An Introduction to Prime Numbers

Introduction. These Notes set down some of the basic, elementary facts about *prime* numbers. It is understood that one is studying the *natural numbers* (denoted by **N**), namely the *positive whole numbers*: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, **...** . It is understood that one is familiar with the basic operations in **N** of *addition, subtraction, multiplication and division*. *Multiplication* means, of course, *repeated addition*:

$$3 \text{ multiplied by } 5 \text{ means } 3+3+3+3+3 = 15, \text{ is denoted by } 3 \times 5,$$
$$5 \text{ multiplied by } 3 \text{ means } 5+5+5 = 15, \text{ is denoted by} 5 \times 3.$$

Trying to 'reverse' multiplication leads to the important notion of a *factor of a number*:

$$26 = 2 \times 13, \text{ and we say that 2 is a } factor \text{ of } 26,$$
$$26 = 13 \times 2, \text{ and we say that 13 is a } factor \text{ of } 26,$$
$$26 = 1 \times 26, \text{ and we say that 1 is a } factor \text{ of } 26,$$
$$26 = 26 \times 1, \text{ and we say that 26 is a } factor \text{ of } 26.$$

Definition. If $n \in \mathbf{N},$ then f is a *factor* of n if $f \in \mathbf{N}$ and $n = fF$ for some $F \in \mathbf{N}.$
Examples. 1, 2, 3 and 6 are (all the) factors of 6. 1 and 13 are (all the) factors of 13. 1 is the only factor of 1. $1, 2, 2^2, 2^3, \dots, 2^{50}$ are all the factors of 2^{50}.

Observation. 1 has only one factor, and any other $n \in \mathbf{N}$ (*i.e.* with $n > 1$) has at least two factors, namely 1 and n itself (these two factors are often called – for obvious reasons – the 'trivial' factors of n) since $n = 1.n = n.1.$ Those natural numbers which have *exactly* two factors have a special name:

Definition. Let p be a natural number with $p > 1,$ then p is said to be a *prime* number (or is said to be *prime*) if p has exactly two factors, namely 1 and p.
Examples. $2, 3, 5, 7, 11, 13$ are primes numbers.

$4, 6, 8, 9, 10, 12, 14, 15, 16$ are not primes since - apart from having factors 1 and themselves - they have (extra) factors 2, 2 (and 3), 2 (and 4), 3, 2 (and 5), 2 (and 3, 4 and 6), 2 (and 7), 3 (and 5), 2 (and 4 and 8). Such numbers have a special name:

Definition. Let c be a natural number with $c > 1,$ then c is said to be a *composite* number (or is said to be *composite*) if it has more than two factors.

Simple consequence. If $c \in \mathbf{N}$ and c is composite, then $c = ab$ for some $a, b \in \mathbf{N}$ with $1 < a < c$ and $1 < b < c.$ (that is, every composite number can be expressed as the product of two natural numbers, each *greater* than 1, and less than the number itself.)

Proof. Since c is composite then c has more than two factors. Let a be one of those factors which is not equal to 1 or c (*i.e.* let a be a factor of c with $1 < a < c$). Then we have $c = ab$ for some $b \in \mathbf{N}$. Now, b could not be 1 (for if it were then $c = ab$ would give that c equalled a, which it doesn't), nor could b be equal to c (for if it were then $c = ab$ would give that a equalled 1, which it doesn't), and so we have $1 < b < c$. Thus $c = ab$ for some $a, b \in \mathbf{N}$ with $1 < a < c$ and $1 < b < c$.

And conversely: If $c \in \mathbf{N}$ and $c = ab$ for some $a, b \in \mathbf{N}$ with $1 < a < c$ and $1 < b < c$, then c is composite (that is, if a natural number can be expressed as a product of two natural numbers, both of which are greater than 1, and less than the number itself, then that number is composite.)

