**The Euclidean Algorithm**

Recall that the Greatest Common Divisor (GCD) of two integers A and B is the **largest integer that divides both A and B**.

The **Euclidean Algorithm** is a technique for quickly finding the **GCD** of two integers.

The Algorithm

The Euclidean Algorithm for finding GCD(A,B) is as follows:

* If A = 0 then GCD(A,B)=B, since the GCD(0,B)=B, and we can stop.
* If B = 0 then GCD(A,B)=A, since the GCD(A,0)=A, and we can stop.
* Write A in quotient remainder form (A = B⋅Q + R)
* Find GCD(B,R) using the Euclidean Algorithm since GCD(A,B) = GCD(B,R)

Example:

Find the GCD of 270 and 192

* A=270, B=192
* A ≠0
* B ≠0
* Use long division to find that 270/192 = 1 with a remainder of 78. We can write this as: 270 = 192 \* 1 +78
* Find GCD(192,78), since GCD(270,192)=GCD(192,78)

    A=192, B=78

* A ≠0
* B ≠0
* Use long division to find that 192/78 = 2 with a remainder of 36. We can write this as:
* 192 = 78 \* 2 + 36
* Find GCD(78,36), since GCD(192,78)=GCD(78,36)

    A=78, B=36

* A ≠0
* B ≠0
* Use long division to find that 78/36 = 2 with a remainder of 6. We can write this as:
* 78 = 36 \* 2 + 6
* Find GCD(36,6), since GCD(78,36)=GCD(36,6)

    A=36, B=6

* A ≠0
* B ≠0
* Use long division to find that 36/6 = 6 with a remainder of 0. We can write this as:
* 36 = 6 \* 6 + 0
* Find GCD(6,0), since GCD(36,6)=GCD(6,0)

A=6, B=0

* A ≠0
* B =0, GCD(6,0)=6

**So we have shown:**

GCD(270,192) = GCD(192,78) = GCD(78,36) = GCD(36,6) = GCD(6,0) = 6

**GCD(270,192) = 6**

Understanding the Euclidean Algorithm

If we examine the Euclidean Algorithm we can see that it makes use of the following properties:

* GCD(A,0) = A
* GCD(0,B) = B
* **If A = B⋅Q + R and B≠0 then GCD(A,B) = GCD(B,R)**where Q is an integer, R is an integer between 0 and B-1

The first two properties let us find the GCD if either number is 0. The third property lets us take a larger, more difficult to solve problem, and **reduce it to a smaller, easier to solve problem**.

The Euclidean Algorithm makes use of these properties by rapidly reducing the problem into easier and easier problems, using the third property,  until it is easily solved by using one of the first two properties.

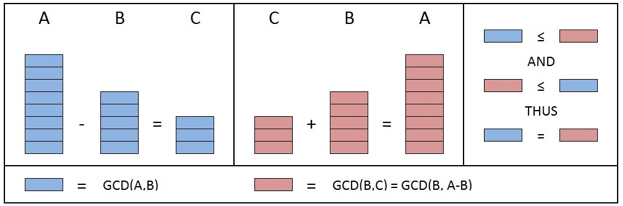
We can understand why these properties work by proving them.

We can prove that GCD(A,0)=A is as follows:

* The largest integer that can evenly divide A is A.
* All integers evenly divide 0, since for any integer, C, we can write C ⋅ 0 = 0. So we can conclude that A must evenly divide 0.
* The greatest number that divides both A and 0 is A.

The proof for **GCD(0,B)=B** is similar. (Same proof, but we replace A with B).

To prove that **GCD(A,B)=GCD(B,R)** we first need to show that **GCD(A,B)=GCD(B,A-B)**.

Suppose we have three integers **A,B** and **C** such that **A-B=C**.

**Proof that the GCD(A,B) evenly divides C**

The GCD(A,B), by definition, evenly divides A. As a result, A must be some multiple of GCD(A,B). i.e. X⋅GCD(A,B)=A where X is some integer

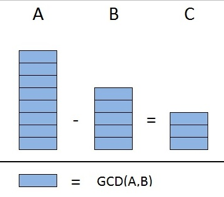
The GCD(A,B), by definition, evenly divides B. As a result,  B must be some multiple of GCD(A,B). i.e. Y⋅GCD(A,B)=B where Y is some integer

A-B=C gives us:

* X⋅GCD(A,B) - Y⋅GCD(A,B) = C
* (X - Y)⋅GCD(A,B) = C

So we can see that GCD(A,B) evenly divides C.

An illustration of this proof  is shown in the left portion of the figure below:

**Proof that the GCD(B,C) evenly divides A**

The GCD(B,C), by definition, evenly divides B. As a result, B must be some multiple of GCD(B,C). i.e. M⋅GCD(B,C)=B where M is some integer

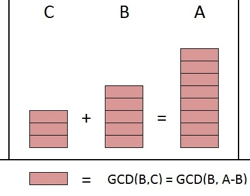
The GCD(B,C), by definition, evenly divides C. As a result,  C must be some multiple of GCD(B,C). i.e. N⋅GCD(B,C)=C where N is some integer

A-B=C gives us:

* B+C=A
* M⋅GCD(B,C) + N⋅GCD(B,C) = A
* (M + N)⋅GCD(B,C) = A

So we can see that GCD(B,C) evenly divides A.

An illustration of this proof  is shown in the figure below

**Proof that GCD(A,B)=GCD(A,A-B)**

* GCD(A,B) by definition, evenly divides B.
* We proved that GCD(A,B) evenly divides C.
* Since the GCD(A,B) divides both B and C evenly it is a common divisor of B and C.

**GCD(A,B) must be less than or equal to, GCD(B,C), because GCD(B,C) is the “greatest” common divisor of B and C.**

* GCD(B,C) by definition, evenly divides B.
* We proved that GCD(B,C) evenly divides A.
* Since the GCD(B,C) divides both A and B evenly it is a common divisor of A and B.

GCD(B,C) must be less than or equal to, GCD(A,B), because GCD(A,B) is the **“greatest”**common divisor of A and B.

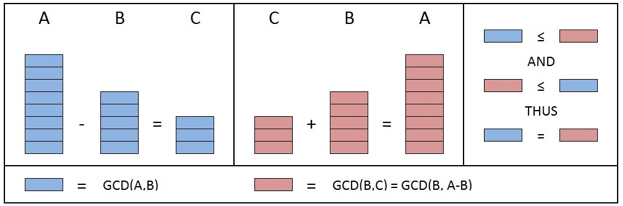
Given that GCD(A,B)≤GCD(B,C) and GCD(B,C)≤GCD(A,B) we can conclude that:

**GCD(A,B)=GCD(B,C)**

Which is equivalent to:

**GCD(A,B)=GCD(B,A-B)**

An illustration of this proof  is shown in the right portion of the figure below.

**Proof that GCD(A,B) = GCD(B,R)**

We proved that GCD(A,B)=GCD(B,A-B)

The order of the terms does not matter so we can say GCD(A,B)=GCD(A-B,B)

We can repeatedly apply GCD(A,B)=GCD(A-B,B) to obtain:

GCD(A,B)=GCD(A-B,B)=GCD(A-2B,B)=GCD(A-3B,B)=...=GCD(A-Q⋅B,B)

But A= B⋅Q + R so  A-Q⋅B=R

Thus **GCD(A,B)=GCD(R,B)**

The order of terms does not matter, thus:

**GCD(A,B)=GCD(B,R)**

In the next article we will show how we can extend the Euclidean Algorithm to find modular inverses.