10. Αν p περιττός πρώτος φυσικός αριθμός και $q=\frac{p-1}{2}$ τότε:

$(q!)^2+(-1)^q\equiv 0\, modp$.

<u>απόδειξη</u>

Είναι $(q!)^2=1^2 2^2 ...(\frac{p-1}{2})^2$

Θεωρούμε την ισοδυναμία

$(x-1^2)(x-2^2)...(x-(\frac{p-1}{2})^2)-(x^{\frac{p-1}{2}}-1)\equiv 0\, modp$ (1)

Η ισοδυναμία $x^{\frac{p-1}{2}}-1\equiv 0\, modp$ έχει το πολύ $\frac{p-1}{2}$ λύσεις.

Θα δείξουμε οτι έχει ακριβώς $\frac{p-1}{2}$ λύσεις.

Έστω $1\leqslant k\leqslant p-1.$ Τότε (k,p)=1 και απο το θεώρημα Fermat-Euler θα έχουμε $k^{p-1}\equiv 1\, modp$ και άρα $(k^2)^{\frac{p-1}{2}}\equiv 1\, modp$ δηλαδή οι αριθμοί k^2 με $1\leqslant k\leqslant p-1$ είναι λύσεις της $x^{\frac{p-1}{2}}-1\equiv 0\, modp$

Αν k_1^2, k_2^2 είναι δυο τέτοιες λύσεις τότε

$k_1^2-k_2^2\equiv 0\, modp\Leftrightarrow (k_1-k_2)(k_1+k_2)\equiv 0\, modp$

και επειδή $|k_1-k_2|<p$ προκύπτει p/k_1+k_2 .

Εκλέγοντας όμως $1\leqslant k\leqslant\frac{p-1}{2}$ τότε προφανώς όλες οι λύσεις k^2 *είναι* διαφορετικές μεταξύ τους και $\frac{p-1}{2}$ σε πλήθος.

Δείξαμε δηλαδή ότι οι λύσεις της ισοδυναμίας $x^{\frac{p-1}{2}}\equiv 1\, modp$ είναι οι $1^2, 2^{2,}..., (\frac{p-1}{2})^2$. Τότε η (1) έχει βαθμό μικρότερο του $\frac{p-1}{2}$ και έχει $\frac{p-1}{2}$ διαφορετικές λύσεις. Συνεπώς όλοι οι συντελεστές του πολυωνύμου $(x-1^2)(x-2^2)...(x-(\frac{p-1}{2})^2)-(x^{\frac{p-1}{2}}-1)$ θα είναι

μηδενικοί στο δακτύλιο $\mathbb{Z}_p$, δηλαδή θα διαιρούνται με τον p.
Ειδικότερα για το σταθερό όρο θα έχουμε $1+(-1)^q(q!)^2\equiv 0\, modp$
οπότε

$$(-1)^q(q!)^2\equiv -1\, modp \Leftrightarrow (q!)^2\equiv -(-1)^q\, modp$$
$$\Leftrightarrow (q!)^2+(-1)^q\equiv 0\, modp \ .$$

Παρατήρηση 1. Όταν $p\equiv 1\, mod4$ τότε η λύση της ισοδυναμίας $x^2+1\equiv 0\, modp$ είναι ο αριθμός q!

Παρατήρηση 2. Όταν $p\equiv 3\, mod4$ τότε $(q!)^2\equiv 1\, modp$.