Gauss' lemma $\Rightarrow$ QRL

(after Reidei, Comm. Math. Helv. 16 (1943), 264)
(reproduced in Habicht, Math. Ann. 139 (1960), 343–365)

Notation: $p \neq 2$ prime, $S_+ = S_+(p) := \{1, 2, \dots, \frac{p-1}{2} \pmod p\} \subset \mathbb{Z}/p\mathbb{Z}$, $S_0 = S_0(p) := \{0 \pmod p\}$

$q \neq 2, p$ prime

$X := (0, \frac{pq}{2}) \cap \mathbb{Z}$, $Y := (0, pq) \cap \mathbb{Z}$

$Z_{*,*'} := \{x \in \mathbb{Z} \mid x \pmod p \in S_*(p),\ x \pmod q \in S_{*'}(q)\}$, $z \in \{X, Y\}$, $*, *' \in \{0, +, -\}$

$Z_{all,*} := \{x \in \mathbb{Z} \mid x \pmod q \in S_*(q)\}$, $Z_{*,all} := \{x \in \mathbb{Z} \mid x \pmod p \in S_*(p)\}$

Gauss' Lemma: $\boxed{(-1)^{|X_{0,-}|} = \left(\frac{p}{q}\right),\ (-1)^{|X_{-,0}|} = \left(\frac{q}{p}\right)}$

Symmetry: $(X_{+,-}) \sqcup (X_{-,+}) \xrightarrow{\sim} Y_{+,-}$

$x \longmapsto x$

$x \longmapsto pq - x$

Chinese remainder thm: $\forall *, *' \in \{+, -\}$ $\quad Y_{*,*'} \xrightarrow{\sim} S_*(p) \times S_{*'}(q)$

$x \longmapsto (x \pmod p,\ x \pmod q)$

$$\Rightarrow \boxed{|X_{+,-}| + |X_{-,+}| = \frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Similarly: $\frac{pq}{2} - \frac{1}{2} = \frac{p-1}{2} + p\frac{q-1}{2} = \frac{q-1}{2} + q\frac{p-1}{2} \Rightarrow |X_{-,all}| = \frac{p-1}{2} \cdot \frac{q-1}{2}$

$|X_{all,-}| = \frac{q-1}{2} \cdot \frac{p-1}{2}$

$$\Rightarrow \begin{aligned} |X_{all,-}| &= |X_{0,-}| + |X_{+,-}| + |X_{-,-}| \\ |X_{-,all}| &= |X_{-,0}| + |X_{-,+}| + |X_{-,-}| \end{aligned}$$

$$\Rightarrow 0 = |X_{all,-}| - |X_{-,all}| = |X_{0,-}| - |X_{-,0}| + \underbrace{|X_{+,-}| - |X_{-,+}|}_{\equiv |Y_{+,-}| = \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2}$$

$$\Rightarrow \boxed{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^{-1} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}}$$