Remark

If $k < n$ s.th $\gcd(k,n) = 1$

$\Rightarrow \langle k \rangle = \mathbb{Z}_n$

$\Rightarrow \exists\, v : \quad vk = 1 \pmod n$

$\Rightarrow \exists\, u : \boxed{vk + un = 1}$

u, v Bezout coefficients

Last time

for $G = (G, +, 0)$ a finite abelian group and

$$\# G = p_1^{n_1} \cdots p_k^{n_k}$$

$$G(p_i) = \left\{ x \in G \mid p_i^n x = 0 \text{ for some } n \right\}$$

"primary p_i-group"

$$G \cong G(p_1) \oplus \cdots \oplus G(p_k)$$

eg: $\#\, G(p_i) = p_i^{n_i}$

$G(p_i)$

$p_i = 5$: $\mathbb{Z}_5 \oplus \mathbb{Z}_5 \ncong \mathbb{Z}_{5^2}$

Lemma: Let G be a finite abelian p-group ($\#G$ is a power of p). Let $a \in G$ be an element of maximal order (ie $o(b) \leq o(a)$ $\forall b \in G$)

Then $\exists\ k \leq G$ s.th

$$G \cong \langle a \rangle \oplus k.$$

Proof: Consider the set of subgroups $H \leq G$ s.th

$\langle a \rangle \cap H = \{0\}$. This set

is non-empty ($\{0\} \in$ this set)

is non-empty (as $\{0\}$ is in it) and is finite since G is finite, hence it has an element k of maximal size ($k \leq G$ $\langle a \rangle \cap k = \{0\}$)

we will show $\boxed{G = \langle a \rangle + k}$

Where $\langle a \rangle + k = \{ ra + k \mid r \in \mathbb{Z}, k \in k \}$

Suppose towards contradiction that $G \neq \langle a \rangle + k$, and let $0 \neq b \in G$ s.th $b \notin \langle a \rangle + k$

Since G is a p-group, there is $j \geq 1$ s.th $p^j \cdot b = 0$

and $\exists$ smallest $1 \leq l \leq j$

s.th $p^l \cdot b \in \langle a \rangle + k$.

Then the element $c = p^{l-1} b$

$\notin \langle a \rangle + k$ by minimality of l,

but $pc = p^{l}b \in \langle a \rangle + k$ so

$\exists\, t \in \mathbb{Z}$ and $k \in K$ s.t.h

$$\underline{pc = ta + k}.$$

Since $o(a) = p^n$ is maximal,

then $\forall x \in G \quad p^n x = 0$, but

then $p^{n-1}(ta+k) = p^{n-1}pc = 0$

so $p^{n-1}ta = -p^{n-1}k$

hence $\underline{p^{n-1}ta = 0}$.

Since $o(a) = p^n$, $p^n \mid p^{n-1}t$

so $t = pm$. This gives

$$pc = ta + k = pma + k$$

$\Rightarrow \quad k = pc - pma = p(c - ma).$

Set $d = c - ma$ so

$$pd = p(c - ma) = k \in k$$

but $d \notin k$ since if

$d = c - ma \in k$ then

$$c = ma + d \in (a) + k$$

Then set

$$H = \{ x + zd \mid x \in k, z \in \mathbb{Z} \}$$

is a subgp of A w/

$k \subseteq H$ ($k \neq H$: $d \in H$ but $d \notin k$)

so by maximality of k

$$H \cap \langle a \rangle \neq \{0\}.$$

Let $0 \neq w \in H \cap \langle a \rangle$. Then

$$w = sa = k_1 + rd$$

for $r, s \in \mathbb{Z}$, $k_1 \in K$.

We claim that $\gcd(p, r) = 1$.

If $\gcd(p, r) > 1$, then $r = py$ for $y \in \mathbb{Z}$. Then as $pd = k \in K$ we would have

$$sa = k_1 + py^r d \in \langle a \rangle \cap K$$

- contradiction.

Thus $\gcd(p, r) = 1$.

Let $u, v \in \mathbb{Z}$ be such that

$$pu + rv = 1.$$

Then

$$c = 1 \cdot c$$

$$= (pu + rv)\, c$$

$$= u(pc) + v(rc)$$

$$= u(ta+k) + v(r(d+ma))$$

$$= u(ta+k) + v(rd + rma)$$

$$= u(ta+k) + v(sa - k_1 + rma)$$

$$= (ut + vs + rm)a + (uk - vk_1)$$

$$\in \langle a \rangle \cap k$$

This contradicts $c \notin \langle a \rangle + k$

So $\underline{G} = \langle a \rangle + k$.

Then we may define

$$f : \langle a \rangle \oplus k \longrightarrow G$$

$$(sa, k) \longmapsto sa + k.$$

and this would be an iso.

(since $\langle a \rangle \cap k = \{0\}$) //

Thm (1st version of the classification theorem):

Every finite abelian gp G is isomorphic to the direct sum of cyclic gps, each of a prime power order, ie

$$\boxed{G \cong \mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_\ell^{s_\ell}}}$$

where $p_1, \ldots, p_\ell$ are (not necessarily unique) primes.

