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 <u>division algorithm repeatedly.</u>

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:

$a = q_1 b + r_1$, where $0 < r < b$
$b = q_2 r_1 + r_2$, where $0 < r_2 < r_1$
$r_1 = q_3 r_2 + r_3$, 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(270, 125)
270 = 2x125 + 20
125 = 6*20 + 5
20 = 4*5,

thus, the GCD(270,125) = 5

Proof That Euclid's Algorithm Works

Now, we should prove that this algorithm really does always give us the GCD of two positive integers, a and b. First, I will show that the number the algorithm produces is indeed a divisor of a and b.

$a = q_1 b + r_1$, where $0 < r < b$
$b = q_2 r_1 + r_2$, where $0 < r_2 < r_1$
$r_1 = q_3 r_2 + r_3$, 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:

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

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:

$a = q_1 b + r_1$.
$r_1 = da' - q_1 db'$ (Substitute for a and b, and solve for r_1.)
$= d(a' - q_1 b')$

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.)

$$b = q_2 r_1 + r_2.$$

$$r_2 = db' - q_2 dr_1'$$
$$= d(b' - q_2 d)$$

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 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

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

As we previously discussed, there are no integer solutions to $ax+by = c$, when c is not divisible by a common divisor of a and b.

Furthermore, the Extended Euclidean Algorithm can be used to find values of x and y to satisfy the equation above. We will then use a single solution for x and y to find all possible ordered pairs (x, y) that satisfy the equation. The algorithm will look similar to the proof in some manner.

Consider writing down the steps of Euclid's algorithm:

$a = q_1 b + r_1$, where $0 < r < b$
$b = q_2 r_1 + r_2$, where $0 < r_2 < r_1$
$r_1 = q_3 r_2 + r_3$, where $0 < r_3 < r_2$
.
.
$r_i = q_{i+2} r_{i+1} + r_{i+2}$, where $0 < r_{i+2} < r_{i+1}$
.
$r_{k-2} = q_k r_{k-1} + r_k$, 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

$r_k = r_{k-2} - q_k r_{k-1}$, **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:

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

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 one possible solution to the equation is x=3, y=-8.

A natural consequence of this work is Bezout's Theorem, which says that for positive integers a and b, if gcd(a, b) = 1, then there exist integers x and y such that ax + by = 1.

We will use this theorem to determine how to find <u>ALL</u> ordered pairs of the form (x, y) that satisfy the equation

ax + by = gcd(a, b).

Now, let's consider how we might get other possible solutions to our previous concrete example.

We have

3*135 – 8*50 = 5

Note that 135 and 50 have a common factor of 5, so

135 = 5*27 and 50 = 5*10

as we'll see in a future lecture, the we can obtain the least common multiple of both 135 and 50 by multiplying each by the unique prime factors that each doesn't have. Thus:

135*10 = (5*27)*10
50*27 = (5*10)*27

It's fairly obvious that these two expressions are equal.

Thus, if we were to add 1350 AND subtract 1350 from a quantity, it would be unchanged.

Specifically, if we know that:

3*135 – 8*50 = 5

Then it's also the case that:

(3 + 10)*135 – (8 + 27)*50 = 5

Let's see why:

(3 + 10)*135 – (8 + 27)*50 =
3*135 + 10*135 – 8*50 – 27*50 =

[3*135 – 8*50] + [10*135 – 27*50] =
5 + 0 =
5

Basically, if we have one solution to 135x + 50y = 5, then we can create another solution x' = x + 10, y' = y – 27, because adding 10 to x adds 1350 to the linear combination, while subtracting 27 from y subtracts 1350 from the linear combination, leaving its value unchanged.

A good question to ask is can we add a positive integer smaller than 10 to x and subtract a positive integer from y smaller than 27 to create a new solution that isn't described here?

In order for us to answer this question, we'll need to use the following lemma: if gcd(a, b) = 1 and a | bc, then a | c.

We will prove this lemma via Bezout's Theorem, which was previously stated.

Let a and b be positive integers with gcd(a, b) = 1 and a | bc. By Bezout's Theorem, there exist integers x and y such that

ax + by = 1

Multiply this through by c:
acx + (bc)y = c

Recall that we are given that a | bc. Therefore, there exists some integer d such that bc = ad. Substitute for ad for bc:

acx + ady = c
a(cx + dy) = c

Now, since c, x, d and y are integers, it follows that cx + dy is an integer and we can conclude that a | c, as desired.

