NORMAL BASES VIA GENERAL GAUSS PERIODS

SANDRA FEISEL, JOACHIM VON ZUR GATHEN, AND
M. AMIN SHOKROLLAHI

ABSTRACT. Gauß periods have been used successfully as a tool for constructing normal bases in finite fields. Starting from a primitive rth root of unity, one obtains under certain conditions a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where r is a prime and $nk = r-1$ for some integer k. We generalize this construction by allowing arbitrary integers r with $nk = \varphi(r)$, and find in many cases smaller values of k than is possible with the previously known approach.

1. INTRODUCTION

Let $\mathbb{F}_q$ be a finite field with q elements. A basis of the vector space $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ of the form $(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$ is a *normal basis*, and in this case α is a *normal element* in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Gauß periods have been used to construct normal bases in the following way: Let $n, k \geq 1$ be integers such that $r = nk+1$ is a prime, and let q be a prime power with $\gcd(q, r) = 1$. Then the group $\mathbb{Z}_r^\times$ of units modulo r is cyclic and has nk elements, and since $q^{nk} \equiv 1 \bmod r$, r divides $q^{nk} - 1 = \#\mathbb{F}_{q^{nk}}^\times$. Hence there exists a primitive rth root of unity $\beta \in \mathbb{F}_{q^{nk}}$, and β^a is well-defined for any $a \in \mathbb{Z}_r^\times$. Let $\mathcal{K} < \mathbb{Z}_r^\times$ be the *unique* subgroup of the cyclic group $\mathbb{Z}_r^\times$ with $\#\mathcal{K} = k$, and

$$\alpha = \sum_{a \in \mathcal{K}} \beta^a. \tag{1}$$

Then α is called a *prime Gauß period of type* (n, k) over $\mathbb{F}_q$.

In this situation we have $\alpha \in \mathbb{F}_{q^n}$, and α is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $\gcd(e, n) = 1$, where e is the index of q modulo r. Starting with [8], this construction has been used to find normal bases, in particular the so-called optimal normal bases; see also [5]. Optimal normal bases using Gauß periods have been generalized in [1] (for $q = 2$), and studied in [10], [7], Chapter 5, and [3]. The latter paper reconciles asymptotically fast arithmetic with normal bases; the cost for arithmetic in $\mathbb{F}_{q^n}$ then depends not only on q and n but also on k.

1991 *Mathematics Subject Classification.* Primary 11T22, secondary 11R18, 12E20, 12F10, 68Q4.

So it is important to find a value for k that is as small as possible. This leads to the following definition:

Definition 1.1. *A pair (n,k) is called a* prime Gauß pair *over $\mathbb{F}_q$ if and only if the prime Gauß period of type (n,k) is a normal element in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We define*

$$\kappa_p(q,n) = \begin{cases} \min k & (n,k) \text{ is a prime Gauß pair over } \mathbb{F}_q, \text{ if such a } k \text{ exists,} \\ \infty & \text{if no such } k \text{ exists.} \end{cases}$$

(The subscript p stands for "prime"). Unfortunately, $\kappa_p(q,n)$ is not always small, and in fact it is sometimes not finite.

Fact 1.2. *(Wassermann* [10]*, Theorem 3.3.4.) Let $p = \mathrm{char}(\mathbb{F}_q)$, $q = p^m$ and $n \in \mathbb{N}$ positive. Then $\kappa_p(q,n) < \infty$ if and only if the following conditions hold:*

(i) $\gcd(m,n) = 1$,
(ii) $4p \nmid n$ *or* $(2p \nmid n$ *and* $p \equiv 1 \bmod 4)$.

Gauß indicated in Article 356 of his *Disquisitiones Arithmeticae* that the construction of Gauß periods might be extended from primes r to arbitrary positive integers. He says: *"Ceterum observamus* [...] *haecce theoremata salva vel potius aucta elegantia sua etiam ad valores quosvis compositos ipsius n extendi posse: sed de his rebus, quae altioris sunt indaginis, hoc loco tacere earumque considerationem ad aliam occasionem nobis reservare oportet."*[1]

It was a well-known habit of Gauß to keep his results to himself rather than to publish them, often to the dismay of his contemporaries who would visit him to explain their great new result only to have Gauß pull it from a drawer. We could not find in the literature "another occasion" where he published his "more elegant theorems."
In this paper we present a generalization of Gauß periods which yields better results in the following sense, for some q:

- There are Gauß pairs (n,k) in the new sense with $k < \kappa_p(q,n)$. Some examples are given in Table 2.
- There are Gauß pairs (n,k) in the new sense where $\kappa_p(q,n) = \infty$; see Table 1.

[1]Besides, we observe that these theorems can with undiminished or even greater elegance be extended to arbitrary composite integers n; but about these matters, which are at a higher level of research, it is appropriate to be silent in this place and to reserve their discussion to another occasion. [Gauß' n corresponds to our r as above.]

In Section 2 we generalize the definition of a Gauß period in finite fields, and state our Main Theorem which gives a necessary and sufficient condition for a Gauß period to be normal. Sections 3 through 5 contain the proof of the Main Theorem. In Section 3 we derive normal bases in finite fields from global normal bases in cyclotomic fields. In Section 4 we exhibit normal p-integral elements in cyclotomic fields and in Section 5 we prove our Main Theorem. In the last section we discuss some experimental results showing the scope of improvement over the previous construction.
Our Main Theorem is a statement about a construction in finite fields. The necessity of the condition can be proven by working in finite fields alone, but we do not have this type of proof for its sufficiency; rather, we make use of global considerations in certain algebraic number fields.

2. Generalization of Gauss periods

The construction of the Introduction, with a prime r, generalizes as follows:
For a prime ℓ and a nonzero integer r we define $\nu_\ell(r)$ as the maximum number f such that ℓ^f divides r. The *squarefree part* of an integer r is the product of all primes ℓ such that $\nu_\ell(r) = 1$.

Definition 2.1. *Let $n, k, r \in \mathbb{N}$ be positive integers such that $\varphi(r) = nk$. Write r as $r = r_1 r_2$ where r_1 is the squarefree part of r, and set*

$$g(x) = x^{r_2} \prod_{\ell \mid r_2} \sum_{1 \le i \le \nu_\ell(r_2)} x^{r\ell^{-i}} \in \mathbb{Z}[x].$$

Let q be a prime power with $\gcd(q, r) = 1$, let $\beta \in \mathbb{F}_{q^{nk}}$ be a primitive rth root of unity, and $\mathcal{K}$ a subgroup of $\mathbb{Z}_r^\times$ of order k. The Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$ is defined as

$$\alpha = \sum_{a \in \mathcal{K}} g(\beta^a).$$

The parameter r on which α also depends is not made explicit; $\mathcal{K}$ is a subgroup of $\mathbb{Z}_r^\times$.

If r is squarefree, i.e., $r_2 = 1$ in the above notation, then $g(x) = x$ and now $\alpha = \sum_{a \in \mathcal{K}} \beta^a$ is called a *squarefree Gauß period* and is of the same form as the prime Gauß period in (1). For a prime r the above definition is thus equivalent to the one in (1). In this case the group $\mathbb{Z}_r^\times$ is cyclic, hence has for each divisor of $\varphi(r) = r - 1$ exactly one subgroup of that order.

Example 2.2. *Let $q = 2, n = 20, k = 2, r = 55$. Then $\varphi(r) = 40 = 2 \cdot 20 = k \cdot n$. The group $\mathbb{Z}_r^\times$ has three subgroups of order k, namely:*

$$\mathcal{K}_1 = \{1, 21\}, \quad \mathcal{K}_2 = \{1, 54\}, \quad \text{and} \quad \mathcal{K}_3 = \{1, 34\}.$$

As we will see in Example 6.2, the resulting Gauß periods are not equivalent. In fact, only the first two of them yield a normal basis in $\mathbb{F}_{2^{20}}$ over $\mathbb{F}_2$.

The following is the main result of this paper and will be proved in Section 5.

Main Theorem. *A Gauß period of type $(n, \mathcal{K})$ is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$.*

We can use this theorem to construct normal elements in finite fields, as is shown in the following examples.

Example 2.3. (1) *Let β be a primitive 9th root of unity over $\mathbb{F}_2$. We apply the theorem with $q = 2$, $r = 9$, and $n = 6$. Since $\langle 2\rangle = \mathbb{Z}_9^\times$, the element $\beta + \beta^3$ is a normal element of $\mathbb{F}_{2^6}$ over $\mathbb{F}_2$.*

(2) *Let $r = 25$. The order of 3 modulo 25 equals $20 = \varphi(25)$. Let $\mathcal{K}$ be the subgroup of order two of $\mathbb{Z}_{25}^\times$, i.e., $\mathcal{K} = \{1, -1\}$. Then $\langle 3, \mathcal{K}\rangle = \mathbb{Z}_{25}^\times$. Applying the theorem with $n = 10$ and $q = 3$ shows that $\beta + \beta^{-1} + \beta^5 + \beta^{-5}$ is a normal element of $\mathbb{F}_{3^{10}}$ over $\mathbb{F}_3$, if $\beta \in \mathbb{F}_{3^{20}}$ is a primitive 25th root of unity.*

One might consider applying (1) for an arbitrary r. In Theorem 5.2 we show that in order to yield a normal element, r then has to be squarefree.
The necessity of the condition given in the Main Theorem is easy to prove.

