Theorem : Every finite Abelian group can be written as a direct product of cyclic groups of prime power order.

Proof. Let G be a finite Abelian group. We will first show that G is a direct product of it's p-Sylow subgroups. Because G is Abelian we have that for all p_i which divides $|G|$ there exists exactly one p_i-Sylow subgroup in G. Letting $P_1, P_2, \ldots P_r$ be said p-Sylow subgroups, we know that $|G| = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$. Define $f : P_1 \bigoplus P_2 \bigoplus \ldots \bigoplus P_r \to G$ by $f(g_1, g_2, \ldots g_r) = g_1 g_2 \ldots g_r$ for $g_i \in P_i$. Then, we see that f is a homomorphism from $P_1 \bigoplus P_2 \bigoplus \ldots \bigoplus P_r$ onto G. We wish to show that f is an isomorphism and therefore f^{-1} is also an isomorphism. To do so, we will show that $\mathrm{Ker}(f)$ is trivial, a sufficient condition. Let $g_1 g_2 \ldots g_r = e$, then: $(g_1 g_2 \ldots g_r)^{\frac{|G|}{p_i^{e_i}}} = e \implies e_1 e_2 \ldots g_i^{\frac{|G|}{p_i^{e_i}}} \ldots e_r = e \implies g_i^{\frac{|G|}{p_i^{e_i}}} = e$ But, notice that since $g_i \in P_i$, we have $|g_i| \big| |Pi|$ and $|g_i|$ is therefore a power of p_i. But p_i does not divide $\frac{|G|}{p_i^{e_i}}$, so $|g_i|$ does not divide $\frac{|G|}{p_i^{e_i}}$ and therefore, we see that $g_i = e$, from which is follows that $g_1 = g_2 = \ldots g_r = e$, and therefore $\mathrm{Ker}(f) = \{e\}$. Hence, f is one to one and therefore an isomorphism from $P_1 \bigoplus P_2 \bigoplus \ldots \bigoplus P_r \to G$. It follows that f^{-1} is also an isomorphism and we see that $G = P_1 \bigoplus P_2 \bigoplus \ldots \bigoplus P_r$.

Next, we'll show that $P_i = p_i^{e_i}$ is isomorphic to $Z_{p_1^{e_1}} \bigoplus Z_{p_2^{e_2}} \bigoplus \ldots \bigoplus Z_{p_r^{e_r}}$. Let $a \in P_i$ and let a have maximal order. Let $| < a > | = p^f$. If $f = e_i$, then we are done so suppose that $f < e$ and let B be the largest subgroup of P_i such that $< a > \cap B = \{e\}$. We wish to show that $< a > B = P$. Suppose that $< a > B \neq P$, then there exists $x \in P$ such that $x \notin < a > B$. Let $x^t = a^i b$, where t is the minimal power which allows $x \in < a > B$. Setting $t = sp^c$ and $i = jp^d$, we have $x^{sp^c} = a^{jp^d} b$. Because the order of x is p^f, by raising each side to the p^{f-c} power, we have: $e = (a^{jp^d} b)^{p^{f-c}} \implies e = a^{jp^{d+f-c}} b^{p^{f-c}}$. Because $< a > \cap B = \{e\}$, we see that $a^{jp^{d+f-c}} = b^{p^{f-c}} = e$, so $(a^{p^{d+f-c}})^j = e$ and further, since p does not divide j, we have $a^{p^{d+f-c}} = e$, $d + f - c \geq f$, so $f \geq c$ and we may therefore take a p^c root: $(x^s)^{p^c} = (a^j)^{p^{d-c}} b$ and so $b = (x^s)(a^{-j})^{p^{d-c}} \in B$. We see then that $< a^{-jp^{d-c}} > +B$ is a larger subgroup than B while still remaining disjoint from $< a >$, so we have contradicted our initial assumption and hence there does not exist $x \in P$ such that $x \notin < a > B$ and $< a > B = P$. By continuing this process (B will be broken down into cyclic groups also) and we have finally that $G = Z_{p_1^{e_1}} \bigoplus Z_{p_2^{e_2}} \bigoplus \ldots \bigoplus Z_{p_r^{e_r}}$, where i, j are not necessarily distinct. □