Α 3. Παρατηρώντας ότι το πλήθος των κύκλων μήκους $\ell \leq n$ τής συμμετρικής ομάδας S_n, ισούται με $n(n-1)\ldots(n-(\ell-1))/\ell$ να αποδείξετε ότι

(α′) το πλήθος των p–Sylow υποομάδων τής S_p, όπου ο p είναι ένας πρώτος αριθμός, ισούται με $(p-2)!$ και κατόπιν να συμπεράνετε ότι

(β′) ο p διαιρεί τον αριθμό $(p-1)!+1$.

Λύση. (α′) Το πλήθος των κύκλων μήκους p ισούται με $(p-1)!$. Κάθε κύκλος μήκους p χορηγεί μια κυκλική υποομάδα τάξης p και αντίστροφα κάθε κυκλική υποομάδα τάξης p έχει ως γεννήτορα έναν κύκλο μήκους p. Επιπλέον, η τομή δύο οποιωνδήποτε διαφορετικών υποομάδων τάξης p είναι μόνο το ταυτοτικό στοιχείο, αφού ο p είναι ένας πρώτος αριθμός. Αν είναι k το πλήθος των διαφορετικών κυκλικών υποομάδων τάξης p, τότε η S_p διαθέτει $k(p-1)$ στοιχεία τάξης p. Έτσι έχουμε $k(p-1) = (p-1)! \Rightarrow k = (p-2)!$.

(β′) Αφού $[S_p : 1] = 1 \cdot 2 \cdot \ldots \cdot (p-1) \cdot p$, συμπεραίνουμε ότι οι p–Sylow υποομάδες συμπίπτουν με τις κυκλικές υποομάδες τάξης p και γι’ αυτό, λόγω τής Θεωρίας Sylow, γνωρίζουμε ότι το πλήθος τους n_p ικανοποιεί την $n_p \equiv 1 \mathrm{mod} p$. Αλλά, $n_p = (p-2)!$. Επομένως,

$(p-2)! \equiv 1 \mathrm{mod} p \Leftrightarrow (p-2)! = 1 + \lambda p$, με $\lambda \in \mathbb{N} \cup \{0\}$ και p πρώτο $\Leftrightarrow$ $(p-1)! = (p-1) + \lambda p(p-1) \Leftrightarrow p \mid (p-1)! + 1$.