Proof. Since $c = ab$ for some $a, b \in \mathbf{N}$ with $1 < a < c$ and $1 < b < c$, then c automatically has more than two factors, since apart from the trivial 1 and c it also has a as a third factor, and so is composite.

Definition. Let $n \in \mathbf{N}$ and let f be a factor of n; then $n = fF$ for some $F \in \mathbf{N}$. F is sometimes called the *co-factor* of f.
Examples.

$$\text{When } n = 12 \text{ and } f = 3, \text{ then } f\text{'s co-factor is } 4,$$
$$\text{When } n = 21 \text{ and } f = 3, \text{ then } f\text{'s co-factor is } 7,$$
$$\text{When } n = 9 \text{ and } f = 3, \text{ then } f\text{'s co-factor is (also) } 3.$$

A reason why primes are important. Primes are important for many reasons, but a very basic one is that they are the 'building blocks' from which all natural numbers, that are greater than 1, are 'built. 'Built' in the sense that:

Theorem One. If $n \in \mathbf{N}$ and $n > 1$ then n is either a prime or is a product of some primes. (Another way of expressing that is to say that every composite number is a product of some prime numbers.)

Examples.

91 $= 7 \times 13$, is a product of primes; **81** $= 3 \times 3 \times 3 \times 3$, is a product of primes;

71 is a prime; **36** $= 2 \times 2 \times 3 \times 3$, is a product of primes; $45 = 3 \times 3 \times 5$, is a product of primes;

$\mathbf{2^{127} - 1} = 170141183460469231731687303715884105727$, is prime;

$\mathbf{2^{32} + 2^{16} + 1} = 4295032833 = 3 \times 7 \times 13 \times 97 \times 241 \times 673$, is a product of primes;

$\mathbf{2^{67} - 1} = 147573952589676412927 = 193707721 \times 761838257287$, is a product of primes.

There are several ways of proving Theorem One. One way is to start with:

Theorem Two. If $n \in \mathbf{N}$ and $n > 1$ then n is divisible by some prime number.

Again, there are several ways of proving *that*, and I will give one in a moment, but first:

If $n \in \mathbf{N}$ and $n > 1$ then n has more than one factor (two when n is prime, and more than two when n is composite). So, when $n > 1$, let its factors in increasing order be: $f_1, f_2, \ldots, f_r$, where $r \geq 2$ ($r = 2$ when n is prime, and $r > 2$ when n is composite), and so, for example, when $n = 12$ these would be 1, 2, 3, 4, 6, 12 (so r would be 6), and when $n = 37$ these would be 1 and 37 (so r would be 2).

With understanding (about $n's$ factors being taken in increasing order) having been made we can now state and prove:

Theorem Three. If $n \in \mathbf{N}$ and $n > 1$ then $n's$ second factor is a prime number.

(The second factor of 6 is 2, is prime; the second factor of 45 is 3, is prime; the second factor of 13 is 13, is prime; the second factor of 91 is 7, is prime; etc.)

Proof. 1 is, of course, the *first* factor of $n (f_1)$. We will now show that f_2, the *second* factor of n, is prime. Suppose that f_2 is not prime, then since $f_2 > 1$ it would mean that f_2 is composite, and so we would have $f_2 = ab$ for some $a, b \in \mathbf{N}$ with $1 < a < f_2$ and $1 < b < f_2$. But that is clearly impossible since it would mean that a is a factor of f_2 which is *greater* than the *first* factor of f_2 and *less* than the *second* factor of f_2. Thus f_2 cannot be composite, and so is prime.

Theorem Two follows immediately from Theorem Three.

Theorem One can also be proved by using the 'method of *Infinite Descent*,' but it can also be immediately deduced by using Theorem Two as follows:

(a) Proof of Theorem One. Since $n > 1$ then n is divisible by *some* prime (that's where we make an appeal to Theorem Two), and so we have $n = p_1 \times n_1$, for some prime p_1 and some $n_1 \in \mathbf{N}$ with $1 \leq n_1 < n$.

