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

Leiden University Repository

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

Chapter 6

Strongly distinguished units

1. Introduction

We defined a distinguished unit in a field $F \supseteq \mathbf{Q}_p(\zeta_p)$ to be a principal unit in $U_{pe/(p-1)}$ having no p-th root in $U_{e/(p-1)}$. Such a unit plays an important role in the exponential representation of principal units. In this section we introduce the notion of a strongly distinguished unit. Throughout this chapter p is a prime number and n is a positive integer. We let F be a finite extension of $\mathbf{Q}_p$ with $\mu_{p^n} \subset F$. We denote the ramification index of F over $\mathbf{Q}_p$ by e.

DEFINITION 6.1. A *strongly distinguished unit of degree* $n \in \mathbf{Z}_{\geq 1}$ is a principal unit $\epsilon_n \in U_1$ with the property that $\mathrm{ord}_F(\epsilon_n - 1) = \frac{pe}{p-1}$ and such that $F(\sqrt[p^n]{\epsilon_n})$ is an unramified extension of F of degree p^n.

As we explained in Chapter 1, it may be of advantage to compute a strongly distinguished unit once and for all if a large number of norm residue symbols in the same field F has to be computed. If a strongly distinguished unit is used, the formula of Lemma 5.7 for the norm residue symbol of order p^n can be simplified, as we will see in Lemma 6.3ii below.

We give a few results that are almost immediate consequences of Definition 6.1 and the results of Chapter 5.

LEMMA 6.2. *Let* $\epsilon \in U_1$ *with* $\mathrm{ord}_F(\epsilon - 1) = pe/(p-1)$. *Then* ϵ *is a strongly distinguished unit of degree* n *if and only if* $\epsilon \notin F^{*p}$ *and* $(u, \epsilon)_{p^n} = 1$ *for every* $u \in \mathcal{O}_F^*$.

PROOF. From Proposition 5.1 of Chapter 5, part vii with $\beta = \epsilon, m = p^n$ and $\alpha' = u \in \mathcal{O}_F^*$, it follows that $(u, \epsilon)_{p^n} = 1$ for every $u \in \mathcal{O}_F^*$ if and only if the extension $F(\sqrt[p^n]{\epsilon_n})$ is unramified. Moreover $\epsilon \notin F^{*p}$ is equivalent to $[F(\sqrt[p^n]{\epsilon_n}) : F] = p^n$. □

LEMMA 6.3. *Let* $\epsilon_n \in U_1$ *be a strongly distinguished unit of degree* n. *Then:*

i. *Let* π, π' *be prime elements of* F. *Then:* $(\pi, \epsilon_n)_{p^n} = (\pi', \epsilon_n)_{p^n}$.
ii. *Let* $x, y \in F^*$. *Write* $x = \omega(a)\pi^{v(x)}w'$ *with* $w' \in U_1$ *and* $a \in k^*$. *Set* $\pi' = w'\pi$. *Then one has*

$$(x, y)_{p^n} = (\pi, \epsilon_n)_{p^n}^{(v(x)-1)\chi(y;\pi,\epsilon_n)+\chi(y;\pi',\epsilon_n)}.$$

PROOF. i: Follows from Lemma 6.2.
ii: Follows from i and Lemma 5.7 from Chapter 5. □

LEMMA 6.4.

i. *Every strongly distinguished unit of degree* $n \in \mathbf{Z}_{\geq 1}$ *is a distinguished unit.*
ii. *Let* $\delta \in F$. *Then* δ *is a strongly distinguished unit of degree* 1 *if and only if* δ *is a distinguished unit.*

PROOF. i: From Lemma 6.2 it follows that a strongly distinguished unit of degree n is not a p-th power.

