Bewijs van Kwadratische reciprociteit

Roland van der Veen

april 2013

1 Inleiding

We geven hier een mooi en elementair bewijs van de stelling van de kwadratische reciprociteit. Het bewijs is een variatie op dat van Rousseau: G. Rousseau, *On the quadratic reciprocity law*, Journal of the Australian Mathematical Society, 51, 03 (1991) 423-425.

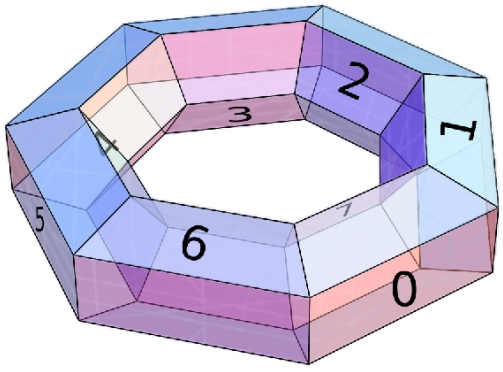
Definitie 1. *Voor oneven priemgetallen p en q definiëren we het Legendresymbool $\left(\frac{q}{p}\right)$ als volgt.*

$$\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{als } a \text{ een kwadraat is} \\ -1 & \text{als } a \text{ geen kwadraat is} \end{cases} \mod p$$

Stelling 1. *Stel p en q zijn twee verschillende oneven priemgetallen. Dan is*

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

In het bewijs hieronder zullen we gebruik maken van de Chinese reststelling en het volgende kriterium van Euler.



Lemma 1. *Eulers kriterium: Als p en q oneven priemgetallen zijn, dan is*

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

2 Het bewijs van de kwadratische reciprociteit

$M = \prod_{k=1,ggd(k,pq)=1}^{\frac{pq-1}{2}} k$ We berekenen op twee manieren M modulo p en M modulo q. Eerst modulo p.

$$M = \frac{\prod_{j=0}^{\frac{q-1}{2}-1} \prod_{k=1}^{p-1}(jp+k)! \prod_{n=1}^{\frac{p-1}{2}}(\frac{q-1}{2}p+n)}{\prod_{n=1}^{\frac{p-1}{2}} nq} = \frac{(p-1)!^{\frac{q-1}{2}}}{q^{\frac{p-1}{2}}} \mod p$$

Wegens symmetrie vinden we een vergelijkbaar antwoord modulo q:

$$M = \frac{(q-1)!^{\frac{p-1}{2}}}{p^{\frac{q-1}{2}}} \mod q$$

De volgende stap is om M modulo p en q te berekenen via de Chinese Reststelling. Hiertoe maken we een tabel van alle getallen 0,1 tot en met $pq-12$. M is immers het product van deze getallen. Van ieder getal zetten we de rest modulo p horizontaal en de rest modulo q verticaal. Zo hebben alle rijen in de tabel dus dezelfde waarde modulo q en alle kolommen dezelfde waarde modulo p. In het figuur staat een voorbeeld voor $p = 5$ en $q = 7$:

		mod 5				
		-2	-1	0	1	2
	3	3		10		17
m	2		9		16	2
o	1	8		15	1	
d	0		14	0		7
	-1	13			6	
7	-2			5		12
	-3		4		11	

Zie hoe opvolgende getallen precies een naar rechts en een omhoog gaan in de tabel. De tabel moet eigenlijk worden opgevat als een torus en daar maken de getallen een spiraal omheen.

Om de tabel af te maken voegen we ook de negatieve getallen -1 tot en met $-\frac{pq-1}{2}$ toe. In het voorbeeld ziet dat er zo uit:

Het is interessant om op te merken dat de 0 in het midden van de tabel fungeert als een symmetriepunt. De getallen k en $-k$ liggen precies tegenover elkaar ten opzichte van de nul. (Dit is natuurlijk eenvoudig te verklaren).

We kunnen nu eenvoudig m reconstrueren door de volgende getallen te vermenigvuldigen: De verzameling H van de getallen met resten ongelijk 0 modulo p en de rijen die horen bij de resten 1 tot en met $\frac{q-1}{2}$ modulo q.

		mod 5				
		-2	-1	0	1	2
	3	3	-11	10	-4	17
m	2	-12	9	-5	16	2
o	1	8	-6	15	1	-13
d	0	-7	14	0	-14	7
	-1	13	-1	-15	6	-8
7	-2	-2	-16	5	-9	12
	-3	-17	4	-10	11	-3

		mod 5				
		-2	-1	0	1	2
	3	3	-11	10	-4	17
m	2	-12	9	-5	16	2
o	1	8	-6	15	1	-13
d	0	-7	14	0	-14	7
	-1	13	-1	-15	6	-8
7	-2	-2	-16	5	-9	12
	-3	-17	4	-10	11	-3

In het voorbeeld is H de verzameling van alle rood gekleurde getallen.

Iedere factor van M is vertegenwoordigd in H, alle k tussen 0 en $\frac{pq-1}{2}$ die relatief priem is met p en q. Preciezer gezegd geldt dat voor ieder getal k uit de tabel dat relatief priem is met p en q of $-k$ in H zit of k in H zit. Maar niet beide. Dit is een direct gevolg van de symmetrie in de tabel ten opzichte van de nul. Min staat tegenover plus.

Het product van de getallen in H is dus gelijk aan ϵM voor een zeker teken $\epsilon = \pm 1$. Dit geeft ons een tweede manier om M of eigenlijk ϵM te berekenen, zowel modulo p als modulo q.

Eerst modulo p. Alle kolommen hebben dezelfde waarde modulo p en er zijn $p-1$ kolommen met waarden $1 \ldots p-1$ dus:

$$\epsilon M = (p-1)!^{\frac{q-1}{2}} \mod p$$

Reduceren modulo q geeft een vergelijkbaar product behalve dat we $(\frac{q-1}{2})!^2$ vervangen door $(-1)^{\frac{q-1}{2}}(q-1)!$ dus:

$$\epsilon M = (\frac{q-1}{2})!^{p-1} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(q-1)!^{\frac{p-1}{2}} \mod q$$

Vergelijken van de twee berekeningen voor M geeft:

$$\epsilon = \left(\frac{q}{p}\right) \mod p \qquad \epsilon(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{p}{q}\right) \mod q$$

Beide zijden van beide vergelijkingen staan alleen maar mintekens dus we kunnen het modulo teken weglaten en ϵ elimineren. De conclusie is:

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

en hiermee is de stelling bewezen.