

## 5. The Euclidean Algorithm

### Theorem 1 (the Euclidean Algorithm)

Suppose that  $a$  and  $b$  are integers with  $a \neq 0$ .

Define sequences  $\{q(i)\}$ ,  $\{r(i)\}$  of integers as follows :

$$r(0) = b, r(1) = a, q(0) = 0.$$

For  $n > 0$ , provided that  $r(n) \neq 0$ ,  $q(n)$  and  $r(n+1)$  are the unique integers with

$$r(n-1) = q(n)r(n) + r(n+1), \text{ and } 0 \leq r(n+1) < r(n)$$

If it ever happens that  $r(n) = 0$ , then  $q(i)$ ,  $i \geq n$ , and  $r(i)$ ,  $i > n$ , are undefined.

Then

- (1) there is a least positive integer  $N$  with  $r(N) = 0$ ,
- (2) with this value of  $N$ ,  $\gcd(a,b) = r(N-1)$ .

The proof is quite intricate. It is certainly NOT examinable. It may help in reading the proof to have an idea of the key steps before we start the formal proof.

Suppose we have got as far as defining  $r(n)$ , and that  $r(n) \neq 0$ .

Since we are given  $r(0)$  and  $r(1)$  at the start, we may assume  $n > 0$ , so that  $r(n-1)$  is defined.

As  $r(n) \neq 0$ , we can apply the Division Theorem to  $r(n)$  and  $r(n-1)$ . That result guarantees the existence of the integers  $q(n)$  and  $r(n+1)$ .

Thus we can define further  $r(n)$  unless we reach a situation where  $r(n) = 0$ .

To see the connection with greatest common divisors, we look at the equation  $r(n-1) = q(n)r(n) + r(n+1)$ . Theorem 2 allows us to deduce that

$$\gcd(r(n), r(n+1)) = \gcd(r(n-1), r(n)).$$

Thus, the value of  $\gcd(r(n), r(n+1))$  is unaltered as we move along the sequence.

For  $n = 0$ ,  $\gcd(r(n), r(n+1))$  is just  $\gcd(b, a)$ , which is the same as  $\gcd(a, b)$

### Proof

The existence of the  $q(n)$  and  $r(n+1)$  is guaranteed by the Division Theorem.

Also, the  $r(n)$  are strictly decreasing, since, provided  $r(n) \neq 0$ ,  $r(n+1) < r(n)$ .

Since a sequence of positive integers cannot decrease forever the values of  $r(n)$  must eventually reach 0.

We assume that this happens *first* for  $n = N$ . This shows that we actually get *finite* sequences  $\{q(i)\}, \{r(i)\}$ .

Applying Theorem 2 repeatedly to the equation  $r(n-1) = q(n)r(n) + r(n+1)$ , where we put  $n = 1, 2$ , and so on, we find that

$$\begin{aligned}
 \gcd(a,b) &= \gcd(a,r(2)) && \text{which is } \gcd(r(1), r(2)) \text{ as } a = r(1) \\
 &= \gcd(r(2),r(3)) && \text{on applying Theorem 2 to } \gcd(r(2), r(1)) \\
 &&& \text{(which is the same as } \gcd(r(1), r(2))) \\
 &= \gcd(r(3), r(4)) && \text{on applying Theorem 2 to } \gcd(r(3), r(2)) \\
 &&& \text{(which is the same as } \gcd(r(2), r(3))) \\
 &&& \vdots \\
 &&& \vdots \\
 &&& \text{And so on, until we reach the zero of } r \\
 &&& \vdots \\
 &&& \vdots \\
 &= \gcd(r(N-1),r(N)) \\
 &= \gcd(r(N-1),0) && \text{as } r(N) = 0 \\
 &= r(N-1) && \text{by the general result that } \gcd(a,0) = a
 \end{aligned}$$

**Example** Find  $\gcd(2765,4655)$ .

**Solution**

$$\begin{aligned}
 4655 &= 1.2765 + 1890 && (1) \\
 2765 &= 1.1890 + 875 && (2) \\
 1890 &= 2.875 + 140 && (3) \\
 875 &= 6.140 + 35 && (4) \\
 140 &= 4.35 + 0
 \end{aligned}$$

We have reached a zero remainder. By the Euclidean Algorithm, we have  $\gcd(2765,4655) = 35$ , the *last non-zero remainder*.