ii: Let δ be a distinguished unit, then we have according to Proposition 5.1x, that $(u, \delta)_p = 1$ for every unit u, and then Proposition 5.1vii, with $m = p$, $\alpha' = u$ and $\beta = \delta$, says that $F(\sqrt[p]{\delta})$ is an unramified extension of F. The degree of this extension equals p, because $\delta \notin (F^*)^p$. Moreover we have $\mathrm{ord}_F(\delta - 1) = \frac{pe}{p-1}$, so δ is a strongly distinguished unit of degree 1. The other implication follows from i. □

In this Chapter we will prove Theorem 1.3 and Theorem 1.4 from Chapter 1. We prove the existence of strongly distinguished units in section 2. In section 3 we exhibit a uniquely solvable system of linear equations over $\mathbf{Z}/p^n\mathbf{Z}$ with the property that its unique solution gives rise to a strongly distinguished unit. This result leads, in section 4, to a polynomial-time algorithm that computes strongly distinguished units. Finally we give an example in section 5.

2. Existence

LEMMA 6.5. *There exists* $\epsilon \in U_1$ *with* $\mathrm{ord}_F(\epsilon - 1) \geq p^n > 0$ *such that* $F(\sqrt[p^n]{\epsilon})$ *is an unramified extension of* F *of degree* p^n.

PROOF. It is a well-known fact that there is a (unique) unramified extension L of F of degree p^n. By Kummer theory there is an element $\alpha \in F$ such that $L = F(\sqrt[p^n]{\alpha})$. There are an integer $i \in \mathbf{Z}$, an element $\beta \in \mathcal{O}_F/\mathfrak{m}_F$ and a principal unit $\epsilon \in U_1$ such that $\alpha = \pi^i \cdot \omega(\beta) \cdot \epsilon$. We have $p^n \mid i$ because the extension $F(\sqrt[p^n]{\alpha})/F$ is unramified. Furthermore $\omega(\beta) \in (F^*)^{p^n}$. This proves that there is a principal unit ϵ such that $L = F(\sqrt[p^n]{\epsilon})$. Because L is an unramified extension of F we have $\mathrm{ord}_F(1-\epsilon) = \mathrm{ord}_L(1-\epsilon)$. There are elements $a_i \in L$ such that $X^{p^n} - \epsilon = \prod_{i=1}^{p^n}(X - a_i)$, a product of p^n factors. Note that $\mathrm{ord}_L(1 - a_i) \geq 1$ since a_i is a principal unit. If we substitute $X = 1$ we obtain

$$\mathrm{ord}_F(1 - \epsilon) = \mathrm{ord}_L(1 - \epsilon) = \sum_{i=1}^{p^n} \mathrm{ord}_L(1 - a_i) \geq p^n \cdot 1 = p^n.$$

□

The theorem below proves the existence of strongly distinguished units.

THEOREM 6.6. *There exists* $\epsilon \in F$ *such that*

i. $\mathrm{ord}_F(\epsilon - 1) = e_{F/\mathbf{Q}_p(\zeta_{p^n})} \cdot p^n = \frac{pe}{p-1}$,
ii. $F(\sqrt[p^n]{\epsilon})$ *is an unramified field extension of* F *of degree* p^n.

There does not exist $\epsilon \in F$ *satisfying* ii *and* $\mathrm{ord}_F(\epsilon - 1) > \frac{pe}{p-1}$.

Proof. Let E be the unique maximal subextension of F which is unramified over $\mathbf{Q}_p(\zeta_{p^n})$. Let $\epsilon \in E$ with $\mathrm{ord}_E(\epsilon - 1) \geq p^n > 0$ such that $E(\sqrt[p^n]{\epsilon})$ is an unramified extension of E of degree p^n (Lemma 6.5). As a consequence, $F(\sqrt[p^n]{\epsilon})$ is an unramified field extension of F of degree p^n. Note that $e_{E/\mathbf{Q}_p} = e_{\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p} = p^{n-1}(p-1)$. Also ϵ is a p-th power in E if $\mathrm{ord}_E(\epsilon - 1) > p \cdot p^{n-1}(p-1)/(p-1) = p^n$ (Corollary 4.4). Hence $\mathrm{ord}_E(\epsilon - 1) = p^n$. It follows that

$$\mathrm{ord}_F(\epsilon - 1) = e_{F/E} \cdot \mathrm{ord}_E(\epsilon - 1) = e_{F/\mathbf{Q}_p(\zeta_{p^n})} \cdot \mathrm{ord}_E(\epsilon - 1) = e_{F/\mathbf{Q}_p(\zeta_{p^n})} \cdot p^n.$$

This proves the first result.

