Prime Numbers and Factorisation

Andrew D Smith
University College Dublin

22 January 2022

1 Introduction

1.1 Prime Numbers

Let n be a positive integer.

Another positive integer f is a *factor* of n if $\frac{n}{f}$ is an integer, or equivalently, if n can be expressed as the product of f and another positive integer.

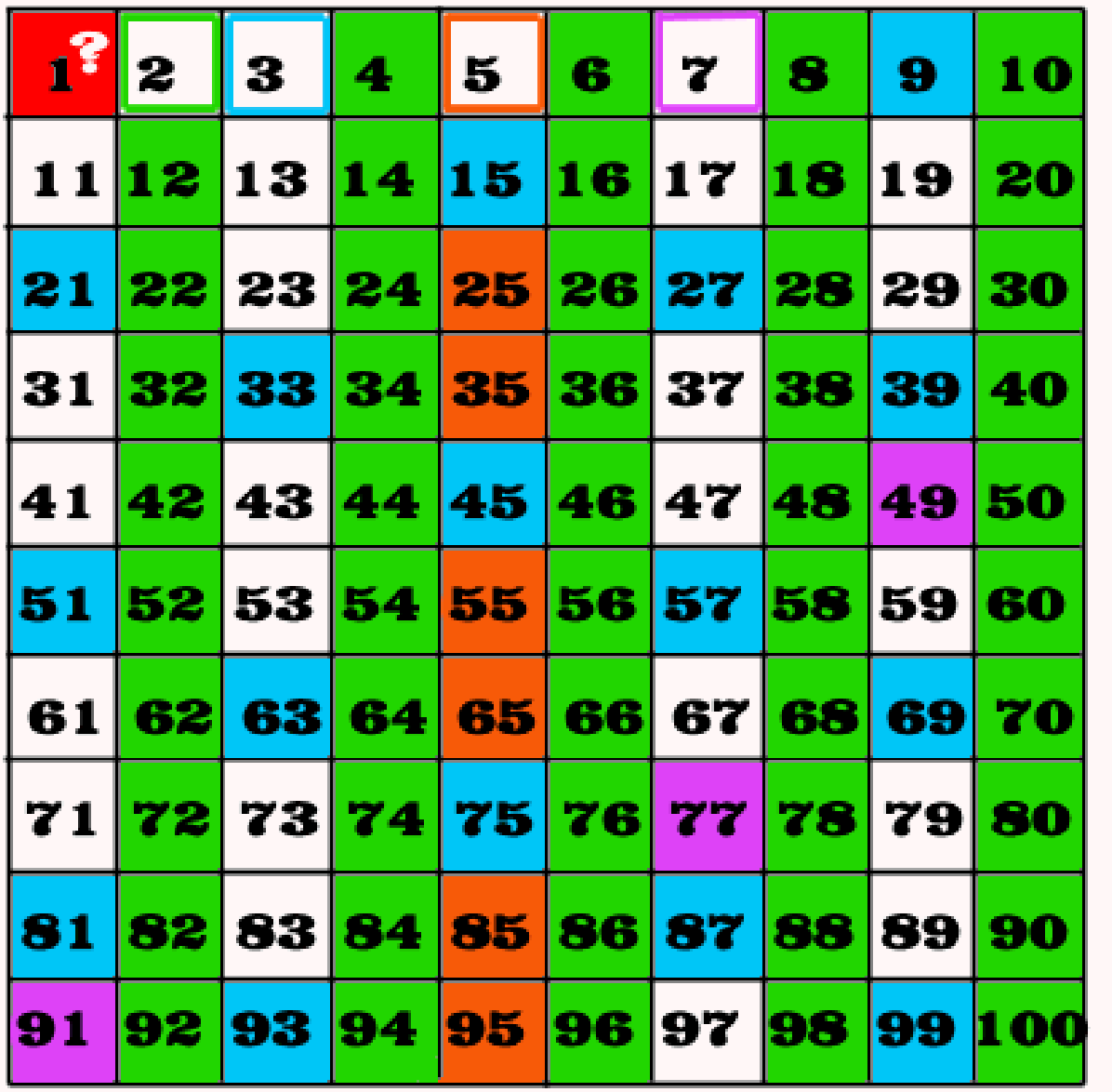
A *proper factor* is a factor of n not equal to 1 or itself.

