Theorem: Let A be a finite abelian group of order n and let $m \mid n$. Then A has a subgroup of order m.

Proof: If n is a prime number, the result is clear: $m=1$ or $m=n$ in this case ($\{e\}$ is a subgroup of order 1, A is a subgroup of order n).

The proof is by induction on the order n of A. Consider an abelian group A of order $n>1$ and assume that the theorem is true for all abelian groups of order less than n. Let $m \mid n$. Take any element $a \in A$, $a \neq e$. Let o be the order of a and let p be a prime divisor of o. Then $b = a^{o/p}$ has order p. Consider the quotient group $A/\langle b \rangle$, which has order $\frac{n}{p}$ and the quotient homomorphism $\pi: A \longrightarrow A/\langle b \rangle$.

Case 1: $p \mid m$. Then $\frac{m}{p} \mid \frac{n}{p}$ and by the inductive assumption the group $A/\langle b \rangle$ has a subgroup B of order $\frac{m}{p}$. Consider the subgroup $\pi^{-1}(B)$ of A. We have $\langle b \rangle \subseteq \pi^{-1}(B)$ and $\pi: \pi^{-1}(B) \longrightarrow B$ is a surjective homomorphism with kernel $\langle b \rangle$. Thus $|\pi^{-1}(B)| = |B| \cdot |\langle b \rangle| = \frac{m}{p} \cdot p = m$ so A has a subgroup of order m.

Case 2: $p \nmid m$. Then $m \mid \frac{n}{p}$, so $A/\langle b \rangle$ has a subgroup D of order m (by the inductive assumption). We may assume $m > 1$ (the case $m = 1$ is clear). Let $w \in D$ be any non-trivial element and let k be the order of w. Then $k \mid m$. Let q be a prime divisor of k. Since π is surjective, there is $u \in A$ such that $\pi(u) = w$. Let l be the order of u, so $q \mid k \mid l$ and $u^{l/q}$ has order q. Now replace b by $u^{l/q}$ and p by q. Since $q \mid k \mid m$, we are in the situation of case 1. Thus A has a subgroup of order m. This completes the proof of the inductive step. □

We will now derive a number of corollaries.

Proposition: Suppose $m \mid n$ and $\gcd(m, \frac{n}{m}) = 1$. Let A be an abelian group of order n and let P, Q be subgroups of A of order m, $\frac{n}{m}$ respectively. Then

(1) $P \cap Q = \{e\}$

(2) A is isomorphic to $P \times Q$

(3) $P = \{a \in A : a^m = e\}$ and $Q = \{a \in A : a^{\frac{n}{m}} = e\}$

Proof: (1) If $a \in P \cap Q$ then the order of a divides m and $\frac{n}{m}$. Since $\gcd(m, \frac{n}{m}) = 1$, the order of a is 1, i.e. $a = e$.

② Since A is abelian, P, Q are normal subgroups of A. Since $P \cap Q = \{e\}$ by ①, the subgroup PQ is isomorphic to $P \times Q$ (we proved it last time). Thus $|PQ| = |P \times Q| = |P| \cdot |Q| = m \cdot \frac{n}{m} = n = |A|$, so $A = PQ$.

③ Let $P_1 = \{a \in A : a^m = e\}$, $Q_1 = \{a \in A : a^{n/m} = e\}$. Then P_1, Q_1 are subgroups of A and $P \subseteq P_1$, $Q \subseteq Q_1$. The same argument as in ① shows that $P_1 \cap Q_1 = \{e\}$. The same argument as in ② shows that $A \simeq P_1 \times Q_1$, so $|P_1| \cdot |Q_1| = n$. Since $|P_1| \geq |P| = m$ and $|Q_1| \geq |Q| = \frac{n}{m}$ and $|P_1| \cdot |Q_1| = n$ we must have $|P_1| = m$, $|Q_1| = \frac{n}{m}$, so $P = P_1$, $Q = Q_1$. ☒

Corollary 1: If $\gcd(m, \frac{n}{m}) = 1$ then a finite abelian group of order n has unique subgroup of order m. Indeed, part ③ tells us that a subgroup of order m consists of all elements a s.t. $a^m = e$.

Corollary 2: If $n = p_1^{s_1} \cdot p_2^{s_2} \cdots p_t^{s_t}$ where $p_1 < p_2 < \dots < p_t$ are prime numbers then any abelian group of order n has unique subgroups P_i of order $p_i^{s_i}$, $i = 1, \dots, t$ and

$$A \simeq P_1 \times P_2 \times \dots \times P_t.$$

Another corollary from our theorem:

Corollary 3: If A is a finite abelian group and a prime p divides the order $|A|$ of A, then A has an element of order p.

Indeed, A has a subgroup of order p, and any non-trivial element in this subgroup has order p (since p is a prime).

Remark: We will prove later that Cor. 3 is true for all finite groups.

Definition: Let p be a prime number. A group G is called a p-group if every element in G has a finite order which is a power of p.

Corollary 4: A finite abelian p-group has order a power of p.

Indeed, if A is a finite abelian p-group and $q \mid |A|$, q prime then A has an element of order q, so $q = p$. In other words, p is the only prime divisor of $|A|$, so $|A|$ is a power of p.

Remark: We will prove later that Cor 4 is true for all finite p-groups.

Remark: If p is a prime and G is a group s.t. $|G| = p^k$ then G is a p-group (since the order of any element in G divides p^k).