Theorem 1. Assume $|G| = p^n m$, p is prime, and q is the number of subgroups of G of size p^n. Then

$$\binom{p^n m - 1}{p^n - 1} \equiv_p q$$

Proof. Let G act on the set of subsets of G by left multiplication, that is,

$$g \cdot X = gX = \{gx | x \in X\}$$

for all $X \subseteq G$. For any subset $X \subseteq G$, the stabilizer of X is $G_X = \{g \mid gX = X\}$ and the orbit of X is $\mathcal{O}_X = \{gX \mid g \in G\}$. Let $X \subseteq G$.

Prop 1. $X \leq G$ iff $X = G_X$.

Proof. If $X = G_X$ then X is a subgroup of G because the stabilizer G_X is always a subgroup of the acting group.

Suppose $X \leq G$. Then $1 \in X$, so if $g \in G_X$ then $gX = X$ (by definition of G_X), hence $g = g1 \in gX = X$. Thus $G_X \subseteq X$. Conversely, if $a \in X$ then $aX \subseteq XX = X$ (where $XX = X$ since $X \leq G$).

Prop 2. $G_X X = X$.

Proof. Consider a typical element gx of $G_X X$, where $g \in G_X$ and $x \in X$. Then $gx \in gX = X$. This shows $G_X X \subseteq X$. Since $1 \in G_X$, we also have $X = 1X \subseteq G_X X$.

Prop 3. $|G_X|$ divides $|X|$.

Proof. By Prop. 2,

$$X = G_X X = \bigcup \{G_X a \mid a \in X\} \tag{1}$$

so X is the union of right cosets of the subgroup G_X. Each of these cosets has size $|G_X|$, so $|X|$ is the number of such cosets multiplied by $|G_X|$.

Prop 4. $G_{aX} = aG_X a^{-1}$.

Proof. $g \in G_{aX}$ iff $gaX = aX$ iff $a^{-1}gaX = X$ iff $a^{-1}ga \in G_X$ iff $g \in aG_X a^{-1}$.

Now we restrict the action of G to the subsets of size p^n. Let $A = \{X \subseteq G \mid |X| = p^n\}$. Let $X \in A$. By (1), X is the union of right cosets of G_X, so there are two cases: X is either a *single* right coset, or else it contains more than one right coset of G_X.

Case 1. X is a single right coset of G_X.

Suppose $X = G_X a$ for some $a \in G$. Then $p^n = |X| = |G_X a| = |G_X|$, so G_X is a subgroup of order p^n. Let $H = a^{-1}G_X a$. Then H is a subgroup of order p^n because $H \cong aHa^{-1} = G_X$. Also, H is in the orbit of X since $H = a^{-1}X$ so $\mathcal{O}_X = \mathcal{O}_H$. Thus $\mathcal{O}_X$ is the set of left cosets of the subgroup H, and $|\mathcal{O}_X| = |G : G_X| = \frac{|G|}{|G_X|} = \frac{p^n m}{p^n} = m$. Every left coset of H in $\mathcal{O}_X$ is a single right coset of a conjugate of H, since $bH = (bHb^{-1})b$.

Case 2. X contains more than one right coset of G_X.

By Prop. 3, $|G_X|$ divides $|X| = p^n$, but $|G_X|$ cannot be equal to p^n, so there is some k such that $0 \leq k < p$ and $|G_X| = p^k$, hence $|\mathcal{O}_X| = |G : G_X| = \frac{|G|}{|G_X|} = \frac{p^n m}{p^k} = p^{n-k}m$. In this case $|\mathcal{O}_X|$ is divisible by both p and m.

If there were a subgroup in $\mathcal{O}_X$, then we would have $gX \leq G$ for some $g \in G$, so by Prop. 1, $gX = G_{gX}$. But $G_{gX} = gG_X g^{-1}$ by Prop. 4, so $p^n = |X| = |gX| = |G_{gX}| = |gG_X g^{-1}| = |G_X|$, a contradiction (since $|G_X| \neq p^n$).

