iv) Le nombre de p-Sylows de G est congru à 1 mod p et divise m. Deux p-Sylows de G sont conjugués. on en connaît un → conjuguer → on les connaît tous

Avant de démontrer cet énoncé, vérifions-le sur les exemples précédents.

exc. : 1) $G = \mathfrak{S}_3$, $p = 2$. On a vu que $\mathfrak{S}_3$ contenait 3 2-Sylows. 3 est bien congru à 1 mod 2 et 3 divise $m = 3$.
Notons H_1, H_2, H_3 les 3 2-Sylows de $\mathfrak{S}_3$. On a bien $H_1 = gH_2g^{-1}$, $H_1 = hH_3h^{-1}$ pour certains $g, h \in \mathfrak{S}_3$. voir
Pour $p = 3$, on a vu que $\mathfrak{S}_3$ ne contient qu'un seul 3-Sylow or $1 = 1 \bmod 3$ et $1 \mid 2 = m$.

2) $G = \mathbb{Z}/n\mathbb{Z}$, $n = mp^r$. On a vu que G contient un et un seul p-sous-groupe de cardinal p^s, pour $s = 0, \dots, r$.
De plus $\frac{n\mathbb{Z}}{n\mathbb{Z}} \subset \dots \subset \frac{mp\mathbb{Z}}{n\mathbb{Z}} \subset \frac{m\mathbb{Z}}{n\mathbb{Z}}$ ← p-Sylow de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ i.e.,
les p-sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ constituent une chaîne dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Preuve : Tout d'abord, montrons ii), iii) et iv) en admettant le i).

✓ ii) Pour tout p-sous-groupe H de G, il existe $g \in G$ tq $H \subseteq gSg^{-1}$:
On va faire agir H sur G/S en définissant $h * \gamma S = (h\gamma)S$ où $h \in H$ et $\gamma S \in G/S$ i.e. $\gamma \in G$ (il faut vérifier que $*$ est bien définie, voir TD). Or H est un p-groupe et
$|G/S| = \frac{|G|}{|S|} = \frac{mp^r}{p^r} = m \neq 0 \bmod p$
Or $|(G/S)^H| \equiv |G/S| \neq 0 \bmod p \longrightarrow (G/S)^H \neq \emptyset$.
Soit $\gamma S \in (G/S)^H$ où $\gamma \in G$ i.e. $\forall h \in H$, $h * \gamma S = \gamma S$.
En particulier : $\forall h \in H : h\gamma \in \gamma S$ $(h\gamma)S$
ou encore $\forall h \in H : h \in \gamma S \gamma^{-1}$ i.e., $H \subseteq \gamma S \gamma^{-1}$.

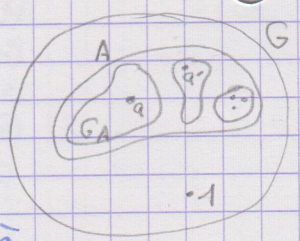
iii) : Soit $H \subseteq G$ un p-sous-groupe. D'après i), il existe $S \subseteq G$ p-Sylow. D'après ii) il existe $g \in G$ tq $H \subseteq gSg^{-1}$. Rappelons que l'application de conjugaison par g $\varphi_g : G \to G$, $x \mapsto gxg^{-1}$ est un automorphisme. $\varphi_{g^{-1}} = \varphi_g^{-1}$
Donc $gSg^{-1} = \varphi_g(S)$ et S ont le même cardinal. Comme $\varphi_g(S)$ est un sous-groupe de G, $\varphi_g(S) = gSg^{-1}$ est un p-Sylow.