If $n_1 = 1$ then $n = p_1$ and so n is prime.

If $n_1 > 1$ then n_1 is divisible by some prime, and so we have $n_1 = p_2 \times n_2$ for some prime p_2 and some $n_2 \in \mathbf{N}$ with $1 \leq n_2 < n_1 < n$. Thus we have:

$$n = p_1 \times n_1 = p_1 \times (p_2 \times n_2) = p_1 \times p_2 \times n_2.$$

If $n_2 = 1$ then $n = p_1 \times p_2$ and so n is a product of (two) primes.

If $n_2 > 1$ then n_2 is divisible by some prime, and so we have $n_2 = p_3 \times n_3$ for some prime p_3 and some $n_3 \in \mathbf{N}$ with $1 \leq n_3 < n_2 < n_1 < n$. Thus we have:

$$n = p_1 \times p_2 \times n_2 = p_1 \times p_2 \times (p_3 \times n_3) = p_1 \times p_2 \times p_3 \times n_3.$$

Once again we observe that if $n_3 = 1$ then $n = p_1 \times p_2 \times p_3$, and so n is a product of (three) primes, but:

if $n_3 > 1$ then n_3 is divisible by some prime, and then have $n_3 = p_4 \times n_4$ for some prime p_4 and some $n_4 \in \mathbf{N}$ with $1 \leq n_4 < n_3 < n_2 < n_1 < n$.

After r such steps (*i.e.* with $n_1 > 1, n_2 > 1, \ldots, n_{r-1} > 1$) we would have:

$$n = p_1 \times p_2 \times \ldots \times p_r \times n_r,$$

for some prime p_r and some $n_r \in \mathbf{N}$ with $1 \leq n_r < \ldots < n_4 < n_3 < n_2 < n_1 < n.$

For each n there must be some r for which $n_r = 1$, and thus n is a product of some r prime numbers (the value of r will, of course, vary as n varies).

Why must there be some r for which $n_r = 1$? One can give any one of two reasons (thought, of course, one reason is enough).

A reason: Just use the fact that each prime is at least 2, and thus from the equation

$$n = p_1 \times p_2 \times \ldots \times p_r \times n_r \text{ we would get } n \geq \overbrace{2 \times 2 \times \ldots \times 2 \times 1}^{\text{there are } r \text{ 2's here}} = 2^r, \text{ and so would have:}$$

$$n \geq 2^r \quad \ldots (1)$$

For each value of n the inequality (1) could only be true for values of r which were small enough, and so there would have to (eventually) be a value of r for which $n_t = 1.$

An alternative reason. If there was an n for which there were *no* value of r for which $n_r = 1,$ then one would get an infinite decreasing sequence of distinct natural numbers:

$$n > n_1 > n_2 > n_3 > \ldots > n_{90} > \ldots > n_{12321} > \ldots \textit{ ad infinitum}$$

which is impossible by the 'Fundamental Property of the Natural Numbers' which states that 'there cannot be an infinite strictly decreasing sequence of natural numbers.'

Comment on the above. The theorem 'If $n \in \mathbf{N}$ and $n > 1$ then n is either a prime or is a product of some primes' is a very simple one, and I have devoted a lot of space to a proof of it. It is more the method of proof that is important above than the theorem itself.

A much more important theorem, which is an extension of this, is the one which says:

Theorem (the *Unique Factorisation Theorem*) If $n \in \mathbf{N}$ and $n > 1$ then n is either a prime or is a **unique** product of primes.

It means, for example, that the number 60 is not just the product of the primes 2, 2, 3 and 5, but that there is no other set of primes whose product is 60. That this sort of thing is true, not only for the number 60, but for all composite natural numbers, is the substance of the Unique Factorisation Theorem. This theorem has got many remarkable consequences.

