NORMAL BASES VIA GENERAL GAUSS PERIODS

JOACHIM VON ZUR GATHEN & SANDRA SCHLINK

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

Abstract. This paper gives a survey on the State of the Art in the area of normal basis arithmetic in finite fields and generalizes the construction of Gauß periods in that instead of a prime $nk + 1$ an arbitrary integer $r > 1$ with $\varphi(r) = nk$ is used. It turns out that this construction yields in some cases smaller values of k than is possible with the previously known method.

1. Introduction

Mathematicians have been interested in the theory of fields with finitely many elements for several centuries. The main structure properties of finite fields have already been discovered by Gauß (1777–1855) and Galois (1811–1832).
In recent years the interest in finite fields has arisen from a more practical point of view. With the development of information and communication theory it has become necessary to find fast algorithms for many finite field properties. For example, in some of the public key cryptosystems it is important to compute powers of finite field elements as fast as possible. In particular, this problem leads to the more general question of how arithmetic operations of finite field elements can be performed in a fast and elegant way:

PROBLEM 1.1. *Let $\mathbb{F}_{q^n}$ be a finite field over a subfield $\mathbb{F}_q$, let $a, b \in \mathbb{F}_{q^n}^\times$ be units, and $l \in \mathbb{N}$.*
At what cost can we compute

$$a + b, \quad a \cdot b, \quad a/b, \quad \text{and} \quad a^l \quad ?$$

By *cost* we mean two complexity measures, namely

- *Time*: We want to know how many operations in $\mathbb{F}_q$ it takes to perform the operation in $\mathbb{F}_{q^n}$.

- *Space*: This measure counts the space which we need for the storage of intermediate results used in the computation.

This paper investigates algorithms which support fast arithmetic in finite fields. Some of the currently best algorithms in the literature make use of a special construction of normal bases, the so–called *Gauß periods* which were invented by Gauß in 1801 in his famous investigation of the construcion of regular polygons by ruler and compass only. So there is an astonishing link between his theory from nearly two hundred years ago and the latest developments in the theory of normal bases with low complexity.
Gauß himself conjectured that his construction could be extended to a more general case, see article 365 in Gauß (1966). The main *new research contribution* of this paper is a systematic study of these *general Gauß periods*. It turns out that they are considerably harder to understand and our results are not as complete as for the usual Gauß periods. The power of our new method is shown in Table (6.2), where we exhibit new Gauß periods (leading to more efficient algorithms) in a fairly large number of cases.

Contents:

- In Section 2 the main foundations of the theory of finite fields are given, together with all the definitions and results which will be needed in the remainder of the paper.

- Section 3 gives a survey on the recent developments in the topic of finite field arithmetic.

- In Section 4 we get to know the historical background for the usage of Gauß periods. We see for which situation Gauß defined the periods and how he used them to show which regular polygons can be constructed with ruler and compass only.

- Section 5 gives a definition of Gauß periods in the way that they have been used in the literature to find normal bases with low complexity. Also, the latest results on these special Gauß periods are presented.

- In Section 6 the construction of Gauß periods is generalized, with a view to improving the results from chapter 5. We will see that a generalization of the definition in chapter 5 leads to completely new normal bases by Gauß periods. In the remainder, several necessary conditions are proved for the existence of normal bases which are constructed with Gauß periods. Several tables with experimental results concerning general Gauß periods show the progress over the known constructions obtained by our new method.

- In the last section of the paper, the algorithms which are needed for the computation of Gauß periods are listed.

  All computations have been done with MuPAD.

The sections 2 to 5 reflect ideas which are already in the literature. Section 6 and 7 contain *new* material.
This paper is essentially the Diplomarbeit of the second author at the University of Paderborn.

We use the following notations for sets of numbers:

$$\begin{aligned} \mathbb{N} &= \{0,1,2,\ldots\} \\ \mathbb{R}^+ &= \{c \in \mathbb{R} | c \geq 0\} \\ \mathbb{R}^* &= \{c \in \mathbb{R} | c \neq 0\} \end{aligned}$$

2. Foundations

In this chapter, the main results in the theory of finite fields are presented, mostly without proofs. A detailed introduction into this topic is given in the second chapter of Lidl & Niederreiter (1983), where also nearly all the proofs can be found.
Another good and more practical introduction into the topic of finite fields is given in the book of McEliece (1987).

2.1. Finite Fields. If $q = p^m$ for a prime p and a positive integer m, then there exists a field with q elements. Conversely, the order of every field with finitely many elements is a prime power. Two finite fields with the same number of elements are isomorphic. A proof for all of this can be found in Lidl & Niederreiter (1983), pages 48–49.

By these results, we are allowed to speak about "the" finite field with q elements, and denote this by $\mathbb{F}_q$.
$\mathbb{F}_q$, where q is as above, has *characteristic* p, i.e., p is the minimal number such that

$$\underbrace{1 + \ldots + 1}_{p} = 0.$$

Hence, we get the following useful formulas:

$$(a+b)^{p^i} = a^{p^i} + b^{p^i}, \tag{2.1}$$

$$p^i \cdot a = 0, \tag{2.2}$$

for arbitrary elements $a, b \in \mathbb{F}_q$ and $i \in \mathbb{N}$ positive.
We will now mention a property of the set of invertible elements of $\mathbb{F}_q$ (which consists exactly of the non–zero elements in $\mathbb{F}_q$, since $\mathbb{F}_q$ is a field). This set of units in $\mathbb{F}_q$ is usually denoted by $\mathbb{F}_q^\times$.

FACT 2.1. *$\mathbb{F}_q^\times$ is a cyclic group for any prime power q.*

For a proof, see Lidl & Niederreiter (1983), page 50.
In particular, since $\mathbb{F}_q^\times$ is a group of order $q-1$, this implies that $a^q = a$ for all $a \in \mathbb{F}_q$ or, equivalently

$$a^{q-1} = 1 \qquad \forall a \in \mathbb{F}_q^\times. \tag{2.3}$$

The subfields of $\mathbb{F}_q$ are exactly the finite fields $\mathbb{F}_{p^i}$ where i divides m, see Lidl & Niederreiter (1983), page 49. A special case for a subfield of $\mathbb{F}_q$ is $\mathbb{F}_p$, the so–called *prime subfield* of $\mathbb{F}_q$, since it contains no proper subfields.
As a conclusion of this, we know that all proper field extensions of $\mathbb{F}_q$ have the form $\mathbb{F}_{q^n}/\mathbb{F}_q$ where $n \in \mathbb{N}, n \geq 2$.
The Galois group of the field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is cyclic of order n, and is generated by the Frobenius automorphism

$$\sigma : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}; a \longmapsto a^q,$$

whose fix point set is $\mathbb{F}_q$, see Jungnickel (1993), pp.15-16 .

2.1.1. Traces over Finite Fields.

DEFINITION 2.2. *Let α be an element in a finite field extension $\mathbb{F}_{q^n}$. Then the* trace $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ *of α over $\mathbb{F}_q$ is defined by*

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$$

REMARK 2.3. *Since* $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ *is fixed under the Frobenius automorphism, it is an element of* $\mathbb{F}_q$. *Furthermore it can be shown that* $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ *is a linear transformation from* $\mathbb{F}_{q^n}$ *onto* $\mathbb{F}_q$, *if* $\mathbb{F}_{q^n}$ *and* $\mathbb{F}_q$ *are regarded as* $\mathbb{F}_q$*-vectorspaces (see Lidl & Niederreiter (1983), page 55).*

For simplicity, we use from now on the notation Tr instead of $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$.

2.2. Congruences and Fermat's Little Theorem. In the remainder of this paper we will use modular arithmetic. So the main terms and results of this topic are introduced now:

DEFINITION 2.4. *Let* $a, b \in \mathbb{Z}$ *and* m *a positive integer. Then we say that*

$$a \equiv b \bmod m$$

(a is congruent to b modulo m) *if and only if* a *and* b *have the same remainder on division by* m, *i.e.,* $m|a-b$.

We assume that this notation is well–known and so we won't explain all the common rules and formulas for modular arithmetic. We only mention the following famous result by Fermat in 1640:

FACT 2.5. *Let* $a \in \mathbb{N}$ *and* p *prime, not dividing* a. *Then*

$$a^{p-1} \equiv 1 \bmod p.$$

This result is known as *Fermat's Little Theorem.* A proof can be found in Bundschuh (1992), page 96.
For a generalization of 2.5 we need the following preparing definition:

DEFINITION 2.6. *For positive* $r \in \mathbb{N}$ *define*

$$\varphi(r) = \#\{s: 1 \leq s \leq r, \gcd(s, r) = 1\}.$$

The function φ *is called* Euler's totient *function.*

REMARK 2.7. *The following formula is useful for the calculation of* $\varphi(r)$*:*
For a positive integer r *with the prime factorization* $r = p_1^{s_1} \cdots p_m^{s_m}$ *with distinct primes* p_i *and positive integers* s_i *for* $i = 1, \ldots, m$, *where* m *is a positive integer, we have*

$$\varphi(r) = r \prod_{1 \leq i \leq m} \left(1 - \frac{1}{p_i}\right). \tag{2.4}$$

The following result by Euler is a generalization of Fact 2.5, since $\varphi(r) = r - 1$ if r is prime:

Fact 2.8. *Let $b, r \in \mathbb{N}, b \neq 0$ with* $\gcd(b, r) = 1$. *Then*

$$b^{\varphi(r)} \equiv 1 \bmod r.$$

For a proof, see Bundschuh (1992), page 97.
We now make the following definition:

Definition 2.9. *Let r be a positive integer and b a non–zero integer with* $\gcd(b, r) = 1$. *Then the* order of b modulo r *is the smallest positive integer exponent o such that*

$$b^o \equiv 1 \bmod r,$$

and the index of b modulo r *is $\varphi(r)/o$.*

By Fact 2.8, it is clear that $b^{\varphi(r)} \equiv 1 \bmod r$ and that the order of b modulo r divides $\varphi(r)$.

Definition 2.10. *Let r be a positive integer and b a non-zero integer with* $\gcd(b, r) = 1$. *Then b is called* primitive root modulo r *if and only if the index of b modulo r is 1.*

2.2.1. The Chinese Remainder Theorem. For the additive group of integers modulo r, we have the following result:

Theorem 2.11. *Let $r = \prod_{1 \leq i \leq m} p_i^{s_i}$ be the prime factorization of a positive integer r. Then we have*

$$\mathbb{Z}_r \cong \mathbb{Z}_{p_1^{s_1}} \times \cdots \times \mathbb{Z}_{p_m^{s_m}}.$$

Proof. Since we will need the following maps, we sketch the proof briefly: Consider the ring homomorphism

$$\begin{array}{rcl} \psi\colon \mathbb{Z}_r & \longrightarrow & \mathbb{Z}_{p_1^{s_1}} \times \cdots \times \mathbb{Z}_{p_m^{s_m}}; \\ a & \longmapsto & (a \bmod p_1^{s_1}, \ldots, a \bmod p_m^{s_m}). \end{array}$$

Regard also the map

$$\begin{array}{rcl} \chi\colon \mathbb{Z}_{p_1^{s_1}} \times \cdots \times \mathbb{Z}_{p_m^{s_m}} & \longrightarrow & \mathbb{Z}_r; \\ (a_1, \ldots, a_m) & \longmapsto & a_1 l_1 + \ldots + a_m l_m \bmod r, \end{array}$$

where l_i for $1 \leq i \leq m$ satisfies

$$l_i \equiv \begin{cases} 1 \bmod p_i^{s_i}, \\ 0 \bmod p_j^{s_j}, \; j \neq i. \end{cases}$$

For example, let $l_i = \prod_{j \neq i} p_j^{s_j} \cdot \prod_{j \neq i} (p_j^{s_j})^{-1}$ where the inverse is taken modulo $p_i^{s_i}$. Then, we have

$$\begin{aligned} \chi \circ \psi(a_1, \ldots, a_m) &= \chi(\sum_{0<i\leq m} a_i l_i) \\ &= (\sum_{0<i\leq m} a_i l_i \bmod p_1^{s_1}, \ldots, \sum_{0<i\leq m} a_i l_i \bmod p_m^{s_m}) \\ &= (a_1, \ldots, a_m) \end{aligned}$$

with the definition of the l_i. □

For the multiplicative group of units modulo r, we obtain the corresponding result as a corollary to Theorem 2.11:

COROLLARY 2.12. *With the above notation, we also have*

$$\mathbb{Z}_r^\times \cong \mathbb{Z}_{p_1^{s_1}}^\times \times \cdots \times \mathbb{Z}_{p_m^{s_m}}^\times .$$

For a proof, see Bundschuh (1992), page 93.

2.3. Primitive roots of unity and cyclotomic polynomials. In the remainder of this paper we will also need the following terms:

DEFINITION 2.13. *Let K be a field of characteristic p, where p is a prime or $p = 0$. Let $r \in \mathbb{N}$ be a positive integer which is not divisible by p. An element β in an extension field of K is called* a primitive rth root of unity *(r–PRU) if and only if $\beta^r = 1$ and $\beta^l \neq 1$ for all $1 \leq l < r$.*
Let $\beta \in K$ be an r–PRU. The polynomial

$$\phi_r(x) = \prod_{\substack{1 \leq s < r \\ \gcd(s,r)=1}} (x - \beta^s)$$

is called the rth cyclotomic polynomial *over K.*

Obviously, β is a root of ϕ_r.

REMARK 2.14. *If β is a primitive rth root of unity then the order of β^a for $1 \leq a \leq r$ can be determined as follows:*

$$\operatorname{ord}(\beta^a) = \frac{\operatorname{ord}(\beta)}{\gcd(a, \operatorname{ord}(\beta))}.$$

In particular, β^a is a primitive rth root of unity if and only if $\gcd(a, r) = 1$.

REMARK 2.15. *Since it is not easy to compute cyclotomic polynomials using only the above definition, the following recursive formula is helpful:*

$$x^r - 1 = \prod_{d|r} \phi_d(x).$$

It can also be shown that the coefficients of ϕ_r are in $\mathbb{F}_p$ in the finite case, and in $\mathbb{Z}$ if $\operatorname{char}(K) = 0$. For a proof, see Lidl & Niederreiter (1983), page 64.

EXAMPLE 2.16. *Let $r = 8$. We want to know the eighth cyclotomic polynomial over $\mathbb{F}_3$. The divisors of 8 are 1,2,4 and 8. Obviously, $\phi_1(x) = x - 1$. With the above formula we get*

$$x^2 - 1 = \phi_2(x) \cdot (x - 1).$$

So the second cyclotomic polynomial is $x + 1$. Applying the formula to $r = 4$ we find that

$$\phi_4(x) = \frac{x^4 - 1}{(x+1)(x-1)} = x^2 + 1.$$

Now we can compute the eighth cyclotomic polynomial:

$$\phi_8(x) = \frac{x^8 - 1}{x(x+1)(x-1)(x^2+1)} = x^4 + 1.$$

We know the factorization pattern of ϕ_r by the following fact:

FACT 2.17. *With the above notation, if $K = \mathbb{F}_q$, then ϕ_r factors over $\mathbb{F}_q$ into $\frac{\varphi(r)}{e}$ distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree e, where e is the order of q modulo r.*
If $\operatorname{char}(K) = 0$ then ϕ_r is irreducible over K.