iv) : Soient $S, S' \subseteq G$ deux p-Sylows. Appliquons le ii) à $H = S'$:
il existe $g \in G$ tq $S' \subseteq gSg^{-1}$, or $|S'| = |gSg^{-1}| = p^r$ d'où $S' = gSg^{-1}$ i.e. S' est un conjugué de S.
On a aussi $|X_r| \equiv 1 \bmod p$ d'après le i).
Il reste à démontrer que $|X_r|$ divise m. Considérons l'action de G sur X_r l'ensemble des p-Sylows de G par conjugaison :
$g * S = gSg^{-1}$. On a bien une action de G sur X_r.
Comme $X_r \neq \emptyset$ (d'après i)) et tous deux p-Sylows de G sont conjugués l'action de G sur X_r est transitive. Autrement dit, X_r est une orbite pour l'action de G sur X_r.
En particulier, $|X_r|$ divise $|G| = n = mp^r$. $|G_x| = |G|/|G_x|$
Or, d'après i), $|X_r| \equiv 1 \bmod p$. En particulier, $\text{pgcd}(|X_r|, p) = 1$ et $\text{pgcd}(|X_r|, p^r) = 1$. Comme $|X_r|$ divise mp^r, $|X_r|$ divise m d'après le Lemme de Gauss.

i) : Il nous reste à démontrer le i) : $|X_s| \equiv 1 \bmod p$. Pour démontrer cet énoncé, il faut un peu de préparation.
Soit E_s l'ensemble des parties de G de cardinal p^s. $|E_s| = \binom{n}{p^s}$
Faisons agir G sur E_s en définissant : $g * A = gA = \{ga / a \in A\}$ i.e. $g * A$ est le translaté à gauche de A par g, où $g \in G$ et $A \in E_s$.
Remarquons qu'on a bien $g * A \in E_s$. Cela définit bien une action de G sur E_s.
Si $A \in E_s$, $G_A = \{g \in G / g * A = A\}$.

Si $A \in E_s$, $G_A = \{g \in G / g * A = A\} = \{g \in G / gA = A\}$
$= \{g \in G / A$ est g-stable$\}$ est le stabilisateur de A.
L'orbite de A sera notée $\mathcal{O}(A) = \{g * A / g \in G\} = \{gA / g \in G\} \subseteq E_s$.
exemple : $G = \mathfrak{S}_3$, $p = 2$, $s = 1$, $E_s = \{\{(1), (123)\}, \{(23), (12)\}, \dots\}$
$X_s \subseteq E_s$
On va caractériser les $A \in E_s$ qui appartiennent à X_s i.e. qui sont des sous-groupes de G.

Lemme : Soit $A \in E_s$. Alors A est réunion disjointe de classes à droite modulo le sous-groupe G_A de G. Il existe $i \in \{0, \dots, s\}$ tq $|G_A| = p^i$. Dans ce cas $|\mathcal{O}(A)| = mp^{r-i}$.



Preuve du lemme : $G_A = \{g \in G / gA = A\}$.
Si on considère l'action de G_A sur G par mult à gauche :
$g * x = gx$, $g \in G_A$, $x \in G$.
A est un sous-ens. G_A-stable de G. Du coup, A est une réunion disjointe d'orbites pour l'action de G_A sur G.
Or une telle orbite est de la forme $G_A a$ i.e. une classe à droite de G modulo G_A. $A = G_A a_1 \cup \dots \cup G_A a_k$ où $a_1, \dots, a_k \in A$
et $G_A a_i \cap G_A a_j = \emptyset$ si $i \neq j$.
Comme $|G_A| = |G_A a_i| = |G_A a_2| = \dots = |G_A a_k|$, $k|G_A| = |A| = p^s$.
D'où $|G_A| = p^i$ avec $i \in \{0, \dots, s\}$ et $|\mathcal{O}(A)| = \dfrac{|G|}{|G_A|} = \dfrac{mp^r}{p^i} = mp^{r-i}$. □

Si $A \subseteq G$, $|A| = p^s$ est un sous-groupe, $A \subseteq G_A$. D'après la prop. précédente, $p^s = |A| \leq |G_A| \leq p^s$ i.e. $G_A = A$.

Cette observation suggère l'équivalence suivante :

Lemme : Soit $A \in E_s$. Les conditions suivantes sont équivalentes :
1) $|G_A| = p^s$ (i.e. G_A est le plus grand possible)
2) $|\mathcal{O}(A)| = mp^{r-s}$ (i.e. $\mathcal{O}(A)$ est la plus petite possible)
3) $|\mathcal{O}(A)| \not\equiv 0 \mod mp^{r-s+1}$
4) A est une classe à droite modulo un sous-groupe de G.
5) $\mathcal{O}(A) \cap X_s \neq \emptyset$
6) $\mathcal{O}(A)$ contient exactement un sous-groupe de G (de cardinal p^s)