By Corollary 4.4 from Chapter 4, any $\epsilon \in U_1$ with $\mathrm{ord}_F(\epsilon - 1) > \frac{pe}{p-1}$ is a p-th power in F. Hence such an ϵ cannot satisfy condition ii. $\square$

Now we have also proven Theorem 1.3.

3. Constructing a unique strongly distinguished unit

Let δ be a distinguished unit and let π be a prime element. We refer to section 2.2 of Chapter 4, where the set $T_{\pi',\delta}$ is defined with π' is a prime element, and to Definition 4.10 where $\mu(x, N)$ is defined. We also refer to Definition 4.11 where the morphism $\chi(\cdot; \pi', \delta) : F^* \longrightarrow \mathbf{Z}/p^s\mathbf{Z}$ is defined. In the next lemma we take $s = n$. Remember that $(\pi, \delta)_{p^n}$ is a primitive p^n-th root of unity (Lemma 5.6). We shall write

$$T^*_{\pi,\delta} = \{z \in T_{\pi,\delta} : \mu(z, pe/(p-1)) \leq n - 1\},$$

which by section 2.1 of Chapter 4 is equal to $\{z \in T_{\pi,\delta} : \mathrm{ord}_F(z-1) \geq e/((p-1)p^{n-2})\}$.

Lemma 6.7.

i. *For $z, z' \in T_{\pi,\delta}$, define $b_{z',z} \in \mathbf{Z}/p^n\mathbf{Z}$ by $(z', z)_{p^n} = (\pi, \delta)_{p^n}^{b_{z',z}}$. Then the system of linear equations*

$$\begin{cases} \sum_{z \in T^*_{\pi,\delta}} b_{z',z} x_z = 0 & \text{for all } z' \in T_{\pi,\delta}, z \neq \delta \\ \quad x_\delta = 1 \end{cases}$$

has a unique solution with all $x_z \in \mathbf{Z}/p^n\mathbf{Z}$.

ii. *The unique solution $(x_z)_{z \in T^*_{\pi,\delta}}$ from* i *satisfies $x_z \in p^{\mu(z,pe/(p-1))}\mathbf{Z}/p^n\mathbf{Z}$ for all z.*

iii. *If $(c_z)_{z \in T^*_{\pi,\delta}} \in \mathbf{Z}^{T^*_{\pi,\delta}}$ satisfies $(c_z \bmod p^n) = x_z$ for all z, with $(x_z)_{z \in T^*_{\pi,\delta}}$ as in* i, *then $\epsilon = \prod_{z \in T^*_{\pi,\delta}} z^{c_z}$ is a strongly distinguished unit of degree n.*

Proof. Let ϵ'_n be a strongly distinguished unit of degree n. By Lemma 6.4i and Lemma 5.6 each of $(\pi, \epsilon'_n)_{p^n}$ and $(\pi, \delta)_{p^n}$ has order p^n. So there is a positive integer a with $p \nmid a$ such that $(\pi, \delta)_{p^n} = (\pi, \epsilon'_n)^a_{p^n} = (\pi, \epsilon'^a_n)_{p^n}$. Choose $\epsilon_n = \epsilon'^a_n$, then ϵ_n is a strongly distinguished unit for which $\chi(\epsilon_n; \pi, \delta) = 1$. Write $\epsilon_n = \prod_{z \in T_{\pi,\delta}} z^{a_z}$ with $a_z \in \mathbf{Z}_p$ (Proposition 4.8ii). Then we have $(a_\delta \bmod p^n) = \chi(\epsilon_n; \pi, \delta) = 1$. From $\epsilon_n \in U_{pe/(p-1)}$ it follows that for every $z \in T_{\pi,\delta}$ we have $p^{\mu(z,pe/(p-1))} \mid a_z$. In particular $(a_z \bmod p^n) = 0$ if $\mu(z, pe/(p-1)) \geq n$ or equivalently if $z \notin T^*_{\pi,\delta}$. From

