GCD and Inverses
Exposition by William Gasarch

How to find the GCD or two numbers.

I give an example:

GCD(270,192)

$270 = 192 \times 1 + 78$

$192 = 78 \times 2 + 36$

$78 = 36 \times 2 + 6$

$36 = 6 \times 6 + 0$

OKAY, so that means that the answer is 6.

But it means MORE than that! Take the second to last line:

$6 = 78 - 36 \times 2$

I CAN write 78 as a combo of 270 and 192

I CAN write 36 as a combo of 192 and 78. I CAN THEN write 78 as a combo of 270 and 192.

POINT: After all of this I can get 6 (the GCD) as a combo of 192 and 270. I will do that NOW:

$6 = 78 - 36 \times 2$

$6 = (270 - 192) - (192 - 78 \times 2) \times 2$

$6 = 270 - 192 - 2 \times 192 + 4 \times 78$

$6 = 270 - 3 \times 192 + 4 \times 78$

$6 = 270 - 3 \times 192 + 4 \times (270 - 192)$

$6 = 270 - 3 \times 192 + 4 \times 270 - 4 \times 192$

$$6 = 5 \times 270 - 7 \times 192$$

Does this help us find inverses. NO. But lets do an example where it does! It will be when the GCD is 1.

GCD(270,193)
$270 = 193 \times 1 + 77$
$193 = 77 \times 2 + 39$
$77 = 39 \times 1 + 38$
$39 = 38 \times 1 + 1$
$38 = 1 \times 38 + 0$
OKAY, so that means that the answer is 1. it means MORE than that! Look at
$1 = 39 - 38$
We write 39 and 38 as combos of prior element and eventually get back to 193 and 270.
$1 = 39 - 38$
$1 = (193 - 77 \times 2) - (77 - 39)$
$1 = 193 - 77 \times 2 - 77 + 39$
$1 = 193 - 77 \times 3 + 39$
$1 = 193 - 77 \times 3 + (193 - 77 \times 2)$
$1 = 193 - 77 \times 3 + 193 - 77 \times 2$
$1 = 193 \times 2 - 77 \times 5$
$1 = 193 \times 2 - (270 - 193) \times 5$
$1 = 193 \times 7 - 5 \times 270$

$$1 = 193 \times 7 - 5 \times 270$$

If I want to find the INVERSE of 193 mod 270, take this equation MOD 270

$$1 \equiv 193 \times 7 - 5 \times 270 \pmod{270}$$

$$1 \equiv 193 \times 7 \pmod{270}$$

GREAT- the inverse of 193 is 7 mod 270.

If I want to find the INVERSE of 270 mod 193 then. NO! WAIT- when dealing mod 193 there is no 270. $270 \equiv 77 \pmod{1}93$.

OKAY- I want to find the inverse of 77 mod 193. Take the equation above mod 193

$$1 \equiv 193 \times 7 - 5 \times 270 \pmod{193}$$

Two things of interest happen: the 193-terms term is 0 and the 270-term is -5×77. So we have

$$1 \equiv -5 \times 77 \equiv 193$$

So -5 is the inverse of 88 mod 193. NO WAIT. We need to find -5 mod 193, which is $193 - 5 = 188$
So the inverse of 88 mod 193 is 188.