Enrichment: topics you could meet in a Mathematics degree

This resource is one of several available on the FMSP website: www.furthermaths.org.uk/maths-preparation

Properties of Prime Numbers

The branch of mathematics called **Number Theory** used to be called ‘higher arithmetic’.

As the name suggests, University courses in Number Theory extend previous knowledge and understanding of properties of numbers (primarily integers) and introduce a range of new concepts such as modulo arithmetic and a wide range of theorems relating to prime numbers. The theorems are frequently easy to explain to a non-mathematician, but the proofs can sometimes be quite complicated and draw on a number of branches of mathematics.

> “It is just this which gives the higher arithmetic that magical charm which has made it the favourite science of the greatest mathematicians, not to mention its inexhaustible wealth, wherein it so greatly surpasses other parts of mathematics."
>
> Karl Friedrich Gauss

http://www.bing.com/images/search?q=gauss+image&FORM=IQFRBA&id=553CF44298F05C18F886B5B877F359FBEABB1FE9&selectedIndex=0#a

To study this topic, you will need to know what is meant by a prime number and be familiar with writing a number as a product of primes, perhaps using a factor tree. For example, 24 = 2 x 2 x 3 x 3 or 2^2 x 3^2.

If you have studied AS Further Mathematics, you may have come across the method of Proof by Induction, which can be used to confirm the truth of several rules in Number Theory. You may also have come across the method of Proof by Contradiction. Knowledge of these methods will be helpful in this topic, but are not essential.

Why are prime numbers interesting?

Mathematicians were fascinated by prime numbers and their properties as long ago as several hundred years B.C. For example, the Greek mathematician Eratosthenes devised a simple method for identifying all the prime numbers up to a chosen value, say 100, called the ‘Sieve of Eratosthenes’ (see Problem 1).

Around the same time, the mathematician Euclid wrote the set of 13 books entitled ‘Euclid’s Elements’, the seventh of which summarised some important facts about prime numbers. One of these facts relates primes and perfect numbers (see Problem 3).

Since then many other mathematicians have studied prime numbers. In 1640, the French mathematician Pierre de Fermat thought he had found a formula for finding prime numbers (see Problem 2) and in the seventeenth century a very famous set of numbers called ‘Mersenne primes’ were first written about, by then French monk Marin Mersenne (see Problem 3). These primes are still being investigated, and in fact the largest prime number ever found $2^{57,885,161} - 1$ is a Mersenne prime. This number was discovered in 2013 through the **Great Internet Mersenne Prime Search (GIMPS)**, and has almost 17.5 million digits!

Despite these many years of study, a lot is still unknown about prime numbers. For example, there is still no known formula for working out prime numbers. However, prime numbers now play a fundamental role in internet security through their role in **Public Key Encryption**. Solving problems involving primes also continues to fascinate modern-day mathematicians, with unproven theorems such as Goldbach's conjecture attracting **prizes** in the order of $1m!

Problem 1

Eratosthene's 'sieve' is a way to filter out all the numbers that are not prime, leaving just those numbers which are prime. In this problem, we will find all the prime numbers up to 100.

On the grid below:

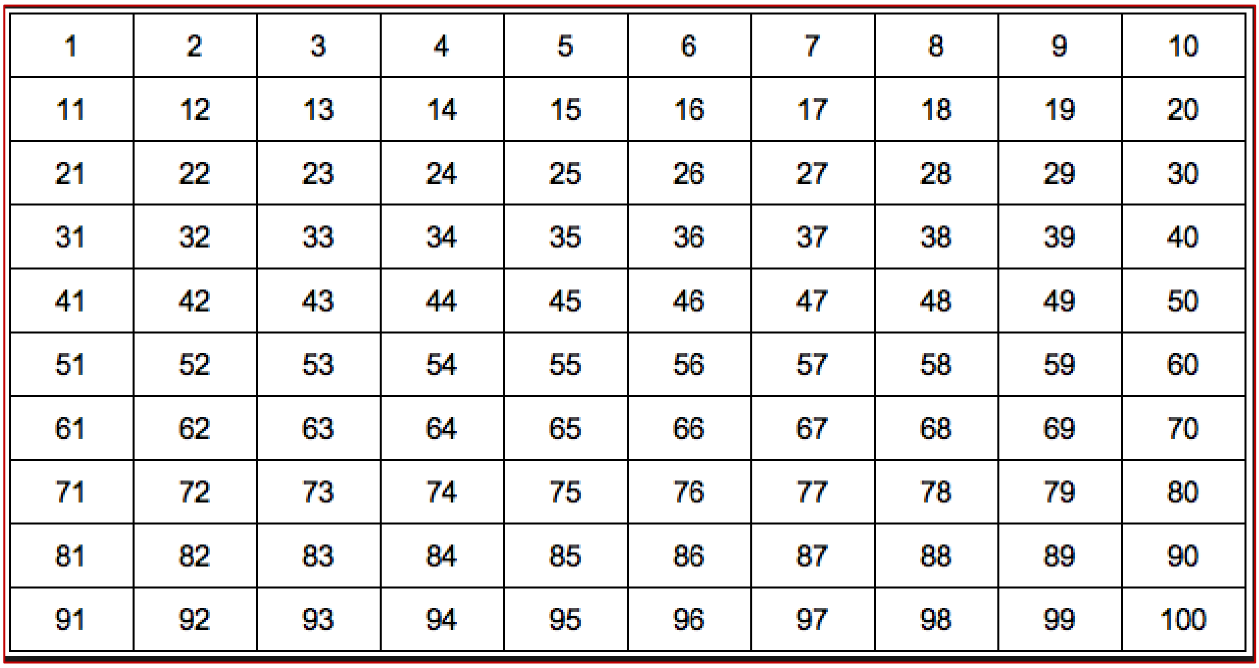
(i) Shade in 1 as this is not a prime number;

(ii) Circle 2 as this is prime. Now go through the grid and shade in all multiples of 2 – they cannot be prime as they have more than two factors (i.e. at least 1, 2 and the number itself).

(iii) Circle the first number in the grid that is not shaded and then go through the grid and shade in all multiples of this number as they cannot be prime.

(iv) Continue to repeat step (iii) until all numbers are either circled or shaded in.

It can be helpful to use a different colour each time you pass through the grid, as this makes patterns easier to identify.



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

How many prime numbers are there under 100?

An interactive version of the Sieve of Eratosthenes which finds the primes up to 400 can be found **here**.

Problem 2

Through the ages, mathematicians have tried to find formulae which generate prime numbers.

(i) Euler's function was proposed in 1772.

$$p(n) = n^2 + n + 41$$

Generate the first 5 terms using this formula, starting with $n = 0$. Does the formula always generate primes?

(ii) In 1640 Fermat proposed a formula for primes:

$$p(n) = 2^{2^n} + 1$$

Generate the first 5 terms using this formula, starting with $n = 0$. Does the formula always generate primes?

Problem 3

What is a Mersenne Prime?

Mersenne primes are prime numbers of the form $2^n - 1$. Of course, the expression $2^n - 1$ does not always yield a prime number. For example, $2^4 - 1 = 15$ which is not prime, and is referred to just as a 'Mersenne number'.

(i) Investigate the values obtained from the expression $2^n - 1$ for $n = 1, 2, 3$ ….. What do you notice?

What is a perfect number?

A perfect number is one which is the sum of all of its own factors, excluding the number itself. For example, 4 is **not** a perfect number because the factors of 4 are 1 and 2 (and 4 itself) but $4 \neq 1 + 2$.

(ii) There is one perfect number under 10 – can you find it?

(iii) There is one number in the 20s that is perfect – can you find it?

All known perfect numbers are even – it is not known whether any odd perfect numbers exist.

How are Mersenne primes and perfect numbers connected?

(iv) Firstly, look at the table below.

By identifying patterns, complete the first two columns of the table.

Then, if the number in the second column is prime, multiply it by the number in the first column and write the answer in the third column. Otherwise leave the third column empty.

[You can check if the larger numbers are prime **here**].

What do you notice about the numbers in the third column?

2	3	
4	7	
8	15	
16	31	

(v) Euclid proved that numbers of the form $2^{p-1}(2^p - 1)$are even perfect numbers.

(Euler later proved that all possible even perfect numbers are of this form. Hence there is a one to one correspondence between Mersenne primes and even perfect numbers).

Verify this result is true for the perfect numbers identified in part (iv). Identify the corresponding Mersenne prime in each case. The following table might be helpful to summarise your results.

Perfect number	**Value of p**	**Mersenne prime $2^p - 1$**	**Formula for perfect number $2^{p-1}(2^p - 1)$**

Problem 4

At GCSE you are likely to have expressed integers as a product of their prime factors.