A proof can be found in Lidl & Niederreiter (1983), page 65.

EXAMPLE 2.18. *Let $q = 3, r = 8$, and $\phi_8(x) = x^4 + 1$ as above. The order of q modulo r is 2, since $3 \not\equiv 1 \bmod 8$, but $3^2 = 9 \equiv 1 \bmod 8$. By the above fact we know that ϕ_8 factors over $\mathbb{F}_3$ into $\varphi(8)/e = 4/2 = 2$ irreducible polynomials of degree $e = 2$. The exact factorization of ϕ_8 is the following:*

$$\phi_8(x) = (x^2 + 2x + 2)(x^2 + x + 2).$$

2.4. The group of units modulo r. Later, we will also make use of $\mathbb{Z}_r^\times$, the group of units modulo r for a positive integer r. As can be easily checked, the elements which are invertible modulo r are exactly the ones which are relatively prime to r. Hence, we get:

$$\mathbb{Z}_r^\times = \{s: 1 \leq s \leq r, \gcd(s, r) = 1\}.$$

With this definition and Definition 2.6, we obviously have $\#\mathbb{Z}_r^\times = \varphi(r)$. It is also clear that $\mathbb{Z}_r^\times$ is an abelian group. For some r, the group of units modulo r is even cyclic:

FACT 2.19.

$$\mathbb{Z}_r^\times \quad \textit{is cyclic} \quad \Leftrightarrow r \in \{1, 2, 4, p^m, 2p^m\},$$

where $m \in \mathbb{N}$ and p is an odd prime.

For a proof, see e.g. Bundschuh (1992), pages 113-116.
In particular, the group of units modulo a prime is cyclic, which we will need in section 5. For most of the possible values for a positive integer r, the group $\mathbb{Z}_r^\times$ is not cyclic. We can only state the following result:

FACT 2.20. *$\mathbb{Z}_r^\times$ is a direct sum of cyclic groups of prime power order.*

This result holds generally for any finite abelian group. We will examine this fact more detailly in Section 7.2.

2.5. Polynomials over $\mathbb{F}_q[x]$. In this section we deal with polynomial bases of finite fields. Therefore, we will need the following results about polynomials over finite fields:

FACT 2.21. *For any $n \in \mathbb{N}$ there exists an irreducible polynomial of degree n over $\mathbb{F}_q[x]$. Let f be such a polynomial. Then f has a root $\alpha = x \bmod f \in \mathbb{F}_q[x]/(f) \cong \mathbb{F}_{q^n}$. All roots of f are simple and are given by the n distinct elements $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$.*
Furthermore, $B = (1, \alpha, \ldots, \alpha^{n-1})$ is a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

For a proof, see Lidl & Niederreiter (1983), pages 51,52,59.

EXAMPLE 2.22. *The polynomial $f = x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible over $\mathbb{F}_2$. This can easily be checked by regarding the values of the polynomial function for 0 and 1. With the above fact, f has a root α in $\mathbb{F}_4$ and the tupel $(1, \alpha)$ forms a basis for $\mathbb{F}_4$ over $\mathbb{F}_2$.*

Another useful fact about roots of irreducible polynomials over finite fields is the following:

FACT 2.23. *Let f be an irreducible polynomial in $\mathbb{F}_q[x]$ of degree n and α a root of f in $\mathbb{F}_{q^n}$. Then, all the roots of f are simple and are given by the n distinct elements $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ of $\mathbb{F}_{q^n}$.*

A proof for this can be found in Lidl & Niederreiter (1983), page 52.

2.6. O and soft–O notation. Since we will consider several algorithms and their running time, it is useful to just mention the main notations for asymptotical complexity:

DEFINITION 2.24. *Let $g: \mathbb{N} \to \mathbb{R}^*$ be an arbitrary function. Then the* order of *g is defined by the following:*

$$O(g) = \{f: \mathbb{N} \to \mathbb{R}^* : \exists c \in \mathbb{R}^+ \quad \exists n_0 \in \mathbb{N} \quad \forall n \geq n_0 \quad f(n) \leq c \cdot g(n)\}.$$

This means that $O(g)$ is the set of all functions f which are upper bounded by a positive real multiple of $g(n)$ for $n \geq n_0$ for all $n \in \mathbb{N}$ which are greater than some special n_0.
We will use the well–known rules for the O–notation for the analysis of algorithms in the remainder of this paper. For a detailed introduction into this topic, see e. g. Brassard & Bratley (1988).
We will also use a special terminology of the O–notation in order to simplify the terms which appear in the running–times of algorithms, the so–called *soft–O*–notation, which ignores logarithmic factors:

DEFINITION 2.25. *$f = O^{\sim}(g)$ if and only if*

$$f = O(g(\log g)^k) \qquad \text{for some constant } k.$$

The definition was introduced in von zur Gathen (1985) and Babai *et al.* (1988).

EXAMPLE 2.26. *The Schönhage & Strassen (1971) algorithm to multiply two polynomials of degree n over a field F can be done with $O(n \log n \log\log n)$ operations in F. Hence, the algorithm is linear in the $O^{\sim}$ notation, i.e., it can be done with $O^{\sim}(n)$ operations in F.*

3. Basis representation of finite fields

3.1. Introduction. There are several possibilities for the representation of elements in a finite field.
The elements of a prime field $\mathbb{F}_p = \{0, \ldots, p-1\}$ can be represented in binary, i.e., every element $0 \le a < p$ can be expressed uniquely as a bit string of length $\lceil log_2(p) \rceil$:

$$a = \sum_{0 \le i \le \lceil log_2(p) \rceil} a_i 2^i,$$

where $a_i \in \{0, 1\}$. So arithmetic in a prime field $\mathbb{F}_p$ can be performed as "binary" arithmetic and the cost can be measured in bit operations.
In this paper we concentrate on the basis representation of finite fields, which will be explained now in detail, and therefore measure the cost for an arithmetic operation in $\mathbb{F}_{q^n}$ in $\mathbb{F}_q$-operations, which can be reduced, as shown above, to bit operations.
Since $\mathbb{F}_{q^n}$ is a vector space over $\mathbb{F}_q$ of dimension n, there exists a basis $B = (\alpha_0, \ldots, \alpha_{n-1})$ for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ such that an element $a \in \mathbb{F}_{q^n}$ can be written as a linear combination of these basis elements:

$$a = \sum_{0 \le i < n} a_i \alpha_i,$$

where $a_i \in \mathbb{F}_q$ for all $i \in \{0, \ldots, n-1\}$. Since this representation is unique, we can identify a with its coefficient vector $(a_1, \ldots, a_{n-1})$ which we will denote by $(a)_B$.
Let $a, b \in \mathbb{F}_{q^n}$ with the corresponding coefficient vectors $(a)_B$ and $(b)_B$. Then the sum of a and b has the coefficient vector $(a+b)_B = (a_1+b_1, \ldots, a_{n-1}+b_{n-1})$. So addition in finite fields using a basis representation can be done in linear time because there are only n additions in $\mathbb{F}_q$ to do. Obviously, no work space is needed to perform an addition in $\mathbb{F}_{q^n}$.
The other arithmetic operations we are interested in, like multiplication, exponentiation and division, are more "expensive". For example, if we want to multiply a and b, we obtain the following formula:

$$a \cdot b = \sum_{0 \le i,j < n} a_i b_j \alpha_i \alpha_j = \sum_{0 \le i,j,k < n} a_i b_j c_{ij}^{(k)} \alpha_k,$$

since $\alpha_i \alpha_j$ is also an element in $\mathbb{F}_{q^n}$ and can therefore be expressed in terms of B as $\alpha_i \alpha_j = \sum_{0 \le k < n} c_{ij}^{(k)} \alpha_k$, where each $c_{ij}^{(k)} \in \mathbb{F}_q$.

The $n \times n \times n$–array of all $c_{i,j}^{(k)}$ is called the *multiplication tensor* of the basis B. It is independent of a and b. If we want to perform arithmetic in $\mathbb{F}_{q^n}$, we have to compute and store the $n \times n$ matrices $(c_{i,j}^{(k)})$ for $0 \le k < n$. So for a multiplication by this method with respect to a general basis n^3 elements of $\mathbb{F}_q$ have to be stored, and $O(n^3)$ $\mathbb{F}_q$–operations are necessary.

REMARK 3.1. *It is also possible to represent finite field elements in a rather different way. One interesting example is the* cyclic representation *of a finite field $\mathbb{F}_{q^n}$ which takes advantage of the fact that the group of units in a finite field, i.e. $\mathbb{F}_{q^n}^\times$, is cyclic, see 2.1. So all elements of $\mathbb{F}_{q^n}^\times$ can be written as a power of a primitive element $\xi \in \mathbb{F}_{q^n}^\times$. In this representation appear rather different problems in finite field arithmetic than in the basis representation of $\mathbb{F}_{q^n}$, e.g., a disadvantage of a cyclic representation is the high amount of space which is needed to perform an addition, while multiplication and exponentiation become "cheap" in this representation, see Jungnickel (1993), pages 84-86.*
For these reasons, it has turned out that the cyclic representation is only useful for applications where the field $\mathbb{F}_{q^n}$ has not too many elements, e.g. in coding theory. For cryptographic purposes, where $\mathbb{F}_{q^n}$ has usually many elements, this method does not seem to be successful. One interesting question is whether the two representations can be combined in a useful way, e.g. for the multiplication of polynomials over finite fields, see Montgomery (1991) and von zur Gathen & Gerhard (1995).

The main operation needed in public key cryptosystems is the exponentiation of field elements. With an arbitrary basis, an exponentiation has to be performed by several multiplications of two field elements. For this reason we need to improve the cubic amount of time and space that is needed so far for one multiplication in $\mathbb{F}_{q^n}$. We will see that this result really can be improved if a special basis is chosen.
There are several possibilities for the choice of a basis B. It has turned out that there are two special kinds of bases which are useful for efficient arithmetic in finite fields. These are *polynomial bases* and *normal bases.*

3.2. Polynomial Bases. Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial with coefficients in $\mathbb{F}_q$ and positive degree $n \in \mathbb{N}$. Such a polynomial always exists by Fact 2.21.
There, we have also seen that f has a root $\gamma = x \bmod f$ in $\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(f)$ and the tupel $B = (1, \gamma, \ldots, \gamma^{n-1})$ forms an $\mathbb{F}_q$–basis of $\mathbb{F}_{q^n}$ which is called *polynomial* basis.

By now, the best known probabilistic algorithm to find an irreducible polynomial of degree n over $\mathbb{F}_q$ has been developed by Shoup (1994) and needs an expected number of $O^\sim(n^2 + n \log q)$ operations in $\mathbb{F}_q$. Deterministically, we have only polynomial time algorithms if we assume that the ERH (Extended Riemann Hypothesis, see e.g. Bundschuh (1992), page 317) holds, see Adleman & Lenstra (1986).

So arithmetic in $\mathbb{F}_{q^n}$ in this case means polynomial arithmetic in $\mathbb{F}_q[x]$ modulo f. With the fast multiplication algorithm via the Fast Fourier Transformation by Schönhage & Strassen (1971), the multiplication of two elements and taking the remainder modulo f can be done in $O(n \log n \log\log n)$ or $O^\sim(n)$ $\mathbb{F}_q$–operations. For the division it is also necessary to find the inverse of a given element $b \in \mathbb{F}_{q^n}$. With the fast version of the Extended Euclidean Algorithm, see Aho *et al.* (1974), page 307, this can be done in $O(n(\log n)^2 \log\log n)$ $\mathbb{F}_q$–operations. So these operations are linear in the soft–O notation, and this is a very good result compared with the amount of $O(n^3)$ operations in the general case. For the aspect of space, we have to store the coefficients of the polynomial, i.e., n elements in $\mathbb{F}_q$.

Exponentiation of an element $a \in \mathbb{F}_{q^n}$ via a polynomial basis can be done with $O(n/\log n)$ multiplications in $\mathbb{F}_{q^n}$, i.e. $O(n^2 \log\log n)$ operations in $\mathbb{F}_q$. This was shown by Brickell *et al.* (1992). In their algorithm $O(n/\log n)$ elements in $\mathbb{F}_{q^n}$ have to be stored. Unfortunately, there also have to be done about n multiplications in $\mathbb{F}_{q^n}$ once, before the algorithm.

This result is quite disappointing, because exponentiation is a very important operation in the applications of finite fields, e. g. in public key cryptosystems like the one of ElGamal (1985).

So it is useful to use a basis which "facilitates" in some sense the exponentiation of field elements. This leads to a different kind of basis which will be introduced now.

3.3. Normal Bases. In this section we investigate a basis type which seems to be more natural for some tasks in the arithmetic in finite fields.

DEFINITION 3.2. *Let $\alpha \in \mathbb{F}_{q^n}$. If $N = (\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$ forms an $\mathbb{F}_q$–basis of $\mathbb{F}_{q^n}$, then α is called* a normal element *and N is called* a normal basis *for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

REMARK 3.3. *Normal bases and polynomials over $\mathbb{F}_q$ are linked by the following property:*

If $f \in \mathbb{F}_q[x]$ is an irreducible polynomial of degree n with linearly independent roots over $\mathbb{F}_q$, then any root $\alpha \in \mathbb{F}_{q^n}$ is a normal element in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. This property is based on Fact 2.23.

