# A little number theory: <u>Divisibility</u>

We'll assume that all numbers are integers $>0$ unless stated otherwise.

<u>Notation:</u> $a|b$ means that $a$ is a factor of $b$

<u>ie</u> $b = a \cdot k$ for some $k$.

$\gcd(a,b) = (a,b) = d$ if $d|a$ & $d|b$

and if $n|a$ & $n|b$,

then $n|d$.

↑ greatest common divisor of $a$ and $b$

How do we find the gcd?

The Euclidean Algorithm.

How does this work? We want to find

$\gcd(a,b)$, where $a<b$.

Divide $a$ into $b$ as far as it goes:

$b = pa + r$ where $p \geq 1$ and $0 \leq r < a$

Claim: if $d$ is a common divisor of $a$ and $b$, then $d$ is a divisor of $r$

proof: $d|a$ & $d|b$ means that $a = kd$ & $b = nd$,

so $r = b - pa = nd - p(kd) = (n-pk)d$,

so $d|r$. //

The idea is to repeat the process with $r$ & $a$, remembering that $r<a$.

0. $b = q_0 a + r_0$ where $q_0 > 0$, $r_0 \geq 0$ & $r_0 < a$.

if $r_0 > 0$,

- if $r_0 = 0$, then $b = q_0 a$ $\Rightarrow a|b$ & $a|a$, so $\gcd(a,b) = a$

1. $a = q_1 r_0 + r_1$ where $q_1 > 0$ & $r_1 \geq 0$ & $r_1 < r_0$

- if $r_1 = 0$, then $a = q_1 r_0$ so $r_0 | a$ & $r_0 | (q_0 a + r_0) = b$

and ~~any~~ common divisor of a & b must divide $b - q_0 a = r_0$, so $r_0 = \gcd(a,b)$.

if $r_1 > 0$,

2. $r_0 = q_2 r_1 + r_2$ s.t. $q_2 > 0$ & $r_2 \geq 0$ & $r_2 < r_1$

- if $r_2 = 0$, then $r_1 | r_0$, so $r_1 | (q_1 r_0 + r_1) = a$ & also $r_1 | (q_0 a + r_0) = b$

so $r_1$ is a common divisor of a & b and any common divisor must divide $r_0$ & also $r_1 = a - q r_0$ so $r_1$ is the gcd.

Repeat as long as $r_k > 0$.

| | | | | |
|---|---|---|---|---|
| 0. | $a, b$ | $b = q_0 a + r_0$ | $q_0 > 0$ | $a$ |
| 1. | $r_0, a$ | $a = q_1 r_0 + r_1$ | $q_1 > 0$ | $\vee$ $r_0$ |
| 2. | $r_1, r_0$ | $r_0 = q_2 r_1 + r_2$ | $q_2 > 0$ | $\vee$ $r_1$ |
| 3. | $r_2, r_1$ | $r_1 = q_3 r_2 + r_3$ | $q_3 > 0$ | $\vee$ $r_2$ $\vee$ |
| | $\vdots$ | $\vdots$ | | $\vdots$ |
| k. | $r_{k-1}, r_{k-2}$ | $r_{k-2} = q_k r_{k-1} + r_k$ | $q_k > 0$ | $\vee$ $r_k$ |
| | $\vdots$ | $\vdots$ | $\vdots$ | |

This process has to stop because ~~any~~ strictly decreasing sequence of positive integers has to be finite.

Once $q_k = 0$, you're done and $r_k = \gcd(a,b)$.

$\Rightarrow$ lets try this with $b = 1017$ and $a = 57$

- Divide $a$ into $b$ as far as it goes

$$\begin{array}{r} 17 \\ 57\overline{)1017} \\ -57\phantom{7} \\ \hline 447 \\ -399 \\ \hline 48 \end{array} \qquad \begin{array}{r} {}^{4}\phantom{7} \\ 57 \\ \times\ 7 \\ \hline 399 \end{array}$$

& $48 < 57$, so we stop

Thus $1017 = 17 \cdot 57 + 48$ $\quad (48 < 57)$

- Divide 48 into 57: $\begin{array}{r} 1 \\ 48\overline{)57} \\ -48 \\ \hline 9 \end{array}$

Thus $57 = 1 \cdot 48 + 9$

- Divide 9 into 48: $\begin{array}{r} 5 \\ 9\overline{)48} \\ -45 \\ \hline 3 \end{array}$

Thus $48 = 5 \cdot 9 + 3$

- Divide 3 into 9: ~~stop~~ $\begin{array}{r} 3 \\ 3\overline{)9} \\ -9 \\ \hline 0 \end{array}$

Thus $9 = 3 \cdot 3 + 0$

Hence the greatest common divisor of 1017 and 57 is

$3 = \gcd(1017, 57)$.