

# Chapter 1

## The Fundamental Theorem of Arithmetic

### 1.1 Primes

**Definition 1.1.** We say that  $p \in \mathbb{N}$  is prime if it has just two factors in  $\mathbb{N}$ , 1 and  $p$  itself.

Number theory might be described as the study of the sequence of primes

$$2, 3, 5, 7, 11, 13, \dots$$

**Definition 1.2.** 1. We denote the  $n$ th prime by  $p_n$ .

2. If  $x \in \mathbb{R}$  then we denote the number of primes  $\leq x$  by  $\pi(x)$ .

Thus

$$p_1 = 2, p_2 = 3, p_3 = 5, \dots,$$

while

$$\pi(-2) = 0, \pi(2) = 1, \pi(\pi) = 2, \dots$$

### 1.2 The fundamental theorem

**Theorem 1.1.** Every non-zero natural number  $n \in \mathbb{N}$  can be expressed as a product of primes

$$n = p_1 \cdots p_r;$$

and this expression is unique up to order.

By convention, an empty sum has value 0 and an empty product has value 1. Thus  $n = 1$  is the product of 0 primes.

Another way of putting the theorem is that each non-zero  $n \in \mathbb{N}$  is uniquely expressible in the form

$$n = 2^{e_2} 3^{e_3} 5^{e_5} \dots$$

where each  $e_p \in \mathbb{N}$  with  $e_p = 0$  for all but a finite number of primes  $p$ .

The proof of the theorem, which we shall give later in this chapter, is non-trivial. It is easy to lose sight of this, since the theorem is normally met long before the concept of *proof* is encountered.

### 1.3 Euclid's Algorithm

**Definition 1.3.** Suppose  $m, n \in \mathbb{Z}$ . We say that  $d \in \mathbb{N}$  is the greatest common divisor of  $m$  and  $n$ , and write

$$d = \gcd(m, n),$$

if

$$d \mid m, d \mid n,$$

and if  $e \in \mathbb{N}$  then

$$e \mid m, e \mid n \implies e \mid d.$$

The term *highest common factor* (or hcf), is often used in schools; but we shall always refer to it as the gcd.

Note that at this point we do not know that  $\gcd(m, n)$  exists. This follows easily from the Fundamental Theorem; but we want to use it in proving the theorem, so that is not relevant.

It is however clear that if  $\gcd(m, n)$  exists then it is unique. For if  $d, d' \in \mathbb{N}$  both satisfy the criteria then

$$d \mid d', d' \mid d \implies d = d'.$$

**Theorem 1.2.** Any two integers  $m, n$  have a greatest common divisor

$$d = \gcd(m, n).$$

Moreover, we can find integers  $x, y$  such that

$$d = mx + ny.$$

*Proof.* We may assume that  $m > 0$ ; for if  $m = 0$  then it is clear that

$$\gcd(m, n) = |n|,$$

while if  $m < 0$  then we can replace  $m$  by  $-m$ .

Now we follow the Euclidean Algorithm. Divide  $n$  by  $m$ :

$$n = q_0m + r_0 \quad (0 \leq r_0 < m).$$

If  $r_0 \neq 0$ , divide  $m$  by  $r_0$ :

$$m = q_1r_0 + r_1 \quad (0 \leq r_1 < r_0).$$

If  $r_1 \neq 0$ , divide  $r_0$  by  $r_1$ :

$$r_0 = q_2r_1 + r_2 \quad (0 \leq r_2 < r_1).$$

Continue in this way.

Since the remainders are strictly decreasing:

$$r_0 > r_1 > r_2 > \cdots,$$

the sequence must end with remainder 0, say

$$r_{s+1} = 0.$$

We assert that

$$d = \gcd(m, n) = r_s,$$

ie the gcd is the last non-zero remainder.