5.1vii and the fact that $F(\sqrt[p^n]{\epsilon_n})$ is an unramified extension of F, it follows that for every $z' \in T_{\pi,\delta}$ we have

$$1 = (z', \epsilon_n)_{p^n} = \prod_{z \in T_{\pi,\delta}} (z', z)_{p^n}^{a_z} = \prod_{z \in T^*_{\pi,\delta}} (z', z)_{p^n}^{a_z} = (\pi, \delta)_{p^n}^{\sum_{z \in T^*_{\pi,\delta}} b_{z',z} a_z}.$$

So for every $z' \in T_{\pi,\delta}$ we have $\sum_{z \in T^*_{\pi,\delta}} b_{z',z}(a_z \bmod p^n) = 0$ in $\mathbf{Z}/p^n\mathbf{Z}$, while we just proved $(a_\delta \bmod p^n) = 1$. Hence $x_z = (a_z \bmod p^n)$ is a solution to the system of linear equations in i, and this solution also satisfies ii.

To prove uniqueness, let $(x_z)_{z \in T^*_{\pi,\delta}}$ be any solution, and let $\epsilon = \prod_{z \in T^*_{\pi,\delta}} z^{c_z}$ be as in iii. Then $\chi(\epsilon; \pi, \delta) = (1 \bmod p^n)$, and for each $z' \in T_{\pi,\delta}$, we have

$$(z', \epsilon)_{p^n} = \prod_{z \in T^*_{\pi,\delta}} (z', z)_{p^n}^{c_z} = (\pi, \delta)_{p^n}^{\sum_{z \in T^*_{\pi,\delta}} b_{z',z} x_z} = (\pi, \delta)_{p^n}^0 = 1.$$

Let $\alpha' \in \mathcal{O}_F^*$. Since α' can by Proposition 4.8ii be written as $\alpha' = \omega(\alpha' \bmod \mathfrak{m}) \cdot \prod_{z' \in T^*_{\pi,\delta}} z'^{d_{z'}}$ with $d'_z \in \mathbf{Z}_p$ and $\omega(k^*) \subset (F^*)^{p^n}$, we obtain $(\alpha', \epsilon)_{p^n} = 1$. Hence Proposition 5.1vii implies that $F(\sqrt[p^n]{\epsilon})$ is an unramified extension of F. By Kummer theory we have $\epsilon = \epsilon_n^i \cdot u^{p^n}$ with $i \in \mathbf{Z}$ and $u \in U_1$. Then $1 = \chi(\epsilon; \pi, \delta) = i \cdot \chi(\epsilon_n; \pi, \delta) + p^n \cdot \chi(u; \pi, \delta) \equiv i \bmod p^n$. Using the exponential representation from Proposition 4.8ii for ϵ, ϵ_n, u we obtain

$$\prod_{z \in T^*_{\pi,\delta}} z^{c_z} = \prod_{z \in T_{\pi,\delta}} z^{i a_z} \cdot \prod_{z \in T_{\pi,\delta}} z^{p^n \cdot e_z}$$

(with $e_z \in \mathbf{Z}_p$). According to Proposition 4.8ii, corresponding exponents are congruent modulo p^n, so for all $z \in T^*_{\pi,\delta}$ we have

$$x_z = (c_z \bmod p^n) = (i a_z \bmod p^n) = (a_z \bmod p^n).$$

This proves that $(a_z \bmod p^n)_{z \in T^*_{\pi,\delta}}$ is the unique solution to our system.

