^n \pmod{3}$. We can more easily see the remainder oscillates between -1 (i.e. 2) and 1 as n increases.

$$2^n + 3^n \equiv \boxed{?} \pmod{3}$$

$$3 \equiv \boxed{?} \pmod{5}$$

$$7 \equiv \boxed{?} \pmod{10}$$

Playing with different moduli

An extremely useful method is to consider your equation in different moduli to see if we can discover anything about the variables.

Question: Is $2^n + 3^n$ ever a perfect square? [Source OEIS]

Hint: See what you find modulo 3 and modulo 5.

Properties of n discovered in modulo 3:

?

Properties of n discovered in modulo 5:

?

Playing with different moduli

Show that $x^2 - y^2 = 2002$ has no integer solutions.
(Hint: try using mod 4)

?

Putting everything together

The following was a particularly badly answered BMO problem. But we can systematically reason through each step using the tips we've seen – no magic required!

Question: Let n be an integer. Show that, if $2 + 2\sqrt{1 + 12n^2}$ is an integer, then it is a perfect square.

1

First note that the question says **IF** [..] is an integer, **THEN** it is a square. We need to start with the assumption, and reason towards the conclusion – don't be tempted to prove the opposite.

2

If $2 + 2\sqrt{1 + 12n^2}$ is an integer, what can we assert about $1 + 12n^2$?

a)
b)

?

3

What equation could we therefore write that would model this?

?

Putting everything together

The following was a particularly badly answered BMO problem. But we can systematically reason through each step using the tips we've seen – no magic required!

Question: Let n be an integer. Show that, if $2 + 2\sqrt{1 + 12n^2}$ is an integer, then it is a perfect square.

4

To reason about factors, we know it's generally a good idea to put an equation in the form where we have the product of expressions on each side.
So rearrange $1 + 12n^2 = (2k + 1)2$

?

5

Use this to reason about the factors (Hint: We've seen this example before!)

?

Putting everything together

The following was a particularly badly answered BMO problem. But we can systematically reason through each step using the tips we've seen – no magic required!

Question: Let n be an integer. Show that, if $2 + 2\sqrt{1 + 12n^2}$ is an integer, then it is a perfect square.

6

When we've used an expression to represent a restriction on a number, we ought to substitute it into the original expression. Use $3n^2 = k(k+1)$

?

7

We earlier found that $k + 1$ is a perfect square so what can we conclude?

?

Fermat’s Little Theorem

Not to be confused with Fermat’s Last Theorem!

If p is prime, and a is any integer (such that a is not a multiple of p), then:

$$a^{p-1} \equiv 1\ (mod\ p)$$

EXAMPLES:

$$3^{10} \equiv 1\ (mod\ 11)$$

$$6^{12} \equiv 1\ (mod\ 13)$$

$$8^{46} \equiv 1\ (mod\ 47)$$

Fermat’s Little Theorem is a special case of Euler’s Theorem, which makes use of something called **Euler’s Totient Function**. It’s not difficult, and worth looking up.

Fermat’s Little Theorem

Show that $31 \mid 3^{150} - 1$.

?

Modular Arithmetic Summary

1 When working in modulo-k arithmetic, all integers that give the same remainder when divided by k are equivalent/‘congruent’.

2 In many problems, it’s useful to consider the possible residues of square numbers and cube numbers, for example to contradict the other side of an equation.

3 If x divided by y gives a remainder of z, then x – z is divisible by y.
Use this in problems which specify the remainders for certain divisions.

4 Experimenting with different modulo can reveal information about your variables, particular for problems involving squared/cubed numbers.

5 If working in modulo-p arithmetic where p is prime, then we see all the possible residues for each p numbers in an arithmetic sequence, unless the common difference is a multiple of p.

Topic 2 – Number Theory

Part 5: Digit Problems

Reasoning about last digits

When we want to find the last digit of some expression, we can do our arithmetic modulo:

?

Using Laws of Modular Arithmetic

Prove that the last digit of a square number can never be 2.

?

Reasoning about last digits

3^{1000}

$$\overset{3^1}{3} \rightarrow \overset{3^2}{9} \rightarrow \overset{3^3}{7} \rightarrow \overset{3^4}{1} \xrightarrow{\qquad\qquad} \overset{3^{1000}}{1} \qquad \pmod{10}$$

$27 \equiv 7 \pmod{10}$, i.e. we only ever need to keep the last digit when we're working modulo-10 arithmetic.

This is a very useful trick!

If $a \equiv 1 \pmod{n}$, then $a^k \equiv 1^k \equiv 1 \pmod{n}$

So if $3^4 \equiv 1 \pmod{10}$, then $(3^4)^{250} \equiv 3^{1000} \equiv 1 \pmod{10}$.