REMARK 3.4. *N is also called the set of* conjugates *of α. Definition (3.2) is only a special case for a normal field, i.e., a field extension L/K which can be obtained by adjunction of the roots of one or more polynomials over the field K to K. Generally, a normal basis is a basis, in which the elements are permuted by the automorphisms of the Galois group of the field extension, see* van der Waerden (1966)*, page 205. In this special case of Definition (3.2), the Galois group of the field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is cyclic and generated by an $\mathbb{F}_q$-automorphism $\sigma: \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}; \sigma(a) = a^q$. Remember from section 2.1, that σ is called the* Frobenius automorphism *and is of great interest in the topic of finite fields.*

The existence of such a basis for any $n \in \mathbb{N}$ with $n \geq 2$ is guaranteed by the *Normal Basis Theorem*, which holds for arbitrary Galois extensions:

FACT 3.5. *For any prime power q and for any positive integer n there exists a normal basis N of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*

The first complete proof was given by Hensel (1888), for a quite elementary proof see Lidl & Niederreiter (1983), page 60.
The above proofs are not constructive, but there are known several algorithms for the construction of a normal basis, see e.g. the probabilistic algorithm of von zur Gathen & Giesbrecht (1990) which can be done with $O\tilde{~}(n^2 + n\log q)$ operations in $\mathbb{F}_q$.
So from now on we can assume that we use a normal basis, and we denote α^{q^i} by α_i.
A useful property of a normal basis will be shown now:
Let $a \in \mathbb{F}_{q^n}$, such that $(a)_N = (a_0, \ldots, a_{n-1})$. Then

$$a^{q^j} = \left(\sum_{0 \leq i < n} a_i \alpha_i \right)^{q^j} = \sum_{0 \leq i < n} a_i^{q^j} \alpha_{i+j} = \sum_{0 \leq i < n} a_i \alpha_{i+j}.$$

using the rules (2.1) and (2.3).
So, a^j has the coordinate vector $(a_{n-j}, a_{n-j+1}, \ldots, a_{n-1}, a_0, a_1, \ldots, a_{n-j-1})$.
Hence, exponentiations with powers of q are only a cyclic shift of the coordinates. By this advantage, von zur Gathen (1991) shows that exponentiation

needs $O(n/\log n)$ multiplications in $\mathbb{F}_{q^n}$ with a storage of $O(n/\log^2 n)$ elements of $\mathbb{F}_{q^n}$ (if we assume that the exponent is smaller than q^n) and without any precomputation stage.
Unfortunately, the situation for the multiplication via normal bases is not as good as for exponentiation:
Let $a, b \in \mathbb{F}_{q^n}$ with the corresponding coordinate vectors $(a)_N = (a_1, \ldots, a_{n-1})$ and $(b)_N = (b_1, \ldots, b_{n-1})$. Then

$$a \cdot b = \sum_{0 \leq i,j <} a_i b_j \alpha_{i+j} = \sum_{0 \leq i,j < n} a_i b_j (\alpha \alpha_{i-j})^{q^j}.$$

For $m \in \{0, \ldots, n-1\}$ we have a representation of $\alpha\alpha_m$ in terms of N:

$$\alpha\alpha_m = \sum_{0 \leq k < n} t_{mk} \alpha_k,$$

where $t_{mk} \in \mathbb{F}_q$ for all $m, k \in \{0 \ldots n-1\}$.
Hence,

$$\begin{aligned} a \cdot b &= \sum_{0 \leq i,j < n} a_i b_j \left(\sum_{0 \leq k < n} t_{i-j,k} \alpha_k \right)^{q^j} = \sum_{0 \leq i,j,k < n} a_i b_j t_{i-j,k} \alpha_{k+j} \\ &= \sum_{0 \leq i,j,l < n} a_i b_j t_{i-j,l-j} \alpha_l \quad \text{for} \quad l = k + j. \end{aligned}$$

By this, we only have to store a $n \times n$–multiplication table $T = (t_{i,j})$, so that the required space can be reduced to $O(n^2)$. But in the worst case it is still possible that the multiplication of two elements in $\mathbb{F}_{q^n}$ with normal bases needs about n^3 $\mathbb{F}_q$–operations. This depends, as we will see now, on the number of non–zero entries in T:

Definition 3.6. *The number of non–zero entries in T is called the* complexity *of N, and is denoted by c_N.*

The notion "complexity" has been originally introduced by Mullin *et al.* (1988) and sounds a bit unlucky because this notation has nothing to do with the aspects of complexity in complexity theory, and it is perhaps more descriptive to speak of the *density* of N.
The cost for one multiplication in $\mathbb{F}_{q^n}$ is $2 \cdot n \cdot c_N$ multiplications and $n(c_N - 1)$ additions in $\mathbb{F}_q$.
So, if c_N is linear in n, we get a multiplication time of $O(n^2)$.
Of course, n^2 is an upper bound on c_N. A lower bound on c_N is given now:

FACT 3.7. *For any normal basis N we have $c_N \geq 2n-1$.*

PROOF. See Mullin *et al.* (1988).
By this fact, we get the following natural definition:

DEFINITION 3.8. *N is called an* optimal normal basis *if $c_N = 2n-1$.*

If N is optimal, only $O(n^2)$ operations in $\mathbb{F}_q$ are needed for one multiplication in $\mathbb{F}_{q^n}$ via normal bases. Although we have to note that this is still worse than the polynomial case, this is an advantage over the general case.
Unfortunately, we have the problem that, unlike normal bases, optimal normal bases do not exist in every case.
A famous result concerning the existence of optimal normal bases is the following:

FACT 3.9. *For given q and n there exists an optimal normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ in one of the following two cases:*

- $n+1$ *prime and* $\langle q\rangle = \mathbb{Z}_{n+1}^{\times}$,
- $2n+1$ *prime,* $q=2$ *and* $\langle 2,-1\rangle = \mathbb{Z}_{2n+1}^{\times}$.

PROOF. see Mullin *et al.* (1988)
For $q=2$, Gao & Lenstra (1992) showed that these are the only cases in which there exists an optimal normal basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. For $q \neq 2$ there can exist other optimal normal bases but it was also shown by Gao & Lenstra (1992) that these are in some sense equivalent to one of the two cases in Fact 3.9.
In the remainder of this chapter, we return to "ordinary" normal bases and we will see, how it can be tested whether a given element $\alpha \in \mathbb{F}_{q^n}$ is a normal basis generator in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

3.3.1. A test for normality. There are several possibilities to test an element $\alpha \in \mathbb{F}_{q^n}$ for normality. Most of the so-far known tests can be found in the books of Jungnickel (1993) and Menezes *et al.* (1993). In the remainder of this section, I will mention only one of them, since it will be used in section 6. This is one of the most interesting tests, since it combines two views of a finite field, the vector space structure and the Galois module structure.
Recall from section 2.1 that the Frobenius map $\sigma: \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ with $\sigma(a) = a^q$ is an $\mathbb{F}_q$-linear transformation of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, i.e. $\sigma(a+b) = \sigma(a)+\sigma(b)$ for $a, b \in \mathbb{F}_{q^n}$ and $\sigma(c\cdot a) = c\cdot\sigma(a)$ for $a \in \mathbb{F}_{q^n}$ and $c \in \mathbb{F}_q$.

DEFINITION 3.10. *Let* $f = \sum_{1 \le i \le m} a_i x^i \in \mathbb{F}_q[x]$ *and* F *be an extension field of* $\mathbb{F}_q$. *For* $\alpha \in F$, *define*

$$f \circ \alpha = \sum_{0 \le i \le m} a_i \sigma^i(\alpha) = \sum_{1 \le i \le m} a_i \alpha^{q^i}.$$

This definition goes originally back to Ore (1934).

REMARK 3.11. *It can be easily checked that the additive group of* F, *together with the above action of* $\mathbb{F}_q[x]$ *on* F, *is a module over* $\mathbb{F}_q[x]$.
Furthermore, we have:

$$\alpha \in \mathbb{F}_{q^n} \Leftrightarrow \sigma^n(\alpha) = \alpha \Leftrightarrow \sigma^n(\alpha) - \alpha = 0 \Leftrightarrow \ (x^n - 1) \circ \alpha = 0. \qquad (3.1)$$

The set $I(\alpha) = \{g \in \mathbb{F}_q[x]: g \circ \alpha = 0\}$ *is an ideal in the polynomial ring* $\mathbb{F}_q[x]$. *As we saw in (3.1),* $I(\alpha)$ *is nonzero for an element* $\alpha \in F$, *since there exists a positive integer* n *such that* $(x^n - 1) \circ \alpha = 0$. $I(\alpha)$ *is called the* annihilator *of* α. *Since* $\mathbb{F}_q[x]$ *is also a principal ideal domain,* $I(\alpha)$ *is generated by one polynomial in* $\mathbb{F}_q[x]$.

This leads to the following definition:

DEFINITION 3.12. *With the above notation, let* $\mathrm{Ord}(\alpha) \in \mathbb{F}_q[x]$ *denote the unique monic polynomial which generates* $I(\alpha)$. $\mathrm{Ord}(\alpha)$ *is called the* additive order *of* α.

So we have:

$$\alpha \in \mathbb{F}_{q^n} \quad \Leftrightarrow \quad \mathrm{Ord}(\alpha) | x^n - 1.$$

Furthermore, we obtain a test for the normality of a given element $\alpha \in \mathbb{F}_{q^n}$, taken from the book of Menezes *et al.* (1993), page 78:

THEOREM 3.13. *Let* $x^n - 1 = \prod_{1 \le i \le s} g_i^{t_i}$ *be the factorization of* $x^n - 1$ *over* $\mathbb{F}_q$ *into irreducible polynomials* $g_i \in \mathbb{F}_q[x]$. *Let* $h_i = x^n - 1/g_i$ *be a maximal proper divisor of* $x^n - 1$.
An element $\alpha \in \mathbb{F}_{q^n}$ *is normal in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$ *if and only if*

$$h_i \circ \alpha \neq 0$$

for all $1 \le i \le s$.

PROOF. By the definition of normality (see 3.2), an element α is normal if and only if the elements $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are linearly independent over $\mathbb{F}_q$. But these are exactly the elements $\sigma^0(\alpha), \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)$. α is normal if and only if no linear combination of these elements is equal to 0, i.e. there is no polynomial of degree less than n which annihilates α. So, we have

$$\alpha \quad \text{normal in} \quad \mathbb{F}_{q^n} \quad \text{over} \quad \mathbb{F}_q \quad \Leftrightarrow \quad \mathrm{Ord}(\alpha) = x^n - 1.$$

But the latter condition is true if and only if $h_i \circ \alpha \neq 0$ for all maximal divisors h_i of $x^n - 1$ and $1 \leq i \leq s$. □

We will see in section 6 that this test will be useful in the situation of general Gauß periods.
In particular, this test becomes easy in a special case for n:

COROLLARY 3.14. *Let $n = p^t$, where p is the characteristic of $\mathbb{F}_q$. Then, an element $\alpha \in \mathbb{F}_{q^n}$ is normal if and only if* $\mathrm{Tr}(\alpha) \neq 0$.

PROOF. The factorization of $x^n - 1$ over $\mathbb{F}_q$ is $x^n - 1 = x^{p^t} - 1 = (x-1)^{p^t}$, i.e., $x - 1$ is the only irreducible factor, and the only maximal divisor of $x^n - 1$ is $h = x^{n-1} + \ldots + x + 1$. But

$$h \circ \alpha = \sum_{0 \leq i < n} \alpha^{q^i} = \mathrm{Tr}(\alpha).$$

From Fact 3.13 α is normal if and only if $\mathrm{Tr}(\alpha) \neq 0$. □

4. Historical motivation for Gauß periods

Since an optimal normal basis does not exist in every case, we are interested in normal bases which are perhaps not optimal, but behave in some sense well in the view of arithmetic operations and have "sparse" multiplication tables,i.e., many entries in the multiplication tables are zero. These investigations are presented in the remainder of this paper.
We use a construction of Gauß, the so–called *Gauß periods* which he described in his Disquisitiones Arithmeticae. Before we investigate the use of his ideas for the problem of arithmetics in finite fields, we look at the origins of the definition of Gauß periods and their use in the theory of the construction of regular polygons with ruler and compass only.

4.1. Original definition of Gauß periods. Gauß periods have been originally invented by Carl Friedrich Gauß (1777–1855). In 1796, at the age of 19, he discovered that the regular 17-gon can be constructed by ruler and compass only. The general theory about the construction for regular polygons is published in his famous book *Disquisitiones Arithmeticae* which appeared for the first time in 1801. For a biography of Gauß, see e.g. Wussing (1976).
In the articles 336–366 of the Disquisitiones Arithmeticae, Gauß developed a theory to find the equations which are important for the sections of a circle. This problem is equivalent to the construction of regular polygons with ruler and compass only. Hence, Gauß searched for representations for the solutions of the equation

$$x^p = 1,$$

where p is an odd prime. Gauß showed that it is sufficient to concentrate on this case because the case for a general positive integer n can be reduced to the case for an odd prime p.
Apart from the trivial solution $x = 1$ the main task is to find the roots of the function

$$X = x^{p-1} + \cdots + x + 1.$$

Let $\omega \in \mathbb{C}$ be a root of X. Gauß showed the correctness of the following properties:

- $\omega^{tp} = 1$ for all integers t.
- Every power of ω is also a root of $x^p - 1$.
- The equation $\omega^\lambda = \omega^\nu$ holds if and only if $\lambda \equiv \nu \bmod p$.

From these results we can draw the following conclusions:
Let Ω denote the set of roots of X. Then we have obviously

$$\Omega = \{\omega, \omega^2, \ldots, \omega^{p-1}\}.$$

Remark 4.1. *In Gauß' notation, let* $[1], [2], [3], \ldots$ *be the residue classes modulo* p *which belong to* $w, w^2, w^3, \ldots$ *and define* $[0] = 1$. *Then* $[\lambda] \cdot [\nu] = [\lambda + \nu]$ *and* $[\lambda]^\nu = [\lambda \cdot \nu]$.
Let g *be a primitive root modulo* p *(which exists, since* p *is a prime). Then it can be easily shown that*

$$\{[1], [g], \ldots, [g^{p-2}]\} = \{[1], [2], \ldots, [p-1]\} = \mathbb{F}_p^\times.$$

Hence, we can identify the set of powers of g *with* Ω.

This property of Ω led Gauß to the following definition:

DEFINITION 4.2. *Let g be a primitive root modulo p, i.e., the order of g modulo p is $p-1$ (see 2.10), and t be a positive divisor of $p-1$, such that $p-1 = t \cdot f$ for a positive integer f. Let λ be an arbitrary integer which is not divisible by p. If $h = g^t$ then*

$$(f, \lambda) = \{[\lambda], [\lambda h], \ldots, [\lambda h^{f-1}]\}$$

is called a period *of roots of X.*

Note that the set (f, λ) is independent of the choice of g as a primitive root modulo p.

EXAMPLE 4.3. *Let $p = 19, g = 2$. It can be easily proved that 2 is a primitive root modulo 19. Then $p - 1 = 18 = t \cdot f$. We choose $t = 3$ and $f = 6$ and determine the period $(6, 1)$: Since $h = g^t = 2^3 = 8$, we get*

$$(6,1) = \{[1], [8], [64], [512], [4096], [32768]\},$$

hence, reduced modulo p this is

$$(6,1) = \{[1], [7], [8], [11], [12], [18]\}.$$

In the same way we obtain the other periods:

$$(6,2) = (6,3) = \{[2], [3], [5], [14], [16], [17]\},$$

and

$$(6,4) = \{[4], [6], [9], [10], [13], [15]\}.$$

For general λ, Gauß showed that

$$\Omega = (f, \lambda) \cup (f, \lambda g) \cup \cdots \cup (f, \lambda g^{t-1}),$$

if λ is not divisible by p. For the example, this means that $\Omega = (6,1) \cup (6,2) \cup (6,4)$.