Every orbit either contains exactly one subgroup of size p^n and its size is m, or else it contains no subgroups of size p^n, and its size is divisible by both m and p.

Therefore q, the number of subgroups of size p^n, is equal to the number of orbits of size m.

A is a disjoint union of the orbits of sets in A, so

$$|A| = \binom{p^n m}{p^n} = qm + pm(\cdots)$$

There are q orbits of size m (which accounts for "qm") and the size of every other orbit is divisible by pm, so pm can be factored out of all of them, leaving "$(\cdots)$". However,

$$\begin{aligned}\binom{p^n m}{p^n} &= \frac{(p^n m)!}{p^n!(p^n m - p^n)!} = \frac{p^n m(p^n m - 1)!}{p^n(p^n - 1)!(p^n m - p^n)!} \\ &= m\frac{(p^n m - 1)!}{(p^n - 1)!(p^n m - 1 - (p^n - 1))!} = m\binom{p^n m - 1}{p^n - 1}\end{aligned}$$

so

$$\binom{p^n m - 1}{p^n - 1} = q + p(\cdots) \equiv_p q$$

Lemma. Assume p is prime. Then $\binom{p^n m - 1}{p^n - 1} \equiv_p 1$.

Proof. The set of subgroups of the cyclic group $\mathbb{Z}_{p^n m}$ which have size p^n is $\{\langle m\rangle\}$, so there is only one subgroup of order p^n. The conclusion follows by Theorem 1, applied to $\mathbb{Z}_{p^n m}$ with $q = 1$.

Theorem 2. Assume $|G| = p^n m$, p is prime, and q is the number of subgroups of G of size p^n. Then $q \equiv_p 1$.

Proof. By Theorem 1 and the Lemma.

Definition. For any group G and prime p, G is a **p-group** if $|G|$ is a power of p. If $|G| = p^n m$ and p does not divide m, then $\mathrm{Syl}_p(G)$ is the set of subgroups of G that have size p^n. Such groups are called **Sylow p-subgroups** of G. By Theorem 2, G must have at least one Sylow p-subgroup.

Theorem 3. Assume $|G| = p^n m$, p is prime, $p \not| m$, q is the number Sylow p-subgroups, and $P \in \mathrm{Syl}_p(G)$. Then (1) every p-subgroup of G is a subgroup of a conjugate of P, (2) all Sylow p-subgroups are conjugate to P, and (3) $q|m$.

Proof. For (1), assume $H \leq G$ and $|H|$ is a power of p. Let H act on G/P by left multiplication. This partitions G/P into orbits, so $m = |G/P|$ is the sum of the sizes of these orbits. The size of the orbit of the coset $aP \in G/P$ is $|H : H_{aP}| = \frac{|H|}{|H_{aP}|}$. Since $|H|$ is a power of p, $|H : H_{aP}|$ is either 1 (if $H_{aP} = H$) or a power of p (if $H_{aP} < H$). Hence m is the sum of numbers that are either equal to 1 or divisible by p. They can't all be divisible by p because they add up to a number m which is not divisible by p. Hence one of the orbits has size 1, say $\{aP\}$ for some $a \in G$. Then, for every $h \in H$, $haP = aP$, so $a^{-1}haP = P$, so $a^{-1}ha \in P$ since $P \leq G$. This shows $a^{-1}Ha \subseteq P$, hence $H \subseteq aPa^{-1}$. If $|H| = p^n$, then $H = aPa^{-1}$, so (2) holds.

For (3), let G act on $A = \{X \subseteq G | p^n m = |X|\}$ by conjugation. Since by part (2) all Sylow p-subgroups are conjugates, the orbit of P under conjugation is $\mathrm{Syl}_p(G)$ and its size is q. The size of an orbit always divides the size of the acting group, so q divides $p^n m$. However, p does not divide q because $q \equiv_p 1$, so $q|m$.