This theorem is so important that it is sometimes called the 'Fundamental Theorem of Number Theory,' though that name is sometimes given to yet another theorem:

Theorem[1]. If p is a prime number (a prime of the Natural Number System) and $a, b \in \mathbf{Z}$ with $p|ab$ then $p|a$ or $p|b$.

These two theorems are 'equivalent' in the sense that each is a consequence of the other.

Let us turn our attention to other matters. Every natural number greater than 1 is either prime or composite; how many of them are prime and how many of them are composite?

The second of those questions has an immediate and trivial answer: there are an infinite numbers of composite numbers. By far the simplest way to show that is to just form all the even numbers starting with $4: 4, 6, 8, 10, 12, 14, 16, etc$. These are just all natural numbers of the form $2n$, with $n \in \mathbf{N}$ and $n > 1$. Such numbers are automatically composite since each of them is the product of two natural numbers each of which is greater than 1.

Of course that construction misses out many composites (infinitely many, in fact) – ones like $9, 15, 21, 25, 27, 33, 35, etc$. – but if you only wish to know how many composites there are then the '$2n$ construction' shows – with a minimum of fuss – that there are an infinite number of them.

Now we get down to the serious business of how many primes there are! This is a much more delicate question! Whereas it is easy – indeed utterly trivial and banal – to give a construction for composites, it is quite a different matter to do something similar for primes.

---

[1] This theorem will – in time – be seen to be a consequence of the 'extended Euclidean Algorithm.'

Before the 18-th. century, the only way that was known to test if a given number was a prime or not was the '*method of Eratosthenes*.' (E., an early Greek mathematician, is credited with being the first person who made a serious attempt at calculating the circumference of the Earth. He is said to have done so to within 90 miles or thereabouts.) This very crude method involves 'testing up as far as the square-root,' and the idea behind it is a very simple one:

Let's say you want to find out if the number 91 (say) is a prime or a composite. If it is a prime then its only factors will be 1 and 91, but if it is composite then we will have that $91 = ab$ for some $a, b \in \mathbf{N}$ with $a > 1$ and $b > 1$. Which of these happens? Well we just do it by trying possible values for a. Could a be 2?, could it be 3?, could it be 4? etc. **...**

> a can't be 2 because $91 = 2 \times 45 + 1$, and so 2 is $\underline{\text{not}}$ a factor of 91,
>
> a can't be 3 because $91 = 3 \times 30 + 1$, and so 3 is $\underline{\text{not}}$ a factor of 91,
>
> a can't be 4 because 2 is $\underline{\text{not}}$ a factor of 91, and so 4 can't be a factor of 91,
>
> a can't be 5 because $91 = 5 \times 18 + 1$, and so 5 is $\underline{\text{not}}$ a factor of 91,
>
> a can't be 6 because 2 is $\underline{\text{not}}$ a factor of 91, and so 6 can't be a factor of 91,
>
> testing $a = 7$ we find that $91 = 7 \times 13$, and thus 91 is composite.

Suppose we tried the same approach with the number 97 (say):

> *a can't be* 2 *because* $97 = 2 \times 48 + 1$, *and so* 2 *is* $\underline{not}$ *a factor of* 97,
>
> *a can't be* 3 *because* $97 = 3 \times 32 + 1$, *and so* 3 *is* $\underline{not}$ *a factor of* 97,
>
> *a can't be* 4 *because* 2 *is* $\underline{not}$ *a factor of* 97, *and so* 4 *can't be a factor of* 97,
>
> *a can't be* 5 *because* $97 = 5 \times 19 + 2$, *and so* 5 *is* $\underline{not}$ *a factor of* 97,
>
> *a can't be* 6 *because* 2 *is* $\underline{not}$ *a factor of* 97, *and so* 6 *can't be a factor of* 97,
>
> *a can't be* 7 *because* $97 = 7 \times 13 + 6$, *and so* 7 *is* $\underline{not}$ *a factor of* 97,
>
> *a can't be* 8 *because* 2 *is* $\underline{not}$ *a factor of* 97, *and so* 8 *can't be a factor of* 97,
>
> *a can't be* 9 *because* 3 *is* $\underline{not}$ *a factor of* 97, *and so* 9 *can't be a factor of* 97,
>
> *a can't be* 10 *because* 2 *is* $\underline{not}$ *a factor of* 97, *and so* 10 *can't be a factor of* 97,
>
> *a can't be* 11 *because* $97 = 11 \times 8 + 10$, *and so* 11 *can't be a factor of* 97,
>
> *a can't be* 12 *because* 2 *is* $\underline{not}$ *a factor of* 97, *and so* 12 *can't be a factor of* 97,
>
> *a can't be* 13 *because* $97 = 13 \times 7 + 6$, *and so* 13 *can't be a factor of* 97, …