Proof: With out loss of generality

$$G = G(p_1) \oplus \cdots \oplus G(p_k)$$

with $\#G = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

each $G(p_i)$ is a p_i-gp

so by the lemma

$$G(p_i) \cong \langle a \rangle \oplus k_i \quad k_i \leq G(p_i)$$

repeating this we get

$$G(p_i) \cong \mathbb{Z}_{p_i^{\beta_1}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{\beta_m}}$$

with $\beta_1 + \cdots + \beta_m = n_i$

(since $G(p_i) = p_i^{n_i}$). //

Example: The integer 100

can be written as a product

of prime powers in 4 ways:

(a) (b) (c) (d)

$2 \cdot 2 \cdot 5 \cdot 5$, $2 \cdot 2 \cdot 5^2$, $2^2 \cdot 5 \cdot 5$, $2^2 \cdot 5^2$

By the classification thm,

if $\#G = 100$, it must be isomorphic to one of

(a) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, (b) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$

(c) $\mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$, (d) $\mathbb{Z}_4 \oplus \mathbb{Z}_{25} \cong \mathbb{Z}_{100}$

Proposition: For $n \geq 1$ w/ prime decomposition $n = p_1^{n_1} \cdots p_k^{n_k}$

$$\mathbb{Z}_n = \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}.$$

Proof: write $m = p_2^{n_2} \cdot \cdots \cdot p_k^{n_k}$

Then $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_m$

bcs $\gcd(p_1^{n_1}, m) = 1$.

By trivial induction

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}. \quad //$$

As a corollary of the classification theorem, we claim that finite abelian gps, admit the converse of Lagrange thm.

Let $\underline{G} = \langle g \rangle$ be a finit cyclic gp, and $n \mid \#G$.

Write $nk = \#G$. Since

$o(g) = nk$, $\langle g^k \rangle = \{0, g^k, \cdots, (g^k)^{n-1}\}$

is a subgp of order n.

Cor: Let G be a finite abelian
$\#G$. Then $\exists H \leq G$

gp and $n \mid \#$ [illegible]

w/ $\#H = n$.

Proof: Let $m = \#G$ and

$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Wlog

$$G = G(p_1) \oplus \cdots \oplus G(p_k)$$

and for each $i \le k$

$$G(p_i) = \mathbb{Z}_{p_i^{\beta_1}} \oplus \cdots \oplus \mathbb{Z}_{p_i^{\beta_{\ell_i}}}$$

$H_1^{(i)}$ $\qquad$ $H_{\ell_i}^{(i)}$

where $\sum_{j=1}^{\ell_i} \beta_j = \alpha_i$

Since $n \mid m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

we can write

$$n = p_1^{\gamma_1} \cdots p_k^{\gamma_k} \quad \text{for}$$

$$0 \le \gamma_i \le \alpha_i .$$

We can find $\delta_1, \ldots, \delta_\ell$ s.t.h

We can write $\beta_i = \delta_1 + \cdots + \delta_{\ell_i}$

$$\delta_1 + \cdots + \delta_{\ell_i} = \gamma_i$$

with $0 \leq \delta_j \leq \beta_j$.

Then $\rho_i^{\delta_j} \mid \rho_i^{\beta_j}$ so

$\exists\ H_j^{(i)} \leq \mathbb{Z}_{\rho_i^{\beta_j}}$ w/

$$\# H_j^{(i)} = \rho_i^{\delta_j}$$

Then

$$H^{(i)} := H_1^{(i)} \oplus \cdots \oplus H_{\ell_i}^{(i)}$$

$$\leq G(\rho_i)$$

and

$$\# H^{(i)} = \rho_i^{\delta_1 + \cdots + \delta_{\ell_i}} = \rho_i^{\gamma_i}$$

Then

$$H = H^{(1)} \oplus \cdots \oplus H^{(k)} \leq$$

$$G(p_1) \oplus \cdots \oplus G(p_k) = G$$

and $H = p_1^{r_1} \cdots p_k^{r_k} = n$ //

We can use the classification thm and the decomposition

$$n = p_1^{n_1} \cdots p_k^{n_k}$$

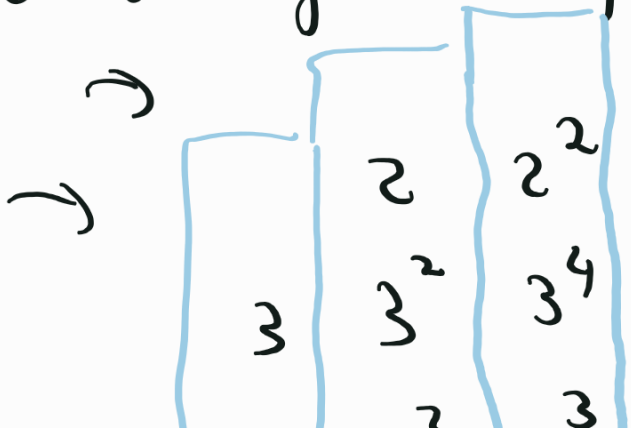
$$\mathbb{Z}_n = \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

to get another classification

Example: Suppose

$$G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{125}$$

we arrange all prime power §s as:



$$G \cong \mathbb{Z}_3 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25}) \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_{81} \oplus \mathbb{Z}_{125})$$

$$= \mathbb{Z}_{3} \oplus \mathbb{Z}_{450} \oplus \mathbb{Z}_{40500}$$

so $3 \mid 450$ and $450 \mid 40500$

This can always be done:

Thm (2nd version of classification theorem of finite abelian gps):

Let G be a finite abelian gp. then

$$G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$$

where $n_i \mid n_{i+1}$

$\forall \quad 1 \leq i \leq k-1$.

Proof: exercise.

Main example E an elliptic curve $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}_p =: \mathbb{F}_p$

$$E(\mathbb{F}_p) = \{ (x,y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + ax + b \} \cup \{\infty\}$$

↑ abelian gp.