## Contents

1 Statement of Euclid’s theorem .................................. 1  
2 Preliminaries for the proof .................................... 2  
   2.1 What is a factor? ........................................ 2  
   2.2 What is a prime number? ................................. 3  
   2.3 The Well-Ordering Principle ............................. 4  
   2.4 A theorem on existence of prime factors .............. 4  
   2.5 What is a finite set?  .................................. 6  
3 The proof of Euclid’s Theorem ................................. 7

### 1 Statement of Euclid’s theorem

About 2,300 years ago, the great mathematician Euclid, in his book the *Elements* (ca. 300 BCE), proved that there are infinitely many prime numbers.

The following version of the proof is not exactly Euclid’s, but is based essentially on the same idea.

First, here is Euclid’s result:

|THEOREM.| The set of prime numbers is infinite.

And now we discuss the proof.
2 Preliminaries for the proof

Before we present Euclid’s proof, we need to prepare the ground by explaining all the concepts that play a role in it.

In the proof, there appear:

1. finite sets,
2. infinite sets,
3. factors,
4. prime numbers.

So we have to explain what all these things mean.

2.1 What is a factor?

Definition 1. Let $m, n$ be natural numbers.

1. We say that $m$ is a factor of $n$ if there exists a natural number $k$ such that
   \[ n = km. \]
2. We say that $m$ divides $n$ if $m$ is a factor of $n$.
3. We say that $n$ is divisible by $m$ if $m$ divides $n$.
4. We write $m | n$ to indicate that $m$ divides $n$.

Remark 1. As the previous definition indicates, “is a factor of” and “divides” mean exactly the same thing. And we can say that $m$ divides $n$, or that $m$ is factor of $n$, using “divisible”, but when you do that the order is different: “$m$ divides $n$” becomes “$n$ s divisible by $m$”.

Example 1.

- 3 is a factor of 6,
- 3 divides 6,
• 6 is divisible by 3,
• 6 is not divisible by 4,
• 4 is not a factor of 6,
• 4 does not divide 6,
• The statement “3|6” is true, but the statement “4|6” is false.
• If $S$ is the set of the all natural numbers that divide 12, then the members of $S$ are 1, 2, 3, 3, 6, and 12, so

$$S = \{1, 2, 3, 4, 6, 12\}.$$  \hspace{1cm} (0.1)

This says that 12 has exactly six natural number factors. \hfill \square

2.2 What is a prime number?

**Definition 2.** A prime number is a natural number $p$ such that

I. $p > 1$,

II. $p$ does not have any natural number factors other than 1 and $p$. \hfill \square

And here is another way of saying the same, in case you do not want to talk about “factors”.

**Definition 3.** A prime number is a natural number $p$ such that

I. $p > 1$,

II. There do no exist natural numbers $j, k$ such that $j > 1$, $k > 1$, and $p = jk$. \hfill \square

**Remark 2.** If you look at the definition of “prime number”, you will notice that, for a number $p$ to qualify as a prime number, it has to satisfy $p > 1$. In other words, the number 1 is not prime. Isn’t that weird? After all, the only natural number factor of 1 is 1, so the only factors of 1 are 1 and itself, and this seems to suggest that 1 is prime.

Well, if we had defined a number $p$ to be prime if $p$ has no natural number factors other than 1 and itself, then 1 would be prime. But we were very careful not to do that. Why?
The reason is, simply, that there is a very nice theorem called the “unique factorization theorem”, that says that every natural number greater than 1 either is prime or can be written as a product of primes in a unique way. (For example: $6 = 3 \cdot 2$, $84 = 7 \cdot 3 \cdot 2 \cdot 2$, etc.)

If 1 was a prime, then the result would not be true as stated. (For example, here are two different ways to write 6 as a product of primes: $6 = 3 \cdot 2$ and $6 = 3 \cdot 2 \cdot 1$.) And mathematicians like the theorem to be true as said, so we have decided not to call 1 a prime.

If you do not like this, just keep in mind that we can use words any way we like, as long as we all agree on what they are going to mean. If we decide that 1 is not prime, then 1 is not prime, and that’s it. If you think that for you 1 is really prime, just ask yourself why and you will see that you do not have a proof that 1 is prime.

\[ \square \]

2.3 The Well-Ordering Principle

The Well-Ordering Principle is one of the basic properties of the natural number system. It says the following:

THE WELL-ORDERING PRINCIPLE. Every nonempty set of natural numbers has a smallest member.

2.4 A theorem on existence of prime factors

In the proof of Euclid’s Theorem, we are going to use an important fact, so we present this fact first.

