Last time Theorem 1.5.3 For a finite set X every $\sigma \in Sym(X)$ can be written as a product of disjoint cycles, uniquely up to order of cycles.

- An integer a divides an integer b if $b = aq$ for some $q \in \mathbb{Z}$.
- We write $a | b$ if $b = aq$ for some $q \in \mathbb{Z}$

  $a \nmid b$ if $\nexists q \in \mathbb{Z}$ with $b = aq$.

Def An integer p is prime if

(i) $p \geq 2$

(ii) $(d | p$ and $d > 0) \Rightarrow d | p$ or $d = 1$.

Proposition 1.6.7. ("division algorithm") For any two integers a, d with $d \geq 1$ there are unique integers q, r with

(1) $a = d \cdot q + r$

(2) $0 \leq r < d$

q is called the quotient, r is the remainder.

To prove 1.6.7 we assume:

Well-ordering principle Every nonempty subset A of non negative integers has a smallest element: $\exists a_0 \in A$ so that

$$a_0 \leq a \quad \text{for all } a \in A.$$

(Aside Well-ordering principle is equivalent to the principle of mathematical induction. We probably won't prove this fact).

Proof of the division algorithm:

(existence) Let $A = \{a - td \mid t \in \mathbb{Z} \quad a - td \geq 0\}$

We'll show: $A \neq \emptyset$. Well-ordering then implies that A has a smallest element. Since $r \in A$, $r = a - qd \ldots$

Why is $A \neq \emptyset$? If $a \geq 0$, $a = a - 0 \cdot d \in A$, so $A \neq \emptyset$

if $a < 0$, $a - ad = a \cdot (1-d) \geq 0$ since $a<0$ and $d \geq 1$.

$\Rightarrow \quad a - a \cdot d \in A. \quad \Rightarrow \quad A \neq \emptyset.$

Now by well-ordering principle $\exists\, r = \min A$
$= \min \{ a - td \mid t \in \mathbb{Z},\ a-td \geq 0 \}.$

Then $r \geq 0$ and $r = a - q \cdot d$ for some $q \in \mathbb{Z}$

$\Rightarrow \quad a = q \cdot d + r.$

Remains to show: $r < d$.

Suppose not: $r \geq d$.

Then $0 \leq r - d = (a - q \cdot d) - d = a - (q+1)\, d$

$\Rightarrow r - d \in A$. Also, since $d > 0$, $r - d < r$.

This contradicts: $r = \min A$.

Conclusion: $r < d$.

(Uniqueness) Suppose $\exists\, q_1, q_2, r_1, r_2 \in \mathbb{Z}$ s.t.

$$\begin{cases} a = q_1 d + r_1 = q_2 d + r_2 \quad \text{and} \\ 0 \leq r_1, r_2 < d. \end{cases}$$

We want to show: $r_1 = r_2$, $q_1 = q_2$.

May assume $r_2 \leq r_1$. Then

$0 \leq r_1 - r_2 = (a - q_1 d) - (a - q_2 d) = (q_2 - q_1)\, d.$

Since $r_1, r_2 < d$, $r_1 - r_2 < d$.

$\Rightarrow \quad (q_2 - q_1)\, d < d$

Also $0 \leq (q_2 - q_1)\, d$. $\Rightarrow \quad 0 \leq q_2 - q_1 < 1$
(since $d > 0$)

Since $q_2 - q_1 \in \mathbb{Z}$, $q_2 - q_1 = 0$.

$\Rightarrow \quad r_1 - r_2 = (q_2 - q_1) d = 0$ as well

$\therefore \quad q_1 = q_2, \quad r_1 = r_2$

$\square$

Proposition 1.6.2 Let a, b, c, u, v be integers.

(a) if $uv = 1$ then either $u = 1 = v$ or $u = -1 = v$.

(b) if $a \mid b$ and $b \mid a$ then $a = \pm b$

(c) if $a \mid b$ and $b \mid c$ then $a \mid c$

(d) if $a \mid b$ and $a \mid c$ then $a \mid (sb + tc)$ for all $s, t \in \mathbb{Z}$

Proof (a) see Goodman

(b) $a \mid b \Rightarrow b = qa$ for some $q \in \mathbb{Z}$

$b \mid a \Rightarrow a = q'b$ for some $q' \in \mathbb{Z}$

$\Rightarrow a = q'b = qq'a. \Rightarrow (qq' - 1)a = 0$

$\Rightarrow a = 0$ or $qq' - 1 = 0$

if $a = 0$ then $b = qa = 0$ and $a = b$.

if $a \neq 0$, $qq' = 1 \Rightarrow q = \pm 1$ by (a). $\Rightarrow b = (\pm 1).a$

(c) $a \mid b \Rightarrow b = qa$ for some $q \in \mathbb{Z}$

$b \mid c \Rightarrow c = q'b$ for some $q' \in \mathbb{Z}$

$\Rightarrow c = q'(qa) = (q'q)a. \Rightarrow a \mid q.$

(d) $a \mid b \Rightarrow b = qa$ for some $q \in \mathbb{Z}$

$a \mid c \Rightarrow c = q'a$ for some $q' \in \mathbb{Z}$

$\Rightarrow sb + tc = sqa + tq'a = (sq + tq')a$

$\Rightarrow a \mid (sb + tc).$ $\square$

Definition 1.6.8 An integer $\alpha > 1$ is a greatest common divisor (g.c.d) of two <u>nonzero</u> integers m, n if

(a) $\alpha \mid m$ and $\alpha \mid n$ ("α is a divisor")

(b) if $\beta \mid m$ and $\beta \mid n$ then $\beta \mid \alpha$.

("α is a greatest divisor")

Remarks 1) g.c.d.'s are unique:

suppose α_1, α_2 are two gcd's of m and n.

Then $d_1 | d_2$ and $d_2 | d_1$. By 1.6.2 (2) $d_1 = \pm d_2$
But d_1, d_2 are both positive. $\Rightarrow$ $d_1 = d_2$.

2. gcd (0,0) doesn't exist. Why not?

<u>Proposition 5.1</u> (For any pair of integers m, n (not both zero)
$d = \gcd(m,n)$ exist. Moreover $\exists\, x, y \in \mathbb{Z}$ so that
$d = xm + yn$.
Furthermore $\gcd(m,n) = \min\{am + bn \mid a, b \in \mathbb{Z}, am+bn > 0\}$.

<u>Proof</u> Consider
$S = \{am + bn \mid a, b \in \mathbb{Z},\ am+bn > 0\}$.
$S \neq \emptyset$ since $m \cdot m + n \cdot n > 0$ (m, n are not both zero)
hence $m \cdot m + n \cdot n \in S$.
By well-ordering principle $d = \min S$ exists.
Since $d \in S$, $d = xm + yn$ for some $x, y \in \mathbb{Z}$.

<u>Claim</u> $d = \gcd(m,n)$

<u>Proof of claim:</u> if $k | m$ and $k | n$, $k | (xm + yn) \Rightarrow k | d$
Remains to show: $d | m$ and $d | n$.
By the division algorithm $n = qd + r$ for $q, r \in \mathbb{Z}$
with $0 \leq r < d$. <u>If</u> $r \neq 0$, $r > 0$.
$\Rightarrow r = n - qd = n - q\,(yn + xm) = (1 - qy)\,n + (-qx)\,m \in S$
Since $r < d$ this contradicts: $d = \min S$.
$\therefore r = 0. \Rightarrow d | n$.
Similarly $d | m$.
$\therefore d = \gcd(m,n)$.