2 NUMBER THEORY I

Recall that a natural number \( p \neq 1 \) is prime if its only divisors are \( \pm 1 \) and \( \pm p \), i.e.,
\[
\forall a \in \mathbb{N}, a | p \Rightarrow a \in \{1, p\}.
\]

We want to prove that there are an infinite number of primes. We’ll get to this via some intermediate results. First we need to understand proof by contradiction.

2.1 Proof by contradiction

We’ll do an example first.

**Proposition 2.1** There do not exist integers \( m \) and \( n \) such that \( 14m + 20n = 101 \).

**Remark:** We can’t prove this directly, as this would involve checking \( 14m + 20n \) for every choice of \( m \) and \( n \).

**Proof.** Suppose that the proposition is false. Hence its negation is true, i.e., there exist integers \( m \) and \( n \) such that \( 14m + 20n = 101 \).

Hence \( 2(7m + 10n) = 101 \). Hence 101 is even. This contradicts the fact that 101 is odd. [Our initial assumption about the existence of \( m \) and \( n \) has lead to nonsense.]

Hence the proposition must be true. \( \square \)

We want to prove that a proposition \( q \) is true. The idea:

(i) Assume that \( q \) is false, i.e., assume that \( \neg q \) is true.

(ii) Deduce from this assumption something which we know to be false, e.g., \( x > 0 \) and \( x < 0 \), or something which contradicts our assumption in (i).

(iii) We conclude that our assumption in (i) must have been false. Hence \( q \) must be true.

In this section we will see some examples of propositions proved by contradiction. It is important to be methodical in structuring proofs, being especially careful to say what every variable means (e.g., “Let \( a \in \mathbb{N} \)”) and to say what you are assuming and what you have deduced. Proofs can get very complicated later, so it is important to get into good habits early on. The proofs in this section will be examples of how you should structure a proof.

**Proposition 2.2** Let \( a, b \in \mathbb{Z} \) with \( a \geq 2 \). Then \( a \nmid b \) or \( a \nmid (b + 1) \).

**Proof.** Suppose that the proposition is false, i.e., that there exist \( a, b \in \mathbb{Z} \) with \( a \geq 2 \) such that it is not true that \( a \nmid b \) or \( a \nmid (b + 1) \). Then \( a | b \) and \( a | (b + 1) \). Hence \( a | ((b + 1) - b) \). So \( a | 1 \). Hence \( a \leq 1 \), contradicting \( a \geq 2 \). Hence our supposition was false, i.e., the proposition is true. \( \square \)
2.2 Prime numbers

The following lemma is necessary for the subsequent result, but we will prove it later in the course:

Lemma 2.3 Let $a$ and $b$ be natural numbers and let $p$ be a prime number. If $p|ab$, then $p|a$ or $p|b$.

Remark: The converse is also true. Let $p$ be a natural number with $p \neq 1$. Suppose that for all natural numbers $a$ and $b$, if $p|ab$, then $p|a$ or $p|b$. Then $p$ is prime. (This is also a proof by contradiction - see exercises).

Along with Lemma 2.3 this gives an alternative characterisation of the prime numbers:

Let $p \in \mathbb{N}$ with $p \neq 1$. Then $p$ is prime if and only if $\forall a, b \in \mathbb{N}; p|ab \Rightarrow (p|a \lor p|b)$.

Proposition 2.4 $\sqrt{2}$ is not a rational number.

Proof. Suppose that the proposition is false, i.e., the negation is true. Hence (we are assuming that) $\sqrt{2}$ is a rational number, and so we may write $\sqrt{2} = \frac{a}{b}$ for natural numbers $a$ and $b$. By dividing common factors from $a$ and $b$ we may assume that $\frac{a}{b}$ is in its lowest terms, i.e., the only common divisors of $a$ and $b$ are 1 and $-1$. Since $\sqrt{2} = \frac{a}{b}$, we have $2 = \frac{a^2}{b^2}$. So $a^2 = 2b^2$, and $2|a^2$. Since 2 is prime, by Lemma 2.3 we have $2|a$. This means that there is a natural number $c$ such that $a = 2c$. Substituting this into $a^2 = 2b^2$, we get $(2c)^2 = 2b^2$, so $4c^2 = 2b^2$. So $2c^2 = b^2$. Hence $2|b^2$, and by Lemma 2.3 $2|b$. Hence we have shown that $2|a$ and $2|b$, contradicting our choice of $a$ and $b$ having no common divisors. Hence our original assumption (that $\sqrt{2}$ is a rational number) must be false. Hence $\sqrt{2}$ is rational.