Lemma 2.4. *With the notation of Definition 2.1, we have $\alpha \in \mathbb{F}_{q^s}$, where s is the multiplicative order of q modulo $\mathcal{K}$. In particular, if $\langle q, \mathcal{K}\rangle \neq \mathbb{Z}_r^\times$, then α is not normal.*

Proof. Our assumptions imply that $(q^s \bmod r) \in \mathcal{K}$. For the first claim, it is sufficient to show $\alpha^{q^s} = \alpha$:

$$\alpha^{q^s} = \left(\sum_{a\in\mathcal{K}} g(\beta^a)\right)^{q^s} = \sum_{a\in\mathcal{K}} g(\beta^{aq^s}) = \sum_{a\in\mathcal{K}} g(\beta^a) = \alpha,$$

by the above. The order s of q modulo $\mathcal{K}$ equals $\#\langle q, \mathcal{K}\rangle/k$, since $\langle q, \mathcal{K}\rangle$ is a disjoint union of $q^i\mathcal{K}$ for $0 \le i < s$. In particular, if $\langle q, \mathcal{K}\rangle \neq \mathbb{Z}_r^\times$, then s is less than n, and α is not normal. □

The next lemma says that although α may depend on the choice of β as a primitive rth root of unity, the normal basis generated by α is independent up to a cyclic shift.

Lemma 2.5. *Let $\beta, \beta' \in \mathbb{F}_{q^{nk}}$ be two primitive rth roots of unity, and $\alpha, \alpha' \in \mathbb{F}_{q^n}$ the corresponding Gauß periods. If $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$, then α and α' are conjugate over $\mathbb{F}_q$.*

Proof. There exists an s with $1 \leq s < m$, $\gcd(s, m) = 1$, and $\beta' = \beta^s$. Since $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$, there exists a $j \in \{0, \ldots, n-1\}$ with $s \in q^j \mathcal{K}$. Thus

$$\alpha' = \sum_{a \in \mathcal{K}} g(\beta'^a) = \sum_{a \in \mathcal{K}} g(\beta^{as}) = \sum_{a \in \mathcal{K}} g(\beta^{aq^j}) = \left(\sum_{a \in \mathcal{K}} g(\beta^a) \right)^{q^j} = \alpha^{q^j},$$

and α and α' are conjugate. □

For the proof of the Main Theorem we have to leave in the next sections the realm of finite fields and work in algebraic number fields. This is, of course, Gauß' original setting for his periods.

3. Modular Normal Bases from Global Normal Bases

In this section we discuss conditions under which reductions modulo prime ideals of normal elements in number fields (*global* normal elements) yield normal elements in finite fields (*modular* normal elements). In the sequel we will use several well-known results from algebraic number theory. Proofs of these results can be found in the first chapter of Lang's book [6].

Let L be a Galois extension of $\mathbb{Q}$ with Galois group G, and let $\alpha \in L$ be a normal element, i.e., the Galois conjugates of α generate L as a vector space over $\mathbb{Q}$. Let $\mathcal{O}_L$ denote the ring of integers of L. For a rational prime p the ideal $p\mathcal{O}_L$ decomposes into a product $(\mathfrak{p}_1 \cdots \mathfrak{p}_r)^e$, where each $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_L$ and has the same residue class degree $f = f(\mathfrak{p}_i/p)$, i.e., $\#(\mathcal{O}_L/\mathfrak{p}_i) = p^f$. Furthermore, $efr = [L : \mathbb{Q}]$. The prime p is called *unramified* if $e = 1$, and it is called *inert* if $e = r = 1$, i.e., if $f = [L : \mathbb{Q}]$.

We fix a prime divisor $\mathfrak{p}$ of $p\mathcal{O}_L$. (We call $\mathfrak{p}$ a prime divisor of p in the sequel.) We would like to obtain conditions under which ($\alpha \bmod \mathfrak{p}$) is a normal element of $\mathbb{F}_{p^f}$. We will first study when the set $\{\alpha^g \bmod \mathfrak{p} \colon g \in G\}$ generates $\mathbb{F}_{p^f}$, for which some preliminaries are needed.

Recall that $\mathcal{O}_L$ is a free $\mathbb{Z}$-module. Any basis of this $\mathbb{Z}$-module is called an *integral basis* of L. The localization of $\mathbb{Z}$ at a prime p is denoted by $\mathbb{Z}_{(p)}$. In other words, $\mathbb{Z}_{(p)} = (\mathbb{Z} \setminus p\mathbb{Z})^{-1}\mathbb{Z}$. The localization of the

$\mathbb{Z}$-module $\mathcal{O}_L$ at p is then $\mathcal{O}_{L,p} = \mathbb{Z}_{(p)}\mathcal{O}_L$. Obviously, $\mathcal{O}_{L,p}$ is a ring, and any integral basis of L forms a basis of this free $\mathbb{Z}_{(p)}$-module.

Definition 3.1. *An integral element $\alpha \in L$ is called* normal p-integral *if it is normal and if $\mathcal{O}_{L,p} = \bigoplus_{g\in G} \mathbb{Z}_{(p)}\alpha^g$; α is called* normal integral *if it is normal p-integral for all primes p, i.e., $\mathcal{O}_L = \bigoplus_{g\in G} \mathbb{Z}\alpha^g$.*

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_L$ of residue class degree f. Our first aim is to show that the set $\{\alpha^g \bmod \mathfrak{p} : g \in G\}$ generates $\mathbb{F}_{p^f}$ as an $\mathbb{F}_p$-vector space if α is normal p-integral. For the following remark, note that if I is any ideal of $\mathcal{O}_L$, then $I\mathcal{O}_{L,p}$ is an ideal of $\mathcal{O}_{L,p}$.

Remark 3.2. *We have a canonical isomorphism $\mathcal{O}_{L,p}/\mathfrak{p}\mathcal{O}_{L,p} \simeq \mathcal{O}_L/\mathfrak{p}$ of rings, for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$.*

Proof. Let $\varphi\colon \mathcal{O}_L/\mathfrak{p} \to \mathcal{O}_{L,p}/\mathfrak{p}\mathcal{O}_{L,p}$ be the map sending $r + \mathfrak{p}$ to $r + \mathfrak{p}\mathcal{O}_{L,p}$. The map is well-defined, as $\mathfrak{p} \subset \mathfrak{p}\mathcal{O}_{L,p}$. To show surjectivity, let $r \in \mathcal{O}_{L,p}$. Then there is an integer N prime to p such that $r = r'/N$, for some $r' \in \mathcal{O}_L$. Let s be an integer congruent to $1/N$ modulo p. Then $\varphi(sr') = r + \mathfrak{p}\mathcal{O}_{L,p}$, and we are done. □

The last remark and the fact that $z \bmod \mathfrak{p}$ lies in $\mathbb{F}_p$ for all $z \in \mathbb{Z}$ immediately imply the following.

Corollary 3.3. *If α is a normal p-integral element of L, then $\{\alpha^g \bmod \mathfrak{p} : g \in G\}$ generates the residue class field of $\mathfrak{p}$ over $\mathbb{F}_p$.*

Normal p-integral elements can be characterized in an alternative way.

Proposition 3.4. *An element $\alpha \in L$ is normal p-integral if and only if it is integral, normal, and for any integral basis $(\gamma_1, \ldots, \gamma_n)$ of L there exist $a_{i,g} \in \mathbb{Z}_{(p)}$ such that $\gamma_i = \sum_{g\in G} a_{i,g}\alpha^g$ for all i.*

Proof. We only need to prove the "if" part. Integrality and normality of α imply that $\bigoplus \mathbb{Z}_{(p)}\alpha^g \subseteq \mathcal{O}_{L,p} = \bigoplus \mathbb{Z}_{(p)}\gamma_i$. The other assumption implies that $\mathcal{O}_{L,p} \subseteq \bigoplus \mathbb{Z}_{(p)}\alpha^g$, and we are done. □

The Galois group G of L over $\mathbb{Q}$ contains an element $\phi = \phi_{\mathfrak{p}}$ such that $\phi(x) \equiv x^p \bmod \mathfrak{p}$ for all $x \in \mathcal{O}_L$. It is uniquely determined if p is unramified. Changing from $\mathfrak{p}$ to another prime divisor of p results in conjugation of ϕ by an element of G. Hence, if G is Abelian (which will be the case in our application), then ϕ only depends on p, and we call it the *global Frobenius automorphism* of p. There is an epimorphism from G to the Galois group of $\mathbb{F}_{p^f}/\mathbb{F}_p$, which maps ϕ to the Frobenius automorphism of the finite field extension. As a result, p is inert if and only if G is cyclic (and hence is generated by ϕ), in which case the sets $\{\alpha^g \bmod \mathfrak{p} : g \in G\}$ and $\{(\alpha \bmod \mathfrak{p})^{p^k} : k = 0, \ldots, f-1\}$ coincide. So, we obtain the following result.