To prove that ϵ is a strongly distinguished unit of degree n, we remark that $c_z \equiv a_z \equiv 0 \bmod p^{\mu(z, pe/(p-1))}$, for $z \in T^*_{\pi,\delta}$ it follows that $\epsilon \in U_{pe/(p-1))}$. Also, from $\chi(\epsilon; \pi, \delta) = 1 \bmod p^n$ it follows that $\epsilon \notin (F^*)^p$ so that in particular $\epsilon \notin U_{1+pe/(p-1)}$. □

4. Computation

Let us now discuss how to compute a strongly distinguished unit.

Algorithm 6.8 (Strongly distinguished unit).
Input: $\mathcal{O}_N$ with $\zeta_{p^n} \in F$ and with $N \geq e/(p-1) + ne + 1$.
Output: A strongly distinguished unit $\epsilon_n \in \mathcal{O}_N$ of degree n.
Steps:

i. Compute $\overline{\delta} \in \mathcal{O}_N$ where $\overline{\delta}$ is a distinguished unit (Algorithm 4.15). If $n = 1$ return $\overline{\epsilon}_1 = \overline{\delta}$ and terminate.
ii. Compute $\overline{T_{\pi,\delta}} = \{\overline{1 - \omega(\gamma^j)\pi^i} \in \mathcal{O}_N, (i,j) \in S\} \cup \{\overline{\delta}\} \subset \mathcal{O}_N$ where $S = \{(i,j) \in \mathbf{Z}^2 : 0 \leq j < f, 1 \leq i < \frac{pe}{p-1}, p \nmid i\}$.

iii. For $\overline{z}, \overline{z'} \in \overline{T_{\pi,\delta}}$ compute $b_{z',z} \in \mathbf{Z}/p^n\mathbf{Z}$ with $(z', z)_{p^n} = (\pi, \delta)_{p^n}^{b_{z',z}}$ (Algorithm 5.15).

iv. Find $\overline{c_z} \in \mathbf{Z}/p^n\mathbf{Z}$ for $z \in T_{\pi,\delta}$, such that $\overline{c_\delta} = 1$ and such that for all $z' \in T_{\pi,\delta}$ we have

$$\sum_{z \in T_{\pi,\delta}} b_{z',z}\overline{c_z} = 0 \in \mathbf{Z}/p^n\mathbf{Z}.$$

v. For every $z \in T_{\pi,\delta}$ choose $c_z \in \{0, 1, \ldots, p^n - 1\}$ such that $(c_z \bmod p^n) = \overline{c_z}$.

vi. Return $\overline{\epsilon_n} \in \mathcal{O}_N$ with $\overline{\epsilon}_n = \prod_{\overline{z} \in \overline{T_{\pi,\delta}}} \overline{z}^{\overline{c_z}}$.

Proposition 6.9. *Algorithm 6.8 is correct and its complexity is* $O((ef)^2 \cdot ((N \log q)^{2[+1]} + Nf^C(\log p)^{1[+1]}))$.

Proof. The correctness of the Algorithm follows from Lemma 6.7. Let us discuss the complexity of the algorithm. Note that $p^n = O(e)$ and $e = O(N)$. Step i costs $O((f+\log p)(\log q)^{1[+1]} + f^C(\log p)^{1[+1]} + N\log q)$ by Algorithm 4.15. Step ii costs less than step iii. Step iii costs $(ef)^2 \cdot O((N\log q)^{2[+1]} + Nf^C(\log p)^{1[+1]})$ (Algorithm 5.15). Step iv is solving an $ef \times ef$ system over $\mathbf{Z}/p^n\mathbf{Z}$, which costs $O((ef)^3(\log p^n)^{1[+1]})$. Step v costs $O(\log p^n \cdot ef \cdot (N\log q)^{1[+1]})$ (Theorem 3.2). □

