Kwadratische reciprociteit

Zij p een oneven priemgetal en zij $a \in \mathbb{Z}$. Dan definiëren we het Legendre symbool $(\frac{a}{p})$ als volgt:

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & p \nmid a \text{ en } a \text{ is een kwadraat modulo } p \\ -1 & p \nmid a \text{ en } a \text{ is geen kwadraat modulo } p \\ 0 & p \mid a \end{cases}$$

Het is vrij eenvoudig in te zien dat geldt $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Het Legendre symbool is hiermee in principe vrij gemakkelijk te bepalen. De volgende relatie is een stuk verrassender: Als p en q verschillende oneven priemgetallen zijn, geldt

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

Deze relatie heet de wet van de kwadratische reciprociteit.

Door de wet van de kwadratische reciprociteit is de vraag of p een kwadraat is modulo q direct te relateren aan de vraag of q een kwadraat is modulo p. Als p veel kleiner is dan q, kan dit het berekenen van $(\frac{p}{q})$ gemakkelijk maken. Als voorbeeld, neem $p = 3$ en $q = 10000000019$. Er geldt $q \equiv -1 \pmod{p}$, dus q is geen kwadraat modulo 3, dus geldt $(\frac{q}{p}) = -1$. Omdat geldt $p \equiv 3 \pmod{4}$, is $\frac{p-1}{2}$ oneven en evenzo is $\frac{q-1}{2}$ oneven. Dit betekent dat $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ gelijk is aan -1. De kwadratische reciprociteitswet zegt nu dat $(\frac{p}{q})$ gelijk is aan 1, dus 3 is een kwadraat modulo 10000000019. Inderdaad geldt $3 \equiv 3803095009^2 \pmod{10000000019}$.