

# The Extended Euclidean Algorithm\*

## 1 The Euclidean Algorithm

Euclid's algorithm recovers the greatest common divisor of two numbers  $a, b$  that is, the largest  $x$  with the property that  $x|a$  and  $x|b$  (we write  $x = \gcd(a, b)$ ). Thus, anything that is true of divisors of  $a$  and  $b$  in general is true of their g.c.d in particular.

To this end, recall that if  $x|a$  and  $x|b$  then  $x|a \pm b$ . Further, if  $x|b$  then  $x|\lambda b$  for any  $\lambda \in \mathbb{Z}$ . Combining the two, we have that

$$x|a \text{ and } x|b \Rightarrow x|(a \pm \lambda b) \quad \forall \lambda \in \mathbb{Z} \quad (1)$$

How does this help us? Since  $\gcd(a, b) = \gcd(b, a)$ , we can assume w.l.o.g that  $a \geq b$ . Then by the quotient-remainder theorem, we can write  $a$  as

$$a = qb + r$$

for some integers  $q, r$  with  $0 \leq r < b$ . Rearranging gives us  $r = a - qb$ , so by (1) we have

$$x|a \text{ and } x|b \Rightarrow x|(a - qb) = r \quad (2)$$

So in particular

$$\gcd(a, b)|a \text{ and } \gcd(a, b)|b \Rightarrow \gcd(a, b)|r \quad (3)$$

So, to solve the question of finding  $\gcd(a, b)$ , we can instead solve the question of finding  $\gcd(b, r)$ . Notice that  $b \leq a$  and  $r < b$ , so this second question is easier.

---

\*G.Taylor, <http://maths.straylight.co.uk>

Repeating this process, the pairs of terms keep decreasing until eventually we have the question “find the g.c.d. of  $r$  and 0” for some  $r$ . But as anything divides 0,  $gcd(r, 0) = r$ . So there is always a final question; that question is easy to answer; and it’s answer is the same as the original g.c.d. we were looking for!

## 1.1 Worked example

Suppose then that we want to find the g.c.d. of 51 and 36. We first appeal to the quotient-remainder theorem:

$$51 = 36 + 15$$

Thus any divisor of 51 and 36 (including the greatest) is also a divisor of 15. So we turn our attention to the easier problem of the g.c.d. of 36 and 15. Again by quotient-remainder

$$36 = 2 \times 15 + 6$$

so it suffices to find  $gcd(15,6)$ . Noting that

$$15 = 2 \times 6 + 3$$

we discover that this is the same as the g.c.d. of 6 and 3. But

$$6 = 2 \times 3 + 0$$

so that’s simply  $gcd(3,0)=3$ . Thus we have

$$gcd(51, 36) = gcd(36, 15) = gcd(15, 6) = gcd(6, 3) = gcd(3, 0) = 3$$

## 2 The Extended Euclidean Algorithm

Typically, one tabulates their progress through the algorithm more compactly; using the previous example we have

$$51 = 36 + 15 \tag{4}$$

$$36 = 2 \times 15 + 6 \tag{5}$$

$$15 = 2 \times 6 + 3 \tag{6}$$

$$6 = 2 \times 3 + 0 \tag{7}$$

With such a representation, we can now tackle a related problem - given  $a, b$ , finding  $x, y$  such that

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

For our example, this means finding  $x, y$  with the property that  $51x + 36y = 3$ . Notice that we do not have an identity in terms of 3, 36 and 51 anywhere in the table. But from (6), we do have an identity for 3 in terms of 15 and 6:

$$3 = 15 - 2 \times 6$$

Then (5) tells us that

$$6 = 36 - 2 \times 15$$

so we can rewrite our result for 3 in terms of 36 and 15 instead of 15 and 6.

In this way, we can chain upwards through the table to an identity for 3 ultimately in terms of 51 and 36- this process is known as the extended euclidean algorithm. Whereas the Euclidean algorithm works down from  $a$  and  $b$ , through simpler and simpler terms to the g.c.d., so the extended version works up from that g.c.d. through increasingly complicated terms to an expression in terms of  $a$  and  $b$ .

For our example, this works as follows:

$$\begin{aligned} 3 &= 15 - 2 \times 6 && \text{by (6)} \\ &= 15 - 2 \times (36 - 2 \times 15) && \text{by (5)} \\ &= 5 \times 15 - 2 \times 36 && \text{(simplifying)} \\ &= 5 \times (51 - 36) - 2 \times 36 && \text{by (4)} \\ &= 5 \times 51 - 7 \times 36 && \text{(simplifying)} \end{aligned}$$

## 2.1 Linear Diophantine Equations

Why is all this useful? In number theory, the study of *Diophantine equations* concerns finding integer solutions to equations, where possible. Typically we seek to classify such equations based on whether we can find infinitely many such solutions, only finitely many, or none at all. The general question as to whether solutions exist is actually undecidable, but in various special cases we can say something.

Armed with the extended euclidean algorithm, we can tackle the case of *linear diophantine equations in two variables*:

For fixed  $a, b, c \in \mathbb{Z}$ , do there exist integer solutions  $x, y$  of  $ax + by = c$  ?

### 2.1.1 Existence

Suppose  $c = \lambda \gcd(a, b)$  for some  $\lambda \in \mathbb{Z}$ . Then, by the extended Euclidean algorithm we have  $x', y'$  with the property  $ax' + by' = \gcd(a, b)$ . So  $x = \lambda x'$ ,  $y = \lambda y'$  solve the linear diophantine equation, since

$$ax + by = a\lambda x' + b\lambda y' = \lambda(ax' + by') = \lambda \gcd(a, b) = c$$

Conversely, suppose  $c$  is not a multiple of  $\gcd(a, b)$ . Then, if the equation had solutions  $x, y$  then we'd have that  $\gcd(a, b) | a|x$  and  $\gcd(a, b) | b|y$  so  $\gcd(a, b) | ax + by = c$ , which is a contradiction.

Hence, the linear diophantine equation in two variables  $ax + by = c$  has integer solutions if and only if  $c$  is a multiple of  $\gcd(a, b)$ .

### 2.1.2 Number of Solutions

Assuming solutions exist, how many are there? Although the g.c.d. is unique, suitable pairs  $(x, y)$  with  $ax + by = \gcd(a, b)$  (and hence solutions to the linear diophantine equation) are not. To see this, consider one of the standard tricks of analysis, adding and subtracting the same thing:

$$ax + by = \lambda \gcd(a, b) \Rightarrow ax + by + ab - ab = \lambda \gcd(a, b) \Rightarrow a(x + b) + b(y - a) = \lambda \gcd(a, b)$$

That is, if  $(x, y)$  satisfy the equation, so do  $(x + b, y - a)$ . Which means we can apply the result again, giving  $(x + 2b, y - 2a)$ . These will always be pairs of integer solutions, and so the existence of just one pair  $(x, y)$  gives us an infinite family  $(x + ib, y - ia)$  of solutions.

Hence we conclude that the linear diophantine equation in two variables  $ax + by = c$  has infinitely many integer solutions if  $c$  is a multiple of  $\gcd(a, b)$ , and none otherwise.