Proposition 3.5. *Let α be a normal p-integral element of the Abelian Galois extension L of $\mathbb{Q}$ in which p is inert. Then the reduction $\overline{\alpha}$ of α modulo the prime ideal $p\mathcal{O}_L$ of $\mathcal{O}_L$ is a normal element of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, where $n = [L : \mathbb{Q}]$.*

In our applications we will obtain normal p-integral elements of L as the trace over L of normal p-integral elements of an extension K of L. The following result shows that these traces are normal p-integral in L.

Proposition 3.6. *Suppose that α is a normal p-integral element of the Galois number field K, and that L is a subfield of K which is Galois over $\mathbb{Q}$. Then the trace of α over L is a normal p-integral element of L.*

Proof. The relevant rings are:

$$\begin{array}{ccccc} \mathcal{O}_K & \subseteq & \mathcal{O}_{K,p} & \subseteq & K \\ | & & | & & |_H \\ \mathcal{O}_L & \subseteq & \mathcal{O}_{L,p} & \subseteq & L \\ | & & | & & |_{G/H} \\ \mathbb{Z} & \subseteq & \mathbb{Z}_{(p)} & \subseteq & \mathbb{Q} \end{array}$$

Since the trace β of α over L is the sum of certain conjugates of α and α is normal in K over $\mathbb{Q}$, it follows that the conjugates of β are linearly independent over $\mathbb{Q}$, and hence that β is normal in L over $\mathbb{Q}$. It remains to show that the conjugates of β under the Galois group of L over $\mathbb{Q}$ form a basis of the $\mathbb{Z}_{(p)}$-module $\mathcal{O}_{L,p}$. We first show that $\mathcal{O}_{L,p}$ is the intersection of $\mathcal{O}_{K,p}$ and L: notice that $\mathcal{O}_L = \mathcal{O}_K \cap L$, hence $\mathcal{O}_{L,p} \subseteq \mathcal{O}_{K,p} \cap L$. Conversely, let $\alpha = \sum a_i\gamma_i \in \mathcal{O}_{K,p}$, where $\gamma_1, \ldots, \gamma_n$ form an integral basis of K, and $a_i \in \mathbb{Z}_{(p)}$. Then $\alpha = \alpha'/N$ for some integer N coprime to p and some $\alpha' \in \mathcal{O}_K$. $\alpha \in L$ implies that $\alpha' \in L$, hence $\alpha' \in \mathcal{O}_L$, which shows that $\alpha = \alpha'/N \in \mathcal{O}_{L,p}$. Thus, $\mathcal{O}_{L,p} = \mathcal{O}_{K,p} \cap L$, and it suffices to show that any element in $\mathcal{O}_{K,p}$ which is invariant under $H := \mathrm{Gal}(K/L)$ is a $\mathbb{Z}_{(p)}$-linear combination of β^g, where g runs over a complete set of representatives of the cosets of $\mathrm{Gal}(K/\mathbb{Q})$ modulo H. Any element of $\mathcal{O}_{K,p}$ can be represented as $a = \sum_{g\in G} a_g\alpha^g$ for some $a_g \in \mathbb{Z}_{(p)}$. For any $\tau \in G$ we have that $a^\tau = \sum_g a_{g\tau^{-1}}\alpha^g$. As a result, a is invariant under H if and only if a_g is constant on cosets of H, i.e., if and only if a is a $\mathbb{Z}_{(p)}$-linear combination of β^g, where g runs over a complete set of representatives of G modulo H. □

The following is the main theorem of this section. The next section will contain applications of this result in the case of cyclotomic fields.

Theorem 3.7. *Let $K \supset L \supset \mathbb{Q}$ be Abelian Galois extensions of $\mathbb{Q}$, α be a normal p-integral element of K over $\mathbb{Q}$, and p be a prime with global Frobenius automorphism $\phi \in \mathrm{Gal}(K/\mathbb{Q})$. If $\langle \phi, \mathrm{Gal}(K/L)\rangle = \mathrm{Gal}(K/\mathbb{Q})$, then p is inert in L, and the reduction $\overline{\beta}$ of the trace β of α over L modulo the prime ideal $p\mathcal{O}_L$ of L is a normal element in $\mathbb{F}_{p^n}$, where $n = [L : \mathbb{Q}]$.*

Proof. By Propositions 3.5 and 3.6 we know that if p is inert in L, then $\overline{\beta}$ has the required property. Thus, we only need to show that the group theoretic criterion stated above implies that p is inert in L. This happens if and only if the Frobenius automorphism ϕ' of p in L generates the Galois group of L over $\mathbb{Q}$. But $\phi' = \phi|_L$, and its image in the isomorphic copy $\mathrm{Gal}(K/\mathbb{Q})/\mathrm{Gal}(K/L)$ of $\mathrm{Gal}(L/\mathbb{Q})$ equals $\phi\mathrm{Gal}(K/L)$. Hence, p is inert if and only if $\langle \phi\mathrm{Gal}(K/L)\rangle = \mathrm{Gal}(L/\mathbb{Q})$. A simple manipulation yields the result. □

Our main application of the previous theorem is to the case where K is a cyclotomic field. Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive rth root of unity. The Galois group of K over $\mathbb{Q}$ is canonically isomorphic to $\mathbb{Z}_r^\times$, where the isomorphism sends the residue class of c modulo r to the automorphism mapping ζ to ζ^c. A prime p is unramified in K if and only if p does not divide r. In that case the Frobenius automorphism ϕ of p is given by $\phi\colon \zeta \to \zeta^p$, which corresponds to the residue class of p modulo r in $\mathbb{Z}_r^\times$. Hence we have the following result.

Corollary 3.8. *Let $r \in \mathbb{N}$ be positive, ζ be a primitive rth root of unity over $\mathbb{Q}$, $K = \mathbb{Q}(\zeta)$, and α be a normal p-integral element in K for some prime p not dividing r. Let L be a subfield of K and $H = \mathrm{Gal}(K/L)$. If $\langle p, H\rangle = \mathbb{Z}_r^\times$, then the ideal $p\mathcal{O}_L$ of $\mathcal{O}_L$ is prime and the reduction $\overline{\beta}$ of the trace β of α over L modulo $p\mathcal{O}_L$ is a normal element of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, where $n = [L : \mathbb{Q}]$.*

4. Normal p-integral elements in cyclotomic fields

In this section we exhibit explicit normal p-integral elements in a cyclotomic field generated by a primitive rth root of unity. We call r the *conductor* of the field in the sequel. Reductions of these elements give normal elements in finite extensions of $\mathbb{F}_p$ via an application of Corollary 3.8.

In a first step we show how to construct normal p-integral elements in the compositum of two linearly disjoint number fields. We will need the following result, a proof of which can be found in [6].

Fact 4.1. *Let K and L be two linearly disjoint number fields over $\mathbb{Q}$ whose discriminants are relatively prime. Then the ring of integers $\mathcal{O}_{KL}$ of KL equals $\mathcal{O}_K\mathcal{O}_L$.*

Proposition 4.2. *Suppose that L and K are linearly disjoint Galois number fields, and that α and β are normal p-integral elements of L and K, respectively, for some prime $p \in \mathbb{N}$. Then $\alpha\beta$ is a normal p-integral element of KL. If α and β are normal integral, then so is $\alpha\beta$.*

Proof. The Galois group of KL over $\mathbb{Q}$ is canonically isomorphic to the direct product of the Galois groups of K and L over $\mathbb{Q}$, and hence $\alpha\beta$ is a normal element of KL. To prove p-integrality, it is sufficient to show that $\alpha\beta$ is integral, and that any integral basis of KL can be represented by $\mathbb{Z}_{(p)}$-linear combinations of conjugates of $\alpha\beta$, see Proposition 3.4. Let $(b_1, \ldots, b_s)$ and $(c_1, \ldots, c_t)$ be integral bases of L and K respectively, and let A and B be the transformation matrices from the normal bases induced by α and β to these integral bases. By Fact 4.1 the basis $D := (b_i c_j : i, j)$ is an integral basis of KL, which, in particular, shows that $\alpha\beta$ is integral. A simple calculation shows that the transformation matrix from the normal basis induced by $\alpha\beta$ to D is the Kronecker product $A \otimes B$, hence has coefficients in $\mathbb{Z}_{(p)}$. If A and B have coefficients in $\mathbb{Z}$, then so does $A \otimes B$. □

Two cyclotomic fields are linearly disjoint over $\mathbb{Q}$ if and only if their conductors are relatively prime. Since the primes dividing the discriminant of a cyclotomic field always divide the conductor, we see that two such fields with relatively prime conductors are linearly disjoint *and* have relatively prime discriminants. Thus, in view of the last proposition we only need to find normal p-integral elements in cyclotomic fields with prime power conductor. This will be done in Proposition 4.4, for which we need an auxiliary result.

