3.7.28. *Demostrar que el producto de todos los residuos cuadráticos positivos y menores que p es congruente con $(-1)^{\frac{p+1}{2}}$.*

Solución: En primer lugar, recordemos que n es residuo cuadrático módulo p si existe x tal que

$$x^2 = n \pmod{p}$$

Supongamos p primo impar.

Si $k \pmod{p}$ es solución de la ecuación anterior, entonces, $-k \pmod{p}$ también lo es, por lo que:

$$\prod_{\substack{0<n<p \\ \left(\frac{n}{p}\right)=1}} n \equiv \prod_{0<k\leq\frac{p-1}{2}} k^2 \pmod{p} \equiv \left(\prod_{0<k\leq p-1} k^2\right)^{\frac{1}{2}} \pmod{p} \equiv$$

$$\equiv \left((-1)^{p-1} \prod_{0<k\leq p-1} k^2\right)^{\frac{1}{2}} \pmod{p} \equiv (-1)^{\frac{p-1}{2}}(p-1)!^{\frac{2}{2}} \pmod{p}$$

El teorema de Wilson dice que si p es primo,

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

Luego

$$(-1)^{\frac{p-1}{2}}(p-1)! \pmod{p} \equiv (-1)^{\frac{p-1}{2}} \cdot (-1) \pmod{p}$$

En caso de $p = 2$, el único residuo cuadrático es 1, y:

$$1 = 1^{\frac{3}{2}} \equiv (-1)^{\frac{3}{2}} \pmod{2}$$

Conclusión:

$$\prod_{\substack{0<n<p \\ \left(\frac{n}{p}\right)=1}} n \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

Problema escrito por Javier Sanz-Cruzado Puig