Esercizio

Sia p un primo dispari. Calcolare $\left(\frac{2}{p}\right)$ mediante il Lemma di Gauss (27.11).

Svolgimento

In base al citato lemma,

$$\left(\frac{2}{p}\right) = (-1)^{|2P\cap Q|},$$

essendo

$$P = \left\{[1]_p,\ \cdots,\ \left[\frac{p-1}{2}\right]_p\right\}, \qquad Q = \left\{-[1]_p,\ \cdots,\ -\left[\frac{p-1}{2}\right]_p\right\}.$$

Quindi l'esponente $s = |2P \cap Q|$ è pari al numero di interi x tali che $1 \le x \le \frac{p-1}{2}$ per i quali $2x > \frac{p-1}{2}$, ossia tali che $\frac{p-1}{4} < x \le \frac{p-1}{2}$.

Se $p \equiv 1 \pmod 4$, allora $s = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}$, ed in tal caso $\left(\frac{2}{p}\right) = 1$ se e solo se $8|p-1$, ossia se e solo se $p \equiv 1 \pmod 8$.

Se $p \equiv 3 \pmod 4$, allora gli interi x da contare sono tutti e soli quelli per i quali $\frac{p+1}{4} \le x \le \frac{p-1}{2}$.

Quindi, in questo caso, $s = \frac{p-1}{2} - \frac{p+1}{4} + 1 = \frac{p+1}{4}$, ed in tal caso $\left(\frac{2}{p}\right) = 1$ se e solo se $8|p+1$, ossia se e solo se $p \equiv 7 \pmod 8$.