Thm (FTFGAG, Elementary divisor decomposition):

If G is an Abelian gp., $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k} < \infty$,

$p_1 < p_2 < \cdots < p_k$ distinct primes, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$. Then:

i) $G \cong G_1 \times \cdots \times G_k$, with $|G_i| = p_i^{\alpha_i}$.

ii) $\forall\, 1 \le i \le k$, $\exists\, t_i \ge 1$, $\beta_{i1} \ge \beta_{i2} \ge \cdots \ge \beta_{it_i} \ge 1$, s.t.

$$G_i \cong \mathbb{Z}_{p_i^{\beta_{i1}}} \times \mathbb{Z}_{p_i^{\beta_{i2}}} \times \cdots \times \mathbb{Z}_{p_i^{\beta_{it_i}}}.$$

iii) This decomp. is unique.

Def: A group G is called a <u>p-group</u> for some prime p if every element of G has order which is a power of p.

Pf of part ii): Let G be a finite Abelian p-group.

Lemma: If G is a finite Abelian p-group and $g \in G$ is an element of maximal order in G then $\exists\, K \le G$ s.t.

i) $G \cong \langle g \rangle \times K$

ii) $\langle g \rangle \cap K = \{e\}$.

Pf of lemma: Write $|G| = p^k$. Pf. by induction on k.

Base case ($k=1$): $|G| = p$, let $g \in G \setminus \{e\}$, $K = \{e\}$. ✓

Ind. hyp: Suppose true for $1 \le k < n$.

Ind. step: Suppose $|G| = p^n$. Let $g \in G$ have maximal order.

If $|g| = p^n$ then take $K = \{e\}$ and we're done.

Suppose $|g| = p^\ell$ for some $1 \le \ell < n$.

Claim: There is a subgroup $H \le G$, $|H| > 1$, satisfying:

i) $\langle g \rangle \cap H = \{e\}$, ii) $|gH| = p^\ell$ in G/H.

Assuming the claim:

First note that gH is an element of maximal order in G/H. Also $|G/H| = |G|/|H| < |G|$.

So by the inductive hypothesis, $\exists\ \overline{K} \le G/H$ s.t.

$G/H \cong \langle gH \rangle \times \overline{K}$, and $\langle gH \rangle \cap \overline{K} = \{eH\}$.

By the 4th Isom. Thm., $\exists\ K \le G$ with $H \le K$ s.t.

$\overline{K} \cong K/H$.

Subclaim: $\langle g \rangle \cap K = \{e\}$.

Pf: Suppose $x \in \langle g \rangle \cap K$. Then

$$xH \in \langle gH \rangle \cap \overset{= \overline{K}}{K/H} = \{eH\}$$

$\Rightarrow x \in H \Rightarrow x \in \langle g \rangle \cap H = \{e\} \Rightarrow x = e.$ ∎

So: $\langle g \rangle K \overset{\langle g \rangle \cap K = \{e\}}{\cong} \langle g \rangle \times K \cong G$, using the fact that

$G/H \cong \langle gH \rangle \times K/H \Rightarrow \underbrace{|G/H|}_{= |G|/|H|} = \underbrace{|\langle gH \rangle|}_{= |g|} \cdot \underbrace{|K/H|}_{= |K|/|H|}$

$\Rightarrow |G| = |g||K|$. (so this proves the thm, assuming claim)

Claim: There is a subgroup $H \leq G$, $|H|>1$, satisfying:

i) $\langle g\rangle \cap H = \{e\}$, ii) $|gH| = p^\ell$ in G/H.

Pf. of claim: Let $h \in G \setminus \langle g \rangle$ be an element of smallest possible order. (note: $|h| = p^i$ for some $1 \leq i \leq \ell$)

Then $|h^p| = \dfrac{|h|}{\gcd(|h|, p)} = \dfrac{|h|}{p} < |h|$

$\Rightarrow h^p \in \langle g \rangle \Rightarrow h^p = g^a$ for some $a \in \mathbb{N}$.

Next since $|h^p| < |h| \leq |g|$,

and also $|h^p| = |g^a| = \dfrac{|g|}{\gcd(\underbrace{|g|}_{=p^\ell}, a)}$

$\Rightarrow p \mid a \Rightarrow h^p = g^{bp}$ for some $b \in \mathbb{N}$.

Let $x = g^{-b} h \in G$. Then:

i) $x^p = e \Rightarrow |x| \mid p$.

ii) $x \notin \langle g \rangle$: If $x = g^c$ for some c then $h = g^{b+c} \in \langle g \rangle$ (contradiction).

Therefore $x \notin \langle g \rangle$. (also from i), $|x| = p$).

Take $H = \langle x \rangle$. Then $|H| > 1$, and:

i) $\langle g \rangle \cap H = \{e\}$. (follows from observing that $x \notin \langle g \rangle$ and $H \cong C_p$).

ii) $|gH| = p^\ell$: $(gH)^m = eH \iff g^m \in H$

$\iff m = p^\ell k$ for some k. $\square$

Part iii): Uniqueness of the decomp. $G \cong G_1 \times \cdots \times G_r$ from part i) follows from the construction we gave.

Uniqueness of the decomp in part ii) follows from comparing elements of given orders. $\square$