# Lecture 2 - Greatest common divisors and Euclid's algorithm 

## Number systems - $\mathbb{Z}$, the integers

$$\mathbb{Z} = \{\ldots, (-1)+(-1)+(-1), (-1)+(-1), -1, 0, 1, 1+1, 1+1+1, \ldots\}$$

with $(-1)+1=0$, $1+(-1)=0$, $0+1=1$, $0+(-1)=-1$,
$1+0=1$, $(-1)+0=-1$.

Let $d \in \mathbb{Z}$. The multiples of $d$ is

$$d\mathbb{Z} = \{\ldots (-d)+(-d)+(-d), (-d)+(-d), -d, 0, d, d+d, d+d+d, \ldots\}$$

Let $a, d \in \mathbb{Z}$. The integer $d$ divides $a$, $d \mid a$, if
$a \in d\mathbb{Z}$.

Let $x, m \in \mathbb{Z}$. The greatest common divisor of $x$ and $m$, $\gcd(x,m)$, is $d \in \mathbb{Z}_{>0}$ such that

(a) $d \mid x$ and $d \mid m$

(b) If $\ell \in \mathbb{Z}_{>0}$ and $\ell \mid x$ and $\ell \mid m$ then $\ell \mid d$.

Let $a, b \in \mathbb{Z}$. Define

$a < b$ if there exists $x \in \mathbb{Z}_{>0}$ such that $a + x = b$;

$a \leq b$ if $a < b$ or $a = b$.

**Theorem** (Euclidean algorithm) Let $a, b \in \mathbb{Z}$.
There exist unique $q, r \in \mathbb{Z}$ such that

(a) $a = bq + r$

(b) $0 \leq r < |b|$, where $|b| = \begin{cases} b, & \text{if } b \in \mathbb{Z}_{>0} \\ 0, & \text{if } b = 0 \\ -b, & \text{if } -b \in \mathbb{Z}_{>0} \end{cases}$

If (a) and (b) hold write $a = r \bmod b$

<u>Example</u> The $15^{th}$ row of the multiplication table for $\mathbb{Z}/36\mathbb{Z}$ is

| $\cdot$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 ... |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 15 | 30 | 9 | 24 | 3 | 18 | 33 | 12 | 27 | 6 | 21 | 36 | 15 | 30 | 9 | 24 | 3 | ... | |

Notice that

(a) $15 \cdot 10 = 150$ in $\mathbb{Z}$,

$150 = 4 \cdot 36 + 6$, and

$15 \cdot 10 = 6$ in $\mathbb{Z}/36\mathbb{Z}$.

(b) The numbers in row 15 of the mutiplication table for $\mathbb{Z}/36\mathbb{Z}$ are

$$3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36$$

(all multiples of 3 in $\mathbb{Z}/36\mathbb{Z}$)

(c) $3 = 15 \cdot 17 + 12(-7)$

<u>Theorem</u> Let $x, m \in \mathbb{Z}$.

There exists $\ell \in \mathbb{Z}_{>0}$ such that

$$\ell\mathbb{Z} = x\mathbb{Z} + m\mathbb{Z}.$$

<u>Theorem</u> Let $x, m \in \mathbb{Z}$.

Let $\ell \in \mathbb{Z}_{>0}$ such that $\ell\mathbb{Z} = x\mathbb{Z} + m\mathbb{Z}$

Let $d = \gcd(x, m)$

Then $d = \ell$.

<u>Theorem</u> (Euclidean algorithm). Let $a, b \in \mathbb{Z}$.
There exist unique $q, r \in \mathbb{Z}$ such that

(a) $a = bq + r$

(b) $0 \le r < |b|$, where $|b| = \begin{cases} b, & \text{if } b \in \mathbb{Z}_{>0} \\ 0, & \text{if } b = 0 \\ -b, & \text{if } -b \in \mathbb{Z}_{>0} \end{cases}$

<u>Proof</u> Assume $a, b \in \mathbb{Z}$

To show: (a) There exist $q, r \in \mathbb{Z}$ such that

(1) $a = bq + r$

(2) $0 \le r < |b|$

(b) $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \le r < |b|$ are unique.

(a) Let $bq$ = the smallest integer in $b\mathbb{Z}$ less than or equal to $a$ and $r = a - qb$

To show: (aa) $a = bq + r$

(ab) $0 \le r < |b|$.

(aa) Since $r = a - qb$ then $a = bq + r$.

(ab) Since $bq \le a$ and $b(q+1) > a$,

$0 \le a - bq$ and $b > a - bq$.

So $0 \le r$ and $b > r$.