Corollary 1 Let  $a$  and  $b$  be integers, not both zero. There exist integers  $x, y$  with

$$ax + by = \gcd(a,b)$$

A formal proof uses complicated notation. Instead, we *outline* the proof, and illustrate the technique with examples.

In the proof of the Euclidean Algorithm, we derived  $r(n+1)$  from the equation

$$r(n-1) = q(n)r(n) + r(n+1).$$

For the corollary, we can work *backwards* through the Euclidean Algorithm calculation. We rearrange the above equation as

$$r(n+1) = q(n)r(n) - r(n-1)$$

Thus, we express  $r(N-1)$  in terms of earlier and earlier  $r(i)$  until we reach  $r(0), r(1)$ , i.e.  $a, b$ .

**Example** Express  $\gcd(2765, 4655)$  as a linear combination of 2765 and 4655.

**Solution** We use the calculation of the gcd given in the previous example.

35	= 875 – 6.140	Using line 4 to replace 35
	= 875 – 6(1890-2.875)	Using line 3 to replace 140
	= 13.875 – 6.1890	Tidying up
	= 13(2765-1890) – 6.1890	Using line 2 to replace 875
	= 13.2765 – 19.1890	Tidying up
	= 13.2765 – 19(4655-2765)	Using line 1 to replace 1890
	= 32.2765 – 19.4655	Tidying up

Thus we have  $35 = 23.2765 - 19.4665$ , a combination of 2765 and 4655.

It should be clear that this will work in general. We describe this process as *backtracking*, since we work *back* through the original calculation.

Some authors refer to our Corollary as “the Euclidean Algorithm”.

Clearly, our theorem and corollary will be used mainly in *numerical* examples, but they also have an important *theoretic* consequence.

**Corollary 2** Any common divisor of the integers  $a$  and  $b$  divides  $\gcd(a,b)$ .

**Proof**

Let  $d = \gcd(a,b)$ . From Corollary 1, there exist *integers*  $x, y$  with  $ax + by = d$ .

Now suppose that  $e$  is a common divisor of  $a$  and  $b$ .

Then  $e$  divides any linear combination of  $a$  and  $b$ . In particular,  $e$  divides  $ax+by$ .

As  $ax+by = d$ , we have shown that  $e$  divides  $d = \gcd(a,b)$ .

This allows us to identify the common divisors of two integers as the divisors of their greatest common divisor.

For example, we found that  $\gcd(2765,4655) = 35$ . Thus the common divisors of the integers 2765 and 4655 are precisely the divisors of 35. By trial and error, these are  $\pm 1$ ,  $\pm 5$ ,  $\pm 7$  and  $\pm 35$ .

A very important consequence of Corollary 1 dates back to Euclid (~300BC).

**Theorem 2 (Euclid's Lemma)**

If  $a, b, c$  are integers with  $\gcd(a,b) = 1$  and  $a \mid bc$ , then  $a \mid c$ .

**Proof**

As  $\gcd(a,b) = 1$ , there are integers  $x, y$  with  $ax + by = 1$ .

As  $a \mid bc$ , there is an integer  $d$  with  $bc = ad$ .

Multiplying this by  $c$ , we get

$$c = c(ax + by) = acx + bcy = acx + a(dy) = a(cx+dy).$$

Thus, as  $a$  is a factor of the right hand side, it is a factor of the left hand side, so that  $a \mid c$ .

Theorem 3 includes the condition that  $\gcd(a,b) = 1$ . This is *vital*. If this does *not* hold, then we may *not* have  $a \mid c$ .

As an example, put  $a = 4, b = 6, c = 10$ . Then we certainly have  $a \mid bc$  since we see that  $4 \mid 6 \cdot 10 = 60$ . But it is not true that  $a \mid c$  since 4 does not divide 10. Note that here  $\gcd(a,b) = \gcd(4,6) = 2$ , not 1.