Theorem 6.10. *There is a polynomial-time algorithm that, given a prime number p, a positive integer n, and a finite extension F of $\mathbf{Q}_p$ containing the p^n-th roots of unity, computes an element ϵ of F satisfying conditions* (i) *and* (ii) *from Theorem 1.3.*

Proof. In Theorem 6.4 we proved the existence of a strongly distinguished unit and in Algorithm 6.8, whose correctness is proven in Proposition 6.9, we gave a polynomial-time algorithm to compute such a unit. This concludes the proof and we have also proven Theorem 1.4 from Chapter 1. □

5. Examples

Example 6.11. Let, as in previous examples, $F \supset \mathbf{Q}_2$ be given by $(p, g, h) = (2, X^2 + X + 1, Y^2 - (2 + 2X)Y - 2Y)$. A distinguished unit, as we have seen Example 4.6, is $\delta = 1 + \pi^4$. We want to compute a strongly distinguished unit ϵ_2 for the 4-th norm residue symbol in F by using the following table where we have computed $(\alpha, \beta)_4 \downarrow (\pi, \delta)_4$ for every $\alpha, \beta \in T_{\pi,\delta} = \{\pi, \delta, 1 - \pi, 1 - \gamma \cdot \pi, 1 - \pi^3, 1 - \gamma \cdot \pi^3\}$. In this table α is in the first column and β is in the first row.

$(\alpha, \beta)_4 \downarrow (\pi, \delta)_4$	π	δ	$1 - \pi$	$1 - \gamma\pi$	$1 - \pi^3$	$1 - \gamma\pi^3$
π	0	1	0	0	0	0
δ	3	0	0	2	0	0
$1 - \pi$	0	0	2	1	1	2
$1 - \gamma\pi$	0	2	3	0	0	1
$1 - \pi^3$	0	0	3	0	0	2
$1 - \gamma\pi^3$	0	0	2	3	2	2

If we put $\epsilon_2 = \delta \cdot (1-\pi)^{x_2} \cdot (1-\gamma\cdot\pi)^{x_3} \cdot (1-\pi^3)^{x_4} \cdot (1-\gamma\cdot\pi^3)^{x_5}$, we derive from the table a system of linear congruences using the fact that $(\epsilon_2, z)_4 \equiv 0 \bmod 4$ for every $z \in T_{\pi,\delta}$. We have

$$\begin{aligned} 2x_3 &\equiv 0 \bmod 4 \\ 2x_2 + x_3 + x_4 + 2x_5 &\equiv 0 \bmod 4 \\ 3x_2 + x_5 &\equiv 2 \bmod 4 \\ 3x_2 + 2x_5 &\equiv 0 \bmod 4 \\ 2x_2 + 3x_3 + 2x_4 + 2x_5 &\equiv 0 \bmod 4. \end{aligned}$$

The solution is $x_2 = x_3 = x_4 = 0 \bmod 4$, and $x_5 = 2 \bmod 4$. So a strongly distinguished unit of degree two in this field is $\epsilon = \delta \cdot (1-\gamma\pi^3)^2$.

EXAMPLE 6.12. Let p be a prime number, let $F = \mathbf{Q}_p(\zeta_p)$ and let $\pi = 1-\zeta_p$ be a prime element. Then F is a totally ramified extension of $\mathbf{Q}_p$ of degree $p-1$. We have $e = p-1$, $f = 1$ and a set of generators for the $F^*/(F^*)^p$ is $T_{\pi,\delta} = \{\pi, 1-\pi, 1-\pi^2, \ldots, 1-\pi^p\}$. The map $\tau_1 : U_1/U_2 \longrightarrow U_p/U_{p+1}$ is the trivial map, so the cokernel of τ_1 is generated by $\delta = 1-\pi^p$ which is a distinguished unit and also a strongly distinguished unit of degree 1.