Greatest Common Divisors

Definition: Given two integers x and y which are not both 0, the *greatest common divisor* of x and y (which we write as $\gcd(x,y)$) is the largest element of $\mathrm{Div}(x) \cap \mathrm{Div}(y)$.

In other words, $\gcd(x,y)$ is the largest d such that $d|x$ and $d|y$.

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

$\mathrm{Div}(42) = \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}$

$\mathrm{Div}(30) = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}$

$\mathrm{Div}(42) \cap \mathrm{Div}(30) = \{\pm 1, \pm 2, \pm 3, \pm 6\} = \mathrm{Div}(6)$

$\gcd(42,30) = 6$

Greatest Common Divisors

Today:

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

2) For all integers x and y which are not both 0,
   a) $Div(x) \cap Div(y) = Div(\gcd(x,y))$
   b) Bézout's Identity: $\exists a,b \in \mathbb{Z} (\gcd(x,y) = ax+by)$

3) Finding $\gcd(x,y)$ from the prime factorizations of x and y.