A strategy to find the last digit in general of a^b therefore is to try and get to 1 by incrementally raising the power, at which point we can multiply the power by anything we like!

Reasoning about last digits

[SMC]: The value of $1^{2004} + 3^{2004} + 5^{2004} + 7^{2004} + 9^{2004}$ is calculated using a powerful computer.
What is the units digit of the correct answer?

A: 9

B: 7

C: 5

D: 3

E: 1

The last digit of 3^4 is 1, as is the last digit of 7^4 and the last digit of 9^2. So the last digit of $(3^4)^{501}$, that is of 3^{2004}, is 1. Similarly, the last digit of $(7^4)^{501}$, that is of 7^{2004}, is 1 and the last digit of $(9^2)^{1002}$, that is of 9^{2004}, is 1. Furthermore, $1^{2004} = 1$ and the last digit of 5^{2004} is 5. So the units digit of the expression is 1 + 1 + 5 + 1 + 1, that is 9.

Reasoning about last digits

Question: Find the last non-zero digit of 50!

Source: Team SMC

?

Representing digit problems algebraically

Suppose we have a 2-digit number “ab”.

Q1: What range of values can each variable have?

a: ?

b: ?

It couldn’t be 0 otherwise we’d have a 1-digit number.

Q2: How could we represent the value (n) of the digit using a and b?

e.g. If $a = 7$ and $b = 2$, we want $n = 72$

$n =$?

Similarly, a 3-digit number “abc” could be represented as $100a + 10b + c$

Representing digit problems algebraically

[Hamilton 2005 Q4] An ‘unfortunate’ number is a positive integer which is equal to 13 times the sum of its digits. Find all ‘unfortunate’ numbers.

Answer: ?

Let’s try 2-digit numbers first. Algebraically:
$10a + b = 13(a + b)$
So $3a + 12b = 0$. But this gives us no solutions because one of a or b would have to be negative.

Now try 3-digit numbers:
$100a + 10b + c = 13(a + b + c)$
This simplifies to $29a = b + 4c$
Suppose a = 1. Then if b=1, c=7, giving 117 as a solution.
We also get a=1, b=5, c=6 and a=1, b=9, c=5.
If a=2 or greater, then the LHS is at least 58. But b + 4c can never be big enough, because at most b=c=9, so b+4c = 45.

Now try 4-digit numbers:
We get $329a + 29b = c + 4d$ after simplification. But when *a* is at its lowest, i.e. a=1, and b=0, the c+4d can clearly never be big enough.

Use what you know!

✓ I can represent the digits algebraically and form an equation.

✓ I know each of my digits can be between 1 and 9 (and 0 if not the first digit)

Topic 5 – Number Theory

Part 6: Rationality and Miscellaneous

Irrationality of $\sqrt{2}$

You may well have seen a proof before for the irrationality of 2. Recall that a rational number is one that can be expressed as a fraction.

Aristotle's Proof

Use a proof by contradiction:
Assume that $\sqrt{2}$ is rational. Then it can be expressed as a fraction in its simplest form a/b, where a and b are coprime (if they weren't coprime, we'd be able to simplify the fraction.

Then squaring both sides:

$$a^2 = 2b^2$$

Then a^2 is even, and so a is even.
Therefore let $a = 2k$.

$$(2k)^2 = 2b^2$$

$4k^2 = 2b^2$ so $2k^2 = b^2$
Therefore b is also even. Then a and b share a common factor of 2, contradicting that a/b is in its simplest form.

Something I just thought of...

Let's reason about the factors on each side of the equation $\boldsymbol{a^2 = 2b^2}$.
We know that the powers in the prime factorisation of a square number need to be even. So for each of a and b, it can either not contain a 2, or its 2s come in pairs.
Either way, we have an even number of 2s on the LHS of the equation, and an odd number on the RHS due to the extra 2.
Thus the equation has no integer solutions, i.e. a square number cannot be twice another square number.

A rationality BMO problem

Question: Let S be a set of rational numbers with the following properties:
1) $1/2$ is an element of S
2) If x is an element of S, then both $1/(x+1)$ is an element of S and $x/(x+1)$ is an element of S
Prove that S contains all rational numbers in the interval $0 < x < 1$.

What would the **structure** of our proof look like?:

?

Solution:

?

A rationality BMO problem

[BMO 2004/05 Q5] Let S be a set of rational numbers with the following properties:
1) $1/2$ is an element of S
2) If x is an element of S, then both $1/(x+1)$ is an element of S and $x/(x+1)$ is an element of S
Prove that S contains all rational numbers in the interval $0 < x < 1$.

e.g. 5/7 → 5/2 →2/5 → 2/3 → 2/1 → 1/2
All that remains therefore is to prove that we can make sure a chain from any $\frac{p}{q}$ to eventually get to $\frac{1}{2}$.