A *prime number* is an integer $p \geq 2$ whose only factors are 1 and itself. Equivalently, $p \geq 2$ is prime if it has no proper factors.

The first few primes are 2, 3, 5, 7, 11, 13, 17, 19.

By convention, 1 is not a prime number.

1.2 Sieve of Eratosthenes



2 Some Facts about Prime Numbers

2.1 There are Infinitely Many Prime Numbers

This is a fact you might know, but how do we prove it is true?

Euclid's proof (around 300 BCE) by contradiction.

Suppose the number of primes, k, is finite Write those primes as $p_1, p_2, p_3, \ldots p_k$.

Define a positive integer q by the product:

$$q = p_1 \times p_2 \times p_3 \times \ldots \times p_k$$

Then, either

- $q + 1$ is a prime, not equal to one on the list.
- $q + 1$ is not a prime, in which case it has a smallest proper factor which is a prime, but also cannot be on the list since ever prime on the list divides q.

This is a contradiction. Therefore there cannot be a finite list of primes.

2.2 A Positive Integer is a Product of Primes

But the primes are not necessarily distinct. For example

$$18 = 2 \times 3 \times 3$$

Why does a prime factorisation always exist?

2.3 Primes modulo 4

Suppose p is a prime number. What can the remainder be when we divide p by 4?

- No prime is a multiple of 4.
- If p has a remainder of 2 (modulo 4) then p is an even number, so must be equal to 2, the only even prime.
- Odd primes must have a remainder of either 1 or 3 when divided by 4.

2.4 A Fact About Numbers Congruent to 1 Mod 4

If we have two integers a and b both of which have a remainder of 1 on division by 4, then their product ab also has a remainder of 1 on division by 4.

Proof:

$$\begin{aligned} a &= 4m + 1 \\ b &= 4n + 1 \\ ab &= (4m + 1)(4n + 1) \\ &= 16mn + 4m + 4n + 1 \\ &= 4(4mn + m + n) + 1 \end{aligned}$$

2.5 Infinitely Many Primes of the form $4n+3$

Suppose (for a contradiction) there are only finitely many primes that are also of the form $4n+3$. Let q the product of these primes. Now decompose $4q-1$ into prime factors. All the prime factors are odd, and none are in the list of primes of the form $4n+3$ since all on the list are factors of $4q$. Therefore all the prime factors of $4q-1$ are of the form $4n+1$. But then so must there product be, implying that $4q-1$ is of the form $4n+1$, a contradiction.

2.6 Infinitely Many Primes of the form $4n+1$

True, but significantly harder to prove. The proof uses the concept of quadratic reciprocity, which you will see later this semester.

2.7 Infinitely Many Primes of the form $6n+5$

Adapt Euclid's proof but consider $6q-1$.

2.8 Dirichlet's Theorem

Suppose a and d are positive integers with no common factors (except 1). Then the sequence

$$a, a+d, a+2d, a+3d, a+4d \ldots$$

contains infinitely many prime numbers.

Proof requires advanced methods.

3 Gaps between Primes

We know much about multiplication of prime numbers. Differences between primes are less well understood.

For example, 523 and 541 are primes, but the 17 numbers between contain no primes. This is an unusually large gap. Are there arbitrarily large and small gaps between primes?

3.1 The Twin Prime Conjecture

The twin prime conjecture is that there are infinitely many primes p such that $p + 2$ is also prime. Pairs such as $(3, 5)$ and $(11, 13)$ are twin primes.

It is widely believed to be true; many large twin primes have been computed. But is is still a conjecture. We do not know how to prove it.