Lemma 4.3. *Let ℓ be a prime, t and s be nonnegative integers with $s < t$, ζ be a primitive ℓ^t-th root of unity, and η be a primitive ℓ^s-th root of unity. Then the trace of ζ in $\mathbb{Q}(\eta)$ is zero if $t \neq 1$ and is -1 if $t = 1$.*

Proof. Suppose first that $s \geq 1$. Then the trace $T(\zeta)$ of ζ equals $\sum_c \zeta^c$, where c runs over all integers between 1 and $\ell^t - 1$ such that $c \equiv 1 \bmod \ell^s$, since $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\eta))$ is isomorphic to the group formed by these c's. Each such c is of the form $k\ell^s + 1$, with k running from 0 to $\ell^{t-s} - 1$. Hence,

$$T(\zeta) = \zeta \sum_{0 \leq k < \ell^{t-s}} \zeta^{\ell^s k} = 0,$$

since ζ^{ℓ^s} is a primitive ℓ^{t-s}-th root of unity.
Suppose now that $s = 0$. If $t > 1$, then the trace of ζ over the field generated by a primitive ℓth root of unity is zero. (Choose $s = 1$ in the previous argument.) As a result, the absolute trace of ζ is zero as well. If $t = 1$, then it is straightforward to check that the trace of ζ equals -1. □

Proposition 4.4. *Let ℓ be a prime, t be a positive integer, and ζ be a primitive ℓ^t-th root of unity. The element*

$$\zeta + \zeta^{\ell} + \cdots + \zeta^{\ell^{t-1}}$$

is a normal p-integral element of $\mathbb{Q}(\zeta)$ for any prime $p \neq \ell$. If $t = 1$, then this element equals ζ and is a normal integral element of $\mathbb{Q}(\zeta)$.

Proof. Let γ denote the element in question. It suffices to represent 1 and all ζ^{ℓ^i} as $\mathbb{Z}_{(p)}$-linear combinations of conjugates of γ. In fact, taking Galois-conjugates this implies that all powers of ζ are $\mathbb{Z}_{(p)}$-linear combinations of conjugates of γ, and we can apply Proposition 3.4. (Note that any power of ζ is a Galois-conjugate of ζ^{ℓ^i} for some i.)
For $c \in \mathbb{Z}_{\ell^t}^{\times}$ we write γ^c for the image of γ under the automorphism corresponding to c. Furthermore, $\sum'$ denotes a sum in which the summation index is supposed to be relatively prime to ℓ and to lie between 1 and $\ell^t - 1$. Let us first compute $\sum'_c \gamma^c$: by Lemma 4.3, for $0 \leq k < t-1$, the sum $\sum'_c \zeta^{\ell^k c}$ vanishes, since it is a multiple of the absolute trace of a ℓ^{t-k}-th root of unity. If $k = t-1$, then this sum is ℓ^{t-1} times the trace of a primitive ℓ-th root of unity regarded as an element of $\mathbb{Q}(\zeta)$, hence equals $-\ell^{t-1}$. Thus, $1 = -\sum'_c \gamma^c / \ell^{t-1}$ is representable as a $\mathbb{Z}_{(p)}$-linear combination of conjugates of γ.
Now consider $\sum'_{c \equiv 1 \bmod \ell} \gamma^c$. By Lemma 4.3 we have $\sum'_{c \equiv 1 \bmod \ell} \zeta^{\ell^k c} = 0$ if $k \neq t-1$. If $k = t-1$, then this sum simply equals $\ell^{t-1} \zeta^{\ell^{t-1}}$, which shows that $\zeta^{\ell^{t-1}}$ is representable as a linear combination of conjugates of γ with coefficients 0 and $1/\ell^{t-1}$. Considering the sums $\sum_{c \equiv 1 \bmod \ell^s} \gamma^c$ with $s = 1, \ldots, \ell^{t-1}$, the same reasoning shows that $\zeta^{\ell^{t-s}}$ is representable as a linear combination of conjugates of γ with coefficients in $\mathbb{Z}_{(p)}$.
If $t = 1$, then $\ell^{t-1} = 1$, and $\gamma = \zeta$ is in fact normal integral. □

Combining the last two propositions we obtain the following result.

Theorem 4.5. *Let $r = r_1 r_2$ be a positive integer with squarefree part r_1, and let ζ be a primitive rth root of unity. Then the element*

$$\zeta^{r_2} \prod_{\ell \mid r_2} \sum_{1 \leq i \leq \nu_\ell(r_2)} \zeta^{r\ell^{-i}}$$

is a normal p-integral element of $\mathbb{Q}(\zeta)$ for any prime p such that p^2 does not divide r. It is normal integral if r is squarefree.

Proof. In the following, ℓ is a parameter ranging over the prime numbers. The integer $u = \sum_{\ell | r_1} r_1/\ell$ is a unit modulo r_1. Let v be a positive integer such that $uv \equiv 1 \bmod r_1$. If $\ell | r_1$, then $\zeta^{r/\ell}$ is a primitive ℓth root of unity, and normal integral by Proposition 4.4. The same is true for $\zeta^{rv/\ell}$. Applying Proposition 4.2 repeatedly, and noting that two cyclotomic fields with relatively prime conductors are linearly disjoint, we find that

$$\prod_{\ell | r_1} \zeta^{rv/\ell} = \zeta^{r_2 uv} = \zeta^{r_2}$$

is normal integral in $\mathbb{Q}(\zeta^{r_2})$.
Now, if $\ell | r_2$, then $\sum_{1 \le i \le \nu_\ell(r)} \zeta^{r\ell^{-i}}$ is normal p-integral in $\mathbb{Q}(\zeta^{r\ell^{-\nu_\ell(r)}})$ for any $p \neq \ell$. Hence, it is normal p-integral for any prime p such that p^2 does not divide r. Applying Proposition 4.2 again, we obtain the assertion. □

Example 4.6. *Suppose that $\zeta \in \mathbb{C}$ is a primitive 180th root of unity. Then*

$$\zeta^{36}(\zeta^{45} + \zeta^{90})(\zeta^{20} + \zeta^{60})$$

is a normal p-integral element of $\mathbb{Q}(\zeta)$ for any $p \neq 2, 3$.

We close this section by remarking that we cannot expect to obtain normal integral elements in cyclotomic fields of squarefull conductors. The reason for this is that there exist primes p with wild ramification in these fields. By a theorem of E. Noether [9] there do not exist normal integral elements in any $\mathfrak{p}$-adic completion of these fields, where $\mathfrak{p}$ is a prime divisor of p. More generally, Abelian number fields with squarefull conductors do not possess normal integral elements for the same reason.

5. Normal modular Gauss periods

Proof of the Main Theorem. Let η denote the element $\sum_{a \in \mathcal{K}} g(\beta^a)$. Since the condition $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$ is necessary for η to be a normal element in $\mathbb{F}_{q^n}$ by Lemma 2.4, we only need to show the sufficiency of this condition. In case $q = p$ is a prime, the assertion follows immediately from Corollary 3.8 and Theorem 4.5. Suppose now that $q = p^m$ and that $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$. The order of q mod $\mathcal{K}$ equals $b/\gcd(b, m)$, where b is the order of p mod $\mathcal{K}$. Hence, $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$ implies that $\gcd(b, m) = 1$, and $b = n$. So $\langle p, \mathcal{K} \rangle = \mathbb{Z}_r^\times$, which implies that η is a normal element of $\mathbb{F}_{p^n}$ by the first part of this proof. As $\gcd(m, n) = 1$, the fields $\mathbb{F}_{p^n}$

and $\mathbb{F}_q$ are linearly disjoint over $\mathbb{F}_p$. As a result, the conjugates of η are linearly independent over $\mathbb{F}_q$ since they are linearly independent over $\mathbb{F}_p$, which shows that η is normal over $\mathbb{F}_q$. □

The Main Theorem shows that a squarefree Gauß period of type $(n, \mathcal{K})$ is always normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$if $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$.
Can we expect an element of the form $\sum_{a\in\mathcal{K}} \beta^a$ to be normal even if r is not squarefree?
The answer is no, and the reason is as follows: if r is not squarefree, then the trace of such an element over $\mathbb{F}_q$ is zero. In particular, the conjugates of this period are not linearly independent. To prove this, we use a detour via cyclotomic fields. Recall the Möbius function μ defined by $\mu(1) = 1$, $\mu(n) = 0$ if n is not squarefree, and $\mu(n) = (-1)^t$ if n is squarefree and has exactly t prime divisors.