Besides, Gauß showed that two periods (f, λ) and (f, λ') are either equal or disjoint.

4.2. Gauß periods in the theory of the construction of regular polygons. Gauß defined periods as a tool in the theory of regular polygons. He used them in the following way:
Gauß decomposed the periods step by step, in such a way that he wrote $t = t' \cdot f'$, where t', f' are positive integers, and so came to the conclusion that each period (f, λ) is the union of t' periods of the form (f', λ_i) for $i = 1, \ldots, t'$. By this, he reduced the equation $X = 0$ to equations $X_{t'}$ of degree t'.
The successive application of this step, leads at last to the prime factorization of $p-1$, namely $p - 1 = \prod_{i=1}^{l} p_i^{s_i}$, where the p_i are distinct primes, and to s_i equations of degree p_i for each $i = 1, \ldots, l$.
In further considerations Gauß showed that only for the case $p = 2^{2^k} + 1$, where $k \in \mathbb{N}$, all these equations are quadratic, and therefore solvable by ruler and compass. In any other case for p there is at least one equation of higher degree. By these results, Gauß was able to construct the regular 17–polygon with ruler and compass only.
More general, he showed that the regular n-gon is constructible if

$$n = 2^a p_1 \cdots p_l, \tag{4.1}$$

where $a \in \mathbb{N}$, and the p_i are l different primes of the form $2^{2^k} + 1$ for $1 \leq i \leq l$, see Wussing (1976), page 20.
Note, that this result is not constructive for the general case. It is rather difficult to construct even the regular 17-gon by ruler and compass, see Stewart (1977).
Gauss also guessed in article 365 that the high-degree equations of which he used at the decomposition of the periods cannot be reduced to equations of lower degree by ruler and compass, i.e. the values for n in equation (4.1) are the only ones which lead to a regular n-gon that can be constructed by ruler and compass only. Gauß himself did not prove this conjecture anymore.
For a detailed discussion of his theory, see e.g. Bachmann (1973), pp. 32–40.

5. Gauß Periods

5.1. Introduction. As we have already seen, for some q and n there does not exist an optimal normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In this section, we will consider constructions and results that have already been done in the literature, and we will obtain a deterministic construction of normal bases.
In the next section, we make a new generalization and obtain new results.

We make use of the construction of Gauß periods that we got to know in Section 4.
Now the situation is the following:
Let $n, k \geq 1$ be integers such that $r = nk + 1$ is prime and $\gcd(q, r) = 1$. Then the group $\mathbb{Z}_{nk+1}^{\times}$ of units modulo $nk + 1$ is cyclic and has nk elements. By Fermat's Little Theorem (Fact 2.5), we have $q^{nk} \equiv 1 \bmod r$, i.e., $r | q^{nk} - 1$. On the other hand, we have $\#\mathbb{F}_{q^{nk}}^{\times} = q^{nk} - 1$ since $\mathbb{F}_{q^{nk}}$ is a field. The group of units in $\mathbb{F}_{q^{nk}}$ is cyclic which we know by Fact 2.1, hence, for any divisor of the group order there is at least one element of this order. So there exists a primitive rth root of unity $\beta \in \mathbb{F}_{q^{nk}}$, and β^a is well–defined for any $a \in \mathbb{Z}_{nk+1}^{\times}$. Then we can define the following element:

Definition 5.1. *Let $\mathcal{K} < \mathbb{Z}_{nk+1}^{\times}$ be the unique subgroup of $\mathbb{Z}_{nk+1}^{\times}$ of order k, and let β be a primitive rth root of unity in $\mathbb{F}_{q^{nk}}$. Then*

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

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

This construction can be found in several documents on finite fields. Mullin *et al.* (1988) and Gao & Lenstra (1992) have dealt with the special case $k = 1$ and $k = 2$ which led to the theory of optimal normal basis, as we saw in section 3. Several authors have considered the situation for general k, e.g., this has been done in the books of Menezes *et al.* (1993) and Jungnickel (1993), and in the articles of Wassermann(1990, 1993) and Ash *et al.* (1989).
In the remainder of this section, the link between a Gauß period and a normal basis is shown. There will also be given some good results that can be achieved with the help of normal bases via Gauß periods.
But first, Definition 5.1 and the original definition of Gauß periods will be compared.

5.2. Relation to original Gauß periods. The construction in Definition 5.1 seems to be rather different from the one in Definition 4.2, since Gauß wanted to find all complex solutions of an equation and we deal with finite fields. But at second sight we find the following relations:
We use the prime $nk + 1$ which is the same as the p in Gauß' considerations. Then we have that $\Omega = \mathbb{Z}_{nk+1}^{\times}$.
Gauß used a subgroup generated by a power of a primitive root modulo $nk+1$. In the case of Definition 5.1 an arbitrary subgroup $\mathcal{K}$ of $\mathbb{Z}_{nk+1}^{\times}$ of order k is taken, where k is a divisor of the group order of $\mathbb{Z}_{nk+1}^{\times}$.

We only consider the case $\lambda = 1$ and instead of a primitive root g we use a prime power q which is a unit modulo $nk + 1$. While Gauß used a power of g as the generator for the subgroup of the residues mod p, in Definition 5.1 q and the subgroup $\mathcal{K}$ of $\mathbb{Z}_{nk+1}^{\times}$ are not necessarily related. According to the original definition (see 4.2) (f, λ) is nothing else than $\mathcal{K}$.
Gauß showed that $\Omega = \bigcup_{i=0}^{e-1}(f, \lambda g^i)$ if λ is not divisible by p. In our notation, we get $\mathbb{Z}_{nk+1}^{\times} = \bigcup_{i=0}^{n-1} q^i\mathcal{K}$. As we will see in Lemma 5.3, the latter condition is not always true. But since we weakened some of the properties which Gauß demanded, this is not astonishing. Nevertheless, the second condition holds in many cases as we will see later.
Note also, that in Definition 4.2 a Gauß period is a set, and not a sum as it is the case in Definition 5.1, where the "actual" Gauß period is used as a set of exponents of a $(nk + 1)$–primitive root of unity β.

5.3. Gauß periods and normal bases. The relation between Gauß periods and normal bases is given in the following theorem:

THEOREM 5.2. *Let all the notations be as in Definition 5.1. The element α is normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if* $\gcd(e, n) = 1$, *where e is the index of q modulo n.*

The proof can be found in Gao *et al.* (1995) or, in a slightly different form, in Wassermann (1993).
Wassermann shows the equivalence of the normality of α to another condition, namely $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^{\times}$. We see now that this makes no difference:

LEMMA 5.3. *With all the notations as above, the two following conditions are equivalent:*

- $\langle q, \mathcal{K}\rangle = \mathbb{Z}_{nk+1}^{\times}$,
- $\gcd(e, n) = 1$.

For a proof, see Gao *et al.* (1995).
While the first condition in Lemma 5.3 is easier to check computationally for given q and n, we will see in section 6 that the second condition is more useful if we want to extend Definition 5.1 to a more general situation.
First, we give an example for a Gauß period:

Example 5.4. *Let $q = 2, n = 4, k = 3$. Then we have $r = nk + 1 = 13$. The unique subgroup of $\mathbb{Z}_{13}^{\times}$ of order 3 is $\{1, 3, 9\}$ and the order of 2 modulo 13 is 12, so the condition of Theorem 5.2 is obviously satisfied. Let β be a 13-PRU. Then we have*

$$
\begin{aligned}
\alpha &= \beta + \beta^3 + \beta^9, \\
\alpha^2 &= \beta^2 + \beta^6 + \beta^5, \\
\alpha^4 &= \beta^4 + \beta^{12} + \beta^{10}, \\
\alpha^8 &= \beta^8 + \beta^{11} + \beta^7, \\
\alpha^{16} &= \beta^3 + \beta^9 + \beta = \alpha.
\end{aligned}
$$

With the definition of Gauß periods and the relation to normal bases arise the following questions:

- Is there, for any given q and n, always a positive integer k which satifies the condition in Theorem 5.2?
- Can we determine upper bounds on the smallest such k?
- What is the complexity of such a normal basis?
- Are there any advantages of these normal bases over arbitrary normal bases concerning the arithmetic in $\mathbb{F}_{q^n}$?

We will try to answer these questions in the remainder of this section.
One of the most interesting questions in this area is, whether for any given q and n a k exists, such that all hypotheses in Theorem 5.2 are true. Since we are also interested in the density of the multiplication table of the resulting basis we want to know, in the case that such a k exists: What is the smallest possible value for k?
This leads to the following definition:

Definition 5.5. *A pair (n, k) is called* a Gauß pair *if and only if the special Gauß period of type (n, k) is a normal element in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Define*

$$
\kappa'_q(n) = \begin{cases} \inf k & : \ (n,k) \text{ is a Gauß pair, if such a } k \text{ exists,} \\ \infty & : \ \text{if no such } k \text{ exists.} \end{cases}
$$

Note that $\kappa'_q(n)$ is always ∞ or a positive integer, because if such a k exists then it has to be at least 1.
If $r = nk + 1$ is prime then we have the following equivalences concerning the existence of k:

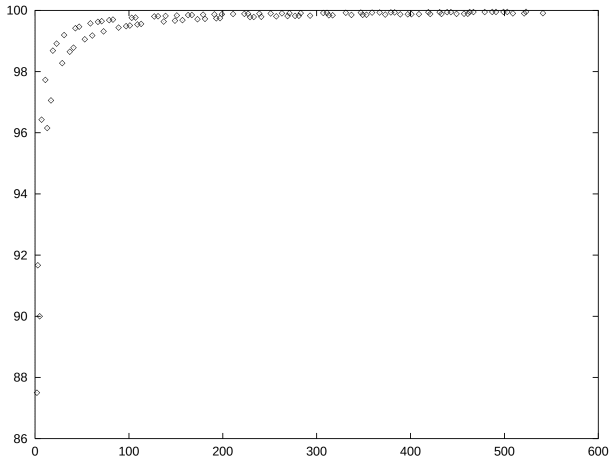

Figure 5.1: success rate for the first one hundred primes

Fact 5.6. *Let $q = p^m$ with the notations from above. Then $\kappa'_q(n) < \infty$ if and only if the following conditions hold:*
$\gcd(m, n) = 1$ *and*

- $2p \not| n$, *if* $p \equiv 1 \bmod 4$,
- $4p \not| n$, *if* $p = 2$ *or* $p \equiv 3 \bmod 4$.

For a proof, see Wassermann (1993).

In Figure 5.1 we get a notion how high the probability for given q and n is that $\kappa'_q(n) < \infty$. As values on the x-axis, the first one hundred primes are taken (the largest one is 541), and the corresponding y-value of the plotted function is the rate (in %) of positive integers n, such that there can be found at least one k with the properties of Theorem 5.2. With the conditions in Lemma 5.6, this value can be easily calculated. For $q = 2$, every integer which is not divisible by 8 leads to a Gauß pair (n, k), hence these are 87.5% of all possible n. For $p \equiv 3 \bmod 4$, we get a success rate of $(100 - 25/p)\%$, and for $p \equiv 1 \bmod 4$, we get $(100 - 50/p)\%$. Obviously, the rate of "good" n becomes large for large primes, but for the most important case in practice, namely $p = 2$, the result in figure 5.1 is not so good.
Nevertheless, we find by this construction many normal bases. The next question is, how "good" the found values for k really are.
As an example, this is shown for $q = 2$ in the following table:

Table for $q = 2$ **and** $2 \leq n \leq 1000$:

k	$\#n$ with $\kappa'_q(n) = k$
1	67
2	172
3,4,5	208
$6 \ldots 10$	270
$11 \ldots 20$	105
$21 \ldots 30$	33
$31 \ldots 40$	6
$41 \ldots 50$	3

5.4. The complexity of normal bases via Gauß periods. A great advantage of normal bases generated by Gauß periods is that the number of entries in the multiplication table can be bounded from above by a multiple of n, as we will see now.

As we saw in Section 3 we need to know how the product of two elements of the normal basis can be expressed in terms of the basis again.

Let t_{ij} be the number of elements $a \in q^i\mathcal{K}$ such that $1 + a \in q^j\mathcal{K}$, i.e.,

$$t_{ij} = |(1 + q^i\mathcal{K}) \cap q^j\mathcal{K}|.$$

Then we obtain the following result:

FACT 5.7. *Let $j_0 < n$ be the unique index, such that $-1 \in q^{j_0}\mathcal{K}$. If we define*

$$\delta_l = \begin{cases} 0 & : \quad l \neq j_0 \\ 1 & : \quad l = j_0 \end{cases}$$

for $0 \leq l < n$, then we have for any $0 \leq i, j < n$:

$$\alpha_i\alpha_j = k\delta_{i-j} + \sum_{0 \leq h < n} t_{j-ih}\alpha_{h+i}.$$

For a proof, see Gao *et al.* (1995).

The matrix $T = (t_{ij})$ is called the *multiplication table* of the normal basis generated by α.

By this, we get a good upper bound for the complexity or density of T.

If $j = j_0$ then $0 \in 1 + q^j\mathcal{K}$, and $1 + q^j\mathcal{K}$ has $k - 1$ non–zero elements. If $j \neq j_0$ then $1+q^j\mathcal{K}$ has k non–zero elements. Hence, the matrix T has $k(n-1)+k-1 = nk - 1$ non-zero elements. So, obviously, it is important to find a small k or, in general, upper bounds for k.

REMARK 5.8. *This notation for a multiplication table is a bit different from the notation for the multiplication tensor in chapter 3, since here we do not have an exact basis representation for $\alpha_i\alpha_j$ because of the summand $k\delta_{i-j}$. If we try to put this in an exact basis representation, we obtain the following: Since β is a primitive $(nk+1)$st root of unity and $x^{nk+1}-1/x-1 = x^{nk}+\cdots+x+1$, we have*

$$-1 = \sum_{1\le i\le nk} \beta^i = \sum_{0\le j<n} \alpha^{q^j}.$$

Hence, k belongs to the coefficient vector $(-k,\ldots,-k)$ with respect to the normal basis generated by α, so the complexity in the sense of Definition 3.6 is

$$c_N = n(k+1)-1.$$

5.5. Fast arithmetic using Gauß periods. Gao *et al.* (1995) show that normal Gauß periods support fast arithmetic in finite fields. They show the following two important results:

- If $\mathbb{F}_{q^n}$ is represented by a normal basis over $\mathbb{F}_q$ generated by a Gauß period of type (n,k), then we have the following:

  Multiplication in $\mathbb{F}_{q^n}$ can be done with $O(nk\log(nk)\log\log(nk))$, division with $O(nk\log^2(nk)\log\log(nk))$ and exponentiation of an arbitrary element in $\mathbb{F}_{q^n}$ can be done with $O(n^2k\log k)$ operations in $\mathbb{F}_q$(for arbitrary q and n). The exponentiation requires also a storage for $O(n/log_q^2 n)$ elements of $\mathbb{F}_{q^n}$.
- The exponentiation of a normal Gauß period can be done with $O(n^2)$ $\mathbb{F}_q$–operations (for small q and infinitely many integers n).