3.2 Prime-Free Intervals

There are arbitrarily long integer intervals containing no prime numbers.

For a positive integer n, define $n!$, called *factorial* by

$$n! = 1 \times 2 \times 3 \times \ldots \times n$$

Why are there no primes in the interval from $n! + 2$ to $n! + n$ inclusive?

3.3 Harmonic Numbers

There is no simple formula for the n^{th} prime but there are some approximations when n is large.

Define the harmonic numbers H_n by:

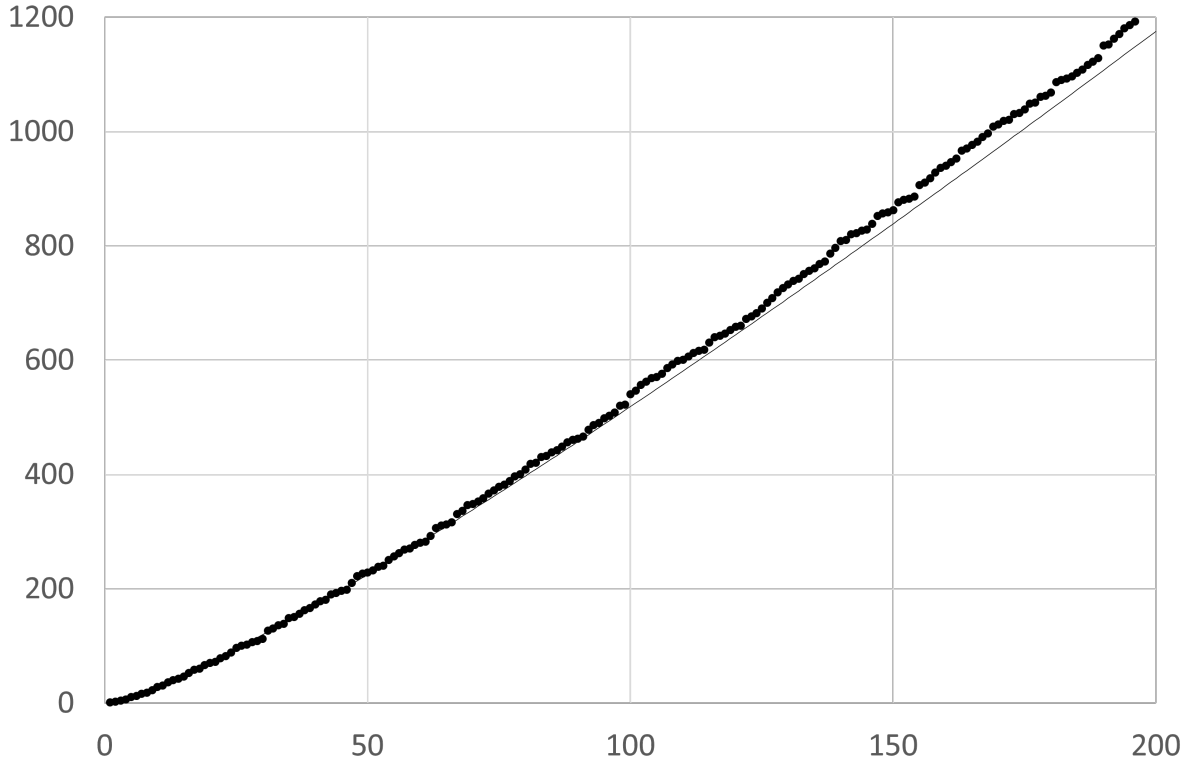
$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} = \sum_{r=1}^{n} \frac{1}{r}$$

Although the changes $1/n$ get smaller and smaller, the harmonic numbers keep getting larger, without limit, as n grows. At least they do in theory, even though on your computer the harmonic numbers stop increasing when $1/n$ is indistinguishable from zero.

