Euclidean Algorithm

Algorith to compute $\gcd(a,b)$. ← two numbers

GCD: Greatest comon divisor

Def:
let a, b be integers so that not both a and b are zero.
The $GCD(a,b)$ is an integer g so that
(i) $g|a$ and $g|b$, and
(ii) for all integers d, if $d|a$ and $d|b$ the $d \le g$.

GCD of 0 & 0 doesn't exist

Lemma: The euclidian algorithm uses:
if $a = bq + r$ then $\gcd(a,b) = \gcd(b,r)$

true statement with a proof

Example:

Find $GCD(321, 123)$ using the Euclidian Algorithm.

$321 = 2 \times 123 + 75$
a q b r

so by lemma ⇒ $GCD(321,123) = GCD(123,75)$

repeat

$123 = 1 \times 75 + 48$ $GCD(75,48)$
$75 = 1 \times 48 + 27$ $GCD(48,27)$
$48 = 1 \times 27 + 21$ $GCD(27,21)$
$27 = 1 \times 21 + 6$ $GCD(21,6)$
$21 = 3 \times 6 + \underline{3}$ $GCD(6,3)$
$6 = 2 \times 3 + 0$ $GCD(3,0) = 3$

Last non-zero remainder is the GCD

useful for next page

From the Euclidean algorithm we can see that
$\gcd(a,b) = xa + yb$ for some integers x and y.

Alternate Table Method

$$\overset{a}{321} = 2 \times \overset{b}{123} + 75$$

	a	b
321	1	0
123	0	1
75	1	-2
48	-1	3
27	2	-5
21	-3	8
6	5	-13
3	-18	47

$$
\begin{aligned}
3 &= 21 - (3 \times 6) \\
&= 21 - 3(27 - 21) \\
&= 4(21) - 3(27) \\
&= 4(48 - 27) - 3 \times 27 \\
&= 4(48) - 7(27) \\
&= 4(48) - 7(75 - 48) \\
&= 11(48) - 7(75) \\
&= 11(123 - 75) - 7(75) \\
&= 11(123) - 18(75) \\
&= 11(123) - 18(321 - 2 \times 123) \\
&= 47(123) - 18(321)
\end{aligned}
$$

So $x = -18$

$\therefore$ $y = 47$