

Section 35 - gcd theorem

The gcd Theorem: Let $a, b \in \mathbb{Z}$, with at least one of them not zero. Then $\gcd(a, b)$ = the smallest positive integer of the form $ax + by$ with $x, y \in \mathbb{Z}$.

Rather than prove this formally, we show how finding x and y can be done with Euclid's algorithm. Since the procedure illustrated here can always be done (assuming one has already proved Euclid's Algorithm), this procedure is proof of the theorem.

Recall how we found $\gcd(48, 18)$

$$48 = 18 * 2 + 12$$

$$18 = 12 * 1 + 6$$

$$12 = 6 * 2 + 0$$

$$\text{So } \gcd(48, 18) = 6.$$

$$12 = 48 - 18 * 2$$

$$6 = 18 - 12 * 1 = 18 - (48 - 18 * 2) = 18 * 3 - 48$$

$$\text{So } 6 = 18 * 3 + 48 * -1$$

Corollary: $\exists x, y \in \mathbb{Z}$ with $ax + by = 1$ iff a, b are relatively prime.

Proposition: Every common divisor of a and b divides $\gcd(a, b)$.

Proof: $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$. If a, b have a common divisor, it will divide $ax + by$ and hence divide $\gcd(a, b)$.

#13. Let a, b be relatively prime and let $a \mid c$ and $b \mid c$.

$\exists x, y \in \mathbb{Z}$ with $ax + by = 1$.

Also, $c = am$ and $c = bn$ for some $m, n \in \mathbb{Z}$.

$c = cax + cby = bnax + amby = (ab)(nx + my)$ and $nx + my \in \mathbb{Z}$.

$ab \mid c$.

Homework: Section 35, P. 307 #2,14-16,18,19