For

$$d = | r_{s-1} \text{ since } r_{s-1} = q_{s+1}r_s.$$

Now

$$\begin{aligned} d \mid r_s, r_{s-1} &\implies d \mid r_{s-2} \text{ since } r_{s-2} = r_s - q_s r_{s-1}; \\ d \mid r_{s-1}, r_{s-2} &\implies d \mid r_{s-3} \text{ since } r_{s-3} = r_{s-1} - q_{s-1} r_{s-2}; \\ &\dots\dots\dots \\ d \mid r_2, r_1 &\implies d \mid m; \\ d \mid r_1, m &\implies d \mid n. \end{aligned}$$

Thus

$$d \mid m, n.$$

Conversely, if  $e \mid m, n$  then

$$\begin{aligned} e \mid r_0 &\text{ since } r_0 = n - q_0m; \\ e \mid r_1 &\text{ since } r_1 = m - q_1r_0; \\ &\dots\dots\dots \\ e \mid r_s &\text{ since } r_s = r_{s-1} - q_s r_{s-1}. \end{aligned}$$

Thus

$$e \mid m, n \implies e \mid d.$$

We have proved therefore that  $\gcd(m, n)$  exists and

$$\gcd(m, n) = d = r_s.$$

To prove the second part of the theorem, which states that  $d$  is a linear combination of  $m$  and  $n$  (with integer coefficients), we note that if  $a, b$  are linear combinations of  $m, n$  then a linear combination of  $a, b$  is also a linear combination of  $m, n$ .

Now  $r_1$  is a linear combination of  $m, n$ , from the first step in the algorithm;  $r_2$  is a linear combination of  $m, r_1$ , and so of  $m, n$ , from the second step; and so on, until finally  $d = r_s$  is a linear combination of  $m, n$ :

$$d = mx + ny.$$

□

We say that  $m, n$  are *coprime* if

$$\gcd(m, n) = 1.$$

**Corollary 1.1.** *If  $m, n$  are coprime then there exist integers  $x, y$  such that*

$$mx + ny = 1.$$

## 1.4 Speeding up the algorithm

Note that if we allow *negative* remainders then given  $m, n \in \mathbb{Z}$  we can find  $q, r \in \mathbb{Z}$  such that

$$n = qm + r,$$

where  $|r| \leq |m|/2$ .

If we follow the Euclidean Algorithm allowing negative remainders then the remainder is at least halved at each step. It follows that if

$$2^r \leq n < 2^{r+1}$$

then the algorithm will complete in  $\leq r$  steps.

Another way to put this is to say that if  $n$  is written to base 2 then it contains at most  $r$  bits (each bit being 0 or 1).

When talking of the efficiency of algorithms we measure the input in terms of the number of bits. In particular, we define the *length*  $\ell(n)$  to be the number of bits in  $n$ . We say that an algorithm completes in polynomial time, or that it is in class  $P$ , if the number of steps it takes to complete its task is  $\leq P(r)$ , where  $P(x)$  is a polynomial and  $r$  is the number of bits in the input.

Evidently the Euclidian algorithm (allowing negative remainders) is a polynomial-time algorithm for computing  $\gcd(m, n)$ .

## 1.5 Example

Let us determine

$$\gcd(1075, 2468).$$

The algorithm goes:

$$2468 = 2 \cdot 1075 + 318,$$

$$1075 = 3 \cdot 318 + 121,$$

$$318 = 3 \cdot 121 - 45,$$

$$121 = 3 \cdot 45 - 14,$$

$$45 = 3 \cdot 14 + 3,$$

$$14 = 5 \cdot 3 - 1,$$

$$3 = 3 \cdot 1.$$

Thus

$$\gcd(1075, 2468) = 1;$$

the numbers are coprime.

To solve

$$1075x + 2468y = 1,$$

we start at the end:

$$\begin{aligned} 1 &= 5 \cdot 3 - 14 \\ &= 5(45 - 3 \cdot 14) - 14 = 5 \cdot 45 - 16 \cdot 14 \\ &= 5 \cdot 45 - 16(3 \cdot 45 - 121) = 16 \cdot 121 - 43 \cdot 45 \\ &= 16 \cdot 121 - 43(3 \cdot 121 - 318) = 43 \cdot 318 - 113 \cdot 121 \\ &= 43 \cdot 318 - 113(1075 - 3 \cdot 318) = 382 \cdot 318 - 113 \cdot 1075 \\ &= 382(2468 - 2 \cdot 1075) - 113 \cdot 1075 = 382 \cdot 2468 - 877 \cdot 1075. \end{aligned}$$

Note that this solution is not unique; we could add any multiple  $1075t$  to  $x$ , and subtract  $2468t$  from  $y$ , eg

$$\begin{aligned} 1 &= (382 - 1075) \cdot 2468 + (2468 - 877) \cdot 1075 \\ &= 1591 \cdot 2468 - 693 \cdot 1075. \end{aligned}$$

We shall return to this point later.