Let p_n be the n^{th} prime. We tabulate p_n relative to nH_n:

n	p_n	H_n	$\frac{p_n}{nH_n}$
1	1	2	2
2	3	$\frac{3}{2}$	1
3	5	$\frac{11}{6}$	$\frac{10}{11}$
4	7	$\frac{25}{12}$	$\frac{21}{25}$
5	11	$\frac{137}{60}$	$\frac{132}{137}$
6	13	$\frac{49}{20}$	$\frac{130}{147}$

Here is a plot of p_n (the blobs) and nH_n (the curve) for $1 \leq n \leq 200$. About 1-in-6 integers from 0 to 1200 are prime.



3.4 Legendre's Conjecture

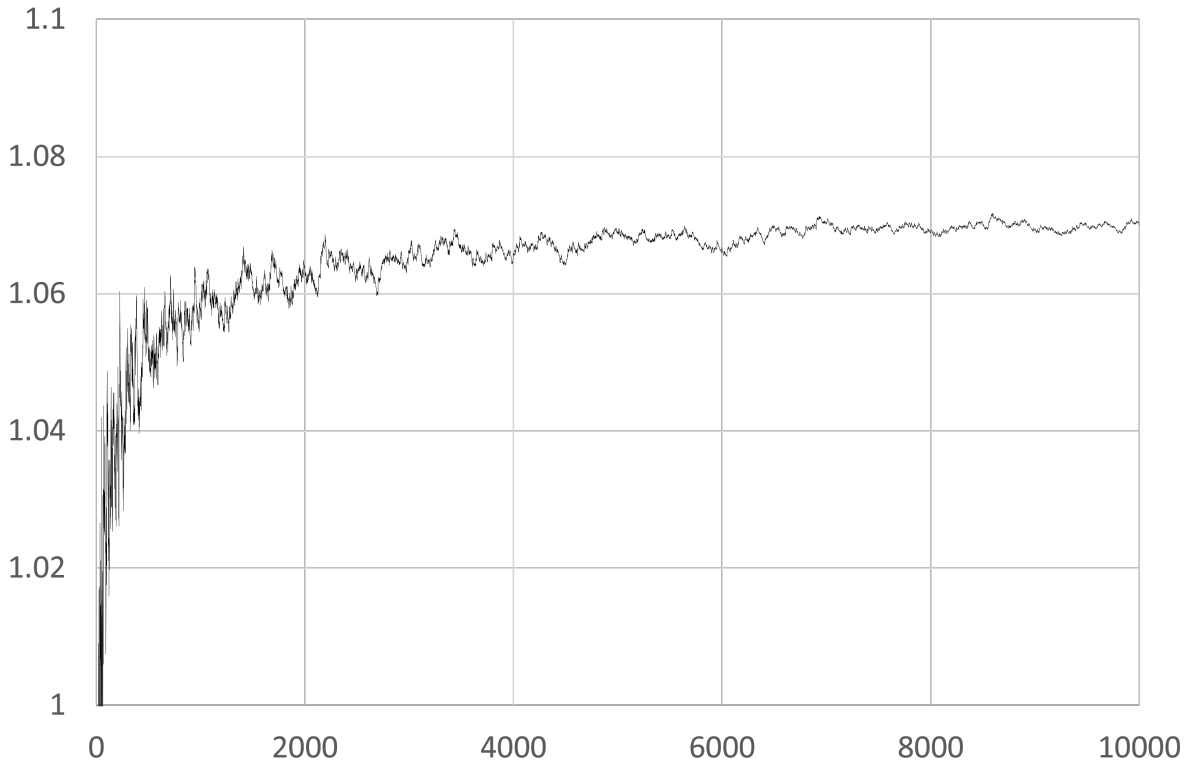
Named after Adrien-Marie Legendre (1752 – 1833) who claimed there is always at least one prime between consecutive perfect squares.

It is still thought to be true, with evidence checked up the first 10^9 squares, but we have no proof.

