Силовская p-подгруппа конечной группы G (где p — простое число) — это подгруппа порядка p^k, где $|G| = p^k m$ и p не делит m.

Теоремы Силова. *Пусть G — конечная группа, а p — простое число. Тогда в группе G*

1) *силовская p-подгруппа существует;*
2) *все силовские p-подгруппа сопряжены; любая p-подгруппа группы G содержится в силовской;*
3) *число силовских p-подгрупп сравнимо с единицей по модулю p (и делит $|G|$).*

Доказательство. Пусть $|G| = p^k m$, где $p \nmid m$.

1) Индукция по $|G|$.
   Случай I: порядок центра $Z(G)$ группы G делится на p.
   В этом случае абелева группа $Z(G)$ содержит элемент z порядка p (это сразу вытекает из теоремы о строении конечно порождённых абелевых групп). Подгруппа $\langle z \rangle$ порядка p нормальна в G (поскольку она центральная), и в факторгруппе $G/\langle z \rangle = \widehat{G}$ (порядка $p^{k-1}m$) есть силовская подгруппа $\widehat{S}$ порядка p^{k-1} по предположению индукции. Рассмотрим канонический гомоморфизм $\varphi\colon G \to G/\langle z \rangle = \widehat{G}$ (где $g \mapsto g\langle z \rangle$). Тогда полный прообраз $S = \varphi^{-1}(\widehat{S})$ подгруппы $\widehat{S}$ имеет порядок p^k, то есть является силовской p-подгруппой в G, что и требовалось.
   Случай II: порядок центра $Z(G)$ группы G не делится на p.
   Рассмотрим действие группы G на себе сопряжением ($g \circ x = gxg^{-1}$) и разложим G в объединение непересекающихся орбит (то есть классов сопряжённости):
   $$|G| = \underbrace{1+1+\ldots+1}_{|Z(G)|\ \textit{штук}} + |G \circ x_1| + \ldots + |G \circ x_l| = |Z(G)| + \frac{|G|}{|C(x_1)|} + \ldots + \frac{|G|}{|C(x_l)|} \quad \text{где все } x_i \notin Z(G). \qquad (*)$$
   Мы здесь воспользовались тем, что класс сопряжённости $G \circ x$ состоит из одного элемента тогда и только тогда, когда $x \in Z(G)$, а также тем, что длина орбиты равна индексу стабилизатора (то есть в данном случае мощность класса сопряжённости равна индексу централизатора).
   Порядок группы группы G делится на p (поскольку мы считаем, что $k > 0$; иначе доказывать нечего), а $|Z(G)|$ не делится на p. Следовательно, одно из слагаемых $\frac{|G|}{|C(x_i)|}$ не делится на p. Стало быть порядок $|C(x_i)|$ одного из централизаторов делится на p^k, и, значит, в нём существует силовская подгруппа порядка p^k по предположению индукции (поскольку $|C(x_i)| < |G|$ в силу нецентральности элемента x_i). Это завершает доказательство — мы нашли в группе подгруппу порядка p^k.
2) Рассмотрим действие левыми сдвигами на множестве $X = \{xS \mid x \in G\}$ левых смежных классов группы G по (какой-то) силовской p-подгруппе S, то есть $g \circ xS \overset{\text{опр}}{=} gxS$. Ограничим это действие на какую-то другую p-подгруппу P группы G. Множество X, состоящие из m элементов, распадётся на непересекающиеся орбиты, длины которых делят порядок группы P, то есть являются степенями числа p, и мы получаем равенство $m = p^{k_1} + \ldots + p^{k_s}$. Число m не делится на p, поэтому один из показателей k_i равен нулю, и соответствующая орбита точки xS состоит из одного элемента: $gxS = xS$ для всех $g \in P$. Это означает, что $P \subseteq xSx^{-1}$, что и требовалось: это доказывает оба утверждения пункта 2).
3) То, что число силовских p-подгрупп делит $|G|$, немедленно вытекает из пункта 2): в пункте 2) утверждается, что

   силовские p-подгруппы составляют одну орбиту при действии группы на множестве своих подгрупп сопряжением,

   а длина орбиты всегда делит порядок группы, как мы знаем.
   Для доказательства сравнимости с единицей по модулю p рассмотрим действие силовской подгруппы S на множестве всех силовских p-подгрупп группы G сопряжением: $s \circ P \overset{\text{опр}}{=} sPs^{-1}$. Множество силовских подгрупп распадётся на непересекающиеся орбиты, и число N_p силовских p-подгрупп разложится в сумму длин этих орбит:
   $$N_p = |S \circ P_1| + \ldots + |S \circ P_t| = l_1 + \ldots + l_t.$$
   Все числа l_i являются степенями числа p (поскольку длина орбиты всегда делит порядок группы, а речь сейчас идёт о действии p-группы S). Одна из орбит — $S \circ S$ — состоит из одной точки (S — это одна из P_i), поэтому одно из чисел l_i равно единице. С другой стороны, все числа l_i являются степенями числа p (поскольку длина орбиты всегда делит порядок группы, а речь сейчас идёт о действии p-группы S). Поэтому для доказательства сравнимости N_p с единицей по модулю p достаточно показать, что все остальные слагаемые l_i отличны от единицы. Пусть $l_k = |S \circ P_k| = 1$, то есть $S \circ P_k = P_k$, то есть $sP_ks^{-1} = P_k$ для всех $s \in S$, то есть подгруппа S нормализует подгруппу P_k, то есть S содержится в нормализаторе $N(P_k)$ подгруппы P_k, но тогда и S, и P_k являются силовскими подгруппами группы $N(P_k)$, и, значит, они сопряжены в группе $N(P_k)$ (по пункту 2)), но P_k нормальна в своём нормализаторе, что означает равенство $S = P_k$, и доказательство закончено.