## 1.6 An alternative proof

There is an apparently simpler way of establishing the result.

*Proof.* We may suppose that  $x, y$  are not both 0, since in that case it is evident that  $\gcd(m, n) = 0$ .

Consider the set  $S$  of all numbers of the form

$$mx + ny \quad (x, y \in \mathbb{Z}).$$

There are evidently numbers  $> 0$  in this set. Let  $d$  be the smallest such integer; say

$$d = ma + nb.$$

We assert that

$$d = \gcd(m, n).$$

For suppose  $d \nmid m$ . Divide  $m$  by  $d$ :

$$m = qd + r,$$

where  $0 < r < d$ . Then

$$r = m - qd = m(1 - qa) - nqd,$$

Thus  $r \in S$ , contradicting the minimality of  $d$ .

Hence  $d \mid m$ , and similarly  $d \mid n$ .

On the other hand

$$d' \mid m, n \implies d' \mid ma + nb = d.$$

We conclude that

$$d = \gcd(m, n).$$

□

The trouble with this proof is that it gives no idea of how to determine  $\gcd(m, n)$ . It appears to be *non-constructive*.

Actually, that is not technically correct. It is evident from the discussion above that there is a solution to

$$mx + ny = d$$

with

$$|x| \leq |n|, \quad |y| \leq |m|.$$

So it would be theoretically possible to test all numbers  $(x, y)$  in this range, and find which minimises  $mx + ny$ .

However, if  $x, y$  are very large, say 100 digits, this is completely impractical.

## 1.7 Euclid's Lemma

**Proposition 1.1.** *Suppose  $p$  is prime; and suppose  $m, n \in \mathbb{Z}$ . Then*

$$p \mid mn \implies p \mid m \text{ or } p \mid n.$$

*Proof.* Suppose

$$p \nmid m.$$

Then  $p, m$  are coprime, and so there exist  $a, b \in \mathbb{Z}$  such that

$$pa + mb = 1.$$

Multiplying by  $n$ ,

$$pna + mnb = n.$$

Now

$$p \mid pna, p \mid mnb \implies p \mid n.$$

□

## 1.8 Proof of the Fundamental Theorem

*Proof.*

**Lemma 1.1.**  *$n$  is a product of primes.*

*Proof.* We argue by induction on  $n$ . If  $n$  is *composite*, ie not prime, then

$$n = rs,$$

with

$$1 < r, s < n.$$

By our inductive hypothesis,  $r, s$  are products of primes. Hence so is  $n$ . □

To complete the proof, we argue again by induction. Suppose

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

are two expressions for  $n$  as a product of primes.

Then

$$\begin{aligned} p_1 \mid n &\implies p_1 \mid q_1 \cdots q_s \\ &\implies p_1 \mid q_j \end{aligned}$$

for some  $j$ .

But since  $q_j$  is prime this implies that

$$q_j = p_1.$$

Let us re-number the  $q$ 's so that  $q_j$  becomes  $q_1$ . Then we have

$$n/p_1 = p_2 \cdots p_r = q_2 \cdots q_s.$$

Applying our inductive hypothesis we conclude that  $r = s$ , and the primes  $p_2, \dots, p_r$  and  $q_2, \dots, q_s$  are the same up to order.

The result follows.  $\square$

## 1.9 A postscript

Suppose  $\gcd(m, n) = 1$ . Then we have seen that we can find integers  $x_0, y_0$  such that

$$mx_0 + ny_0 = 1.$$

We can now give the general solution to this equation:

$$(x, y) = (x_0 + tn, y_0 - tm)$$

for  $t \in \mathbb{Z}$ .

Certainly this is a solution. To see that it is the general solution note that

$$\begin{aligned} mx + ny = d &\implies mx + ny = mx_0 + ny_0 \\ &\implies m(x - x_0) = n(y_0 - y). \end{aligned}$$

Now  $n$  has no factor in common with  $m$ , by hypothesis. Hence all its factors divide  $x - x_0$ , ie

$$\begin{aligned} n \mid x - x_0 &\implies x - x_0 = tn \\ &\implies x = x_0 + tn \\ &\implies y = y_0 - tm. \end{aligned}$$