

Section 35 - GCDs

Def: Let $a, b \in \mathbb{Z}$. If $d \in \mathbb{Z}$ such that $d \mid a$ and $d \mid b$, then d is called a *common divisor* of a and b . The greatest of all such common divisors is called the *greatest common divisor* of a and b and is denoted by $\gcd(a, b)$.

Ex: Common divisors of 18 and 24 are $\pm 1, \pm 2, \pm 3, \pm 6$. So $\gcd(18, 24) = 6$.

Note: If $a \in \mathbb{Z}^+$ and $a \mid b$, then $\gcd(a, b) = a$.

Prop: If $a, b, c \in \mathbb{Z}$ and $a \bmod b = c$, then $\gcd(a, b) = \gcd(c, b)$. That is, the gcd of a and b is the same as the gcd of the remainder when a is divided by b and b .

Proof: Let $a, b, c \in \mathbb{Z}$ such that $a \bmod b = c$.
Then, $\exists q \in \mathbb{Z}$ with $a = qb + c$. Also, $c < b$.
For convenience, let $g = \gcd(a, b)$.
Then $g \mid a$ and $g \mid b$.
So $gj = a$ and $gk = b$ for some $j, k \in \mathbb{Z}$.
Thus, substituting into the equation above, $gj = qgk + c$.
So $c = g(j - qk)$ and $j - qk \in \mathbb{Z}$.
So $g \mid c$.
Thus g is a common divisor of c and b .
Suppose FSO, $\gcd(a, b) \neq \gcd(c, b)$.
Then, $\exists h > g$ so that $h \mid c$ and $h \mid b$.
Then, $hm = c$ and $hn = b$ for some $m, n \in \mathbb{Z}$.
Substituting again, we get $a = qhn + hm = h(qn + m)$ and $qn + m \in \mathbb{Z}$.
Thus $h \mid a$.
But this makes h a common divisor of a and b with $h > g$.
This is impossible because $g = \gcd(a, b)$.
 $\therefore \gcd(a, b) = \gcd(c, b)$

This gives us a useful way to compute gcds of large numbers.

Ex: Find $\gcd(2280, 171)$

$$\begin{aligned} 2280 &= (171)(13) + 57 \\ 171 &= (3)(57) + 0 \end{aligned}$$

So, $57 \mid 171$ and thus $\gcd(57, 171) = 57$.

Now, since $57 = 2280 \bmod 171$, we have $\gcd(2280, 171) = \gcd(57, 171)$ by the last proposition.

So $\gcd(2280, 171) = 57$.

This process is called Euclid's Division Algorithm.

To find $\gcd(a, b)$ where $a > b$.

- Step 1: Find $a \bmod b$.
- Step 2: If $a \bmod b = 0$ then $\gcd(a, b) = b$. Stop.
- Step 3: Let $c = a \bmod b$.
- Step 4: Go back to Step 1 with b in place of a and c in place of b .

Ex: Find $\gcd(180, 108)$

$$180 = (1)(108) + 72$$

$$108 = (1)(72) + 36$$

$$72 = (2)(36) + 0$$

$$\text{So } \gcd(180, 108) = 36$$

Def: Let $a, b \in \mathbb{Z}$. If $\gcd(a, b) = 1$ then a and b are called *relatively prime*.

Ex: 8 and 9 are relatively prime.

Homework: Section 35, P. 307 #1,9(a,b,c - just convince yourself, do not prove),10,11