How much longer should one continue doing this sort of thing before knowing one way or the other what is the nature of the number 97?

Eratosthenes' simple idea was that as far as 97 was concerned it was unnecessary to have done any more calculations once every a from 2 to 9 had been tested. Those calculations alone are sufficient to enable one to conclude that 97 is a prime number.

Why is that, and *what about* other numbers? (57? 1234235321? **...**). The key to it all is:

(Simple) Theorem (of Eratosthenes) If $n \in \mathbf{N}$ and n is composite, then at least one of the non-trivial factors of n ('non-trivial' means not equal to 1) is at most $\sqrt{n}$.

Proof.   Since n is composite then $n = ab$ for some $a, b \in \mathbf{N}$ with $a > 1$ and $b > 1$. Now we could not have $a > \sqrt{n}$ and $b > \sqrt{n}$, because if we did then we would have $ab > \sqrt{n}.\sqrt{n} = n,$ and so would have $ab > n,$ which is not so, since $ab = n$.

Thus, either $a \le \sqrt{n}$ or $b \le \sqrt{n}$, and thus 'at least one of the non-trivial factors of n ('non-trivial' means 'not equal to 1'.) is at most $\sqrt{n}$.' **(end of proof.)**

Because of this simple result we know (for example) that if 91 is composite then it will have a non-trivial factor (so it will be: 2 or 3 or 4 or 5 or **...**) which will be at most $\sqrt{91}$. But since $9 < \sqrt{91} < 10$, it means that we need only test for possible factors up as far as 9. And, not only that, but we don't have to test all of those because of this:

Simple Observation.   Let $A, B, n \in \mathbf{N},$ such that that A is a factor of B. If A is not a factor of n then B is not a factor of n.

Proof.   Since A is a factor of B then $B = Ab,$ for some $b \in \mathbf{N}$. Suppose that B is a factor of n, then $n = Bn'$ for some $n' \in \mathbf{N},$ and thus $n = (Ab)n' = A(bn') = An'',$ for some $n'' \in \mathbf{N}.$ But that would mean that A is a factor of n, which it isn't. Thus B cannot be a factor of n. **(end of proof**.)

Because of this last (simple) observation, then – in testing to see if a natural number n is prime or not – we do not need to test all possible factors of n up as far as its square-root; we only need to test the possible prime factors up as far as the square-root of n.

Eratosthenes' Test. If $n \in \mathbf{N},$ and $n > 1,$ then n is composite if and only if n is divisible by some prime number which is at most $\sqrt{n}$.

Proof. (First the 'if' part:) Suppose n is divisible by some prime which is at most $\sqrt{n}$. Then $n = pn'$ for some prime p $(p \le \sqrt{n})$ and some $n' \in \mathbf{N}$. Then n' cannot be 1 or n: if n' were 1 then we would have $n = p$ which is impossible since $p \le \sqrt{n} < n,$ and if n' were equal to n then we would have $p = 1,$ which is impossible since primes (by definition) are greater than 1.

(Secondly, the 'only if' part) Suppose that n is composite. Then n has a non-trivial factor which is at most $\sqrt{n}$. Let a be such a factor, then $n = ab$ for some $b \in \mathbf{N}$.