Now, let's return to our problem at hand:

Let M be the integer we add to a solution for x and N be the integer we subtract from a corresponding solution to y, in the general case of ax + by = gcd(a, b)

Thus, we know

ax + by = c (for the time being c = gcd(a, b), but this proof doesn't rely on this fact)

we want to know the smallest positive integer value of M for which:

a(x+M) + b(y – N) = c

This infers that

aM – bN = 0
aM = bN

Thus, we want to know the smallest positive integer value M for which:

aM = bN

Let d = gcd(a, b). Divide this equation through by d:

$$\frac{aM}{d} = \frac{bN}{d}$$

Let a' = a/d and b' = b/d:

$$a'M = b'N$$

Recall that gcd(a', b') = 1 by definition (we divided out the gcd, so no further common factors remain).

Given this equation, it follows that b' | (a'M). Since gcd(a', b') = 1, we can conclude that b' | M. It follows that the smallest positive integer value M for which this equation is satisfiable is b' = $\frac{b}{gcd(a,b)}$, and the corresponding solution for N is a' = $\frac{a}{gcd(a,b)}$.

This means that if x and y are integer solutions to the equation

ax + by = c,

then the minimal second solution (x', y') with x' > x is

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

It follows that, if we find a single integer solution (x_0 , y_0) to the equation,

ax + by = c,

then we can express ALL solutions as follows:

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

Thus, for our original problem:

Find all integer solutions to 135x + 50y = 5, the answer is:

{(x, y) | $x = 3 + 10c, y = -8 - 27c, c \in Z$}

Thus, we've found all integer solutions to the equation ax + by = c, when $gcd(a,b) \nmid c$ and when $c = gcd(a,b)$. What about the situation where $gcd(a,b)|c \wedge c > gcd(a,b)$?

This is easier to handle than it looks. Let's modify our original example to be:

Find all integer solutions (x, y) to

135x + 50y = 35

Let's do all the work we did before to arrive at the solution x = 3, y=-8 for

135 x 3 + 50 x (-8) = 5

Since 35/5 = 7, let's just take the equation above and multiply it through by 7:

$$\mathbf{7 \times (135 \times 3) + 7 \times \big(50 \times (-8)\big) = 7 \times 5}$$

$$\mathbf{135 \times (7 \times 3) + 50 \times (-8 \times 7) = 35}$$

$$\mathbf{135 \times 21 \times +50 \times (-56) = 35}$$

It follows that a single solution to our new equation is x = 21, y = -56. We can easily tack on all solutions the same way as before:

{(x, y) | $\boldsymbol{x = 21 + 10c, y = -56 - 27c, c \in Z}$**}**

For aesthetic purposes, notice that if we plug in c = -2, we can obtain the alterative base solution x = 21 – 10(2) = 1 and y = -56 – 27(-2) = -2. Thus, we can express this same solution as:

{(x, y) | $\boldsymbol{x = 1 + 10c, y = -2 - 27c, c \in Z}$**}**

One final note: since we are plugging in all integers for c in the solution set, we don't have to put a plus sign for the additive factor for x, we can equivalently express this solution as:

{(x, y) | $x = 1 - 10c, y = -2 + 27c, c \in Z$**}**

Notice though, that the signs must be opposite, if the sign for 10 changes to a minus, then the sign for 27c must be a plus.

Modular Inverses

One final note. If gcd(a, b) = 1, then we define b^{-1} mod a to be the value modulo a such that $b \times b^{-1} \equiv 1 \ (mod\ a)$. There is exactly one such value in the range [0, a – 1] that satisfies this criterion. To find a modular inverse, we can simply use the Extended Euclidean Algorithm.

Let's say that we've used the EEA to find that one integer solution to

135x + 98y = 1 is x = -45 and y = 62. Thus,
135(-45) + 98(62) = 1

Consider this equation mod 135:

$$135(-45) + 98(62) \equiv 1 \ (mod\ 135)$$
$$(0) \times (-45) + 98(62) \equiv 1 \ (mod\ 135)$$
$$98(62) \equiv 1 \ (mod\ 135)$$

We typically say $98^{-1} \equiv 62 \ (mod\ 135)$.

Modular inverses are important when we are solving equations of the form:

$$98x \equiv 53 \ (mod 135)$$

We can't divide both sides of this equation by 98 to solve for x, but what we can do is multiply both sides by 62, 98's modular inverse mod 135:

$$62(98x) \equiv 62(53) \ (mod 135)$$
$$x \equiv 3286 \ \equiv 46 \ (mod 135)$$

Thus, we were able to solve for x because we were able to find the modular inverse of 98 mod 135 via the Extended Euclidean Algorithm.