5.6. Upper bounds on k. For the above algorithms and the density of the multiplication table of a normal basis generated by a Gauß period it is important to find a reasonable small value for $\kappa'_q(n)$.

If $\kappa'_q(n)$ is searched experimentally, it can be seen that $\kappa'_q(n)$ is, if finite , fairly small, as we have already seen in Table 5.3. As another example, Figure 5.2 shows, how $\kappa'_q(n)$ for $q=3$ and $2\le n\le 10000$ is distributed.
As values on the x-axis, all values for $\kappa'_q(n)$ which appear for $2\le n\le 10000$ are taken, and the corresponding y-value of the plotted functions is the number of values $2\le n\le 10000$, such that $\kappa'_q(n)=x$. We see that most of the Gauß

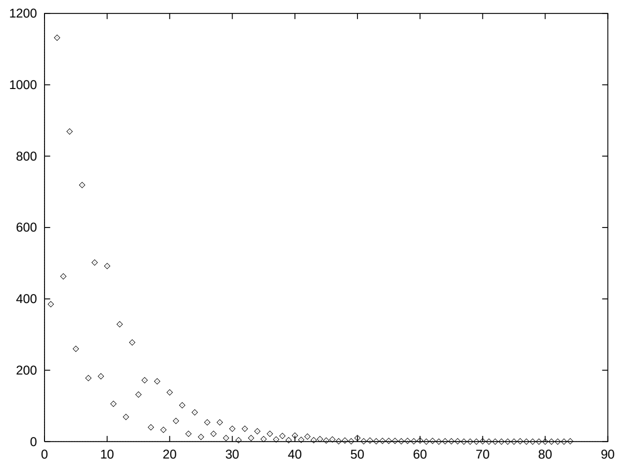

Figure 5.2: The number of values k for $2 \leq n \leq 10000$ such that $\kappa_3(n) = k$

pairs imply a $\kappa'_q(n)$ which is smaller than 10. The highest appearing value for $\kappa'_q(n)$ is 84, so an upper bound for $\kappa'_q(n)$ would be $\sqrt{n}$.
The only upper bound which is proven so far, needs the ERH:

FACT 5.9. *Let $q = p^m$ be a prime power and n be a positive integer which satisfies all the conditions from Fact 5.6. Then, assuming the ERH, there is an integer $k < cn^3 \log^2(np)$ such that $nk+1$ is a prime and $\gcd(nk/e, n) = 1$, where e is the order of q modulo $nk+1$.*

This result is taken from Adleman & Lenstra (1986), and comes originally from Bach & Shallit (1989).

6. Normal bases via general Gauß Periods

In this section we give the *new results* of this paper. While the previous sections presented the State of the Art in this area, none of the following material is in literature (except some preparatory lemmata about abelian groups).

6.1. Introduction. Gauß periods are useful to construct normal bases which support fast arithmetic in finite fields. We recall once again the notations from Section 5:
Let $n, k \geq 1$ be integers such that $r = nk + 1$ is a prime and let q be a prime power with $\gcd(q, nk+1) = 1$. Let $\beta \in \mathbb{F}_{q^{nk}}$ be a primitive $(nk+1)$st root of

unity and $\mathcal{K} < \mathbb{Z}_{nk+1}^{\times}$ be the unique subgroup of $\mathbb{Z}_{nk+1}^{\times}$ with $\#\mathcal{K} = k$. Define

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

Remember, that we call α a *Gauß period of type (n, k)* over $\mathbb{F}_q$.
In this situation we have that $\alpha \in \mathbb{F}_{q^n}$ 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 $nk + 1$, see Theorem 5.2.
With the help of this construction we have found many normal bases.
It turned out that the cost for arithmetic in $\mathbb{F}_{q^n}$ with normal bases generated by Gauß periods of type (n, k) depends not only on the size of n but also on the size of k. Hence, for arithmetic in finite fields with Gauß periods it is important to find a value for k that is as small as possible. Unfortunately, there are not always such good values. For some q and n there does not exist a value k at all such that the Gauß period of type (n, k) over $\mathbb{F}_q$ is really a normal element in $\mathbb{F}_{q^n}$, as we saw in Fact 5.6 and Figure 5.1.
Gauß himself conjectured in article 365 of the *Disquisitiones Arithmeticae* that the construction of Gauß periods might be extended from primes r to arbitrary positive integers. He says:
"These theorems retain the same or even greater elegance when they are extended to composite values of n. But these matters are on a higher level of investigation, and we will reserve their consideration for another occasion." (see Gauß, pp.438)
It is 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 the remainder of this paper this generalization is done in a way which yields better results in the following sense for given q:

- There are values of n for which the minimal value for k such that (n, k) is a Gauß pair in the new sense is strictly smaller than $\kappa'_q(n)$.
- There are integers n such that in the special case $\kappa'_q(n) = \infty$, but in the new sense there exists a k such that the corresponding Gauß period generates a normal basis.

Now, we consider the situation for an arbitrary positive integer r:

6.2. Generalization of Gauß periods. In the literature until now, only the case where $nk+1$ is prime has been studied. In the sequel, this will be referred to as the "special case". In this paper, we investigate the generalized situation with an arbitrary natural number r instead of a prime:

Let $n, k, r \in \mathbb{N}$ and q be a prime power such that $\gcd(r,q) = 1$, and $\varphi(r) = nk$. From Euler's theorem we have

$$q^{\varphi(r)} = q^{nk} \equiv 1 \bmod r, \qquad \text{hence} \qquad r \mid q^{nk} - 1.$$

Since $\#\mathbb{F}_{q^{nk}}^{\times} = q^{nk} - 1$, there exists a primitive rth root of unity $\beta \in \mathbb{F}_{q^{nk}}$. The number of units in $\mathbb{Z}_r$, i.e., the order of $\mathbb{Z}_r^{\times}$, is nk.
In the case $r = nk+1$ with r prime, the group of units modulo r is cyclic and has therefore for any divisor d of its order exactly one subgroup of order d. For an arbitrary r, the group of units modulo r is not always cyclic. The first goal is to show that in this case $\mathbb{Z}_r^{\times}$ has for any divisor of its group order *at least* one subgroup of this order.
This fact is, more generally, true for any finite abelian group G:

LEMMA 6.1. *Let G be a finite abelian group. Then G has, for any divisor of $\#G$, a subgroup of this order.*

PROOF. We let $\#G = \prod_{i=1\dots l} p_i^{s_i}$ be the prime factorization of $\#G$. According to the Fundamental Theorem for finite abelian groups, G can be written as a direct product of abelian subgroups of the orders $p_i^{s_i}$ for $1 \le i \le l$. So from now on we can assume that $\#G = p^s$ with $s \in \mathbb{N}$ positive, and p prime.
First, we show that G has a subgroup of order p. This can be seen by the following considerations:
Let $1 \neq g \in G$. Then the cyclic group $\langle g \rangle$, generated by g, is a subgroup of G with $\langle g \rangle \neq \{1\}$. Hence, $p \mid \langle g \rangle$. For a cyclic group there exists a unique subgroup for any divisor of the group order, and so there exists a subgroup U of $\langle g \rangle$ with $\#U = p$. Since U is also a subgroup of G, the claim is proven.
It is now sufficient to show that any group of order p^s has a subgroup of order p^{s-1}. This is shown by induction on s:
s=1: Then $\#G = p$ and there is nothing to show.
$s \to s+1$: Let $\#G = p^{s+1}$. As we have already seen, G has a subgroup of order p, which we denote by U. U is normal in G since G is abelian. So we can build the factor group $G/U = \nu(G)$ where ν is the canonical homomorphism from G onto G/U. G/U has p^s elements and therefore, by induction, a subgroup

V with $\#V = p^{s-1}$. Let $H = \nu^{-1}(V)$; then H is a subgroup of G of order $p \cdot p^{s-1} = p^s$, so the statement is also true for $s+1$. $\square$

For our situation, this lemma has the following consequence:
Since k is a divisor of the order of $\mathbb{Z}_r^\times$ there exists a subgroup $\mathcal{K} < \mathbb{Z}_r^\times$ with $\#\mathcal{K} = k$.
In contrast to the special case, where exactly one subgroup of order k exists, now there can be several different subgroups of $\mathbb{Z}_r^\times$ of order k. This leads to the following definition:

Definition 6.2. *Let $r, n, k \in \mathbb{N}$ and $r > 1$ with $\varphi(r) = nk$, and let q be a prime power which is coprime to r. 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 such that $q^n \in \mathcal{K}$. Then*

$$\alpha = G(n, \mathcal{K}) = \sum_{a \in \mathcal{K}} \beta^a$$

is called a general Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$. *The notation is meant to imply that $\mathcal{K}$ includes the information about the value of r.*

Note that in contrast to the special case α not only depends on the values of n and k but also on the choice of $\mathcal{K}$ as a subgroup of $\mathbb{Z}_r^\times$.

Example 6.3. *Let $q = 2, r = 55, n = 20, k = 2$. Then $\varphi(r) = 40 = 2 \cdot 20 = k \cdot n$. The group of units modulo r has three subgroups of order k, namely:*

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

Since we want to have that $\alpha \in \mathbb{F}_{q^n}$, we first need to know if for any k a subgroup $\mathcal{K}$ exists such that $\alpha = \alpha(n, \mathcal{K}) \in \mathbb{F}_{q^n}$. To prove this we need the following lemma:

Lemma 6.4. *Let r, n, k, q be as in Definition 6.2. Let $\mathcal{K}$ be an arbitrary subgroup of $\mathbb{Z}_r^\times$ of order k. Then we have $q^n \in \mathcal{K}$.*

Proof. Let $\mathcal{K}$ be a subgroup of order k of $\mathbb{Z}_r^\times$. Regard the map $\nu: \mathbb{Z}_r^\times \to \mathbb{Z}_r^\times/\mathcal{K}; a \mapsto a \bmod \mathcal{K} = \overline{a}$. The group $\mathbb{Z}_r^\times/\mathcal{K}$ has order $nk/k = n$, so $\overline{q}^n = 1$ in $\mathbb{Z}_r^\times/\mathcal{K}$, i.e. $q^n \in \mathcal{K}$. $\square$

Lemma 6.5. *With the above notation, we have $\alpha \in \mathbb{F}_{q^n}$.*

PROOF. It is sufficient to show $\alpha^{q^n} = \alpha$:

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

since $q^n \in \mathcal{K}$. □

Hence, by this construction we can really find elements in $\mathbb{F}_{q^n}$.
Now, the following questions arise:

- For which r and $\mathcal{K}$ is α a generator for a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$?
- Is α independent of the choice of β as a primitive rth root of unity?

These questions will be discussed now.

6.3. When is a Gauß period normal? Remember from section 5 that there are two equivalent conditions which are in the special case both necessary and sufficient for the normality of α in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. These are the following:

$$\gcd(e, n) = 1, \tag{6.1}$$

$$\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times. \tag{6.2}$$

Note, that condition (6.1) is easier to check computationally than condition (6.2).
In the general case, the equivalence does not hold anymore. Only one implication is true, as we will see now. In preparation, we need the following lemma:

LEMMA 6.6. *If $0 \le i < j < n$ and $q^i\mathcal{K} \cap q^j\mathcal{K} \ne \emptyset$, then $q^i\mathcal{K} = q^j\mathcal{K}$.*

PROOF. Assume that $q^i\mathcal{K} \cap q^j\mathcal{K} \ne \emptyset$ for some indices $i \ne j$. Then there exist $s, t \in \mathcal{K}$ such that $sq^i = tq^j$. Then $ts^{-1} = q^{i-j}$, hence, $q^{i-j} \in \mathcal{K}$, since $\mathcal{K}$ is a subgroup of $\mathbb{Z}_r^\times$.
Let $x \in q^i\mathcal{K}$, so that $x = q^i x'$ with $x' \in \mathcal{K}$. Then

$$x = q^i x' = q^i q^{-(i-j)} q^{i-j} x' = q^j q^{i-j} x' \in q^j\mathcal{K},$$

since $q^{i-j} \in \mathcal{K}$. By symmetry, we also have $q^j\mathcal{K} \subseteq q^i\mathcal{K}$, hence the two sets are equal. □

Now we see that one implication is still true:

Lemma 6.7. *In the above notation, if* $\gcd(e,n)=1$, *then* $\langle q,\mathcal{K}\rangle = \mathbb{Z}_r^\times$.

Proof. It is sufficient to show that $q^i\mathcal{K}\cap q^j\mathcal{K}=\emptyset$ for all $0\le i<j<n$, because in that case $\#\bigcup_{0\le l<n} q^l\mathcal{K} = \sum_{0\le l<n}\#q^l\mathcal{K} = nk = \#\mathbb{Z}_r^\times$ and hence $\langle q,\mathcal{K}\rangle=\mathbb{Z}_r^\times$.

We assume the contrary: $q^i\mathcal{K}\cap q^j\mathcal{K}\ne\emptyset$ for some $0\le i<j<n$. From Lemma 6.6 we get $q^i\mathcal{K}=q^j\mathcal{K}$. Hence, $q^{j-i}\in\mathcal{K}$ and $(q^{j-i})^k\equiv 1 \bmod r$ with $1\le j-i<n$. Thus for o, the order of q modulo r, we have $o\mid (j-i)k$ and since $o\mid nk$, there exists a proper divisor d of n with $o\mid dk$. This implies that $\frac{n}{d}\mid\frac{nk}{o}=e$ and $\frac{n}{d}>1$. So $\gcd(e,n)>1$ and this contradiction proves the lemma. □

But the two conditions are not equivalent anymore as the following example shows:

Example 6.8. *We choose the values* $r=8, n=2, k=2, q=3$, *so that* $\varphi(8)=4=nk$. *Let* $\mathcal{K}=\{1,5\}$. *This is a subgroup of the group of units modulo 8 and it is easy to see that* $\langle 3,\{1,5\}\rangle=\{1,3,5,7\}=\mathbb{Z}_8^\times$. *But* $3^2\equiv 1 \bmod 8$, *so that* $e=2$ *and* $\gcd(e,n)=2$.

We see in the next two sections whether the conditions (6.1) and (6.2) still have a meaning for the normality of a Gauß period α. We first deal with condition (6.1):

6.3.1. The condition "$\gcd(e,n)=1$**".** This condition is not sufficient anymore for the normality of α, as the following example shows.