But since $a > 1$ then a is divisible by some prime p (which itself must be at most a), and so $a = pA$ for some $A \in \mathbf{N}.$ But then we have we have $n = ab = (pA)b = p(Ab) = pc$ for some $c \in \mathbf{N}.$ Thus $n = pc,$ for some $c \in \mathbf{N},$ and so n is divisible by some prime number which is at most $\sqrt{n}$.

A consequence of Eratosthenes' Test. If $n \in \mathbf{N},$ and $n > 1,$ then n is **prime** if and only if n is **not** divisible by any prime number which is at most $\sqrt{n}$.

Worked examples of the Eratosthenes Test, and a consequence. Test the following numbers for primality: 427, 569 and 1681.

$\sqrt{427} = 20....,$ and so we need only test for possible prime factors up as far as 20 (and so only up as far as 19, since 19 is the largest prime up as far as 20):

$$2 \text{ is not a factor of 427 because } 427 = 2 \times 213 + 1,$$
$$3 \text{ is not a factor of 427 because } 427 = 3 \times 142 + 1,$$
$$5 \text{ is not a factor of 427 because } 427 = 5 \times 85 + 2,$$
$$7 \text{ is a factor of 427 because } 427 = 7 \times 61,$$

and thus 427 is composite.

$\sqrt{569} = 23....,$ and so we need only test for possible prime factors up as far as 23.

$$2 \text{ is not a factor of 569 because } 569 = 2 \times 284 + 1,$$
$$3 \text{ is not a factor of 569 because } 569 = 3 \times 189 + 2,$$
$$5 \text{ is not a factor of 569 because } 569 = 5 \times 113 + 4,$$
$$7 \text{ is not a factor of 569 because } 569 = 7 \times 81 + 2,$$
$$11 \text{ is not a factor of 569 because } 569 = 11 \times 51 + 8,$$
$$13 \text{ is not a factor of 569 because } 569 = 13 \times 43 + 10,$$
$$17 \text{ is not a factor of 569 because } 569 = 17 \times 33 + 8,$$
$$19 \text{ is not a factor of 569 because } 569 = 19 \times 29 + 28,$$
$$23 \text{ is not a factor of 569 because } 569 = 23 \times 24 + 17,$$

and thus 569 is prime.

$\sqrt{1681} = 41,$ and thus $1681 = 41 \times 41,$ and so (automatically) 1681 is composite.

The Eratosthenes Test suffers from one major drawback: it is (virtually) **useless**!! As *n* increases in size so too does $\sqrt{n}$, and the amount of *possible* calculation increases tremendously[2].

You can, of course, be lucky: if you take the largish number 863,978,063,137 whose square-root is 929,504.2028 **...** then to test if it is prime or not – using the Eratosthenes method – then you need only test possible prime factors up to 929,501 (which is the largest prime up to 929,504). You quickly see that 2, 3 and 5 don't divide 863,978,063,137 and when you try 7 you get that it does divide, and so 863,978,063,137 is composite.

But if you happened to try the number 863,978,063,147 (whose square-root is 29,504**.**2028 …) then you would not be so lucky. Not only would 2, 3, 5, 7 not divide it, but no other prime up to the square-root of 863,978,063,147 does either.

And how many 'other primes' are there up as far as the square-root of 863,978,063,147? Well, and you may wonder how I know, there are something like 65,000 of them!

Later we will meet some very sophisticated methods for telling if a number is a prime or not, but for now it's about time we got to the first serious theorem about primes:

Euclid's Theorem on the infinitude of prime numbers. There are an infinite number of prime numbers.

Comment. I will give two forms of the proof (they look very similar) that Euclid gave (there are over a hundred different proofs of the infinitude of primes). The first one will be given as it was given by Euclid himself – as (what we call) a 'proof *by contradiction*' – and the second proof (a re-wording of Euclid's proof) is an example of (what we call) a *constructive* proof.

