Euclid's Algorithm

Euclid's algorithm for finding $\gcd(x,y)$:

Initialization: Set $a = \max\{|x|,|y|\}$ and $b = \min\{|x|,|y|\}$.

Iterative step: While $b > 0$:

1) We divide a by b and let r be the remainder.
2) Set $a = b$ and $b = r$.

Output: When $b = 0$, we output a.

Example: If $x = 42$ and $y = 30$, then

$a = 42$, $b = 30$

$42 = 1 \cdot 30 + 12$

$a = 30$, $b = 12$

$30 = 2 \cdot 12 + 6$

$a = 12$, $b = 6$

$12 = 2 \cdot 6 + 0$

$a = 6$, $b = 0$.

Output $a = 6$.

$\gcd(42, 30) = 6$

Extended Euclid's Algorithm

When applying Euclid's algorithm, we can also keep track of what a and b are in terms of x and y. This allows us to find $\gcd(x,y)$ in terms of x and y.

Example: If $x=19$ and $y=7$ then

$a=19, \quad b=7$	$a=x \quad b=y$
$19=2\cdot 7+5 \quad r=5$	$r=a-2b=x-2y$
$a=7 \quad b=5$	$a=y \quad b=x-2y$
$7=1\cdot 5+2 \quad r=2$	$r=a-b=3y-x$
$a=5 \quad b=2$	$a=x-2y \quad b=3y-x$
$5=2\cdot 2+1 \quad r=1$	$r=a-2b=(x-2y)-2(3y-x)$ $=3x-8y$
$a=2 \quad b=1$	$a=3y-x \quad b=3x-8y$
$2=2\cdot 1+0 \quad r=0$	$r=a-2b=3y-x-2(3x-8y)=19y-7x$
$a=1=3x-8y \quad b=0=19y-7x$	
$\gcd(x,y)=1=3x-8y$	