

# Euclid's Algorithm

The Greatest Common Divisor(GCD) of two integers is defined as follows:

An integer  $c$  is called the GCD( $a,b$ ) (read as the greatest common divisor of integers  $a$  and  $b$ ) if the following 2 conditions hold:

- 1)  $c \mid a \wedge c \mid b$
- 2) For any common divisor  $d$  of  $a$  and  $b$ ,  $d \mid c$ .

Rule 2 ensures that the divisor  $c$  is the greatest of all the common divisors of  $a$  and  $b$ .

One way we could find the GCD of two integers is by trial and error. Another way is that we could prime factorize each integer, and from the prime factorization, see which factors are common between the two integers. However, both of these become very time consuming as soon as the integers are relatively large.

However, Euclid devised a fairly simple and efficient algorithm to determine the GCD of two integers. The algorithm basically makes use of the division algorithm repeatedly.

Let's say you are trying to find the GCD( $a,b$ ), where  $a$  and  $b$  are integers with  $a \geq b > 0$

**Euclid's algorithm says to write out the following:**

$$\mathbf{a = q_1b + r_1, \quad \text{where } 0 < r < b}$$

$$\mathbf{b = q_2r_1 + r_2, \quad \text{where } 0 < r_2 < r_1}$$

$$\mathbf{r_1 = q_3r_2 + r_3, \quad \text{where } 0 < r_3 < r_2}$$

•

•

$$\mathbf{r_i = q_{i+2}r_{i+1} + r_{i+2}, \quad \text{where } 0 < r_{i+2} < r_{i+1}}$$

•

•

$$\mathbf{r_{k-1} = q_{k+1}r_k}$$

**Euclid's algorithm says that the  $\text{GCD}(a,b) = r_k$**

**This might make more sense if we look at an example:**

**Consider computing  $\text{GCD}(125, 87)$**

$$\mathbf{125 = 1*87 + 38}$$

$$\mathbf{87 = 2*38 + 11}$$

$$\mathbf{38 = 3*11 + 5}$$

$$\mathbf{11 = 2*5 + 1}$$

$$\mathbf{5 = 5*1}$$

**Thus, we find that  $\text{GCD}(125,87) = 1$ .**

**Let's look at one more quickly,  $\text{GCD}(125, 20)$**

$$\mathbf{125 = 6*20 + 5}$$

$$\mathbf{20 = 4*5,}$$

**thus, the  $\text{GCD}(125,20) = 5$**

## Proof That Euclid's Algorithm Works

Now, we should prove that this algorithm really does always give us the GCD of the two numbers "passed to it". First I will show that the number the algorithm produces is indeed a divisor of  $a$  and  $b$ .

$$\begin{aligned} a &= q_1b + r_1, & \text{where } 0 < r_1 < b \\ b &= q_2r_1 + r_2, & \text{where } 0 < r_2 < r_1 \\ r_1 &= q_3r_2 + r_3, & \text{where } 0 < r_3 < r_2 \\ &\cdot \\ &\cdot \\ r_i &= q_{i+2}r_{i+1} + r_{i+2}, & \text{where } 0 < r_{i+2} < r_{i+1} \\ &\cdot \\ &\cdot \\ r_{k-1} &= q_{k+1}r_k \end{aligned}$$

From the last equation, we know that  $r_k \mid r_{k-1}$ . So, we know that we can express  $r_{k-1} = cr_k$ , where  $c$  is an integer. Now consider the previous equation:

$$r_{k-2} = q_k r_{k-1} + r_k = q_k c r_k + r_k = r_k(q_k c + 1)$$

Thus, we have that  $r_k \mid r_{k-2}$ .

In our equation previous to that one, we have:

$$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1}$$

From here , since  $r_k \mid r_{k-1}$  and  $r_k \mid r_{k-2}$ , using our rules of divisibility we have that  $r_k \mid r_{k-3}$ . As you can see, we can continue this process, considering each previous equation until we get to the last two, where we will find that  $r_k \mid a$  and  $r_k \mid b$ . Thus, we find that Euclid's algorithm indeed gives us a common factor of  $a$  and  $b$ .

Now, we have one more part to prove – and that is to show that the common divisor that Euclid's algorithm produces is the largest possible. This proof is going to look similar to the previous one, but it is different in that we will start by assuming that  $a$  and  $b$  have a common factor  $d$ , and then show that  $d \mid r_k$ .

Consider an arbitrary common factor  $d$  of  $a$  and  $b$ . If  $d$  is a common factor, we can rewrite  $a$  and  $b$  as follows:

$a = da'$       $b = db'$ , where  $d, a', b'$  are all positive integers.