Proof 1 (the proof 'by contradiction'). Suppose that there are only a finite number of primes, and let *p* be the largest prime number (such a largest would exist as a consequence of there being only a finite number of primes).

Let's then say that *p* is the *n*-th. prime, where *n* is some natural number.

Form the natural number *P*, by setting $P = (2 \times 3 \times 5 \times 7 \times \ldots \times p) + 1$.

That is, *define* the number *P* by:

$$P = p_1 \times p_2 \times p_3 \times \ldots \times p_n + 1 \qquad \ldots (i)$$

---

[2] Later in your Number Theory studies you will come across an incredibly important and powerful theorem - Fermat's 'little' theorem - which will enable you to sometimes show that a number is composite without actually finding a proper factor of it!!!

where $p_1 (= 2)$, $p_2 (= 3)$, $p_3 (= 5)$, ... , $p_n (= p)$ are all the primes from the first of them (p_1), up to the n-th. of them (p_n).

Now clearly we have $P > p$, and so since p is the largest prime number then P cannot be prime, and so P must be composite. But every composite number is a product of prime numbers, and so we would have:

$$\overbrace{P = q_1 \times q_2 \times \quad ... \quad \times q_s}^{s \text{ primes in this product}}, \text{ where } q_1, q_2, \quad ... \quad , q_s \text{ are some } s \text{ prime numbers.}$$

(There is no suggestion that those s primes are all different. It doesn't matter anyway.)

But then:

$$P = p_1 \times p_2 \times p_3 \times \ ... \ \times p_n + 1 = q_1 \times q_2 \times \ ... \ \times q_s \quad ... \ (ii)$$

and since p ($= p_n$) is the largest prime then every one of the primes $q_1, q_2, \ ... \ , q_s$ is at most p_n, and so every one of those primes occurs somewhere in the product of all the primes from 2 up to p_n.

In particular, picking on the prime q_1 (one could also have picked on q_2, ... , or q_s – it doesn't matter), it must one of the primes from 2 up to p_n. Thus the equation (ii) can be rewritten as:

$$q_1 B + 1 = q_1 A \quad ... (iii)$$

where $B, A \in \mathbf{N}$ (B is the product of all the primes from 2 up to p_n with q_1 excluded, and A is the product of all the other primes on the R.H.S. of (ii) apart from the q_1 at the start)

But that equation (iii) is clearly impossible since it leads immediately to:

$$1 = q_1 A - q_1 B = q_1 (A - B) = q_1 C, \text{ where } C = (A - B) \in \mathbf{N} \quad ... (iv)$$

which is impossible since it means that q_1 divides 1 (which it doesn't).

Thus there cannot be a largest prime - in other words, there cannot be (only) a finite number of primes. (**proves Euclid's theorem.**)

Proof 1 of Euclid's theorem is a classic example of what is known of as a proof '*by contradiction.*' The basic structure of such proofs is very simple: there is something which you wish to prove is true, and you prove it is true by this means: you say '*suppose it* wasn't *true*,' and then by some means (that's the hard part, of course!) you argue that that would lead to some conflict, some 'contradiction' (the very word 'contradiction' means 'saying otherwise (or differently)'; *contra* is the Latin word for 'against', and

dictare is the Latin for 'to speak'). You conclude that what you *claimed* to be true, *is* true.

Proof 1 then proves that there are an infinite number of primes, but it doesn't (at first) give you any idea as to how you might find another prime larger than one you already had.

However just a very slight rewording of it does enable you to do so, and to make what is called a *constructive proof* of Euclid's theorem:

Euclid's Theorem on the infinitude of prime numbers. There are an infinite number of prime numbers.

Proof 2 (the proof 'by construction'). We will show that there are an infinite number of primes by showing that if p is any prime then there is another prime q (whose value we can find *constructively* – meaning that there is an actual calculation – which when carried out - will produce the claimed q) with $q > p$.