Lemma 1. If $n$ is any natural number such that $n > 1$, then $n$ has a prime factor. (That is, there exists a prime number $p$ such that $p$ is a factor of $n$, i.e., equivalently, $p | n$.)
PROOF.
Let $n$ be a natural number such that $n > 1$.
Let $F$ be the set of all natural numbers $m$ such that $n > 1$ and $m$ is a factor of $n$.
Then $F$ is nonempty. (Proof: The number $n$ is obviously a factor of $n$. And $n > 1$. So $n \in F$.)
By the Well-ordering principle, $F$ has a smallest member.
Let $q$ be the smallest member of $F$.
Then $q$ is a factor of $n$, and $q > 1$.
Furthermore, we claim that $q$ is prime.

PROOF THAT $q$ IS PRIME:

Suppose $q$ was not prime.
Then either $q = 1$ or $q$ has a natural number factor other than 1 and $q$.
Pick one such factor and call it $r$.
Then $r$ is a factor of $q$, so $q = rk$ for some natural number $k$.
And $q$ is a factor of $n$, so $n = qj$ for some natural number $j$.
So $n = qj = (rk)j = r(jk)$.
So $r$ is a factor of $n$.
But $r < q$, because $r$ is a factor of $q$ and $r$ is not $q$.
And $r > 1$, because $r$ is a factor of $q$ and $r$ is not 1.
Since $r$ is factor of $n$ and $r > 1$, it follows that $r \in F$.
Since $r < q$ and $r \in F$, $q$ is not the smallest member of $F$.
But $q$ is the smallest member of $F$.
So we have reached a contradiction.
So $q$ is prime.

Hence $q$ is a prime number which is a factor of $n$. So $n$ has a prime factor.
Q.E.D.

What does “Q.E.D.” mean?

“Q.E.D.” stands for the Latin phrase *quod erat demonstrandum*, meaning “which is what was to be proved”. It is used to indicate the end of a proof.
2.5 What is a finite set?

We now want to explain what a “finite set” is. For that purpose, we first have to say what it means for a set to have \( n \) members for a particular natural number \( n \).

**Definition 4.**

1. If \( n \in \mathbb{N} \) (i.e., if \( n \) is a natural number), and \( S \) is a set, we say that \( S \) has \( n \) members if it is possible to write a list

\[
L = (s_1, s_2, \ldots, s_n)
\]

of length \( n \) such that

a. All the entries of the list \( L \) are members of \( S \). (That is, precisely: for every \( j \), the entry \( s_j \) belongs to \( S \).)
b. Every member of \( S \) is an entry of \( L \). (That is, if \( s \in S \) then there exists \( j \) such that \( s = s_j \).)
c. The list \( L \) has no repetitions. (That is, if \( i, j \) are any two different indeces, then \( s_i \neq s_j \).)

2. An empty set\(^1\) is said to have —underlinezero members. \( \square \)

**Definition 5.** A set \( S \) is finite if either \( S \) is empty or \( S \) has \( n \) members for some natural number \( n \). \( \square \)

**Definition 6.** A set \( S \) is infinite if it is not finite. \( \square \)

---

\(^1\)Later we will see that there is only one empty set. So I really should have said the empty set rather than an empty set. But for the moment, since I haven’t explained that there is only one empty set, I say an empty set.
3 The proof of Euclid’s Theorem

Let $S$ be the set of all prime numbers.

We want to prove that $S$ is an infinite set.

Suppose $S$ is not infinite, so $S$ is a finite set.

Let $L = (p_1, p_2, \ldots, p_n)$ be a list\(^2\) of all the members of $S$.
Let $M = p_1p_2\cdots p_n$. (That is, $M$ is the product of all the entries of the list $L$.)
Let $N = M + 1$.

Then $N$ has a prime factor.

Pick a prime number which is a factor of $N$, and call it $q$.

We will show that the prime number $q$ is not on the list $L$.

Suppose $q$ was one of the entries of the list $L$.

Then we may pick $j$ such that $j \in \mathbb{N}, 1 \leq j \leq n$, and $q = p_j$.

Then $q$ is a factor of the number $M$, because $p_j$ is a factor of the product $p_1p_2\cdots p_n$.
But $q$ is also a factor of $N$.
So $q$ is a factor of $N - M$, i.e. $q$ is a factor of 1 (because $N - M = 1$).
But $q$ is a prime number, so $q$ cannot be a factor of 1.
The two previous statements contradict each other. So we have derived a contradiction.

Hence the assumption that $q$ is one of the entries of the list $L$ is impossible. So $q$ is not an entry of $L$.
But $q$ is a prime number.
Hence $L$ is not a list of all the primes.
But we have assumed that $L$ is a list of all the primes.
So we have established a contradiction. This contradiction arose from assuming that $S$ is a finite set.
So $S$ is an infinite set.

Q.E.D.

\(^2\)I say “a list” rather than “the list”, because you can list the primes in different ways, for example: in increasing order, or in decreasing order.