(b) Assume $q_1, r_1 \in \mathbb{Z}$ and $a = bq_1 + r_1$ and $0 \le r_1 < |b|$ and assume $q_2, r_2 \in \mathbb{Z}$ and $a = bq_2 + r_2$ and $0 \le r_2 < |b|$.

To show: $q_1 = q_2$ and $r_1 = r_2$

Since $a - r_1 = bq_1$ and $0 \le r_1 < |b|$, $bq_1$ is the largest integer in $b\mathbb{Z}$ which is $\le a$.

Since $a - r_2 = bq_2$ and $0 \le r_2 < |b|$, $bq_2$ is the largest integer in $b\mathbb{Z}$ which is $\le a$.

So $bq_1 = bq_2$ and $q_1 = q_2$

So $r_1 = a - bq_1 = a - bq_2 = r_2$. //.

<u>Example</u> Using Euclids algorithm find

$$\gcd(1288, 1144)$$

Hodgson says:

If $a = bq + r$ with $0 \le r < |b|$ then

$$\gcd(a,b) = \gcd(b,r).$$

$1288 = 1144 + 144$

$1144 = \cancel{8 \cdot 144}\ 7 \cdot 144 + 136$

$144 = 136 + 8$

$136 = 17 \cdot 8 + 0.$

$9 \cdot 144 = 1296$

$8 \cdot 144 = 1152$

$7 \cdot 144 = 1008$

So

$$\begin{aligned} \gcd(1288, 144) &= \gcd(1144, 144) \\ &= \gcd(144, 136) \\ &= \gcd(136, 8) \\ &= \gcd(8, 0) = 8. \end{aligned}$$

Note:

$$\begin{aligned} 8 &= 144 - 136 \\ &= 144 - (1144 - 7 \cdot 144) = 8 \cdot 144 - 1144 \\ &= 8(1288 - 1144) - 1144 \\ &= 8 \cdot 1288 - 9 \cdot 1144 \end{aligned}$$

<u>Proposition</u> Let $x, m \in \mathbb{Z}_{>0}$ with $1 \le x \le m$.
There exists $l \in \mathbb{Z}_{>0}$ such that
$$l\mathbb{Z} = x\mathbb{Z} + m\mathbb{Z}.$$

<u>Proof</u> Let $l$ be minimal such that $l \in x\mathbb{Z} + m\mathbb{Z}$.

To show: $l\mathbb{Z} = x\mathbb{Z} + m\mathbb{Z}$

To show: (a) $l\mathbb{Z} \subseteq x\mathbb{Z} + m\mathbb{Z}$

(b) $x\mathbb{Z} + m\mathbb{Z} \subseteq l\mathbb{Z}$.

(a) Since $l \in x\mathbb{Z} + m\mathbb{Z}$,
$$l\mathbb{Z} \subseteq x\mathbb{Z} + m\mathbb{Z}$$

(b) Assume $y \in x\mathbb{Z} + m\mathbb{Z}$

To show: $y \in l\mathbb{Z}$.

Since $l$ is minimal $y \geq l$.

So $y = ql + r$ with $0 \le r < l$.

So $r = y - ql \in x\mathbb{Z} + m\mathbb{Z}$

So $r = 0$, since $l$ is minimal positive int. in $x\mathbb{Z} + m\mathbb{Z}$.

So $y = ql$.

So $y \in l\mathbb{Z}$.

So $l\mathbb{Z} = x\mathbb{Z} + m\mathbb{Z}$

<u>Proposition</u> Let $x, m \in \mathbb{Z}$.

Let $\ell \in \mathbb{Z}_{>0}$ such that $\ell\mathbb{Z} = x\mathbb{Z} + m\mathbb{Z}$.

Let $d = \gcd(x, m)$

Then $d = \ell$.

<u>Proof</u> Let $d = \gcd(x, m)$

Let $\ell \in \mathbb{Z}_{>0}$ such that $\ell\mathbb{Z} = x\mathbb{Z} + m\mathbb{Z}$.

To show: $\ell = d$.

To show: (a) $d \mid \ell$

(b) $\ell \mid d$.

(a) Since $x \in \ell\mathbb{Z}$, then $\ell \mid x$.

Since $m \in \ell\mathbb{Z}$, then $\ell \mid m$.

Since $d = \gcd(x, m)$, then $\ell \mid d$.

(b) Since $d \mid x$ and $d \mid m$, then $x \in d\mathbb{Z}$ and $m \in d\mathbb{Z}$.

So $x\mathbb{Z} + m\mathbb{Z} \subseteq d\mathbb{Z}$.

So $\ell\mathbb{Z} \subseteq d\mathbb{Z}$.

So $\ell \in d\mathbb{Z}$.

So $d \mid \ell$. //