



Universiteit  
Leiden  
The Netherlands

## On the computation of norm residue symbols

Bouw, J.

### Citation

Bouw, J. (2021, May 19). *On the computation of norm residue symbols*. Retrieved from <https://hdl.handle.net/1887/3176464>

Version: Publisher's Version

License: [Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden](#)

Downloaded from: <https://hdl.handle.net/1887/3176464>

**Note:** To cite this publication please use the final published version (if applicable).

Cover Page



Universiteit Leiden



The handle <https://hdl.handle.net/1887/3176464> holds various files of this Leiden University dissertation.

**Author:** Bouw, J.

**Title:** On the computation of norm residue symbols

**Issue Date:** 2021-05-19

# Stellingen

behorende bij het proefschrift

*"On the computation of norm residue symbols"*

van Jan Bouw

In onderstaande stellingen is  $p$  een priemgetal en  $\zeta_{p^n}$  met  $n \in \mathbb{Z}_{>0}$  een primitieve  $p^n$ -de eenheidswortel.

1. Stel  $F$  is een lichaam dat compleet is ten opzichte van de exponentiële valuatie  $\text{ord}_F$ . Stel  $f(X) = \sum_{i=0}^{\deg f} a_i(X - \alpha)^i \in F[X]$  met  $\alpha \in F$ ,  $\deg f \geq 1$  en  $a_0 \neq 0$ . Wanneer voor alle  $2 \leq j \leq \deg f$  geldt dat

$$(j-1) \cdot \text{ord}_F(a_0) + \text{ord}_F(a_j) > j \cdot \text{ord}_F(a_1),$$

dan convergeert de rij  $\{x_i\}_{i=0}^\infty$ , met  $x_0 = \alpha$  en  $x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$ , kwadratisch naar een nulpunt van  $f$  in  $F$ . Voor  $\deg f = 2$  is deze voorwaarde ook nodig voor convergentie van de rij.

2. Een polynoom  $f(X) = \sum_{i=0}^m a_i X^i \in \mathbb{F}_p[X]$  van graad  $m \in \mathbb{Z}_{>0}$  heet *speciaal*, wanneer het irreducibel is en de coëfficiënten  $a_{m-1}$  en  $a_1$  ongelijk zijn aan nul. Als  $f$  een speciaal polynoom is van graad  $m$  en  $g(X) = f(X^p - X)$ ,  $h(X) = X^{mp} \cdot g(\frac{1}{X})$  en  $k(X) = h(X+1)$ , dan is  $k$  een speciaal polynoom van de graad  $mp$ . Definieer de verzameling  $V_{p,m} = \{f \in \mathbb{F}_p[X] : f \text{ is speciaal van graad } m\}$ . Er geldt dat  $V_{p,m} = \emptyset \Leftrightarrow p = 2$  en  $m = 3$ .
3. Stel  $g = X^{\deg g} + \sum_{i=1}^{\deg g} a_i X^{\deg g - i} \in \mathbb{Z}_p[X]$  is een monisch polynoom dat irreducibel modulo  $p$  is en  $\gamma \in \overline{\mathbb{Q}}_p$  een nulpunt van  $g$ . Laat  $h = 0$  zijn als  $p \nmid \deg g$  en  $h = \min\{i : ia_i \not\equiv 0 \pmod{p}\}$  als  $p \mid \deg g$ . Dan is  $\delta = 1 + \gamma^h \cdot \pi^p$  een "distinguished unit" van het lichaam  $F = \mathbb{Q}_p(\gamma, \zeta_p)$ , zoals gedefinieerd in Definition 4.5 van dit proefschrift.
4. Een alternatief algoritme dat Theorem 1.4 uit dit proefschrift bewijst, construeert eerst een onvertakt uitbreidingslichaam van  $F$  van de graad  $p^n$  en berekent vervolgens de  $p^n$ -de macht van een geschikt gekozen Lagrange-resolvente.
5. Als  $L \supset K$  een eindige, cyclische uitbreiding van locale lichamen is, dan is er een eindige, cyclische lichaamsuitbreiding  $K' \supset K$  zodanig dat  $K' \otimes_K L$  een lichaam is dat onvertakt over  $K'$  is. Dit feit heeft zowel theoretisch als (potentieel) algoritmisch belang.

6. Stel  $n \in \mathbb{Z}_{>0}$  en verder dat  $F$  een eindige uitbreiding is van  $\mathbb{Q}_p(\zeta_{p^n})$  met vertakkingsindex  $e$  over  $\mathbb{Q}_p$ . Stel verder dat  $u \in U_i$  en  $v \in U_j$  met  $i, j \in \mathbb{Z}_{>0}$  zo dat  $i + j > (n + \frac{1}{p-1}) \cdot e$ . Dan geldt dat  $(u, v)_{p^n} = 1$ .
7. Stel  $F = \mathbb{Q}_p(\zeta_p)$ . Dan geldt dat  $\delta = 1 - \pi^p$  een "distinguished unit" is en  $(\pi, \delta)_p = \zeta_p^{-1}$  waarbij  $\pi = 1 - \zeta_p$ .
8. Zij  $p > 3$  en stel  $S = \{a + b \cdot \mathbf{i} : a, b \in \mathbb{Z}, a + b = p, 1 \leq a \leq p - 1\} \subset \mathbb{Z}[\mathbf{i}]$ , dan geldt

$$\sum_{t \in S} \frac{1}{t} \equiv 0 \pmod{p^2} \text{ en } \sum_{t \in S} \frac{1}{t^2} \equiv 0 \pmod{p}.$$

9. a. Als van twee cirkelschijven met straal 1 precies de helft van de oppervlakte van de ene cirkel binnen de andere cirkel ligt en de afstand van de middelpunten van beide cirkels gelijk is aan  $d_1$ , dan geldt dat

$$4 \cdot \arcsin\left(\frac{d_1}{2}\right) + d_1 \sqrt{4 - d_1^2} = \pi.$$

- b. Als van twee bollen met straal 1 precies de helft van de inhoud van de ene bol binnen de andere bol ligt en de afstand van de middelpunten van beide bollen gelijk is aan  $d_2$ , dan geldt dat  $d_2^3 - 12d_2 + 8 = 0$

10. Zij  $n \geq 3$  een geheel getal. Voor de oppervlakte  $A(n)$  van het vlakdeel, dat bedekt wordt door  $n$  cirkelschijven met straal 1 waarvan de middelpunten de hoekpunten zijn van een regelmatige  $n$ -hoek die beschreven is in een cirkel met straal 1, geldt

$$A(n) = 2\pi + n \cdot \sin\left(\frac{2\pi}{n}\right).$$