Lemma 5.1. *The trace in $\mathbb{Q}$ of a primitive rth root of unity equals $\mu(r)$.*

Proof. Let ζ be a primitive rth root of unity, $G = \mathbb{Z}_r^\times$ the Galois group of $K = \mathbb{Q}(\zeta)$ over $\mathbb{Q}$, so that $f(r) = \sum_{c\in G} \zeta^c$ is the trace of ζ. Then $g(r) = \sum_{d|r} f(d)$ is the sum over all dth roots of unity, which is 1 if $r = 1$ and 0 otherwise. Möbius inversion yields $f(r) = \mu(r)$. □

This result together with the Main Theorem and Lemma 2.4 implies the following.

Theorem 5.2. *With the above notation, a Gauß period of the form $\alpha = \sum_{a\in K} \beta^a$ is a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$ and r is squarefree.*

6. Some Experiments

As in the case of prime Gauß periods, we want to determine for given n and q the lowest value for k such that a normal Gauß period of type $(n, \mathcal{K})$, where $\#\mathcal{K} = k$, exists over $\mathbb{F}_q$:

Definition 6.1. *A pair $(n, \mathcal{K})$ is called a (squarefree)* Gauß pair *if and only if the (squarefree) Gauß period of type $(n, \mathcal{K})$ is a normal element in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$; "squarefree" means that r is squarefree. We define*

$$\kappa_s(q, n) = \begin{cases} \min k & (n, \mathcal{K}) \text{ is a squarefree Gauß pair with } \#\mathcal{K} = k, \\ & \text{if such a } \mathcal{K} \text{ exists,} \\ \infty & \text{if no such } \mathcal{K} \text{ exists,} \end{cases}$$

$$\kappa_g(q,n) = \begin{cases} \min k & (n,\mathcal{K}) \text{ is a Gauß pair with } \#\mathcal{K} = k, \\ & \text{if such a } \mathcal{K} \text{ exists,} \\ \infty & \text{if no such } \mathcal{K} \text{ exists.} \end{cases}$$

The subscripts s and g stand for "squarefree" and "general", respectively. Obviously, we have $\kappa_g(q,n) \le \kappa_s(q,n) \le \kappa_p(q,n)$ for all q and n, see Definition 1.1. We now will see that sometimes $\kappa_g(q,n) < \kappa_p(q,n)$.

Example 6.2. *Let $q = 2$ and $n = 20$. Then $\kappa_p(2,20) = 3 > \kappa_s(2,20) = 2 > \kappa_g(2,20) = 1$. Namely, for the squarefree Gauß period we take $r = 55$, and the three subgroups from Example 2.2. Now $2^{10} \equiv 34 \bmod 55$ and $34^2 \equiv 1 \bmod 55$, 2 generates a subgroup of order 20, and $\langle 2,\mathcal{K}_1\rangle = \langle 2,\mathcal{K}_2\rangle = \mathbb{Z}_{55}^\times$, but $\langle 2,\mathcal{K}_3\rangle = \langle 2\rangle \ne \mathbb{Z}_{55}^\times$. Thus we have normal elements of type $(20,\mathcal{K}_1)$ and $(20,\mathcal{K}_2)$ of $\mathbb{F}_{2^{20}}$ over $\mathbb{F}_2$. In particular, $\kappa_s(2,20) \le 2$, and equality holds, since 2 is not primitive modulo 21, and hence $\kappa_s(2,20) \ne 1$.*
For the general Gauß period we consider $r = 25$, which is coprime to 2. Then $\phi(r) = 20$ and with $n = 20$ and $k = 1$ we have found a normal Gauß period of type $(20,\{1\})$. Hence, $\kappa_g(2,20) = 1$.

More examples for $q = 2$ are exhibited in Table 2. The $\square$ in all tables indicates that the corresponding r is not squarefree. Tables for prime Gauß periods are in [8], [1], and [4].
Gauß periods also yield normal bases in situations where $\kappa_p(q,n) = \infty$. Table 1 shows all such values for which $q \in \{3,5,7,11\}$ and $2 \le n \le 100$. More generally, Gao [2] has shown that the values where $\kappa_s(q,n) < \infty$ are exactly the following:

(i) $\gcd(m,n) = 1$, where $q = p^m$ and $p = \mathrm{char}(\mathbb{F}_q) \ne 2$,
(ii) $8 \not| n$ for $\mathrm{char}(\mathbb{F}_q) = 2$.

So, compared to Fact 1.2, we have $\kappa_s(q,n) < \infty$ for $q \ne 2$ in many more cases than in the prime case. Unfortunately, no such improvement occurs in characteristic 2.
Tables 3 and 4 show the improvements for $q = 3$ and $q = 5$, respectively. For $q = 2$, we have 96 values of n between 2 and 400 with $\kappa_g(q,n) < \kappa_p(q,n)$. For $q = 3$, there are 126, and for $q = 5$ there are 120 such values, i.e., more than 25% which yield a better result. The largest improvement we found is $\kappa_p(5,272)/\kappa_g(5,272) = 23$.
The (geometric) average improvement ratio for $2 \le n \le 400$ is 1.49 for $q = 2$ (including the cases where $\kappa_p(q,n)=\kappa_g(q,n)$), while for $q = 3$ and $q = 5$ the (geometric) average ratios are 1.44 and 1.45, respectively. In the latter two cases we only consider values of n for which $\kappa_p(q,n) < \infty$.

7. Acknowledgments

Part of the research on this paper was done while the second author was visiting the International Computer Science Institute in Berkeley whose hospitality is gratefully acknowledged. The research of the third author was funded by a Habilitationsstipendium of the Deutsche Forschungsgemeinschaft, Grant Sh-57/1. Many thanks go to Hendrik W. Lenstra, Jr., and Tomas Sander for very helpful conversations.
Different preliminary versions of this paper appeared as Technical Report tr-ri-96-177 at University of Paderborn and as Technical Report TR-97-020 at ICSI Berkeley.

Table 1: Gauß periods for $q \in \{3, 5, 7, 11\}$ and $2 \leq n \leq 100$ with $\kappa_p(q, n) = \infty$:

q	n	r		$\kappa_g(q, n)$	$\mathcal{K}$
3	12	35		2	{1, 6}
3	24	119		4	{1, 50, 69, 118}
3	36	95		2	{1, 56}
3	48	119		2	{1, 69}
3	60	155		2	{1, 61}
3	72	323		4	{1, 18, 305, 322}
3	84	203		2	{1, 146}
3	96	896	□	4	{1, 321, 575, 895}
5	10	33		2	{1, 10}
5	20	176	□	4	{1, 23, 65, 87}
5	30	77		2	{1, 76}
5	40	187		4	{1, 67, 120, 186}
5	50	303		4	{1, 10, 91, 100}
5	60	407		6	{1, 100, 175, 232, 307, 406}
5	70	473		6	{1, 122, 221, 252, 351, 472}
5	80	187		2	{1, 120}
5	90	297	□	2	{1, 109}
5	100	1616	□	8	{1, 111, 313, 495, 697, 807, 1009, 1415}
7	28	145		4	{1, 12, 133, 144}
7	56	493		8	{1, 86, 186, 220, 273, 307, 407, 492}
7	84	377		4	{1, 12, 144, 220}
11	44	368	□	4	{1, 137, 47, 183}
11	88	391		4	{1, 183, 254, 344}