Another application of Corollary 1 tells us when the square root of an integer is a rational number.

**Theorem 3** Let  $N \in \mathbf{N}$ . Then  $\sqrt{N} \in \mathbf{Q} \Leftrightarrow \sqrt{N} \in \mathbf{N}$ .

**Proof (examinable)**

The  $\Leftarrow$  part is trivial. If a number is in  $\mathbf{N}$ , then it is certainly in  $\mathbf{Q}$ .

Now for the  $\Rightarrow$  part.

We suppose that  $\sqrt{N} \in \mathbf{Q}$ . Then  $\sqrt{N} = a/b$  for some *integers*  $a$  and  $b$ .

We can assume that  $\gcd(a,b) = 1$  since, if they have a common factor other than  $\pm 1$ , we can cancel it from top and bottom.

By Corollary 2, there exist *integers*  $x, y$  with  $ax + by = 1$ .

Multiplying through by  $\sqrt{N}$ , we get the equation

$$(*) \quad a\sqrt{N}x + b\sqrt{N}y = \sqrt{N}.$$

Now  $\sqrt{N} = a/b$ , so  $a = \sqrt{N}b$ , and so  $a\sqrt{N} = bN$ . Substituting these into (\*), we get

$$bNx + ay = \sqrt{N}$$

But then the left hand side is clearly an integer, so the right hand side is also an integer, i.e.  $\sqrt{N} \in \mathbf{Z}$ . As  $\sqrt{N} > 0$ , we have  $\sqrt{N} \in \mathbf{N}$ , as required.

### Remark

This shows that, for  $N \in \mathbf{N}$ , either

- $N$  is a *perfect square*, i.e the square of an *integer*, or
- $\sqrt{N}$  is an *irrational* number, i.e. is in  $\mathbf{R}$ , but *not* in  $\mathbf{Q}$ .

If we can find an integer  $n$  with  $n^2 < N < (n+1)^2$ , then  $N$  is *not* a perfect square, and hence  $\sqrt{N}$  is irrational.

**Example** Show that  $\sqrt{2}$  is irrational.

### Solution

Observe that  $1^2 < 2 < (1+1)^2$ . Now apply the above remark with  $n = 1$ .

### Exercise

By choosing suitable values for  $n$ , show that  $\sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{7}, \sqrt{8}$  are all irrational.

The numbers  $\pm\sqrt{N}$  are the roots of the diophantine equation  $x^2 - N = 0$ . Then Theorem 2 may be restated as saying that any *rational* root must be *integral*. This can be extended to a wide range of diophantine equations. This extension uses a rather technical result.

**Lemma** If  $a, b$  are integers with  $\gcd(a,b) = 1$  and  $a \mid b^n$ , with  $n \in \mathbf{N}$ , then  $a = \pm 1$

**Proof**

As  $\gcd(a,b) = 1$ , there exist integers  $x, y$  with  $1 = ax + by$ . Then, taking the  $n^{\text{th}}$  power of each side and applying the Binomial Theorem, we get

$$1 = 1^n = (ax + by)^n = (ax)^n + {}_n C_1 (ax)^{n-1} (by) + \dots + {}_n C_{n-1} (ax) (by)^{n-1} + (by)^n,$$

where  ${}_n C_r$  is the *integer* giving the number of ways of choosing  $r$  objects out of  $n$ .

Now all but the last term on the right have an explicit factor  $a$ . The last is  $b^n y^n$ . We are given that  $a \mid b^n$ , so the last term also has a factor  $a$ .

Thus the entire right hand side has a factor  $a$ .  
i.e. the equation has the form  $1 = ka$  for some integer  $k$ .

It follows that  $a \mid 1$ , so  $a = \pm 1$ .

A polynomial  $f(x)$  is *monic* if the coefficient of the highest power of  $x$  is equal to 1.

