# Divisibility

**Def:** For integers $a$ and $b$, we say $a \mid b$ ($a$ divides $b$) if there is some $k \in \mathbb{Z}$ w/ $b = ak$.

Some basic properties of divisibility:

- $a \mid b$ and $b \mid c \Rightarrow a \mid c$
- $a \mid a$
- $a \mid b$ and $b \mid a \Rightarrow a = \pm b$

- $a \mid b$ and $a \mid c \Rightarrow$

  $a \mid bx + cy$ for any $x, y \in \mathbb{Z}$

**Def:** The greatest common divisor of $a$ and $b$ written $\gcd(a,b)$ or $(a,b)$ is the largest integer $d$ such that $d|a$ and $d|b$.

Why does this integer exist?
it will follow from the following lemma:

**lemma:** if $a|b$ (and $b \neq 0$) then $|a| \leq |b|$

**Proof:** If $a|b$, then $b = ak$

for some $k \in \mathbb{Z}$. So

$|b| = |ak| = |a| \cdot |k|$. Since

$a, b \neq 0$, then $|k| \geq 1$ so

$$|b| = |a| \cdot |k| \geq |a| \quad \square$$

In particular, this says an integer has finitely many divisors, so it's now clear that a gcd of two integers exist.

Rmk: if $(a,b) = 1$, we call $a$ and $b$ co-prime.

How to Compute the gcd of two integers?

- Compute via factoring
- Euclidean algorithm

In general, factoring is hard, so the first method is bad unless the integers are small!

Example: $a = 19088597$

$b = 39083$

$a = 11^2 \cdot 19^3 - 23$

$b = 11^2 \cdot 17 \cdot 19$

$\gcd(a,b) = 11^2 \cdot 19 = 2299$

## Euclidean Algorithm

The division algorithm:

For $a, b > 0$ there exist unique integers $q$ and $r$ with

$$a = bq + r$$

and $0 \leq r < b$.

Example: $a = 100$, $b = 13$

$$\begin{array}{r} 7 \\ 13\overline{)100} \\ -91 \\ \hline 9 \end{array}$$

$$100 = 13 \cdot 7 + 9$$

## Euclidean Algorithm:

Let $a, b > 0$. Repeatedly carry out division alg. as follows:

$$a = bq_1 + r_1 \qquad 0 \le r_1 < b$$

$$b = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3 \qquad 0 \le r_3 < r_2$$

$$\vdots$$

The sequence of integers $r_1, r_2, \ldots$ eventually hits 0 and the last non-zero remainder is the gcd of $a$ and $b$.

Note: the Euclidean Algorithm is very efficient even for large integers.

Example: With $a = 1908597$
$b = 39083$
as above

$$19088597 = 39083 \cdot 488 + 16093$$

$$39083 = 16093 \cdot 2 + 6897$$

$$16093 = 6897 \cdot 2 + \boxed{2299}$$

$$6897 = 2299 \cdot 3 + 0$$

So $\gcd(a,b) = 2299$.

Example: $a = 3997$

$b = 2947$

$$3997 = 2947 \cdot 1 + 1050$$

$$2947 = 1050 \cdot 2 + 847$$

$$1050 = 847 \cdot 1 + 203$$

$$847 = 203 \cdot 4 + 35$$

$$203 = 35 \cdot 5 + 28$$

$$35 = 28 \cdot 1 + \boxed{7}$$

$$28 = 7 \cdot 4 + 0$$

So $\gcd(a, b) = 7$.

Why is Euclidean Algorithm useful?

## Theorem (Bezout's lemma)

For non-zero integers $a, b$ there exist integers $x$ and $y$ such that

$$ax + by = \gcd(a, b).$$

i.e. $\gcd(a, b)$ is a linear combination of $a$ and $b$.

How to find the integers $x$ and $y$ in the above theorem? Run Euclidean Algorithm backwards!

Example: $a = 19088547$

$b = 39083$

We showed $(a,b) = 2299$.

The theorem says there are

$x, y$ such that $ax + by = 2299$.

$19088547 = 39083 \cdot 488 + 16093$

$39083 = 16093 \cdot 2 + 6897$

$16093 = 6897 \cdot 2 + \boxed{2299}$

$2299 = 16093 - 6897 \cdot 2$

$6897 = 39083 - 16093 \cdot 2$

$\Rightarrow$

$2299 = 16093 - (39083 - 16093 \cdot 2) \cdot 2$

$$= 16093 \cdot 5 - 39083 \cdot 2$$

$$16093 = 19088597 - 39083 \cdot 488$$

$\Rightarrow$

$$2299 = (19088597 - 39083 \cdot 488) \cdot 5 - 39083 \cdot 2$$

$$= 19088597 \cdot 5 - 39083 \cdot 2442$$

So $x = 5$

$y = -2442$

Is the solution unique?

No!

We've found one solution $(x_0, y_0)$ with $ax_0 + by_0 = 2299$.

$ax + by$

$$a(x_0 + t) + b(y_0 - s)$$

$$ax_0 + at + by_0 - bs$$

In particular, if $at = bs$,

this just equals

$$ax_0 + by_0 = 2299.$$

Can choose $t, s$ by finding least common multiple of $a$ and $b$.

$t = 17$

$s = 6303$

So another soln is

$(22, -10745)$.