Table 2: Improvements for $q = 2$ and $2 \leq n \leq 400$:

n	$\kappa_p(2,n)$	$\kappa_g(2,n)$	ratio	r		$\mathcal{K}$
6	2	1	2.0	9	□	{1}
20	3	1	3.0	25	□	{1}
21	10	2	5.0	49	□	{1, 48}
22	3	2	1.5	69		{1, 68}
27	6	2	3.0	81	□	{1, 80}
34	9	6	1.5	309		{1, 46, 47, 262, 263, 308}
42	5	2	2.5	147	□	{1, 146}
44	9	2	4.5	115		{1,91}
46	3	2	1.5	141		{1, 140}
54	3	1	3.0	81	□	{1}
55	12	2	6.0	121	□	{1, 120}
57	10	6	1.67	361	□	{ 1, 68, 69, 292, 293, 360}
68	9	6	1.5	515	□	{1, 46, 56, 356, 366, 411}
70	3	2	1.5	213		{1, 212}
75	10	8	1.25	707		{ 1, 111, 293, 302, 405, 414, 596, 706}
78	7	2	3.5	169		{1, 168}
84	5	2	2.5	203		{1, 202}
92	3	2	1.5	235		{1, 46}
102	6	2	3.0	309		{1, 308}
108	5	2	2.5	405	□	{1, 404}
110	6	1	6.0	121	□	{1}
111	20	8	2.5	1043		{1, 148, 342, 491, 552, 701, 895, 1042}
114	5	3	1.67	361	□	{1, 68, 292}
116	3	2	1.5	295		{1, 176}
123	10	4	2.5	581		{1, 167, 414, 580}
125	6	4	1.5	625	□	{1, 182, 443, 624}
132	5	2	2.5	299		{1, 298}
140	3	2	1.5	319		{1, 318}
145	10	4	2.5	649		{1, 296, 353, 648}
147	6	2	3.0	343	□	{1, 342}
150	19	4	4.75	707		{1, 302, 405, 706}
154	25	4	6.25	667		{1, 231, 505, 597}
156	13	1	13.0	169	□	{1}
159	22	4	5.5	749		{1, 106, 643, 748}
164	5	2	2.5	415		{1, 414}
166	3	2	1.5	501		{1, 500}
171	12	2	6.0	361	□	{1, 360}
190	10	2	5.0	573		{1, 190}

Table 2: Improvements for $q = 2$ and $2 \leq n \leq 400$:

n	$\kappa_p(2,n)$	$\kappa_g(2,n)$	ratio	r	$\mathcal{K}$
195	6	4	1.5	869	{1, 78, 791, 868}
198	22	2	11.0	437	{1, 436}
203	12	4	3.0	841 □	{1, 41, 800, 840}
204	3	2	1.5	515	{1, 411}
212	5	2	2.5	535	{1, 534}
220	3	2	1.5	575 □	{1, 551}
222	10	4	2.5	1043	{1, 148, 342, 552}
225	22	8	2.75	1919	{1, 495, 607, 818, 1101, 1312, 1424, 1918}
228	9	6	1.5	1603	{1, 134, 323, 1280, 1469, 1602}
234	5	4	1.25	1007	{1, 476, 531, 1006}
237	10	8	1.25	2219	{1, 316, 748, 1065, 1154, 1471, 1903, 2218}
238	7	2	3.5	717	{1, 716}
242	6	5	1.2	1331 □	{1, 124, 632, 735, 1170}
246	11	2	5.5	581	{1, 580}
249	8	4	2.0	1169	{1, 335, 834, 1168}
250	9	2	4.5	625 □	{1, 624}
252	3	2	1.5	551	{1, 436}
253	10	2	5.0	529 □	{1, 528}
255	6	4	1.5	1133	{1, 516, 617, 1132}
258	5	4	1.25	1211	{1, 174, 1037, 1210}
260	5	2	2.5	583	{1, 54}
262	3	2	1.5	789	{1, 262}
267	8	4	2.0	1253	{1, 538, 715, 1252}
274	9	6	1.5	2469	{1, 997, 998, 1471, 1472, 2468}
275	14	8	1.75	2323	{1, 91, 919, 1011, 1312, 1404, 2232, 2322}
276	3	2	1.5	611	{1, 610}
285	10	4	2.5	1337	{1, 190, 1147, 1336}
290	5	2	2.5	649	{1, 296}
294	3	2	1.5	1029 □	{1, 685}
297	6	4	1.5	1863 □	{1, 323, 1540, 1862}
300	19	2	9.5	707	{1, 405}
301	10	6	1.67	1849 □	{1, 423, 424, 1425, 1426, 1848}
308	15	2	7.5	667	{1, 436}
310	6	2	3.0	933	{1, 932}
315	8	4	2.0	1349	{1, 569, 780, 1348}
318	11	2	5.5	749	{1, 643}

Table 2: Improvements for $q = 2$ and $2 \leq n \leq 400$:

n	$\kappa_p(2,n)$	$\kappa_g(2,n)$	ratio	r	$\mathcal{K}$
322	6	4	1.5	1363	{1, 46, 563, 753}
324	5	2	2.5	815	{1, 651}
332	3	2	1.5	835	{1, 834}
333	24	4	6.0	1369 □	{1, 117, 1252, 1368}
335	12	8	1.5	2959	{1, 351, 725, 1077, 1882, 2234, 2608, 2958}
339	8	4	2.0	1589	{1, 680, 909, 1588}
342	6	1	6.0	361 □	{1}
351	10	8	1.25	4293 □	{1, 242, 1295, 1538, 2755, 2998, 4051, 4292}
356	3	2	1.5	895	{1, 536}
357	10	4	2.5	1673	{1, 477, 1196, 1672}
358	10	2	5.0	1077	{1, 358}
361	30	18	1.67	6859 □	{1, 333, 623, 956, 1145, 1689, 2819, 2820, 2834, 4025, 4039, 4040, 5170, 5714, 5903, 6236, 6526, 6858}
365	24	8	3.0	3223	{1, 155, 1310, 1464, 1759, 1913, 3068, 3222}
366	22	2	11.0	1101	{1, 733}
369	10	4	2.5	1577	{1, 248, 1329, 1576}
370	6	4	1.5	1639	{1, 595, 1044, 1638}
377	14	8	1.75	3127	{1, 235 , 825, 1061, 2066, 2302, 2892, 3126}
380	5	2	2.5	955	{1, 381}
382	6	2	3.0	1149	{1, 382}
385	6	4	1.5	1633	{1, 70, 1563, 1632}
390	3	2	1.5	869	{1, 868}
396	11	2	5.5	851	{1, 850}

Table 3: Improvements for $q = 3$ and $2 \leq n \leq 400$:

n	$\kappa_p(3,n)$	$\kappa_g(3,n)$	ratio	r		$\mathcal{K}$
2	2	1	2.0	4	□	{1}
10	3	2	1.5	25	□	{1, 24}
12	∞	2		35		{1, 6}
20	5	1	5.0	25	□	{1}
22	3	2	1.5	92	□	{1, 91}
24	∞	4		119		{1, 50, 69, 118}
32	8	2	4.0	128	□	{1, 127}
33	6	4	1.5	161		{1, 22, 139, 160}
36	∞	2		95		{1, 56}
38	15	9	1.67	361	□	{1, 28, 54, 62, 68, 99, 234, 245, 292}
40	7	4	1.75	187		{1, 21, 67, 98}
46	3	2	1.5	188		{1, 187}
48	∞	2		119	□	{1, 69}
55	6	4	1.5	253		{1, 45, 208, 252}
58	4	2	2.0	236	□	{1, 235}
60	∞	2		155		{1, 61}
62	21	10	2.1	1244	□	{1, 305, 317, 621, 717, 881, 897, 969, 985, 1149}
64	4	2	2.0	256	□	{1, 127}
66	3	2	1.5	161		{1, 22}
70	3	2	1.5	284	□	{1, 283}
72	∞	4		323		{1, 132, 208, 305}
80	5	2	2.5	187		{1, 186}
82	9	2	4.5	332	□	{1, 165}
84	∞	2		203		{1, 202}
85	16	12	1.33	1133		{1, 56, 252, 263, 516, 562, 571, 617, 870, 881, 1077, 1132}
90	7	2	3.5	209		{1, 208}
92	5	2	2.5	235		{1, 46}
96	∞	4		896	□	{1, 321, 575, 895}
102	11	6	1.83	721		{1, 57, 253, 365, 561, 617}
106	10	2	5.0	428	□	{1, 427}
108	∞	4		545		{1, 76, 251, 326}
114	5	3	1.67	361	□	{1, 68, 292}
120	∞	4		527		{1, 30, 123, 373}
123	6	4	1.5	581		{1, 167, 414, 580}
124	13	10	1.3	1555		{1, 6, 36, 216, 259, 1296, 1339, 1519, 1549, 1554}
130	4	2	2.0	524	□	{1, 261}

