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:

$a = q_1b + r_1$, where $0 < r < b$
$b = q_2r_1 + r_2$, where $0 < r_2 < r_1$
$r_1 = q_3r_2 + r_3$, where $0 < r_3 < r_2$
.
.
$r_i = q_{i+2}r_{i+1}+ r_{i+2}$, where $0 < r_{i+2} < r_{i+1}$
.
.
$r_{k-1} = q_{k+1}r_k$

Euclid's algorithm says that the GCD(a,b) = r_k

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

Consider computing GCD(125, 87)

125 = 1*87 + 38
87 = 2*38 + 11
38 = 3*11 + 5
11 = 2*5 + 1
5 = 5*1

Thus, we find that GCD(125,87) = 1.

Let’s look at one more quickly, GCD(125, 20)
125 = 6*20 + 5
20 = 4*5,

thus, the 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.

$a = q_1b + r_1,$ where $0 < r < b$
$b = q_2r_1 + r_2,$ where $0 < r_2 < r_1$
$r_1 = q_3r_2 + r_3,$ where $0 < r_3 < r_2$
.
.
$r_i = q_{i+2}r_{i+1}+ r_{i+2},$ where $0 < r_{i+2} < r_{i+1}$
.
.
$r_{k-1} = q_{k+1}r_k$

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:

$r_{k-2} = q_kr_{k-1}+ r_k = q_kcr_k, + r_k = r_k(q_kc + 1)$

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:

$a = q_1b + r_1$.
$r_1 = da' - q_1db'$ (Substitute for a and b, and solve for r_1.)
$\quad = d(a' - q_1b')$

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.)

$b = q_2r_1 + r_2$.

$r_2 = db' - q_2dr_1'$
$\quad = d(b' - q_2d)$

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:

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

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

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 is must be the largest possible common factor, or the 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:

$a = q_1b + r_1$, where $0 < r < b$
$b = q_2r_1 + r_2$, where $0 < r_2 < r_1$
$r_1 = q_3r_2 + r_3$, where $0 < r_3 < r_2$
.
.
$r_i = q_{i+2}r_{i+1} + r_{i+2}$, where $0 < r_{i+2} < r_{i+1}$
.
$r_{k-2} = q_kr_{k-1} + r_k$, where $0 < r_k < r_{k-1}$
$r_{k-1} = q_{k+1}r_k$

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

$r_k = r_{k-2} - q_kr_{k-1}$, or

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

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:

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

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 of r_{k-2} in terms of of r_{k-3} and r_{k-4}, so that the gcd(a,b) can be expressed as the linear combination of 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 GCD(135, 50):

135 = 2*50 + 35
50   = 1*35 + 15
35   = 2*15 + 5
15   = 3*5

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

5 = 35 - 2*15, from the second to last equation 35   = 2*15 + 5.

But, we have that
15 = 50 - 35, 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.

Solving Equations of the form ax + by = c

To find all integer solutions of an equation of the form ax+by = c where a, b and c are given integers, do the following:

1) Check if gcd(a,b) | c. If not, there are no solutions. This is because if gcd(a,b) evenly divides into the left-hand side of the equation, but not the right, it's impossible for the two sides to be equal.

2) Otherwise, run the Extended Euclidean algorithm with a and b, multiplying the whole equation through if necessary. Consider the solving the following equation:

135x + 50y = 35.

From our previous work, we know that

135(3) + 50(-8) = 5. Since 35 = 7x5, multiply the whole equation through by 7:

135(3)(7) + 50(-8)(7) = 5(7)
135(21) + 50(-56) = 35

Thus, a solution for (x,y) is (21, -56).

3) This will give you a base solution (x_0, y_0). Now, consider the following equation:

ax + by = 0
ax = -by

Dividing both sides by gcd(a,b), we obtain:

$$\frac{a}{\gcd(a,b)}x = -\frac{b}{\gcd(a,b)}y$$

The "smallest" satisfying ordered pair (x,y) to this equation is $(\frac{b}{\gcd(a,b)}, -\frac{a}{\gcd(a,b)})$

Now, we can represent all solutions as follows:

$$x = x_0 + \frac{b}{\gcd(a,b)}k, y = y_0 - \frac{a}{\gcd(a,b)}k, k \in Z$$

The key idea here is that adding and subtracting the given offsets from the initial solution don't change the value of ax+by at all, thereby creating another valid solution.

Problem: Determine all solutions to the equation 405x + 141y = 12.

Here is the Euclidean Algorithm run on 405 and 141:

405 = 2x141 + 123
141 = 1x123 + 18
123 = 6x18 + 15
18 = 1x15 + 3
15 = 5x3

Now, run the Extended Euclidean Algorithm as follows:

18 – 1x15 = 3
18 – 1x(123 – 6x18) = 3
18 – 1x123 + 6x18 = 3
7x18 – 1x123 = 3
7x(141 – 1x123) - 1x123 = 3
7x141 – 7x123 – 1x123 = 3
7x141 – 8x123 = 3
7x141 – 8x(405 – 2x141) = 3
7x141 – 8x405 + 16x141 = 3
23x141 – 8x405 = 3, now, multiply this through by 4:
92x141 – 32x405 = 12
So, x_0 *=-32 and* y_0 *= 92 is a solution to the original equation.*

Now, take

405x + 141y = 0
405x = -141y, now, just divide through by gcd(405, 141)
135x = -47y
So a solution is x=47, y=-135.

Using this, we can a complete solution to our original equation:

x = -32 + 47k, y = 92-135k, $k \in Z$*.*

Using the Extended Euclidean Algorithm to Solve for Modular Inverses

A modular inverse is defined as follows:

a^{-1} mod n is the value (in between 1 and n-1) such that

$a(a^{-1}) \equiv 1$ mod n

This only exists if gcd(a,n) = 1, which will be evident once we show the procedure for obtaining a^{-1} mod n.

Consider the following example:

Determine 14^{-1} mod 23

This means we must find some integer such that

$14x \equiv 1$ mod 23

This is equivalent to finding integers x and y such that

$14x + 23y = 1$.

Clearly, this can only be done if 14 and 23 do NOT share any common factors. If they don't then the previous algorithm shown can be used to solve for both x and y. (Of course, the only value we care about is x.) Here is the work:

23 = 1x14 + 9
14 = 1x9 + 5
9 = 1x5 + 4
5 = 1x4 + 1
4 = 4x1

5 – 1x4 = 1
5 – (9 – 5) = 1
2x5 – 9 = 1
2(14 – 9) – 9 = 1
2x14 – 3x9 = 1
2x14 – 3(23 – 14) = 1
5x14 – 3x23 = 1

It follows that $14^{-1} \equiv 5$ mod 23, since $14x5 \equiv 1$ mod 23.