All prime and composite (non-prime) numbers greater than 1 can be expressed this way.

For example,
48 = 2 x 2 x 2 x 2 x 3
22 = 2 x 11
13 = 13 (a trivial example but it still works!)

But can you prove that this is always the case?
i.e. can you prove **The Fundamental theorem of Arithmetic**:

> Every integer n (where n > 1) can be expressed as a product of prime numbers.

Hint: Use proof by induction.

If you have not studied proof by induction, there are some useful online resources which introduce the topic and give some examples.

- **NRICH Introduction to Mathematical Induction**
- **Mathshelper Example from AS Core Maths**
- **FMSP Online Revision Videos (OCR FP1)**

Problem 5

How many prime numbers are there? Ten? One hundred? A thousand?

In fact….

…there are an infinite number of prime numbers

Can you prove that this is true?

Hint: Use proof by contradiction.

If you have not studied proof by contradiction, there are some useful online resources which introduce the topic and give some examples.

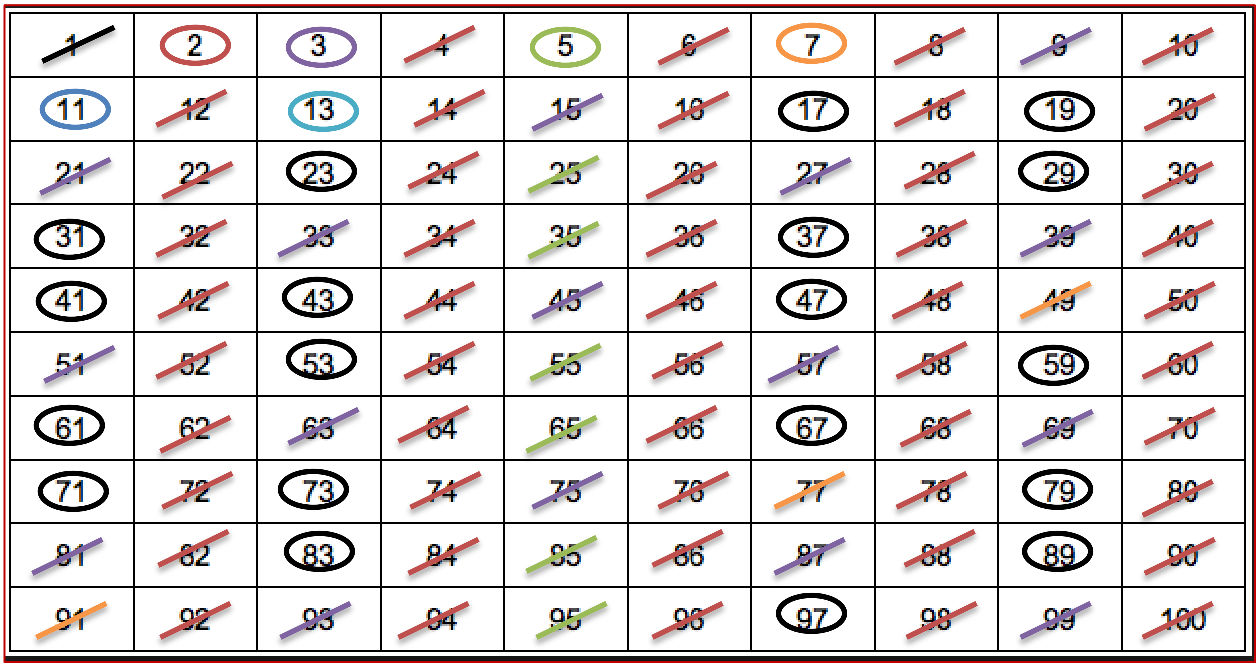
- **Video introduction to proof by contradiction**
- **Common Example - Proof that the square root of 2 is irrational (University of York)**

and if you read the solution and still aren't sure, here is a video link to an explanation of the solution.

- **Video - Proof of infinitely many prime numbers (University of Nottingham)**

Solutions

Solution 1



~~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~~

There are 25 prime numbers under 100.

Solution 2

(i) Using Euler's formula the first five values are 41, 43, 47, 53 and 61. This formula is known to work for values below $n = 40$.

(ii) Using Fermat's formula the first five values are 3, 5, 17, 257 and 65537. These numbers are all prime; however, Euler later showed that $2^{2^5} + 1 = 4{,}294{,}967{,}297$ has a factor of 641 and so is not prime.