Table 3: Improvements for $q = 3$ and $2 \leq n \leq 400$:

n	$\kappa_p(3,n)$	$\kappa_g(3,n)$	ratio	r		$\mathcal{K}$
132	∞	4		623		{1, 90, 533, 622}
144	∞	2		323		{1, 18}
145	10	4	2.5	649		{1, 296, 353, 648}
147	10	2	5.0	343	□	{1, 342}
150	5	4	1.25	707		{1, 302, 405, 706}
153	14	12	1.17	1957		{1, 514, 562, 767, 768, 881, 1076, 1189, 1190, 1395, 1443, 1956}
156	∞	2		371		{1, 370}
159	34	4	8.5	749		{1, 106, 643, 748}
164	5	2	2.5	415		{1, 414}
166	3	2	1.5	668	□	{1, 667}
168	∞	4		731		{1, 429, 472, 560}
170	8	6	1.33	1133		{1, 56, 263, 870, 1077, 1132}
171	12	2	6.0	361	□	{1, 360}
174	9	2	4.5	413		{1, 176}
178	15	2	7.5	716	□	{1, 357}
180	∞	2		475	□	{1, 151}
182	14	8	1.75	1537		{1, 423, 476, 637, 900, 1061, 1114, 1536}
184	7	4	1.75	799		{1, 140, 234, 424}
186	15	4	3.75	1492	□	{1, 745, 1015, 1223}
190	3	2	1.5	764	□	{1, 381}
192	∞	4		1792	□	{1, 769, 1023, 1791}
195	10	4	2.5	869		{1, 78, 791, 868}
201	10	8	1.25	1883		{1, 351, 456, 806, 1077, 1427, 1532, 1882}
203	12	4	3.0	841	□	{, 411, 800, 840}
204	∞	4		959		{1, 174, 237, 547}
208	10	4	2.5	901		{1, 30, 871, 900}
212	5	2	2.5	535		{1, 534}
216	∞	8		1853		{1, 76, 217, 621, 764, 871, 1341, 1668}
218	15	10	1.5	4364	□	{1, 93, 305, 801, 1381, 1877, 2089, 2181, 2261, 4285}
220	4	2	2.0	575	□	{1, 551}
226	15	2	7.5	908	□	{1, 907}
228	∞	4		1145		{1, 336, 351, 686}
234	5	4	1.25	1007		{1, 476, 531, 1006}
238	4	2	2.0	956	□	{1, 477}

Table 3: Improvements for $q = 3$ and $2 \leq n \leq 400$:

n	$\kappa_p(3,n)$	$\kappa_g(3,n)$	ratio	r	$\mathcal{K}$
240	∞	2		527	{1, 526}
245	24	8	3.0	2167	{1, 395, 408, 802, 1365, 1759, 1772, 2166}
246	3	2	1.5	581	{1, 580}
249	8	4	2.0	1169	{1, 335, 834, 1168}
250	3	2	1.5	625 □	{1, 624}
252	∞	2		551	{1, 436}
253	4	2	2.0	529 □	{1, 528}
258	5	4	1.25	1211	{1, 253, 785, 1037}
261	6	4	1.5	1121	{1, 58,, 1063 1120}
262	3	2	1.5	1052 □	{1, 1051}
264	∞	2		623	{1, 622}
272	5	1	5.0	289 □	{1}
273	10	8	1.25	2279	{1, 560, 818, 902, 1377, 1461, 1719, 2278}
275	12	8	1.5	2323	{1, 91, 919, 1011, 1312, 1404, 2232, 2322}
276	∞	2		695	{1, 694}
288	∞	4		2432 □	{1, 191, 2241, 2431}
290	20	4	5.0	1475 □	{1, 707, 943, 1299}
294	5	1	5.0	343 □	{1}
300	∞	2		707	{1, 405}
301	10	6	1.67	1849 □	{1, 423, 424, 1425, 1426, 1848}
306	7	6	1.17	1957	{1, 767, 1076, 1189, 1395, 1443}
310	15	2	7.5	1244 □	{1, 621}
312	∞	4		1343	{1, 475, 868, 1342}
314	14	10	1.4	6284 □	{1, 621, 825, 1189, 1953, 2317, 2521, 3141, 3321, 6105}
318	17	2	8.5	749	{1, 106}
321	18	12	1.5	4501	{1, 466, 821, 1108, 1109, 1287, 3214, 3392, 3393, 3680, 4035, 4500}
324	∞	2		815	{1, 651}
328	7	4	1.75	1411	{1, 84, 1327, 1410}
332	8	2	4.0	835	{1, 834}
333	6	4	1.5	1369 □	{1, 117, 1252, 1368}
334	15	14	1.07	9356 □	{1, 357, 1065, 2149, 2529, 3613, 4321, 4677, 5693, 5821, 5965, 8069, 8213, 8341}
336	∞	2		731	{1, 171}

Table 3: Improvements for $q = 3$ and $2 \leq n \leq 400$:

n	$\kappa_p(3,n)$	$\kappa_g(3,n)$	ratio	r		$\mathcal{K}$
339	10	4	2.5	1589		{1, 680, 909, 1588}
342	13	1	13.0	361	□	{1}
346	3	2	1.5	1388	□	{1, 1387}
348	∞	4		1631		{1, 232, 1399, 1630}
351	22	16	1.37	5777		{1, 76, 796, 871, 1854, 2256, 2649, 2726, 3051, 3128, 3521, 3923, 4906, 4981, 5701, 5776}
356	11	2	5.5	895		{1, 536}
358	4	2	2.0	1436	□	{1, 717}
360	∞	8		3077		{1, 19, 162, 361, 705, 1087, 1628, 2191}
361	30	18	1.67	6859	□	{1, 333, 623, 956, 1145, 1689, 2819, 2820, 2834, 4025, 4039, 4040, 5170, 5714, 5903, 6236, 6526, 6858}
364	7	4	1.75	1537		{1, 637, 1061, 1114}
365	18	8	2.25	3223		{1, 155, 1310, 1464, 1759, 1913, 3068, 3222}
366	5	4	1.25	2932	□	{1, 1465, 1819, 2579}
368	11	2	5.5	799		{1, 798}
372	∞	4		1865		{1, 477, 1388, 1864}
377	14	8	1.75	3127		{1, 235, 825, 1061, 2066, 2302, 2892, 3126}
380	5	2	2.5	955		{1, 381}
381	20	8	2.5	3563		{1, 510, 1226, 1735, 1828, 2337, 3053, 3562}
382	10	2	5.0	1532	□	{1, 765}
384	∞	4		1799		{1, 755, 1301, 1541}
385	6	4	1.5	1633		{1, 70, 1563, 1632}
387	14	8	1.75	3287		{1, 172, 1291, 1464, 1823, 1996, 3115, 3286}
390	5	2	2.5	869		{1, 868}
393	10	4	2.5	1841		{1, 790, 1051, 1840}
396	∞	2		995		{1, 994}

Table 4: Improvements for $q = 5$ and $2 \leq n \leq 400$:

n	$\kappa_p(5,n)$	$\kappa_g(5,n)$	ratio	r		$\mathcal{K}$
4	3	2	1.5	16	□	{1, 15}
10	∞	2		33		{1, 32}
18	2	1	2.0	27	□	{1}
20	∞	4		176	□	{1, 23, 65, 87}
27	4	2	2.0	81	□	{1, 80}
30	∞	2		77		{1, 76}
32	3	2	1.5	128	□	{1, 127}
33	10	4	2.5	161		{1, 22, 139, 160}
38	12	10	1.2	573		{1, 49, 109, 152, 184, 389, 421, 464, 524, 572}
40	∞	4		187		{1, 21, 67, 98}
44	8	4	2.0	368		{1, 47, 137, 183}
45	12	4	3.0	209		{1, 56, 153, 208}
50	∞	4		303		{1, 10, 91, 100}
54	8	1	8.0	81	□	{1}
55	6	2	3.0	121	□	{1, 120}
58	4	2	2.0	177		{1, 176}
60	∞	6		407		{1, 100, 175, 232, 307, 406}
63	12	8	1.5	551		{1, 75, 115, 191, 360, 436, 476, 550}
64	3	2	1.5	256	□	{1, 127}
66	6	2	3.0	161		{1, 139}
70	∞	6		473		{1, 122, 221, 252, 351, 472}
80	∞	2		187		{1, 186}
81	10	2	5.0	243	□	{1, 242}
84	8	4	2.0	688	□	{1, 257, 431, 687}
90	∞	2		297	□	{1, 109}
100	∞	8		1616	□	{1, 111, 313, 495, 697, 807, 1009, 1415}
104	9	8	1.12	901		{1, 30, 52, 242, 659, 849, 871, 900}
110	∞	2		253		{1, 208}
114	13	4	3.25	687		{1, 457, 565, 580}
120	∞	6		803		{1, 65, 210, 593, 738, 802}
123	10	4	2.5	581		{1, 167, 414, 580}
126	6	4	1.5	783	□	{1, 28, 244, 568}
130	∞	2		393		{1, 392}
134	14	4	3.5	807		{1, 268, 620, 725}
140	∞	8		1243		{1, 131, 208, 747, 835, 903, 1002, 1145}
144	3	2	1.5	323		{1, 18}