Legendre's conjecture implies that $p_n < (n+1)^2$, which is known to be true (hard to prove).

3.5 The Prime Number Theorem

Now let us compute the ratio $\frac{p_n}{nH_n}$ for the first 10,000 primes.



Although the ratio seems to stabilise around 1.07, for sufficiently large primes it does in fact tend back down to 1 when n is large enough.

Then the *prime number theorem* states that:

$$\lim_{n\uparrow\infty} \frac{p_n}{nH_n} = 1$$

The proof is complex and you won't be expected to know this. One implication is that gaps between primes can get arbitrarily large.

4 Unique Factorisation

Consider the number 17,120,443. We know we can break it up into prime factors. Is that factorisation unique (apart from the order) or are there numbers we can factorise into primes in more than one way.

In fact we have

$$17,120,443 = 3599 \times 4757 = 3953 \times 4331 = 4087 \times 4189$$

These are distinct factorisations. But are they prime?

If you check carefully, it turns out that none of these factors are primes. The prime factors are

$$17,120,443 = 59 \times 61 \times 67 \times 71$$

4.1 Fundamental Theorem of Arithmetic

The *fundamental theorem of arithmetic* states that the representation as a prime product is unique (up to the order of the prime factors).

Can you explain why this is true?

It is *not* obvious. The proof has several steps but can be followed with school level mathematics. You can quote the theorem in maths competitions.

5 Factorising Large Numbers

5.1 Testing if a Number is Prime

The brute force way to test if a number n is to check all integers between 1 and $\sqrt{n}$ to see if they are factors. It is not necessary to test possible factors greater than $\sqrt{n}$ (why?).

This calculation is very tedious if n is large. For example, the largest known prime number is $2^{82,589,933} - 1$. This is an example of a Mersenne number (one less than a power of 2). Think of the amount of calculation needed to check all those cases.

Although $2^{82,589,933} - 1$ is (at the time of writing) the largest known prime, we also know it is not the largest prime. There must be even bigger primes but we have not discovered them yet.

5.2 Fermat's Little Theorem

Suppose that p is an odd prime number. Then *Fermat's little theorem* states that $2^{p-1} - 1$ is divisible by p. We can use this as a test whether an odd number p is prime.

p	Remainder of $[2^{p-1} - 1] \div p$	Prime?
3	0	TRUE
5	0	TRUE
7	0	TRUE
9	3	FALSE
11	0	TRUE
13	0	TRUE
15	3	FALSE
17	0	TRUE
19	0	TRUE
21	3	FALSE
23	0	TRUE
25	15	FALSE
27	12	FALSE
29	0	TRUE
31	0	TRUE
33	3	FALSE
35	8	FALSE
37	0	TRUE
39	3	FALSE

This is an easier test to compute for large p than testing all factors up to $\sqrt{p}$ (why?).

5.3 Pseudoprimes

Unfortunately, Fermat's little theorem is a necessary but not sufficient condition for p to be prime. Exceptions (composite numbers

that still pass the test) are called pseudoprimes.

There are infinitely many pseudoprimes. The pseudoprimes less than 10000 are 341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821, 3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911.

We do not have a perfect way to test an arbitrary large number for primality, but we have tests which have very low rates of pseudoprimes.

We have rigorous proofs of primality for large numbers with particular forms. The current largest known prime is a Mersenne number, which is one less than a power of 2. There are clever ways for testing the primality of Mersenne numbers which do not work on arbitrary large odd numbers.

5.4 Factorising Large Numbers

For practical purposes we have ways to generate large primes (with a very small rate of pseudoprimes).

It is much more difficult to factorise large composite numbers n into primes, especially if the prime factors are large. The best methods we know are not much better than searching possible factors between 1 and $\sqrt{n}$.

Some public-key crypto-systems (including the RSA algorithm) exploit the difficulty of factorising large numbers. Someone can tell everyone exactly how to encrypt a message using the product of two primes. Decryption requires knowledge of the factorisation.