The next result, as well as being a nice example of a proof by contradiction, will be needed later on.

Proposition 2.5 Every natural number greater than one has a prime divisor.

Proof. Suppose that the proposition is false. Then there is a natural number $n > 1$ which has no prime divisor.

Let $m$ be the smallest natural number such that $m > 1$ and $m$ has no prime divisor (so $m \leq n$).

Now $m|m$, so $m$ cannot be prime (or it would be a prime divisor of itself). Hence $m = ab$ for some natural numbers $a$ and $b$ with $a \neq 1$ and $a \neq m$. So $1 < a < m$. By choice of $m$, this means that $a$ must have a prime divisor, say $p$. Hence there is some natural number $d$ such that $a = pd$. But then $m = ab = (pd)b = p(db)$, and so $p|m$, a contradiction since $m$ has no prime divisor. Hence our initial assumption is false, and every natural number greater than one has a prime divisor.

This method of proof is often called proof by minimal counterexample.

The proposition above allows us to prove a much more impressive theorem, due to Euclid.
**Theorem 2.6 (Euclid)** There are infinitely many prime numbers.

**Proof.** Suppose that the theorem is false. Then there are only finitely many prime numbers, say $p_1, p_2, \ldots, p_k$.

Write $m = p_1 p_2 \ldots p_k + 1$. Then $m$ is a natural number and $m > 1$, so by Proposition 2.5 $m$ has a prime divisor, say $p_j$. Hence $m = ap_j$ for some natural number $a$.

We have

$$ap_j = m = (p_1 p_2 \ldots p_{j-1} p_{j+1} \ldots p_k)p_j + 1.$$  

So

$$(a - p_1 p_2 \ldots p_{j-1} p_{j+1} \ldots p_k)p_j = 1.$$  

This means that $p_j | 1$. The only natural number dividing 1 is 1, so $p_j = 1$, a contradiction since $p_j$ is prime. Hence our original assumption that there are only finitely many primes is false. Hence the theorem is true. \(\square\)

**Proof by contrapositive**

This is a special case of proof by contradiction.

Suppose that we want to prove $p \Rightarrow q$. Recall that this is equivalent to $(\neg q) \Rightarrow (\neg p)$. So to prove $p \Rightarrow q$ it suffices to assume $\neg q$ and deduce $\neg p$.

**Compare to a proof of $p \Rightarrow q$ by contradiction:** Assume false, i.e., that $(\neg p \Rightarrow q)$ is true. But $(\neg p \Rightarrow q) \equiv p \land (\neg q)$. If we manage to show that $(\neg q) \Rightarrow (\neg p)$, then we must have that $(\neg q) \land p$ is false, contradicting our assumption.

To illustrate proof by contrapositive, we apply it to a (trivial) result which it would be hard to prove otherwise:

**Proposition 2.7** Let $a$ and $b$ be integers. If $a + b \geq 9$, then $a \geq 5$ or $b \geq 5$.

**Proof.** We want to show that for all integers $a$ and $b$ we have $p \Rightarrow q$, where $p$ is “$a + b \geq 9$” and $q$ is “$a \geq 5$ or $b \geq 5$.”.

$\neg q$ is “$a < 5$ and $b < 5$”.

$\neg p$ is “$a + b < 9$”.

Let $a$ and $b$ be integers. Suppose that $\neg q$ is true. So $a \leq 4$ and $b \leq 4$. Then $a + b \leq 4 + 4 = 8 < 9$. So $\neg p$ is true.

Hence $\neg q \Rightarrow \neg p$ is true, and so $p \Rightarrow q$ is true. \(\square\)