Now, consider the first equation from Euclid's algorithm:

$$a = q_1b + r_1.$$

$$\begin{aligned} r_1 &= da' - q_1db' \text{ (Substitute for } a \text{ and } b, \text{ and solve for } r_1.) \\ &= d(a' - q_1b') \end{aligned}$$

Thus, we have that  $d \mid r_1$ .

Now, consider the second equation, and repeat the steps we did on the first, this time solving for  $r_2$ . (Note: We will let  $r_1 = dr_1'$ , where  $r_1'$  is an integer.)

$$b = q_2r_1 + r_2.$$

$$\begin{aligned} r_2 &= db' - q_2dr_1' \\ &= d(b' - q_2d) \end{aligned}$$

As you can see, we can continue this process through each of the equations until we hit the second to last one, where we will have:

$$r_{k-2} = q_k r_{k-1} + r_k$$

$$r_k = dr_{k-2}' - q_k dr_{k-1}' = d(r_{k-2}' - q_k r_{k-1}'),$$

thus,  $d \mid r_k$ .

But this says that any arbitrary common factor of  $a$  and  $b$  that we originally picked divides into  $r_k$ , the value that Euclid's algorithm produced. Since we know that  $r_k$  IS a common factor to both  $a$  and  $b$ , this shows that it must be the largest possible common factor, or the  $\text{GCD}(a,b)$ .

## Extended Euclidean Algorithm

One of the consequences of the Euclidean Algorithm is as follows:

Given integers  $a$  and  $b$ , there is always an integral solution to the equation

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

Furthermore, the Extended Euclidean Algorithm can be used to find values of  $x$  and  $y$  to satisfy the equation above. The algorithm will look similar to the proof in some manner.

Consider writing down the steps of Euclid's algorithm:

$$\begin{aligned} a &= q_1b + r_1, & \text{where } 0 < r_1 < b \\ b &= q_2r_1 + r_2, & \text{where } 0 < r_2 < r_1 \\ r_1 &= q_3r_2 + r_3, & \text{where } 0 < r_3 < r_2 \\ &\cdot \\ &\cdot \\ r_i &= q_{i+2}r_{i+1} + r_{i+2}, & \text{where } 0 < r_{i+2} < r_{i+1} \\ &\cdot \\ r_{k-2} &= q_k r_{k-1} + r_k, & \text{where } 0 < r_k < r_{k-1} \\ r_{k-1} &= q_{k+1} r_k \end{aligned}$$

Consider solving the second to last equation for  $r_k$ . You get

$$r_k = r_{k-2} - q_k r_{k-1}, \text{ or}$$

$$\gcd(a,b) = r_{k-2} - q_k r_{k-1}$$

Now, solve the previous equation for  $r_{k-1}$ :

$$r_{k-1} = r_{k-3} - q_{k-1} r_{k-2},$$

**and substitute this value into the previous derived equation:**

$$\begin{aligned}\gcd(a,b) &= r_{k-2} - q_k(r_{k-3} - q_{k-1}r_{k-2}) \\ \gcd(a,b) &= (1 + q_kq_{k-1})r_{k-2} - q_kr_{k-3}\end{aligned}$$

**Notice that now we have expressed  $\gcd(a,b)$  as a linear combination of  $r_{k-2}$  and  $r_{k-3}$ . Next we can substitute for  $r_{k-2}$  in terms of  $r_{k-3}$  and  $r_{k-4}$ , so that the  $\gcd(a,b)$  can be expressed as the linear combination of  $r_{k-3}$  and  $r_{k-4}$ . Eventually, by continuing this process,  $\gcd(a,b)$  will be expressed as a linear combination of  $a$  and  $b$  as desired.**

**This process will be much easier to see with examples:**

**Find integers  $x$  and  $y$  such that**

$$135x + 50y = 5.$$

**Use Euclid's Algorithm to compute  $\text{GCD}(135, 50)$ :**

$$\begin{aligned}135 &= 2*50 + 35 \\ 50 &= 1*35 + 15 \\ 35 &= 2*15 + 5 \\ 15 &= 3*5\end{aligned}$$

**Now, let's use the Extended Euclidean algorithm to solve the problem:**

$$5 = 35 - 2*15, \text{ from the second to last equation } 35 = 2*15 + 5.$$

**But, we have that**

$$15 = 50 - 35, \text{ from the third to last equation } 50 = 1*35 + 15.$$

**Now, substitute this value into the previously derived equation:**

$$5 = 35 - 2*(50 - 35)$$

$$5 = 3*35 - 2*50$$

**Now, finally use the first equation to determine an expression for 35 as a linear combination of 135 and 50:**

$$35 = 135 - 2*50.$$

**Plug this into our last equation:**

$$5 = 3*(135 - 2*50) - 2*50$$

$$5 = 3*135 - 8*50$$

**So, a set of solutions to the equation is  $x=3$ ,  $y=-8$ .**