Preuve du lemme : D'après le lemme précédent, $|G_A| = p^i$ où $i \in \{0, \dots, s\}$ et $|\mathcal{O}(A)| = mp^{r-i}$.
Du coup $|G_A| = p^s \iff i = s \iff |\mathcal{O}(A)| = mp^{r-s}$.
On a bien l'équivalence $1 \iff 2$.
Si $|\mathcal{O}(A)| = mp^{r-s}$, $|\mathcal{O}(A)| \not\equiv 0 \mod mp^{r-s+1}$.
Si $|\mathcal{O}(A)| \neq mp^{r-s}$, $|\mathcal{O}(A)| = mp^{r-i} = mp^{r-s} p^{s-i} = mp^{r-s+1} \cdot p^{s-i-1} \equiv 0 \mod mp^{r-s+1}$
car $s - i - 1 \geq 0$ car $i \leq s - 1$.
Cela montre l'équivalence $2 \iff 3$.
$1 \Rightarrow 4$: On suppose que $|G_A| = p^s$. Montrons que A est une classe à droite de G mod G_A.
D'après le lemme précédent, A est réunion de telles classes. Ces classes sont de card $p^s = |A|$. D'où A est une classe à droite mod G_A.
$4 \Rightarrow 5$: Supposons que $A = H\gamma$ où $\gamma \in G$ et $H \subseteq G$ sous-groupe.
Comme $|A| = p^s$, $|H| = |H\gamma| = |A| = p^s$ i.e. $H \in X_s \subseteq E_s$.
On a $\gamma^{-1} A = \gamma^{-1} H \gamma$ et $\gamma^{-1} H \gamma \subseteq G$ est un sous-groupe de G de cardinal p^s.
D'où $\gamma^{-1} H \gamma \in \mathcal{O}(A)$ i.e., $\mathcal{O}(A) \cap X_s \neq \emptyset$.
$5 \Rightarrow 6$: On suppose que $\mathcal{O}(A) \cap X_s \neq \emptyset$. Soit $H \in \mathcal{O}(A) \cap X_s$. Comme $H \in \mathcal{O}(A)$, $\mathcal{O}(H) = \mathcal{O}(A)$. Du coup $\mathcal{O}(A) = \mathcal{O}(H) = \{gH / g \in G\}$.
H est l'unique sous-groupe appartenant à cette collection de sous-ens. de G.
$6 \Rightarrow 1$: On suppose que $\mathcal{O}(A)$ contient exactement un seul sous-groupe H de G. Mq $|G_A| = p^s$.
Or, $H \in \mathcal{O}(A)$ i.e. $H = \gamma A$ où $\gamma \in G$.
G agit sur E, $gx = y$: $G_y = g G_x g^{-1}$.

$G_H = \gamma G_A \gamma^{-1}$ i.e., G_H est un conjugué de G_A. En particulier $|G_H| = |G_A|$
Or $G_H = \{g \in G / gH = H\} = H$ et $|H| = p^s = |G_H| = |G_A|$. □

Lemme : On a la congruence $\binom{n}{p^s} \equiv |X_s| \cdot mp^{r-s} \bmod mp^{r-s+1}$.

De plus $|X_s| \bmod p$ ne dépend pas de G mais seulement de n, p et s.

Preuve : $E_s = \bigcup_{i=1}^{N} \mathcal{O}(A_i)$ où $A_i \in E_s$ et $\mathcal{O}(A_i) \cap \mathcal{O}(A_j) = \emptyset$ si $i \neq j$.

Supposons que $\mathcal{O}(A_1), \dots, \mathcal{O}(A_M)$ sont les orbites de cardinal mp^{r-s} (les petites) et que $\mathcal{O}(A_{M+1}), \dots, \mathcal{O}(A_N)$ sont de cardinal mp^{r-i} avec $i < s$.

$$|E_s| = \sum_{i=1}^{N} |\mathcal{O}(A_i)| = \sum_{i=1}^{M} |\mathcal{O}(A_i)| \bmod mp^{r-s+1}$$

$$= \sum_{i=1}^{M} mp^{r-s} = |X_s| \, mp^{r-s}.$$