Failed to Find Numbers of Isomorphism Classes of Finite Group

Qige Wang

January 2026

1 An easier problem

Let $f(n)$ be the number of groups up to isomorphism of order n. This is not easy. One may start with a weaker form of the problem, namely, to consider some prime to some power $n = p^k$.

Intuitively, $f(p^k)$ seems quite independent of p, or at least independent of most p for most primes, and such independence becomes weaker and weaker as k increases. Therefore, one should start from examining $f(p^k)$ with small k. When a general proof of some small k fails when k increases, one should check $f(2^k)$ and $f(3^k)$.

For $k = 1$, by Lagrange's theorem, $f(p) = 1$. Namely, the only group with order p is $\mathbb{Z}/p\mathbb{Z}$.

2 Some group action stuff

Groups with order p^k with $k > 1$ are not simple. One wants to show that through a stronger statement, i.e., they have nontrivial centers. To show which, one should consider the inner automorphism acting on the group itself.

Consider conjugation group $\mathrm{Inn}(G)$. Specifically, $\mathrm{Inn}(G) := \{\rho_g(x) := gxg^{-1} | g \in G\}$. In fact, G is homomorphic to $\mathrm{Inn}(G)$, and the kernel is $\mathrm{Z}(G)$. Therefore $G/\mathrm{Z}(G) = \mathrm{Inn}(G)$, and so

$$|\mathrm{Inn}(G)| = \frac{|G|}{|\mathrm{Z}(G)|}$$

$\mathrm{Inn}(G)$ acts on G. The action is defined trivially as $\rho x = \rho(x)$. Consider the orbit $O(x) := \{\rho x | \rho \in \mathrm{Inn}(G)\}$ and stabilizer $S(x) := \{\rho \in \mathrm{Inn}(G) | \rho x = x\}$. Orbits are equivalence classes of G, and stabilizer is a subgroup of $\mathrm{Inn}(G)$.

Claim that the map $\psi(\rho) : \mathrm{Inn}(G) \to O(x), \rho_g \mapsto \rho_g(x)$ is bijection. It's by definition surjective. Now check injectivity. If $\psi(\rho_{g_1}) = \psi(\rho_{g_2})$, $\rho_{g_1}(x) = \rho_{g_2}(x)$. Apply $\rho_{g_2}^{-1}$ on both sides, $\rho_{g_2}^{-1}\rho_{g_1}x = x$ so equivalently $\rho_{g_2}^{-1}\rho_{g_1} \in S(x)$. This defines the equivalent relation of cosets of $S(x)$, so

$$|O(x)| = \frac{|\mathrm{Inn}(G)|}{|S(x)|}$$

3 $\mathrm{Z}(G)$ is not trivial if $|G| = p^k$

As said, orbits are equivalent classes on G, so

$$G = \sqcup_{\alpha \in A} O_\alpha$$

Consider the sizes of orbits. Notice that $|O(x)| = 1$ if $x \in \mathrm{Z}(G)$. So one can write

$$|G| = |Z(G)| + \Sigma_{i,|O_i|>1} O_i$$

For each O_i,

$$|O_i| = \frac{|\mathrm{Inn}(G)|}{|S_i|}$$

$|\mathrm{Inn}(G)| = \frac{|G|}{|\mathrm{Z}(G)|}$ is some power of p and so does $|S_i|$ as $S_i \leq \mathrm{Inn}(G)$. Therefore $|O_i|$ is also a power of p. Given $|O_i| > 1$, $|O_i| \geq p$, so $p||O_i|$. Notice that it implies $|G| \equiv |\mathrm{Z}(G)| (\mathrm{mod}\ p)$, therefore $p||\mathrm{Z}(G)|$.

4 $k = 2$

Given the very helpful lemma, $|\mathrm{Z}(G)| \in \{p, p^2\}$. We claim that $f(p^2) = 2$, regardless of p.

Case 1: $|\mathrm{Z}(G)| = p^2$

G is abelian. We claim that the only abelian groups with order p^2 are $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}$. Specifically, for any $g \neq e$, $|g| = \{p, p^2\}$.

If there exists $|g| = p^2$, g generates G, so $G = \mathbb{Z}/p^2\mathbb{Z}$.

If every $g \neq e$ has $|g| = p$, pick a, b such that $a \neq e$ and $b \notin \langle a \rangle$. Consider $H = \{a^i b^j | i, j < p\}$. This is a subgroup because G is abelian. H has at most p^2 elements. If there exists $a^i b^j = a^{i'} b^{j'}$, $a^{i-i'} = b^{j'-j}$, then $b \in \langle a \rangle$. So $H = G$. Define $\varphi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G$ by

$$\varphi(i, j) = a^i b^j$$

Obviously this is an isomorphism and we are done. Similar isomorphisms will be omitted later.

Case 2: $|\mathrm{Z}(G)| = p$

If so, $\mathrm{Z}(G)$ and $G/\mathrm{Z}(G)$ are both $\mathbb{Z}/p\mathbb{Z}$. Say $G/\mathrm{Z}(G) = \langle g\mathrm{Z}(G) \rangle$ for some g. Then every element is uniquely written as $a^n z$ for some $z \in \mathbb{Z}(G)$, so G is still abelian, which falls to Case 1.

5 $k = 3$

Similarly, $|Z(G)| \in \{p, p^2, p^3\}$. We claim $f(p^3) = 5$, regardless of p. But foreseeably, the case of $k = 3$ will be significantly harder, as $G/Z(G)$ is no longer guaranteed to have order p or 1 and thus be abelian, and nonabelian case is inevitable here.

Case 1: $|Z(G)| = p^3$

G is abelian. We use a similar strategy by considering the greatest order of elements.

If there exists an element of order p^3, then $G = \mathbb{Z}/p^3\mathbb{Z}$.

If the maximal order is p^2, we have $|\langle a \rangle| = p^2$. Take $b \neq e$ and $b \notin \langle a \rangle$. $|b|$ cannot be p^2 If so, it will generate a second subgroup of order p^2. Their intersection subgroup must have at least order p, so $\langle a^p \rangle = \langle b^p \rangle$. Contradict. Therefore $|b| = p$.

If there is any $c \neq e$ and $c \in \langle a \rangle \cap \langle b \rangle$, it will generates a cyclic group of order p, so $\langle b \rangle \in \langle a \rangle$. Contradict. Therefore

$$\langle a \rangle \cap \langle b \rangle = \{e\}$$

Thus $\langle a, b \rangle = G$, so $G = \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Finally, if the maximal order is p, then for the similar reasons as when in $k = 2$, $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Case 2: $|Z(G)| = p^2$

If so, $G/Z(G)$ is cyclic thus G is abelian. Contradict.

Case 3: $|Z(G)| = p$

To be honest, this is the hardest case, and I almost tried to approach it by looking at multiplication tables. Anyway, we have $|G/Z(G)| = p^2$, and from the case of $k = 2$, it's either $\mathbb{Z}p^2\mathbb{Z}$ or $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Obviously the former is impossible, as if so then G is abelian.

So $G/Z(G) = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Pick $x, y \in G$ such that $G/Z(G) = \langle xG(Z), yZ(G) \rangle$. Let $Z(G) = \langle z \rangle = \mathbb{Z}/p\mathbb{Z}$. Since $xZ(G)$ and $yZ(G)$ both have order p, $x^p, y^p \in Z(G)$. Say $x^p = z^a$ and $y^p = z^b$.