Informally, we could argue that as the numerator or denominator can always decrease in each step, then one of them will reach 1. If the denominator reaches 1 first and we have $\frac{k}{1}$, we know $\frac{1}{k+1}$ is in the set. If we have $\frac{1}{k}$, then we can always use our $\frac{p}{q} \rightarrow \frac{p}{q-p}$ rule to reduce k by 1 each time until we reach $\frac{1}{2}$.

A more formal proof could use a proof by contradiction, found here:
http://www.theproblemsite.com/problems/mathhs/2008/Jun_1_solution.asp

BMO

Round 2

Round 1

Topic 2 – Number Theory

Part 7: ‘Epilogue’

The rest of these slides don’t explore any theory that is likely to be use in any Maths Challenges/Olympiads or university interviews, but explore an interesting area of Number Theory...

Let’s finish with something light...

Analytic Number Theory!

= ‘Mathematical analysis’ + Number Theory

Using differentiation, integration, limits, and usually considering real and complex numbers.

Properties of integers.

That’s interesting: we’re using analysis, which concerns **real and complex** numbers, to reason about the **integers**.

Let’s finish with something light...

Analytic Number Theory!

There’s broadly two types of problem studied in this field:

× Those involving **multiplication**

...which includes reasoning about factors. Usually concerns properties of prime numbers.

+ Those involving **addition**

e.g. The yet unproven Goldbach Conjecture: “every even integer is the sum of two primes”.

Let’s have a tiny bit of a look at prime numbers...

Distribution of primes

Prime Number Theorem:

The probability that a randomly chosen large number N is prime is approximately 1 in $ln(N)$

Since the graph of ln(N) always increases but gradually slows down, this suggests (as we might expect) that primes gradually become more spread out for larger numbers, but that the gap between prime numbers gradually levels off.

P(10,000 is prime) = $\frac{1}{\ln(10000)} = 0.11$

So around this number we'd 'expect' roughly 1 in 10 numbers to be prime.

P(1 billion is prime) = $\frac{1}{\ln(1\ 000\ 000\ 000)} = 0.048$

So around this number we'd 'expect' roughly 1 in 20 numbers to be prime.

Counting primes

$\pi(x)$ **The 'prime-counting function', i.e. the number of primes up to and including x.**

So $\pi(10) = 4$, because there are 4 prime numbers (2, 3, 5, 7) up to 10.
(Note that the π symbol is being used a function here, not as the constant you know and love!)

Could we use the Prime Number Theorem to come up with an estimate for $p(x)$?

Consider 100 people who have been asked to come to your party. If each person has a 0.3 chance of coming to your party, you'd expect $100 \times 0.3 = 30$ people to come. But more generally, if each person had different probabilities of coming to your birthday, you could add the probabilities to get an estimate for the total coming.

Similarly, if we added up the probability of each number of prime up to x, we'd get an estimate of the number of primes up to x. So:

$$\pi(x) \sim \sum_{k=2}^{x} \frac{1}{\ln(k)}$$

Counting primes

But since ln(x) is a continuous function, we may as well use integration instead, finding the area under the graph:

$$\pi(x) \sim \int_{k=2}^{x} \frac{1}{\ln(k)}$$

The function on the RHS is known as the "**logarithmic integral**", written $\boldsymbol{Li(x)}$