Example 6.9. *Let* $q=2, r=9, n=6$, *and* $k=1$. *Then* $\varphi(r)=6=nk$. *For* e, *the index of 2 modulo 9, we have* $e=1$ *and hence* $\gcd(e,n)=1$. *So we get the Gauß period* $\alpha=\beta\in\mathbb{F}_{2^6}$, *where* β *is a primitive 9th root of unity. The conjugates of* α *over* $\mathbb{F}_2$ *are* $\alpha^2=\beta^2, \alpha^{2^2}=\beta^4, \alpha^{2^3}=\beta^8, \alpha^{2^4}=\beta^7$ *and* $\alpha^{2^5}=\beta^5$. *The minimal polynomial of* β *over* $\mathbb{F}_2$ *is* $\phi_9=x^6+x^3+1$. *So* $\alpha^{2^4}=\beta^7=\beta^4+\beta=\alpha^{2^2}+\alpha$, *i.e., the conjugates of* α *are not linearly independent and so* α *is not normal over* $\mathbb{F}_2$.

Another example shows that the condition is not necessary either:

Example 6.10. *Let* $r=21, n=6, k=2$, *and* $q=2$; *then* $\varphi(21)=12=nk$. *Choose* $\mathcal{K}=\{1,20\}$, *hence* $\alpha=\beta+\beta^{20}$ *for a primitive 21st root of unity* β. *The order of 2 modulo 21 is 6, so* $e=2$. *Then, we have* $g=\gcd(2,6)=2>1$, *but it can be shown that* α *is normal in* $\mathbb{F}_{2^6}$ *over* $\mathbb{F}_2$.

The condition (6.1) is only necessary for the normality of α if $\mathbb{Z}_r^\times$ is cyclic, which we will see now. In preparation, we need the following two lemmata:

LEMMA 6.11. *Let G be a finite abelian group and $g \in G$ with ord$(g) = e_1$. Let e_2 be a divisor of $\#G$ with $e_1 \mid e_2$. Then there exists a subgroup $U < G$ with $\#U = e_2$ and $g \in U$.*

PROOF. Let $V = \langle g \rangle$, so that $V < G$ and $\#V = e_1$. Since G is an abelian group, V is normal. Let $\nu : G \to G/V$ be the canonical homomorphism from G to G/V. Then $\#(G/V) = \frac{\#G}{e_1}$. Let W be a subgroup of G/V with order $\frac{e_2}{e_1}$ which exists by Lemma 6.1.
Claim: W can be written as U/V where $U < G$, $g \in U$ and $\#U = e_2$.
Let $U = \nu^{-1}(W)$. As homomorphic preimage of a subgroup, U is a group itself, and $W = U/V$.
Since $\nu(g) = 1_{G/V} \in W$, g is an element of U.
Furthermore, $\#W = \frac{\#U}{\#V}$, hence $\#U = \#W \cdot \#V = \frac{e_2}{e_1} \cdot e_1 = e_2$. □

LEMMA 6.12. *If $g = \gcd(e, n)$, then there exists a subgroup $\mathcal{K}$ of order k of $\mathbb{Z}_r^\times$ with $q^{n/g} \in \mathcal{K}$.*

PROOF. Let o be the order of q modulo r. Then, we have

$$\begin{aligned} g \mid e = \frac{nk}{o} \quad &\Rightarrow \quad o \mid \frac{nk}{g} \Rightarrow q^{nk/g} \equiv 1 \bmod r \\ &\Rightarrow \quad \left(q^{n/g}\right)^k \equiv 1 \bmod r \quad (\text{since } g \mid n) \\ &\Rightarrow \quad \mathrm{ord}_r(q^{n/g}) \mid k. \end{aligned}$$

Lemma 6.11 implies the existence of $\mathcal{K}$, as claimed. □

We will see now that if α is normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and $g > 1$, then the subgroup of Lemma 6.12 is not the right choice for a normal basis generator α.

LEMMA 6.13. *Let α be a normal Gauß period of type $(n, \mathcal{K})$ in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. If $g = \gcd(e, n) > 1$, then $q^{n/g} \notin \mathcal{K}$.*

PROOF. Let $\alpha = \sum_{a \in \mathcal{K}} \beta^a$. If $q^{n/g} \in \mathcal{K}$ then:

$$\alpha^{q^{n/g}} = \left(\sum_{a \in \mathcal{K}} \beta^a\right)^{q^{n/g}} = \sum_{a \in \mathcal{K}} \beta^{a q^{n/g}} = \sum_{a \in \mathcal{K}} \beta^a = \alpha.$$

Since $q^{n/g} \in \mathcal{K}$, we have $\alpha \in \mathbb{F}_{q^{n/g}}$ with $n/g < n$, and α is not normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. This contradiction proves the Lemma. □

Corollary 6.14. *With the above notation, if $\mathbb{Z}_r^\times$ is cyclic and α is a generator for a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then $g = 1$.*

Proof. If $\mathbb{Z}_r^\times$ is cyclic then there exists a unique subgroup $\mathcal{K} < \mathbb{Z}_r^\times$ of order k. We have $q^{n/g} \in \mathcal{K}$ from Lemma 6.12. If $g > 1$, then Lemma 6.13 shows that α generates no normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. So $g = 1$ holds. $\square$

Recall from Fact 2.19 that the numbers r for which $\mathbb{Z}_r^\times$ is cyclic are exactly the following:

$$r \in \{1, 2, 4, p^m, 2p^m\},$$

where p is an odd prime and $m \in \mathbb{N}$.
As we can see, these include the special case "r prime", for which condition (6.1) is sufficient and necessary for the normality of α, as we saw in section 5. We hope now that condition (6.2) is more useful for the normality of general Gauß periods.

6.3.2. The condition "$\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$". This condition is, unlike condition (6.1), necessary for the normality of α, as we will see in the following theorem:

Theorem 6.15. *If the Gauß period $\alpha = G(n, \mathcal{K})$ generates a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, then $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$.*

Proof. If we assume that $\langle q, \mathcal{K}\rangle \neq \mathbb{Z}_r^\times$, then there are indices $0 \le i < j < n$ with $q^i\mathcal{K} = q^j\mathcal{K}$, by Lemma 6.6. Then

$$\begin{aligned}\alpha^{q^i} &= \left(\sum_{a\in\mathcal{K}} \beta^a\right)^{q^i} = \sum_{a\in\mathcal{K}} \beta^{aq^i} = \sum_{a\in q^i\mathcal{K}} \beta^a \\ &= \sum_{a\in q^j\mathcal{K}} \beta^a = \sum_{a\in\mathcal{K}} \beta^{aq^j} = \left(\sum_{a\in\mathcal{K}} \beta^a\right)^{q^j} = \alpha^{q^j}.\end{aligned}$$

So α is not normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and this contradiction proves the theorem. $\square$

Hence, we have found a necessary condition for the normality of α for an arbitrary positive integer r.

Unfortunately, the condition "$\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$" is complicated to check, so that we hope to find other necessary conditions which are easier to check, like the one of (6.1). We will see some of them in section 6.4.

The condition "$\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$" is not sufficient for the normality of α, as the following example shows:

EXAMPLE 6.16. *Let $r = 8$, $q = 3, n = k = 2$. So $\varphi(8) = 4 = 2\cdot 2 = n\cdot k$. Using the subgroup $\mathcal{K} = \{1,5\}$ of $\mathbb{Z}_8^\times = \{1,3,5,7\}$, we have $\langle q,\mathcal{K}\rangle = \langle 3,\{1,5\}\rangle = \mathbb{Z}_8^\times$. So the hypothesis of Theorem 6.15 is satisfied.*
Let β be a primitive 8th root of unity, so that $\alpha = \beta + \beta^5$. The minimal polynomial for β over $\mathbb{F}_3$ is x^2+x+2 but $x^5+x = (x^2+x+2)(x^3+2x^2+2x)$, hence $x^2+x+2 | x^5+x$. So $\alpha = 0$ in $\mathbb{F}_9$, and is therefore not normal in $\mathbb{F}_9$ over $\mathbb{F}_3$.

Hence, we have found a necessary condition for the normality of α, and, what is really good, under this condition the construction of the normal basis does not depend on the choice of β as a primitive rth root of unity:

LEMMA 6.17. *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. If β is a primitive rth root of unity, then all other rth primitive roots of unity are given by β^s where $1 \le s < m$ and $\gcd(s,m) = 1$. So $\beta' = \beta^s$ for such an s. Since $\langle q,\mathcal{K}\rangle = \mathbb{Z}_r^\times$, there is an index $j \in \{0,\ldots,n-1\}$ with $s \in q^j\mathcal{K}$. Thus

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

and α and α' are conjugate. □

So under this condition, the same set of conjugates is generated, no matter which rth primitive root of unity is chosen. In particular, this is true whenever the resulting Gauß period is normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

In the next section we get to know another necessary condition for the normality of α which can not be derived from the special case.

6.3.3. The condition "r is squarefree". As we will see in this part of the paper, it is necessary for the normality of α that the positive integer r which is used to construct α is a squarefree number, i.e., r has no prime power with an exponent greater than 1 as a divisor.
It will also be shown that for some special cases for n we have determined *all* general Gauß periods.
Before we obtain this result, we have to do some preparations.

Definition 6.18. *The* Möbius function $\mu\colon \mathbb{N} \to \mathbb{Z}$ *is a function on the positive integers, which is defined as follows:*

$$\mu(r) = \begin{cases} 1 & \text{if } r = 1, \\ 0 & \text{if } r \text{ is not squarefree,} \\ (-1)^s & \text{if } r \text{ is a product of } s \text{ distinct primes.} \end{cases}$$

Lemma 6.19. *Let q be a prime power, r be a positive integer with $r > 1$ which is coprime to q, and F be an arbitrary field with* $\operatorname{char}(F) = 0$ *or* $\gcd(\operatorname{char}(F), q) = 1$. *Let $I = \{i \in \mathbb{N}\colon 1 \le i < r$ and $\gcd(i,r) = 1\}$ be the usual set of representatives for $\mathbb{Z}_r^\times$ and $f = \sum_{i\in I} x^i \in F[x]$. Then we have*

$$f \equiv \mu(r) \bmod \phi_r.$$

Proof. We distinguish two cases: "r is not squarefree" and "r is squarefree". If r is not squarefree, then we can write $r = u \cdot v$ where $u, v \in \mathbb{N}, u|v$ and $u > 1$. Let $f = \sum_{i\in I} x^i \in F[x]$. For every $i \in I$ there exists a unique representation of i as $i = j \cdot v + l$ with $j, l \in \mathbb{N}$ and $0 \le l < v$ and $0 \le j < u$ (division with remainder). We note that

$$\gcd(i,r) = 1 \Leftrightarrow \gcd(i,v) = 1 \Leftrightarrow \gcd(l,v) = 1,$$

since v and r have the same prime divisors. So, if $J = \{0, \ldots, u-1\}$ and $L = \{l \in \mathbb{N}\colon 1 \le l < v$ and $\gcd(l,v) = 1\}$, then

$$\begin{array}{rcl} J \times L & \longrightarrow & I \\ (j,l) & \longmapsto & j \cdot v + l \end{array}$$

is a bijection.
Hence, we get

$$\begin{aligned} f &= \sum_{i\in I} x^i = \sum_{j\in J, l\in L} x^{jv+l} = \sum_{l\in L} x^l \cdot \sum_{j\in J} x^{jv} \\ &= \sum_{l\in L} x^l \cdot \left(\frac{x^{uv}-1}{x^v-1}\right) = \sum_{l\in L} x^l \cdot \left(\frac{\prod_{d|r} \phi_d}{\prod_{t|v} \phi_t}\right). \end{aligned}$$

In particular, ϕ_r divides the numerator of this fraction. Since $u > 1$, ϕ_r does not divide the denominator of the fraction, so that ϕ_r divides the whole expression, i.e., $\phi_r | f$ and therefore we have $f \equiv 0 = \mu(r) \bmod \phi_r$.
For the second part of the proof let r be squarefree, i.e. $r = \prod_{1\le i\le s} p_i$, where the p_i are distinct primes for $1 \le i \le s$.

For $1 \leq i \leq s$, let $A_i = \{1, \ldots, p_i - 1\}$ and $l_i \in \mathbb{Z}$ such that

$$l_i \equiv \begin{cases} 1 \bmod p_i, \\ 0 \bmod p_l,\ l \neq i. \end{cases}$$

Then

$$\begin{array}{rcl} \chi : A_1 \times \cdots \times A_s & \longrightarrow & I \\ (a_1, \ldots, a_s) & \longmapsto & a_1 l_1 + \cdots + a_s l_s \text{ rem } r \end{array}$$

(where rem is the remainder at division of $a_1 l_1 + \cdots + a_s l_s$ by r) is a bijection, by the Chinese Remainder Theorem (see 2.11).
Let $i = \chi(a_1, \ldots, a_s)$, then we have $x^i \equiv x^{\chi(i)} \bmod x^r - 1$.
Hence, we can write f in the following way:

$$\begin{aligned} f &= \sum_{i \in I} x^i \equiv \sum_{a_1 \in A_1} \cdots \sum_{a_s \in A_s} x^{l_1 a_1 + \cdots + l_s a_s} \bmod x^r - 1 \\ &= \prod_{1 \leq j \leq s} \Big(\sum_{i \in A_j} (x^{l_j})^i \Big) \bmod x^r - 1 \\ &= \prod_{1 \leq j \leq s} (\phi_{p_j}(x^{l_j}) - 1) \bmod x^r - 1. \end{aligned}$$

Since ϕ_r divides $x^r - 1$, we also have

$$f \equiv \prod_{1 \leq j \leq s} (\phi_{p_j}(x^{l_j}) - 1) \bmod \phi_r.$$

We now show that the l_j-th power of a root of ϕ_r is a root of ϕ_{p_j} for each $1 \leq j \leq s$.
Let β be a root of ϕ_r in an extension field of F. Since ϕ_r is the r-th cyclotomic polynomial, β is a primitive r-th root of unity.
From Remark 2.14, we know that β^{l_j} is a primitive root of unity of order $r/\gcd(r, l_j) = p_j$. So $\phi_{p_j}(\beta^{l_j}) = 0$, $\phi_r(x) | \phi_{p_j}(x^{l_j})$ and

$$f \equiv (-1)^s = \mu(r) \bmod \phi_r.$$

□

With the help of this lemma we can make a conclusion for a general Gauß period α:

THEOREM 6.20. *Let $r > 1$ be a positive integer, n, k, q, β be as in Definition 6.2 and let $\mathcal{K}$ be a subgroup of order k of $\mathbb{Z}_r^\times$ such that $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$. If α is a Gauß period of type $(n, \mathcal{K})$ then*

$$\mathrm{Tr}(\alpha) = \overline{\mu(r)},$$

where $\overline{\mu(r)} = \mu(r) \bmod \mathrm{char}(\mathbb{F}_q) \in \mathbb{F}_q$.