So, let p be any prime, suppose that it is the n-th.prime (for some $n \in \mathbf{N}$), and define the natural number P by setting:

$$P = p_1 \times p_2 \times p_3 \times \ \ldots \times p_n + 1 \qquad \ldots (1)$$

where $p_1 (= 2)$, $p_2 (= 3)$, $p_3 (= 5)$, $\ldots$, $p_n (= p)$ are all the primes from the first of them (p_1), up to the n-th. of them (p_n).

Then P is a natural number which, being greater than 1, must be divisible by some prime number (that's just what Theorem Two, on Page 3 these Notes: every natural number that is greater than 1 is divisible by some prime number). Call it q (there may be several such values for it). Then we have:

$$P = p_1 \times p_2 \times p_3 \times \ \ldots \ \times p_n + 1 = qA, \text{ for some } A \in \mathbf{N} \qquad \textbf{...} (2)$$

We claim that that q must be greater than p. Why?

Suppose it wasn't. Then q would have to be either the first prime, or the second prime, or the third prime, **...** , or the n-th prime. So we would have $q = p_k$ for some value of k with $1 \le k \le n$. Then equation (2) would become:

$$qB + 1 = qA, \text{ for some } B \in \mathbf{N} \qquad \textbf{...} (3)$$

(*B* would be the product of all the primes from the first to the n-th, but with the k-th of them excluded). But (3) is clearly impossible since it leads to:

$$1 = qA - qB = q(A - B) = qC, \text{ where } C = (A - B) \in \mathbf{N} \quad \textbf{...} (4)$$

which is impossible since it means that q divides 1 (which it doesn't).   Thus the prime q can't be any of the primes from the first of them up to the n-th. of them, and so it must be greater than the n-th. of them. Thus the prime q is greater than p. (**end of proof**.)

So, given a prime p we can actually *constructively* find a larger prime q.

Definition. Let p be a prime number, and suppose that p is the n-th prime. Then by the *Euclidean number E_p* we mean the number E_p defined by:

$$E_p = p_1 \times p_2 \times p_3 \times \ ... \ \times p_n + 1,$$

and we will call E_p the n-th. *Euclidean number*.

Examples. The first 7 Euclidean numbers are:

$E_2 = 2 + 1 = 3$, is prime,
$E_3 = 2 \times 3 + 1 = 7,$ is prime,
$E_5 = 2 \times 3 \times 5 + 1 = 31$, is prime,
$E_7 = 2 \times 3 \times 5 \times 7 + 1 = 211$, is prime,
$E_{11} = 2 \times 3 \times 5 \times 7 \times 11 + 1 = 2311$, is prime,
$E_{13} = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30{,}031 = 59 \times 509$, is composite
$E_{17} = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 + 1 = 510{,}511 = 19 \times 97 \times 277$, is composite.

As you see they get big quickly.

In the computer laboratory we will be able to use Maple to perform many interesting calculations in connection with these, and other, related numbers.

Some variations on the Euclidean numbers defined above.

(**1**) One could also use the numbers e_p defined by $e_p = p_1 \times p_2 \times p_3 \times \ ... \ \times p_n - 1$, but now with p at least 3 (so as to guarantee that $e_p > 1$, and so is divisible by some prime).

Exercise. Make a proof of the infinitude of primes that uses these numbers in the proof, instead of the numbers E_p .

Also do **Maple** factorisations of several of these numbers.

(**2**) One could also have used the numbers $(p! + 1)$.

(**3**) And also one could have used the numbers $(p! - 1)$. (here again you need p at least 3 to guarantee that $(p! - 1) > 1,$ so as to have it divisible by some prime.

Exercise. Make a proof of the infinitude of primes that uses these numbers in the proof, instead of the numbers e_p and E_p.

Also do **Maple** factorisations (especially using the '**ifactor**(n, easy)' command) of several of these numbers.

―――――――――――