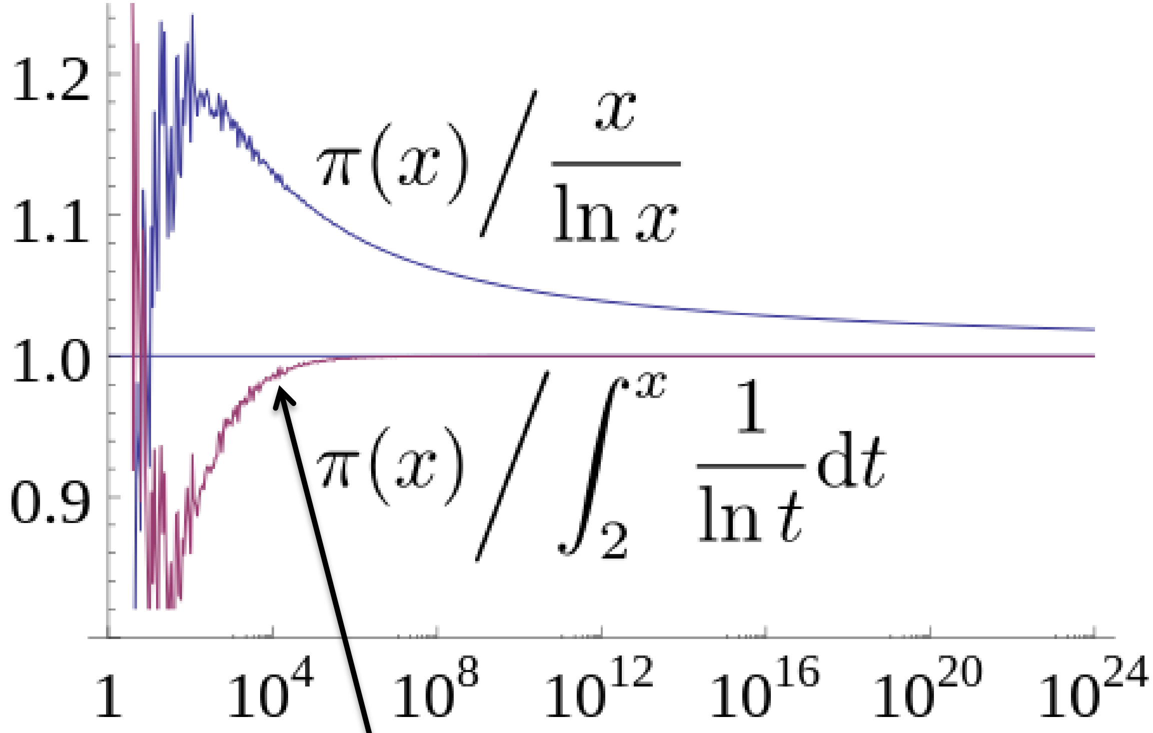
But if we consider the graph of ln(x), and note that as x becomes large, the gradient of ln(x) becomes 0, and thus we could come up with a looser but easier to calculate approximation that assumes we use the same probability ln(x) for all numbers up to x (rather than calculate ln(k) for each k up to x as before).
Then, given the probability is constant, then going back to our party analogy, we can just multiply this constant probability by the number of people to get the estimate attendance, i.e. Multiply 1/ln(x) by x to get an estimate number of primes:

$$\pi(x) \sim \frac{x}{\ln(x)}$$

Counting primes

The graph indicates how accurate these two estimates area compared to the true number of primes $\pi(x)$.

1.1 means we've overestimated by 10%



We can see that this estimate is 99% accurate once we consider the number of primes up to about 100,000

The x^{th} prime?

There's currently no formula to generate the x^{th} prime.
But we can use the approximation $\pi(x) = \frac{x}{\ln(x)}$ seen earlier.

If there are $\frac{x}{\ln(x)}$ prime numbers up to x, this suggests that the $(\frac{x}{\ln(x)})^{\text{th}}$ prime number is roughly x.
That means that the $\boldsymbol{x}^{\text{th}}$ **prime number will be roughly $\boldsymbol{x\ ln(x)}$**

Example:
The actual 100,000th prime number is just under 1.3 million
And $100000 \times \ln(100000) =$ 1.15 million.

This percentage error is reduced as the number becomes larger.

The probability two numbers are coprime?

To solve this problem, let's first consider the **Riemann Zeta Function** (which these resources are named after!)

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

So for example:

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots$$

Which curiously comes to $\frac{\pi^2}{6}$ (and yes, π here means 3.14…)

Euler proved that such as sum **is related to a product involving primes**:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

For example:

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \frac{1}{\left(1 - \frac{1}{2^2}\right)\left(1 - \frac{1}{3^2}\right)\left(1 - \frac{1}{5^2}\right)\left(1 - \frac{1}{7^2}\right)\ldots}$$

The probability two numbers are coprime?

How then is this related to the probability of two numbers being coprime?

What’s the probability an integer is divisible by 4?

?

What’s the probability that two numbers are divisible by some number p?

?

What’s the probability that neither of two numbers is divisible by a number p?

?

To consider whether two numbers are coprime, we need to test whether each possible prime p is a factor of both.
We need not test whether they’re both divisible by non-primes, because if for example both numbers are divisible by 8, we would have already earlier found that they are divisible by 2. It also ensures we have independence: the probability of a number being divisible by 2 is not affected by the probability of being divisible by 3, but if a number is divisible by 2 say, then this increases the chance it’s divisible by 4 (from 0.25 to 0.5).

The probability two numbers are coprime?

Then by considering all possible primes p, the probability is:

$$\prod_{p}^{\infty}\left(1-\frac{1}{p^2}\right)=\prod_{p}^{\infty}\left(\frac{1}{1-p^{-2}}\right)^{-1}$$

The RHS looks familiar! We saw that the product of such expressions involving primes was the same as the Riemann Zeta Function.

So the probability is $\zeta(2)^{-1}$, which is $(\pi^2/6)^{-1}$

$$=\frac{6}{\pi^2}$$

I find this remarkable, that π, usually associated with circles, would arise in a probability involving coprimality!