PROOF. Let I, f be as in Lemma 6.19. Then $f \equiv \mu(r) \bmod \phi_r$, i.e. $\phi_r | f - \mu(r)$. Since $\phi_r(\beta) = 0$, we have

$$\overline{\mu(r)} = f(\beta) = \sum_{i \in I} \beta^i = \sum_{0 \le j < n} \sum_{l \in q^j \mathcal{K}} \beta^l = \sum_{0 \le j < n} \alpha^{q^i},$$

since $\langle q, \mathcal{K}\rangle = I$. But

$$\sum_{0 \le j < n} \alpha^{q^i} = \mathrm{Tr}(\alpha),$$

so the claim holds. □

As a first corollary, we obtain a new necessary condition for the normality of α:

COROLLARY 6.21. *With the notation of Theorem 6.20, if α is normal then r is squarefree.*

PROOF. If α is normal, we have shown in Theorem 6.15, that $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$. So all the assumptions of Theorem 6.20 are true. If $r > 1$ is not squarefree, then $\mathrm{Tr}(\alpha) = 0$, so $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ are not linearly independent, and therefore, α is not normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Hence, r is a squarefree integer. □

In some cases, the condition "r squarefree" is even sufficient for the normality of α:

COROLLARY 6.22. *Let $n = p^t$, where p is the characteristic of $\mathbb{F}_q$ and t is a positive integer. With the notation from above we have*

$$\alpha \text{ normal in } \mathbb{F}_{q^n}/\mathbb{F}_q \Leftrightarrow \left\{ \begin{array}{c} \langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times \\ r \text{ squarefree} \end{array} \right\} \tag{6.3}$$

PROOF. In Corollary 3.14, it is shown for general elements $\alpha \in \mathbb{F}_{q^n}$ that α is normal over $\mathbb{F}_q$ if and only if $\mathrm{Tr}(\alpha) \neq 0$. But by Theorem 6.20 we know that $\mathrm{Tr}(\alpha) \neq 0$ if and only if $r > 1$ is squarefree. □

CONJECTURE 6.23. *The statement (6.3) holds for arbitrary n.*

6.4. Other necessary conditions. From a computational point of view, the condition $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$ is not as easy to check as, e.g., the condition "$\gcd(e,n) = 1$". So it is perhaps easier to check if the latter condition is satisfied, and if this is not the case, the computation can be stopped.
Some other conditions of this type, i.e., which are necessary for "$\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$" and therefore for the normality of α, but which are not sufficient, will be shown in the following lemma:

LEMMA 6.24. *Let all the notations be as above. If $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$, then the following conditions are true:*

1. *$q^n \in \mathcal{K}$,*
2. *$o \geq n$, where o is the order of q modulo r,*
3. *The factor group $\mathbb{Z}_r^\times/\mathcal{K}$ is cyclic.*

PROOF.

1. Assume that $q^n \notin \mathcal{K}$. Then $q^n \in q^j\mathcal{K}$ for some $j \in \{1, \ldots, n-1\}$, since $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$. Thus $q^{n-j} \in \mathcal{K}$. Then $\mathbb{Z}_r^\times = \bigcup_{i=0}^{n-j-1} q^i\mathcal{K}$, and therefore
$$nk = \#\mathbb{Z}_r^\times \leq k(n-j) = nk - jk < nk.$$
Hence, $q^n \in \mathcal{K}$.

2. With a similar argument as in 1.) and 2.) we get that $o \geq n$. Assume that $o < n$. Then $q^o = 1 \in \mathcal{K}$, and $\mathbb{Z}_r^\times$ can be written as $\mathbb{Z}_r^\times = \bigcup_{i=0}^{o-1} q^i\mathcal{K}$. Hence, $nk = \#\mathbb{Z}_r^\times \leq ok < nk$. By this contradiction, we get $o \geq n$.

3. $\mathbb{Z}_r^\times/\mathcal{K}$ can be written in the following way:
$$\begin{aligned} \mathbb{Z}_r^\times/\mathcal{K} &= \{a\mathcal{K} \mid a \in \mathbb{Z}_r^\times\} \\ &= \{a\mathcal{K} \mid a \in \bigcup_{i=0}^{n-1} q^i\mathcal{K}\} \\ &= \{q^i\mathcal{K} \mid i = 0, \ldots, n-1\} \,(\text{since}\, a \in q^j\mathcal{K} \Rightarrow a\mathcal{K} \subseteq q^j\mathcal{K}). \end{aligned}$$
Define $\eta\colon \mathbb{Z}_r^\times/\mathcal{K} \to \mathbb{Z}_n$ by $\eta(q^i\mathcal{K}) := i$. Then it can be easily checked that η is a surjective group homomorphism. Since $\#(\mathbb{Z}_r^\times/\mathcal{K}) = n$, we have that η is a group isomorphism. But $\mathbb{Z}_n$ is cyclic and therefore the proposition is proved.

REMARK 6.25. *Unfortunately, none of the conditions in Lemma 6.24 is equivalent to* $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$, *as we will see now: Let* $r = 8$, *and* $q = 3$. *Then* $\varphi(8) = 4 = 2 \cdot 2$. *Let* $n = k = 2$ *and* $\mathcal{K} = \{1, 3\}$, *then we have that* $\mathbb{Z}_r^\times/\mathcal{K}$ *is cyclic, since it has only 2 elements and* $e = 2 = n$ *and* $q^n = 3^2 = 1 \in \mathcal{K}$, *so the three conditions in Lemma 6.24 are true, but* $\langle 3, \{1, 3\}\rangle = \{1, 3\} = \mathcal{K} \neq \mathbb{Z}_8^\times$.

The last condition is obviously not easy to check, but if we want to construct general Gauß periods, we have to find all subgroups of a given order k of $\mathbb{Z}_r^\times$. For this reason, we have to determine the type of the group $\mathbb{Z}_r^\times$ (see Section 7.2) and so it is possible to concentrate on special types for a subgroup $\mathcal{K}$ of order k such that the factor group $\mathbb{Z}_r^\times/\mathcal{K}$ has to be cyclic.
Another condition which is probably better to check is even equivalent to $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$:

LEMMA 6.26. *Let* q, r, n, k *be as above and let* $\mathcal{K}$ *be a subgroup of order* k *of* $\mathbb{Z}_r^\times$. *Then we have*

$$\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times \Leftrightarrow q^{\frac{n}{s}} \notin \mathcal{K}$$

for any prime s *which divides* n.

PROOF. We consider the map $\nu\colon \mathbb{Z}_r^\times \to \mathbb{Z}_r^\times/\mathcal{K}$ with $\nu(a) = a\mathcal{K} = \overline{a}$. ν is a surjective group homomorphism. Now we have

$$\#\langle q, \mathcal{K}\rangle = nk \Leftrightarrow q^i\mathcal{K} \cap q^j\mathcal{K} = \emptyset \Leftrightarrow \overline{q}^i \cap \overline{q}^j = \emptyset$$

for $0 \le i < j < n$. But this is true if and only if the order of $\overline{q}$ in $\mathbb{Z}_r^\times/\mathcal{K}$ is n, and this is true if and only if $\overline{q}^{n/s} \neq 1$ in $\mathbb{Z}_r^\times/\mathcal{K}$, i.e. $q^{n/s} \notin \mathcal{K}$. □

To check this condition, it is necessary to factor n and to check the condition for all the prime factors of n. This is in general not as costly as the test for the condition $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$ by enumerating $\langle q, \mathcal{K}\rangle$.

6.5. Experimental results with general Gauß periods. We know by now that we can construct normal bases in a more general way. The question is whether the efforts for the generalization are really worth–while, e. g. whether lower values for k can be found in this case.
As in the special case, 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 $\#\mathcal{K} = k$, over $\mathbb{F}_q$ exists:

Definition 6.27. *A pair* $(n, \mathcal{K})$ *is called* a Gauß pair *if and only if the Gauß period of type* $(n, \mathcal{K})$ *is a normal element in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$. *Define*

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

Obviously, we have $\kappa_q(n) \leq \kappa'_q(n)$ for all q and n, see Definition 5.5.
We now will see that there are cases for given q and n in which $\kappa_q(n) < \kappa'_q(n)$:

Example 6.28. *The following example shows that the generalized construction of Gauß periods improves the special case:*
Let $q = 2$. *For* $n = 20$ *we find a smaller value for* k *than in the special case. While* $\kappa'_2(20) = 3$, *in the general case* $k = 2$ *is sufficient. We take* $r = 55$, *so that* $\varphi(r) = 40$, *and the two subgroups*

$$\mathcal{K}_1 = \{1, 21\} \quad \textit{and} \quad \mathcal{K}_2 = \{1, 54\}$$

yield normal elements of type $(n, \mathcal{K}_1)$ *and* $(n, \mathcal{K}_2)$ *of* $\mathbb{F}_{2^{20}}$ *over* $\mathbb{F}_2$ *such that* $\kappa_2(20) = 2$.

More examples for $q = 2$ can be seen in Table 6.1.
Another success of the generalization of Gauß periods is the fact that there can now be found normal Gauß periods in situations where $\kappa'_q(n) = \infty$. Some of them are given in Table 6.2.

The 31 values for $2 \le n \le 200$ with $\kappa_2(n) < \kappa_2'(n) < \infty$

n	$\kappa_q'(n)$	$\kappa_q(n)$	difference	r	$\mathcal{K}$
20	3	2	1	55	$\{1, 54\}$
21	10	8	2	203	$\{202, 41, 1, 162, 99, 146, 57, 104\}$
22	3	2	1	69	$\{22, 1\}$
34	9	6	3	309	$\{46, 47, 1, 308, 262, 263\}$
42	5	4	1	203	$\{202, 1, 146, 57\}$
44	9	2	7	115	$\{91, 1\}$
46	3	2	1	141	$\{1, 140\}$
55	12	4	8	253	$\{252, 45, 208, 1\}$
68	9	6	3	515	$\{459, 46, 1, 514, 469, 56\}$
70	3	2	1	213	$\{1, 212\}$
75	10	8	2	707	$\{706, 293, 111, 596, 414, 1, 302, 405\}$
78	7	2	5	237	$\{1, 236\}$
84	5	2	3	203	$\{1, 146\}$
92	3	2	1	235	$\{1, 234\}$
102	6	2	4	309	$\{1, 308\}$
110	6	2	4	253	$\{45, 1\}$
111	20	8	12	1043	$\{342, 895, 552, 1, 1042, 491, 148, 701\}$
116	3	2	1	295	$\{1, 176\}$
123	10	4	6	581	$\{414, 1, 580, 167\}$
132	5	2	3	299	$\{183, 1\}$
140	3	2	1	319	$\{1, 175\}$
145	10	4	6	649	$\{296, 1, 648, 353\}$
150	19	4	15	707	$\{706, 1, 302, 405\}$
154	25	4	21	667	$\{436, 666, 231, 1\}$
156	13	2	11	371	$\{1, 370\}$
159	22	4	18	749	$\{643, 1, 748, 106\}$
164	5	2	3	415	$\{1, 331\}$
166	3	2	1	501	$\{1, 166\}$
190	10	2	8	573	$\{1, 190\}$
195	6	4	2	869	$\{868, 1, 791, 78\}$
198	22	2	20	437	$\{436, 1\}$

Table 6.1

New Gauß periods for $q \in \{3,5,7,11\}$ and $2 \leq n \leq 100$

q	n	r	$\kappa_q(n)$	$\mathcal{K}$
3	12	35	2	{1,34}
3	24	119	4	{1,50,69,180}
3	36	95	2	{1,56}
3	48	119	2	{1,118}
3	60	155	2	{1,61}
3	72	323	4	{1,18,322,305 }
3	84	203	2	{1,146}
3	96	1799	16	{1,64,253,258,321,498,510,755,1044,1289,1301, 1478,1541,1546,1735,1798}
5	10	33	2	{1,10}
5	20	143	6	{1,10,43,100,133,142}
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	407	4	{1,186,221,406}
5	100	1313	12	{1,100,302,313,495,607,807,809,919,1101,1121,1303}
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	299	6	{1,22,68,139,183,185}
11	88	391	4	{1,137,254,390}

Table 6.2

For $q \in \{3,5,7,11\}$ these are all values for $2 \leq n \leq 100$ which $\kappa'_q(n) = \infty$. For $q = 2$, I have found no values for n where $\kappa'_2(n) = \infty$ and $\kappa_2(n) < \infty$.

6.6. Open questions. The following questions concerning general Gauß periods have not been answered yet:

- What are the exact conditions under which general Gauß periods form normal bases of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$? (See Conjecture 6.23.)
- Does the success of fast arithmetic achieved in the special case carry over to the general case?

7. The computation of $\kappa_q(n)$

For the computation of $\kappa'_q(n)$, there is not much to do because Lemma 5.6 and Theorem 5.2 give exact conditions for the normality of a Gauß period and these conditions are fairly easy to check.
To compute $\kappa_q(n)$, we do several preparations. E.g., one task is to find all possible values r for given n and k such that $\varphi(r) = nk$. Furthermore, we have to find for a given r and k all subgroups of $\mathbb{Z}_r^\times$ of order k.
In this section, we will present the main algorithms and their ideas.

7.1. The inverse of Euler's φ-function. We want to solve the following problem:

PROBLEM 7.1. *Given a positive integer m, find all integers n with $\varphi(n) = m$.*

DEFINITION 7.2. *Let m be a positive integer. Then*

$$\mathcal{O}(m) = \{n \in \mathbb{N}: n > 0; \varphi(n) = m\}$$

is the set of all integers which are mapped to m by Euler's φ-function.

No upper bound for the number of elements in $\mathcal{O}(m)$ has been proven so far for a general positive integer m.
Nevertheless, for an *odd* positive integer $m > 1$ it can be stated that $\mathcal{O}(m) = \emptyset$, since $\varphi(n)$ is even for $n > 2$, see Formula (2.4).
Furthermore, a conjecture of Carmichael (1907) states that $\#\mathcal{O}(m) \neq 1$ for all positive integers m. Schlafly & Wagon (1994) show that this conjecture is valid for all m below $10^{10,000,000}$.
Since there is no explicit formula to compute $\mathcal{O}(m)$ for a given m, we do the following computation:

Algorithm 7.3. *Computation of* $\reflectbox{$\varphi$}(m)$ *for all* $m \leq M$.
Input: *A positive integer* M.
Output: *An array* B *of length* M *with* $B_m = \reflectbox{$\varphi$}(m)$ *for* $1 \leq m \leq M$.

1. *Compute a bound* A_M. *(We explain this later.)*
2. *For* $1 \leq i \leq M$ *set* $B_i = \emptyset$.
3. *For* $1 \leq i \leq A_M$ *set* $B_{\varphi(i)} = B_{\varphi(i)} \cup \{i\}$.