Solution 3

(i) The Mersenne number sequence begins 1, 3, 7, 15, 31, 63, …. Note that if the answer is a prime number then the value of n is prime. For example, 31 is a prime number and the corresponding value of n is 5.
However, further investigation shows that n being prime is not a sufficient condition to ensure the Mersenne number is prime – take $n = 11$ for example: 2^{11} – 1= 2047 which is not prime (23 x 89 = 2047).
It has not yet been determined whether there the set of Mersenne primes is finite or infinite. A list of known Mersenne primes can be found **here**.

(ii) 6 is perfect as 6 = 1 + 2 + 3

(iii) 28 is perfect as 28 = 1 + 2 + 4 + 7 + 14
[The next two perfect numbers are 496 and 8128]

(iv)

2	3 (prime)	6
4	7 (prime)	28
8	15	
16	31(prime)	496
32	63	
64	127 (prime)	8 128
128	255	
256	511	
512	1023	
1024	2047	
2048	4095	
4096	8191(prime)	33 550 336

The first column are powers of 2. The second column are one less than the power of two on the next line.

The third column shows the first five perfect numbers, which can be checked **here**.

(v) Checking the formula $2^{p-1}(2^p - 1)$ for each even perfect number in the table above gives the following:

Perfect number	**Value of p**	**Mersenne prime $2^p - 1$**	**Formula for perfect number $2^{p-1}(2^p - 1)$**
6	$p = 2$	$(2^2 - 1) = 3$	$2^1(2^2 - 1) = 2 \times 3$
28	$p = 3$	$(2^3 - 1) = 7$	$2^2(2^3 - 1) = 4 \times 7$
496	$p = 5$	$(2^5 - 1) = 31$	$2^4(2^5 - 1) = 16 \times 31$
8128	$p = 7$	$(2^7 - 1) = 127$	$2^6(2^7 - 1) = 64 \times 127$
33 550 336	$p = 13$	$(2^{13} - 1) = 8191$	$2^{12}(2^{13} - 1) = 4096 \times 8191$

Note that the second column in the table in part (iv) picks out the relevant Mersenne prime.

Solution 4

Every integer n (where n > 1) can be expressed as a product of prime numbers.

We can prove this using proof by induction, with n ≥ 2.

First prove true for n = 2. 2 is itself a (trivial) product of a single prime number and so the theorem holds.

Now assume the result holds for any positive integer less than n.

Now let's look at the number n. If n is a prime number, then it is a product of one prime, and so the theorem holds.

If n is not a prime, it must be a composite number and so can be written as a product of two smaller numbers n_1 and n_2, i.e. $n = n_1n_2$. We know that each of the numbers n_1 and n_2 can be expressed as a product of primes p_i and q_i by our assumption earlier, therefore:

$$n_1 = p_1p_2p_3\ldots p_r \quad \text{and} \quad n_2 = q_1q_2q_3\ldots q_t.$$

Therefore $n = n_1n_2 = p_1p_2p_3\ldots p_r\ q_1q_2q_3\ldots q_t$ and so n is now written as a product of primes, as required.

Hence every integer n can be expressed as a product of primes, and so the result is true by induction.

Solution 5

…there are an infinite number of prime numbers

We will use proof by contradiction here. This involves assuming the opposite result is true and following through a logical procedure to arrive at a point which contradicts the original starting point.

So, let's assume that there are a finite (fixed) number of prime numbers and call these

$p_1, p_2, p_3, \ldots p_r$.

Now let's generate a number $n = p_1p_2p_3\ldots p_r + 1$ i.e. the product of all the primes add 1.

We can rearrange this to get $n - p_1p_2p_3\ldots p_r = 1$.

We know that n is not prime as it is not on our list of prime numbers.

We also know that n is not divisible by any of the p_i, because if it was, then $n - p_1p_2p_3\ldots p_r$ would be divisible by the number p_i and hence 1 would be divided by the number p_i which cannot be true. This means that n is not divisible by any of our list of prime numbers.

But we know from solution 2 that all integers greater than 1 can be expressed as a product of primes, i.e. are divisible by one or more of the p_i .

The only way around this is if n = 1, which is impossible as $n = p_1p_2p_3\ldots p_r + 1$.

Hence we have a contradiction and so our assumption that there are a fixed number of primes is untrue.

By contradiction there is therefore an infinite number of prime numbers.