**Theorem 4** Let  $f(x)$  be a monic polynomial with *integral* coefficients, and suppose that  $\alpha$  is a zero of  $f(x)$ , i.e.  $f(\alpha) = 0$ . Then

$$\alpha \in \mathbf{Q} \Leftrightarrow \alpha \in \mathbf{Z}$$

**Proof**

The  $\Leftarrow$  part is trivial as any integer is rational.

For the other direction, suppose that  $\alpha$  is rational. Now,  $\alpha$  is zero or non-zero.

If  $\alpha = 0$ ,  $\alpha$  is obviously in  $\mathbf{Z}$ .

If  $\alpha \neq 0$ , then we can write  $\alpha$  in the form  $p/q$ , with  $p, q \in \mathbf{Z}$ , and  $p \neq 0$  as  $\alpha \neq 0$ . As in an earlier proof (Theorem 3) we can assume that  $\gcd(p,q) = 1$ .

Now  $f(x)$  has the form  $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ . Replacing  $x$  with  $\alpha$ , we get

$$0 = f(\alpha) = f(p/q) = p^n/q^n + a_{n-1}p^{n-1}/q^{n-1} + \dots + a_1p/q + a_0$$

Multiplying through by  $q^n$ , we get the integral equation

$$0 = p^n + a_{n-1}p^{n-1}.q + \dots + a_1p.q^{n-1} + a_0q^n.$$

Clearly  $q$  divides all terms on the right after the first. It follows that  $q \mid p^n$ .

As  $\gcd(p,q) = 1$ , the Lemma applies to show that  $q = \pm 1$ .

Then  $\alpha = p/q = \pm p$ , i.e.  $\alpha$  is an integer.

**Example** If  $N, k \in \mathbf{N}$ , then  $N^{1/k}$  is irrational or  $N = m^k$  for an *integer*  $m$

**Solution**

The real number  $\alpha = N^{1/k}$  is a zero of the monic polynomial  $x^k - N$ .

Theorem 4 says that, if  $\alpha$  is rational, then it must be an integer.

Thus, either  $\alpha$  is irrational or  $\alpha = m$  for some *integer*  $m$ .

In the latter case  $N = \alpha^k = m^k$ .

**Example** If  $a, b \in \mathbf{N}$  and  $a^k \mid b^k$ , then  $a \mid b$ .

**Solution**

As  $a^k \mid b^k$ ,  $b^k = Na^k$ , for some  $N \in \mathbf{N}$ .

Thus,  $N^{1/k} = b/a \in \mathbf{Q}$ .

By the previous example,  $N^{1/k} = m \in \mathbf{N}$

Thus  $b/a = m$  so that  $b = ma$ , i.e.  $a \mid b$ .

## Additional examples

### Example

Express  $\gcd(407, 518)$  as a linear combination of 407 and 518.

### Solution

The Euclidean Algorithm

$$518 = 1 \cdot 407 + 111$$

$$407 = 3 \cdot 111 + 74$$

$$111 = 1 \cdot 74 + 37$$

$$74 = 2 \cdot 37 + 0$$

This column need not appear

$$(1) \quad 518 - 407 = 111$$

$$(2) \quad 3 \cdot 111 = 333, \quad 407 - 333 = 74$$

$$(3) \quad 111 - 74 = 37$$

$$(4)$$

Hence  $\gcd(407, 518) = 37$

Backtracking

$$37 = 111 - 1 \cdot 74 \quad (3)$$

$$= 111 - 1 \cdot (407 - 3 \cdot 111) \quad (2) \text{ says } 74 = 407 - 3 \cdot 111$$

$$= 4 \cdot 111 - 1 \cdot 407 \quad \text{tidy up}$$

$$= 4 \cdot (518 - 407) - 1 \cdot 407 \quad (1) \text{ says } 111 = 518 - 407$$

$$= 4 \cdot 518 - 5 \cdot 407 \quad \text{tidy up}$$

Hence  $37 = 407x + 518y$ , with  $x = -5$ ,  $y = 4$

We often use theorem 3 in the form

“if  $N$  is *not* the square of an integer, then  $\sqrt{N}$  is irrational.”