Table 4: Improvements for $q = 5$ and $2 \leq n \leq 400$:

n	$\kappa_p(5,n)$	$\kappa_g(5,n)$	ratio	r	$\mathcal{K}$
145	10	4	2.5	649	{1, 296, 353, 648}
147	10	2	5.0	343 □	{1, 342}
150	∞	2		453	{1, 452}
159	20	4	5.0	749	{1, 106, 643, 748}
160	∞	4		1408 □	{1, 65, 1343, 1407}
162	11	1	11.0	243 □	{1}
164	14	4	3.5	1328 □	{1, 663, 831, 1161}
170	∞	6		1133	{1, 56, 263, 870, 1077, 1132}
171	12	2	6.0	361 □	{1, 360}
174	3	2	1.5	413	{1, 176}
178	12	2	6.0	537	{1, 536}
180	∞	2		407	{1, 186}
183	22	12	1.83	2569	{1, 283, 450, 451, 817, 1100, 1469, 1752, 2118, 2119, 2286, 2568}
184	9	4	2.25	799	{1, 140, 234, 424}
190	∞	6		1713	{1, 109, 110, 1604, 1603, 1712}
194	8	4	2.0	1167	{1, 388, 893, 1052}
195	10	4	2.5	869	{1, 78, 791, 868}
200	∞	8		1717	{1, 203, 596, 798, 919, 1121, 1514, 1716}
201	10	8	1.25	1883	{1, 351, 456, 806, 1077, 1427, 1532, 1882}
203	12	4	3.0	841 □	{1, 41, 800, 840}
207	24	4	6.0	893	{1, 189, 704, 892}
208	9	4	2.25	901	{1, 30, 871, 900}
210	∞	2		473	{1, 87}
212	8	4	2.0	1712 □	{1, 215, 1497, 1711}
218	12	10	1.2	3273	{1, 79, 1012, 1090, 1381, 1396, 2089, 2275, 2968, 2983}
220	∞	4		1936 □	{1, 727, 1209, 1935}
228	9	8	1.12	3664 □	{1, 809, 1375, 1481, 2183, 2289, 2855, 3663}
230	∞	2		517	{1, 142}
237	10	8	1.25	2219	{1, 316, 748, 1065, 1154, 1471, 1903, 2218}
238	4	2	2.0	717	{1, 716}
240	∞	4		1037	{1, 72, 965, 1036}
243	12	2	6.0	729 □	{1, 728}
246	22	2	11.0	581	{1, 167}

Table 4: Improvements for $q = 5$ and $2 \leq n \leq 400$:

n	$\kappa_p(5,n)$	$\kappa_g(5,n)$	ratio	r		$\mathcal{K}$
250	∞	6		2253		{1, 73, 679, 823, 1429, 1501}
253	4	2	2.0	529	□	{1, 528}
254	9	4	2.25	1527		{1, 208, 301, 508}
259	18	16	1.12	4321		{1, 552, 597, 1148, 1491, 1683, 2042, 2087, 2234, 2279, 2638, 2830, 3173, 3724, 3769, 4320}
260	∞	2		583		{1, 582}
264	8	6	1.33	1679		{1, 137, 300, 804, 1013, 1103}
270	∞	2		891	□	{1, 406}
272	23	1	23.0	289	□	{1}
275	14	8	1.75	2323		{1, 91, 919, 1011, 1312, 1404, 2232, 2322}
280	∞	4		1243		{1, 98, 241, 903}
286	7	4	1.75	1219		{1, 507, 553, 1059}
290	∞	4		1947		{1, 296, 353, 1297}
294	9	1	9.0	343	□	{1}
297	8	4	2.0	1863	□	{1, 323, 1540, 1862}
300	∞	4		2416	□	{1, 303, 2113, 2415}
301	10	6	1.67	1849	□	{1, 423, 424, 1425, 1426, 1848}
310	∞	2		933		{1, 932}
314	14	10	1.4	4713		{1, 382, 1189, 1570, 1750, 2317, 2521, 3763, 3967, 4534}
315	20	12	1.67	4009		{1, 197, 210, 407, 1280, 1281, 2728, 2729, 3602, 3799, 3812, 4008}
318	17	2	8.5	749		{1, 643}
320	∞	4		2816	□	{1, 639, 2177, 2815}
321	30	12	2.5	4501		{1, 466, 821, 1108, 1109, 1287, 3214, 3392, 3393, 3680, 4035, 4500}
324	9	4	2.25	3888	□	{1, 487, 1457, 1943}
328	7	4	1.75	1411		{1, 84, 1327, 1410}
330	∞	2		847		{1, 846}
333	6	4	1.5	1369	□	{1, 117, 1252, 1368}
334	24	14	1.71	7017		{1, 1015, 1052, 1196, 1274, 1982, 2149, 4868, 5035, 5821, 5743, 5965, 6002, 7016}
339	8	4	2.0	1589		{1, 680, 909, 1588}
340	∞	4		1507		{1, 648, 958, 1407}
342	6	2	3.0	1083	□	{1, 1082}
348	7	4	1.75	1631		{1, 232, 1399, 1630}

Table 4: Improvements for $q = 5$ and $2 \leq n \leq 400$:

n	$\kappa_p(5,n)$	$\kappa_g(5,n)$	ratio	r	$\mathcal{K}$
350	∞	4		2103	{1, 700, 1267, 1537}
351	10	8	1.25	4293 □	{1, 242, 1295, 1538, 2755, 2998, 4051, 4292}
354	8	4	2.0	2127	{1, 1322, 1417, 1514}
356	6	4	1.5	2864 □	{1, 1431, 1791, 2505}
357	6	4	1.5	1673	{1, 477, 1196, 1672,}
358	4	2	2.0	1077	{1, 358}
360	∞	2		803	{1, 439}
361	30	18	1.67	6859 □	{1, 333, 623, 956, 1145, 1689, 2819, 2820, 2834, 4025, 4039, 4040, 5170, 5714, 5903, 6236, 6526, 6858}
365	18	8	2.25	3223	{1, 155, 1310, 1464, 1759, 1913, 3068, 3222}
366	11	6	1.83	2569	{1, 83, 650, 1184, 1469, 1751}
368	9	2	4.5	799	{1, 798}
369	10	4	2.5	1577	{1, 248, 1329, 1576}
370	∞	6		2453	{1, 263, 485, 1968, 2190, 2452}
377	14	8	1.75	3127	{1, 235, 825, 1061, 2066, 2302, 2892, 3126}
380	∞	12		5027	{1, 133, 780, 1695, 1827, 2419, 2608, 3200, 3332, 4247, 4894, 5026}
385	10	8	1.25	3509 □	{1, 969, 1090, 1451, 2058, 2419, 2540, 3508}
387	14	8	1.75	3287	{1, 172, 1291, 1464, 1823, 1996, 3115, 3286}
390	∞	2		917	{1, 785}
392	18	8	2.25	3349	{1, 577, 1378, 1393, 1956, 1971, 2772, 3348}
400	∞	4		1717	{1, 596, 919, 1514}

References

1. David W. Ash, Ian F. Blake, and Scott A. Vanstone, *Low complexity normal bases*, Discrete Applied Mathematics **25** (1989), 191–210.
2. Shuhong Gao, *Gauß periods, groups, and normal bases*, preprint, 1997.
3. Shuhong Gao, Joachim von zur Gathen, and Daniel Panario, *Gauss periods and fast exponentiation in finite fields*, Proc. Latin '95, Valparaiso, Chile, Springer Lecture Notes in Computer Science **911**, 1995, pp. 311–322.
4. S. Gao, J. von zur Gathen, and D. Panario, *Gauss periods: orders and cryptographical applications*, to appear in *Mathematics of Computation*, 1997.
5. Shuhong Gao and Hendrik W. Lenstra, *Optimal normal bases*, Designs, Codes, and Cryptography **2** (1992), 315–323.
6. Serge Lang, *Algebraic number theory*, Addison-Wesley, Reading MA, 1970.
7. Alfred J. Menezes, Ian F. Blake, XuHong Gao, Ronald C. Mullin, Scott A. Vanstone, and Tomik Yaghoobian, *Applications of finite fields.*, Kluwer Academic Publishers, Norwell MA, 1993.
8. Ronald C. Mullin, I. M. Onyszchuk, Scott A. Vanstone, and Richard M. Wilson, *Optimal normal bases in GF(p^n)*, Discrete Applied Math. **22** (1989), 149–161.
9. Emmy Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, Journal für die reine und angewandte Mathematik **167** (1932), 147–152.
10. Alfred Wassermann, *Zur Arithmetik in endlichen Körpern*, Bayreuther Math. Schriften **44** (1993), 147–251.

Fachbereich 17 Mathematik-Informatik, Universität-GH Paderborn, D-33095 Paderborn, Germany, {feisel,gathen}@uni-paderborn.de

International Computer Science Institute, 1947 Center Street, Berkeley, CA 94704-1198, USA, amin@icsi.berkeley.edu