So, after a precomputation stage, the computation of $\reflectbox{$\varphi$}(m)$ is only a table-look-up at the mth position of this array.
Note also that the space of this array can be easily reduced to half, since $\reflectbox{$\varphi$}(m) = \emptyset$ for an odd integer $m > 1$.
It remains to determine the upper bound A_M up to which $\varphi(n)$ has to be computed in the above algorithm, so that we are sure to find all elements of $\reflectbox{$\varphi$}(m)$ for a given $m \leq M$. For this reason, the following inequality is useful: For $n > 2$,

$$\frac{\varphi(n)}{n} > \frac{c}{\ln \ln n} \cdot \left(1 - \frac{1.41}{\ln^2 \ln n}\right),$$

where $c = e^{-C} \approx 0.56146$ and C is Euler's constant (see von zur Gathen & Giesbrecht (1990), Fact (3.5)).
As an example, we obtain by this inequality $A_{1000} = 5512$, $A_{10000} = 56541$, and $A_{100000} = 583647$.

7.2. Finding all subgroups of $\mathbb{Z}_r^\times$ **of a given order.** The other major task for the computation of $\kappa_q(n)$ is to find for given r and k with $k \mid \varphi(r)$ all subgroups of $\mathbb{Z}_r^\times$ of order k, see Definition 6.2. To do this, we use a general algorithm which determines an isomorphism between a finite abelian group and a direct sum of cyclic groups of prime power order.
The decomposition of a finite abelian group into a direct sum of cyclic groups can be done in two steps, namely

1. the decomposition into groups of prime power order (Notation: p-groups), and
2. the decomposition of these p-groups into a direct sum of cyclic groups.

For the first step, we have the following well-known result:

THEOREM 7.4. *A finite abelian group of order $p_1^{a_1} \cdot \dots \cdot p_s^{a_s}$ (where $p_i \neq p_j$ for all $i \neq j$, p_i prime, $a_i \in \mathbb{N}$, and $a_i > 0$ for $1 \leq i \leq s$) is the direct sum of s abelian groups P_i of order $\#P_i = p_i^{a_i}$ for $1 \leq i \leq s$.*

For a proof, see e.g. Speiser (1956), page 47.
In the literature, the P_i are called the *p_i-Sylow subgroups* of G.
The first step is rather easy to do:
The element $g \in G$ is an element in P_i if and only if $g^{p_i^{a_i}} = 1$ in G. For the determination of the p_i-Sylow subgroups, all elements in G are checked in that way.
Since the p_i-Sylow subgroups of a subgroup $\mathcal{K}$ of G are obviously subgroups of P_i, it is sufficient to determine all subgroups of P_i of a given order.
From now on, we assume that we are given a group P of prime power order, i.e. $\#P = p^a$, where $a \in \mathbb{N}$.
For the next result, we need to know the notion of a *basis* of an abelian group.

DEFINITION 7.5. *A set $B = \{b_1, \dots, b_m\}$ is a basis of a finite abelian group G if the elements of B generate G and if they are independent, in the sense that, if we are given elements $\nu_1, \dots, \nu_m$ with $0 \leq \nu_i < \mathrm{ord}(b_i)$ for all $0 < i \leq m$, where $\nu_i > 0$ for at least one integer $0 < i \leq m$, then we have, written additively*

$$\nu_1 b_1 + \cdots + \nu_m b_m \neq 0.$$

Note that this situation is equivalent to $G = \langle b_1 \rangle \oplus \cdots \oplus \langle b_l \rangle$.
Now, for p-groups, we have the following result:

THEOREM 7.6. *An abelian p-group P has a basis and is a direct sum of cyclic groups.*
More precisely:
Let $B = \{b_1, \dots, b_l\}$ be a basis of P, then the orders $p^{t_1}, \dots, p^{t_l}$ of $b_1, \dots, b_l$ are uniquely determined up to permutation.

For a proof, see Speiser (1956), pp. 49-50.
As a notation, we say: P_i has the *type* $T_i = [p^{t_1}, \dots, p^{t_l}]$. As a convention, we assume that $t_j \geq t_{j+1}$ for all $1 \leq j < l$.
Note that only the type, but not the concrete basis of P is uniquely determined.
In the algorithm, we use a constructive proof for this theorem by Douglas (1951), which works in the following way:
The elements of P are ordered in the way that the orders are non-increasing, i.e. $P = (g_1, \dots, g_{p^a})$ with $\mathrm{ord}(g_j) \geq \mathrm{ord}(g_{j+1})$ for all $1 \leq j < p^a$. Proceeding

from left to right, we mark the elements g_j which are generated by unmarked elements except themselves. This is done for all elements $g_j \in P$. Douglas (1951) shows that the elements which are, at the end of this process, not yet marked, form a basis for P.
After doing this step, we have split P into a direct sum of *cyclic* p-groups, since $P = \langle b_1 \rangle \oplus \cdots \oplus \langle b_l \rangle$.
Since we need to find *all* bases of P, we execute this algorithm for all series of elements in P with non-increasing orders.
About the subgroups of order p^b of P, where $b \leq a$, we can state the following result:

THEOREM 7.7. *Any subgroup of order p^b of a finite abelian p-group P with $\#P = p^a$, $a \geq b$, and type $T = [p^{t_1}, \ldots, p^{t_l}]$, has the type $V = [p^{v_1}, \ldots, p^{v_l}]$, where $v_j \leq t_j$ for all $0 < j \leq l$ and $\sum_{0<j\leq l} v_j = b$.*
On the other hand, for any *combination of b as a sum of $v_1, \ldots, v_l$, where $v_j \leq t_j$ for all $0 < j \leq l$, there exists at least one subgroup of P of type $[p^{v_1}, \ldots, p^{v_l}]$.*

So the next task is to find all possibilities for the type of a subgroup of a given order p^b of a p-group P. The number of these possibilities is fairly high.
Afterwards, we can build the possible bases of the subgroup using all the bases of P:
If P has the type $T = [p^{t_1}, \ldots, p^{t_l}]$, the subgroup has the type $V = [p^{v_1}, \ldots, p^{v_l}]$, and $(b_1, \ldots, b_l)$ is a basis for P then $(b_1^{p^{t_1 - v_1}}, \ldots, b_l^{p^{t_l - v_l}})$ is a basis for a subgroup of type V.
On the other hand, for any subgroup U of type V of P there exists a basis $(b_1, \ldots, b_l)$ of P such that the above construction yields a basis of U.
Note that it is possible that the same subgroup can result from many different bases of P.
At the end of our algorithm, we return to general finite abelian groups and put together all generators of subgroups of the p-Sylow subgroups of G and compute the concrete elements of the resulting subgroups of G of order k.
We regard the whole algorithm:

ALGORITHM 7.8. *Finding all subgroups of order k of $\mathbb{Z}_r^\times$.*
Input: *A positive integer r with $\varphi(r) = p_1^{a_1} \cdots p_s^{a_s}$ and an integer $k = p_1^{b_1} \cdots p_s^{b_s}$ such that $b_i \leq a_i$ for all $0 < i \leq s$.*
Output: *The set of all subgroups of order k of $\mathbb{Z}_r^\times$.*

1. *For each index i with $p_i | k$ determine the p_i-groups P_i of $\mathbb{Z}_r^\times$.*

2. *For each index i with $p_i | k$ do*

   (a) *Determine the type and all bases of P_i.*

   (b) *Find all N possible types $(V_{ij})_{1 \le j \le N}$ of a subgroup of P_i of order $p_i^{b_i}$.*

   (c) *For all $1 \le j \le N$ find all bases which generate a subgroup of type V_{ij}, using the bases of P_i as described above.*

3. *Combine all found bases of the p_i-subgroups of P_i to bases of subgroups of $\mathbb{Z}_r^\times$ of order k.*

4. *Compute the concrete elements of the subgroups.*

Note that this algorithm is very expensive, and that this is perhaps not the most clever way to do this. It seems that Magma solves this problem quite faster.
After these preparations, we can show how $\kappa_q(n)$ is computed:

7.3. The computation of $\kappa_q(n)$. Another problem about the computation of $\kappa_q(n)$ is the fact that Conjecture 6.23 is not proven yet. In the following algorithm, we determine the possible Gauß periods, afterwards we have to test if they are really normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The guarantee that the found results are the only possible ones is given by Theorem 6.21.
Now, the algorithm to find $\kappa_q(n)$ under the assumption that Conjecture 6.23 is valid, is the following:

ALGORITHM 7.9. *Computation of $\kappa_q(n)$.*
Input: *A prime power $q = p^m$ and a positive integer $n > 1$.*
Output: *$\kappa_q(n)$, together with a positive integer r and a subgroup $\mathcal{K}$ of $\mathbb{Z}_r^\times$ of order $\kappa_q(n)$.*
We assume that the necessary values for $\mathcal{A}$ (see Algorithm 7.3) are precomputed and stored in B.

1. *Set $k = 1$.*

2. *While TRUE do*

   i. *$L := B[n \cdot k]$ is the list with the elements in $\mathcal{A}(n \cdot k)$;*

   ii. *For r in L do*

      A. *If $\gcd(q, r) = 1$ and r is squarefree then*
      S:= set of subgroups of $\mathbb{Z}_r^\times$ of order $\mathcal{K}$
      (see Algorithm 7.8)

B. for $\mathcal{K}$ in S do
if $\langle q, \mathcal{K}\rangle = \mathbb{Z}_r^\times$ then break and output: $k, r, \mathcal{K}$
iii. k:=k+1

If we assume that $\kappa'_q(n) < \infty$, then the algorithm is guaranteed to terminate and returns the lowest possible value for $\kappa_q(n)$. In the case $\kappa'_q(n) = \infty$, the algorithm not always terminates but in some of these cases there is still $\kappa_q(n) < \infty$, see Table 6.5.
Afterwards, we have to check whether the resulting Gauß period is really normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and we do this by a linear independence test.
In all the computations which we have done so far, this test confirms the normality of the Gauß periods found by Algorithm 7.9.

References

L. Adleman and H. W. Lenstra, Finding irreducible polynomials over finite fields. In *Proc. 18th Ann. ACM Symp. Theory of Computing*, Berkeley CA, 1986, 350–355.

A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading MA, 1974.

D. W. Ash, I. F. Blake, and S. A. Vanstone, Low complexity normal bases. *Discrete Applied Mathematics* **25** (1989), 191–210.

L. Babai, E. M. Luks, and A. Seress, Fast management of permutation groups. (1988), 272–282.

E. Bach and J. Shallit, Factoring with cyclotomic polynomials. *Math. Comp.* **52** (1989), 201–219.

P. Bachmann, Über Gauss' zahlentheoretische Arbeiten. In *Carl Friedrich Gauss: Werke*, vol. X.2. Olms, 1973. Nachdruck.

G. Brassard and P. Bratley, *Algorithmics*. Prentice–Hall, 1988.

E. F. Brickell, D. M. Gordon, K. S. McCurley, and D. B. Wilson, Fast exponentiation with precomputation. In *Proc. Eurocrypt'92*, Balatonfűred, Hungary, 1992.

P. Bundschuh, *Einführung in die Zahlentheorie*. Springer, 1992.

R.D. Carmichael, On Euler's φ-function. *Bull. Amer. Math. Soc.* **13** (1907), 241–243.

JESSE DOUGLAS, On the existence of a basis of every finite abelian group. *Proceedings of the National Academy of Sciences* **37** (1951), 359–362.

T. ELGAMAL, A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Info. Th.* **31** (1985), 469–472.

S. GAO AND H. W. LENSTRA, Optimal normal bases. *Designs, Codes and Cryptography* **2** (1992), 315–323.

S. GAO, J. VON ZUR GATHEN, AND D. PANARIO, Gauss periods and fast exponentiation in finite fields. In *Proc. Latin '95, Valparaiso, Chile*, Springer Lecture Notes in Computer Science **911**, 1995, 311–322.

J. VON ZUR GATHEN, Irreducibility of multivariate polynomials. *J. Computer System Sciences* **31** (1985), 225–264.

J. VON ZUR GATHEN, Efficient and optimal exponentiation in finite fields. *comput complexity* **1** (1991), 360–394.

J. VON ZUR GATHEN AND J. GERHARD, Fast multipoint evaluation and interpolation at arbitrary linear subspaces of finite fields. Preprint, 1995.

J. VON ZUR GATHEN AND M. GIESBRECHT, Constructing normal bases in finite fields. *J. Symbolic Computation* **10** (1990), 547–570.

CARL FRIEDRICH GAUSS, *Untersuchungen über höhere Arithmetik.* Chelsea, New York, 1889. Nachdruck 1981.

CARL FRIEDRICH GAUSS, *Disquisitiones Arithmeticae.* Springer, New York, 1966. reprint 1986.

K. HENSEL, Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor. *J. Reine Angew. Math.* **103** (1888), 230–7.

D. JUNGNICKEL, *Finite Fields.* BI-Wissenschaftsverlag, 1993.

R. LIDL AND H. NIEDERREITER, *Finite Fields.* Addison-Wesley, 1983.

R. J. MCELIECE, *Finite Fields for Computer Scientists and Engineers.* Kluwer Academic Publishers, 1987.

ALFRED J. MENEZES, IAN F. BLAKE, XUHONG GAO, RONALD C. MULLIN, SCOTT A. VANSTONE, AND TOMIK YAGHOOBIAN, *Applications of Finite Fields.* Kluwer Academic Publishers, 1993.

P. L. Montgomery, Factorization of $X^{216091} + X + 1 \bmod 2$ – a problem of Herb Doughty. Preprint, 1991.

R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson, Optimal normal bases in $GF(p^n)$. *Discrete Applied Mathematics* **22** (1988), 149–161.

O. Ore, Contributions to the theory of finite fields. *Trans. Amer. Math. Soc.* **36** (1934), 243–274.

Aaron Schlafly and Stan Wagon, Carmichael's conjecture on the euler function is valid below $10^{10,000,000}$. *Mathematics of Computation* **63**(207) (1994), 415–419.

A. Schönhage and V. Strassen, Schnelle Multiplikation großer Zahlen. *Computing* **7** (1971), 281–292.

V. Shoup, Fast construction of irreducible polynomials over finite fields. *J. Symbolic Computation* **17** (1994), 371–391.

A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung*. Birkhäuser, Basel, 1956.

Ian Stewart, Gauss. *Scientific American* **7** (1977), 123–131.

B. L. van der Waerden, *Algebra, Erster Teil.* Springer-Verlag, Berlin, 7th edition, 1966.

A. Wassermann, Konstruktion von Normalbasen. *Bayreuther Mathematische Schriften* **31** (1990), 155–164.

A. Wassermann, Zur Arithmetik in endlichen Körpern. *Bayreuther Mathematische Schriften* **44** (1993), 147–251.

H. Wussing, *C.F.Gauß*. Teubner, Leipzig, 2nd edition, 1976.