**Example** Show that, for  $n \in \mathbf{N}$ ,  $\sqrt{n(n+1)}$  is irrational.

**Solution** Observe that, for  $n \in \mathbf{N}$ ,  $n^2 < n^2 + n < n^2 + 2n + 1 = (n+1)^2$

Thus  $n(n+1)$  is *not* the square of an integer.

By Theorem 3,  $\sqrt{n(n+1)}$  is irrational.

**Exercise to reader** Show that, for  $n \in \mathbf{N}$ ,  $\sqrt{(n^2 + n+1)}$  is irrational.

**Example** Show that  $\sqrt{6}$  is irrational. Deduce that  $\sqrt{2} + \sqrt{3}$  is irrational.  
Hint. If  $q \in \mathbf{Q}$ , then  $q^2 \in \mathbf{Q}$ .

**Solution** Observe that  $2^2 = 4 < 6$ , and  $3^2 = 9 > 6$ .

Thus  $2 < \sqrt{6} < 3$ , so that  $\sqrt{6}$  is *not* an integer.

Then, by Theorem 3,  $\sqrt{6}$  is irrational.

[As is often the case with proofs of irrationality, we use contradiction]

Suppose that  $\sqrt{2} + \sqrt{3}$  is *rational*. Then  $\sqrt{2} + \sqrt{3} = m/n$  with  $m, n \in \mathbf{N}$ .

Then we get,  $m^2/n^2 = (\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{6} + 3 = 5 + 2\sqrt{6}$ .

Thus,  $2\sqrt{6} = m^2/n^2 - 5 = (m^2 - 5n^2)/n^2$

and so,  $\sqrt{6} = (m^2 - 5n^2)/2n^2$ , which is *rational*.

But, in the first part,  $\sqrt{6}$  is *irrational*

This contradiction shows that we must have  $\sqrt{2} + \sqrt{3}$  irrational.

## The Euclidean Algorithm is *fast*

In the proof of the Euclidean Algorithm for finding  $\gcd(a,b)$ , we saw that the process takes *at most*  $a$  steps. For *large* value of  $a$ , this would not be practical.

In fact, the process is *very much faster* than this suggests. This can be justified by looking at the effect on the remainders of *two* steps in the algorithm.

**Lemma** In the notation of the Euclidean Algorithm, for any  $n > 0$ ,

$$r(n+2) < \frac{1}{2} r(n).$$

### Proof

We know that the definition of the  $r(i)$  shows that  $0 \leq r(n+1) < r(n)$ .

We split the range in two, and prove our result in either case.

Case 1 :  $r(n+1) \leq \frac{1}{2} r(n)$ .

We know that  $r(n+2) < r(n+1)$ , so that  $r(n+2) < \frac{1}{2} r(n)$ , as required.

Case 2 :  $\frac{1}{2} r(n) < r(n+1) < r(n)$ .

Now consider the application of the Division Theorem to  $r(n+1)$  and  $r(n)$ , the next step of the algorithm. Note that, in this case  $r(n+1) < r(n) < 2 \cdot r(n+1)$ , so we *have* to choose  $q(n+1) = 1$ , and then  $r(n+2)$  is given by

$$r(n) = 1 \cdot r(n+1) + r(n+2).$$

Then  $r(n+2) = r(n) - r(n+1) < \frac{1}{2} r(n)$  since  $r(n+1) > \frac{1}{2} r(n)$ .

**Theorem 5** If the binary form of the integer  $a$  has  $d$  digits, then the determination of  $\gcd(a,b)$  requires at most  $2d$  steps.

### Proof

Recall that, as the binary form of  $a$  has  $d$  digits,  $a < 2^d$ .

After  $2d$  applications of the Lemma, we get  $r(2d+1) < (\frac{1}{2})^d \cdot a < 1$ .

But  $r(2d+1)$  is a non-negative integer, so  $r(2d+1) = 0$ .

In other words, the process *must* have halted after  $2d$  steps.

As an indication of how fast the algorithm really is, consider a case with  $a$  equal to one billion. Then  $d = 30$ , so the process takes at most 60 steps!