3. Unique factorisation

The main result of this section will be the:

Theorem 3.1 (Fundamental Theorem of Arithmetic)**.** *Every non-zero integer a is of the form*

$$\pm 1 \cdot p_1 \cdot p_2 \cdot \dots \cdot p_n,$$

where $p_1, p_2, \dots, p_n$ are prime numbers.

The key result is the following:

Proposition 3.2. *If p is a prime number and $p|ab$ then either $p|a$ or $p|b$.*

Proof. We may suppose that p does not divide a. As the only divisors of p are p and 1, and p does not divide a, it follows that the greatest common divisor of p and a is 1.

By (2.9) it follows that we may find integers λ and μ such that

$$1 = \lambda p + \mu a.$$

Multiplying both sides by b we get

$$\begin{aligned} b &= b \cdot 1 \\ &= b(\lambda p + \mu a) \\ &= (b\lambda)p + \mu ab. \end{aligned}$$

Now the first term is visibly divisible by p and the second term is divisible by p by assumption. Thus p divides b. □

Proof of (3.1)*.* We first prove existence. If a is negative and

$$|a| = p_1 \cdot p_2 \cdot \dots \cdot p_n,$$

then

$$a = -p_1 \cdot p_2 \cdot \dots \cdot p_n.$$

Thus we may assume that a is positive. We proceed by induction on a. If $a = 1$ there is nothing to prove. Assume the result for all natural numbers less than a. If a is prime there is nothing to prove. Otherwise we may write

$$a = bc,$$

where b and c are both greater than one and both less than a. By induction b and c are products of primes,

$$b = q_1 \cdot q_2 \cdot \dots \cdot q_m \qquad \text{and} \qquad c = r_1 \cdot r_2 \cdot \dots \cdot r_n.$$

In this case

$$bc = q_1 \cdot q_2 \cdot \dots \cdot q_m \cdot r_1 \cdot r_2 \cdot \dots \cdot r_n,$$

is also a product of primes. This completes the proof of existence.

Now suppose that we can factor a into two different products of primes,

$$\pm q_1 \cdot q_2 \cdot \dots \cdot q_m = \pm r_1 \cdot r_2 \cdot \dots \cdot r_n.$$

We have

$$q_1 \cdot q_2 \cdot \dots \cdot q_m = r_1 \cdot r_2 \cdot \dots \cdot r_n.$$

Consider the prime q_1. It divides the LHS and so it divides the RHS. But we have already shown that if a prime divides a product it must divide one of the factors. Thus q_1 divides r_j for some j. As r_j is prime and q_i is not one it follows that $q_1 = r_i$. It is then easy to see that $q_1 = r_1$. Cancelling, we are done by induction on the number of prime factors. $\square$

It is worth pointing out that we can compute the greatest common divisor using uniqueness of factorisation. Suppose that we want to find the greatest common divisor of two natural numbers a and b. We can factor both a and b into into primes. Collecting together like primes and possibly allowing zero as an exponent, we may write

$$a = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k} \qquad \text{and} \qquad b = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}.$$

Suppose that d is the greatest common divisor. We may aslo assume that d has the same form:

$$d = p_1^{o_1} p_2^{o_2} \dots p_k^{o_k}.$$

We can calculate the exponents o_i prime by prime. In fact

$$o_i = \min(m_i, n_i).$$

In fact, as d divides a, we must have $o_i \leq m_i$. As d divides b we must have $o_i \leq n_i$.