Published in *In Finite Fields and Applications*, DIETER JUNGNICKEL & HARALD NIEDERREITER, editors, 162-177. Springer-Verlag.

Gauß Periods in Finite Fields

JOACHIM VON ZUR GATHEN[1] and IGOR SHPARLINSKI[2]

[1] Fachbereich 17 Mathematik-Informatik, Universität Paderborn
D-33095 Paderborn, Germany
gathen@upb.de
[2] Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@comp.mq.edu.au

1 Introduction

In this survey, we review two recent applications of a venerable tool: Gauß periods.
In Section 2, we describe Gauß' original construction, and how it can be used to generate normal bases in extensions of finite fields.
Section 3 contains the first application: finding elements of exponentially large order in certain finite fields. This can be viewed as a step towards solving the famous open problem of finding efficiently a primitive element in a given finite field. A pleasant feature is that the prime factorization of the order of the multiplicative group is not required. In Section 4 we give another example of the method, yielding a different kind of bound: among the q shifts $\beta + a$ of an element β of an extension of $\mathbb{F}_q$, where a runs through $\mathbb{F}_q$, at most one has "small" order.
The second application, in Section 5, deals with efficient exponentiation in finite fields, an important subroutine in some cryptographic systems. Gauß periods lead to the fastest algorithms for this problem, both in theory and in practice. In Section 6 we describe a recent generalization of Gauß construction.
Our two applications are, in turn, useful in several areas: cryptography, coding theory, pseudo-random element generation, and combinatorial designs. Actually, the two work in tandem: where one of them is required, usually the other one is as well.
The results of Section 4 are new, while the others report on the recent literature.

2 Normal bases via Gauß periods

Gauß (1801) introduced his periods as follows. He lets n, k, and r be integers, with r prime, and

$$nk = \varphi(r) = r - 1.$$

Furthermore, $\zeta \in \mathbb{C}$ is a primitive rth root of unity, and $\mathcal{K} \subseteq \mathbb{Z}_r^\times = \mathrm{Gal}\,(\mathbb{Q}(\zeta):\mathbb{Q})$ the unique subgroup of order k of the cyclic group $\mathbb{Z}_r^\times$. Then

$$\eta = \sum_{i \in \mathcal{K}} \zeta^i \in \mathbb{Q}(\zeta)$$

is the **Gauß period** of type $(n, \mathcal{K})$ over $\mathbb{Q}$.
The fields involved in this construction are as follows:

$$\begin{array}{c} \text{primitive } r\text{th root of unity } \zeta \in \mathbb{Q}(\zeta) \\ \Big| k \\ \eta = \textstyle\sum_{i \in \mathcal{K}} \zeta^i \in \mathbb{Q}(\eta) \\ \Big| n \\ \mathbb{Q} \end{array}$$

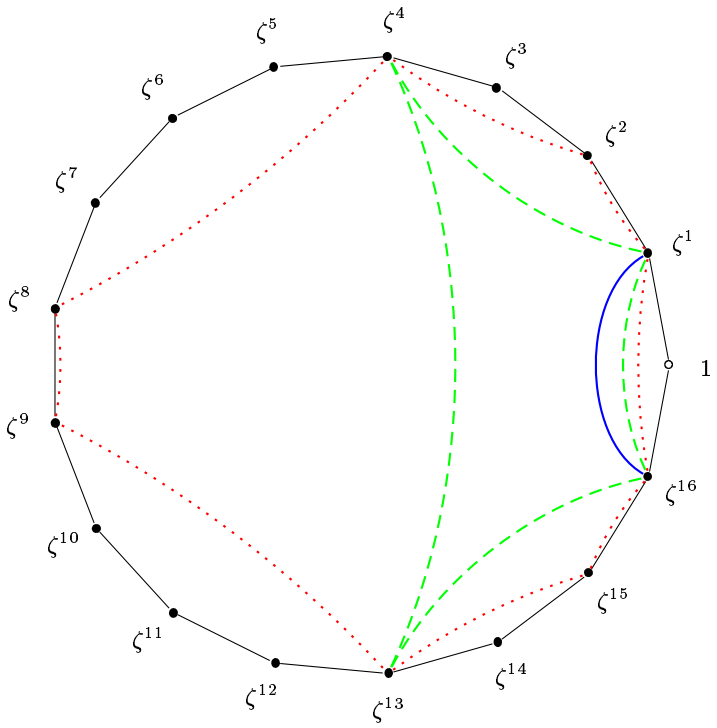

Fig. 1. 17-gon with Gauß periods of order 2, 4, and 8

As illustrated in Figure 1, Gauß used the three subgroups of orders 2 (solid line), 4 (dashed line), and 8 (dotted line) of $\mathbb{Z}_{17}^\times = \mathrm{Gal}(\mathbb{Q}(\zeta):\mathbb{Q})$ whose periods

describe a tower of field extensions from $\mathbb{Q}$ to the field generated by the primitive 17th root of unity $\zeta = e^{2i\pi/17}$, where each extension degree equals 2. This shows that the regular 17-gon can be constructed by ruler and compass. Over a finite field $\mathbb{F}_q$ with q elements, we can consider the analogous situation: we have n, k, r, and $\mathcal{K} \subseteq \mathbb{Z}_r^\times$ as above, and also require $\gcd(q, r) = 1$:

$$\begin{array}{r} \text{primitive } r\text{th root of unity } \beta \in \mathbb{F}_{q^{r-1}} \\ | k \\ \alpha = \sum_{i \in \mathcal{K}} \beta^i \in \mathbb{F}_{q^n} \\ | n \\ \mathbb{F}_q \end{array}$$

Then α is a Gauß period of type $(n, \mathcal{K})$ over $\mathbb{F}_q$. (The required β exists in $\mathbb{F}_{q^{r-1}}$, but $\mathbb{F}_q(\beta)$ may be a proper subfield of $\mathbb{F}_{q^{r-1}}$.)

A **normal basis** for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $(\gamma, \gamma^q, \ldots, \gamma^{q^{n-1}})$ of $\mathbb{F}_{q^n}$ as a vector space over $\mathbb{F}_q$. Then $\gamma \in \mathbb{F}_{q^n}$ is called *normal* over $\mathbb{F}_q$. We will see in Section 5 that this data structure for representing the elements of $\mathbb{F}_{q^n}$ is particularly useful for exponentiation. Wassermann (1990) shows that Gauß periods often generate normal bases, namely that α is normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ if and only if q and $\mathcal{K}$ together generate the multiplicative group $\mathbb{Z}_r^\times$: $\langle q \bmod r, \mathcal{K} \rangle = \mathbb{Z}_r^\times$.

3 Elements of large order

The group $\mathbb{F}_q^\times$ of units of $\mathbb{F}_q$ is cyclic of order $q - 1$. An element $\gamma \in \mathbb{F}_q^\times$ is **primitive** if and only if its order is $q - 1$.

Such elements are useful for a variety of tasks. How can we find one? Gauß writes in article 73 of his *Disquisitiones Arithmeticae* (1801): *Methodi radices primitivas inveniendi maximam partem tentando innituntur. [...] Ill. Euler confitetur, maxime difficile videri, hos numeros assignare, eorumque indolem ad profundissima numerorum mysteria esse referendam. At tentando satis expedite sequenti modo determinari possunt. Exercitatus operationis prolixitati per multifaria artificia particularia succurrere sciet: haec vero per usum multo citius quam per praecepta ediscuntur.*[1]

Gauß' method is a clever variant of exhaustive search and, in modern parlance, uses exponential time and space.

The importance of primitive elements for the human computers of the 19th century is illustrated by several publications. The *Canon arithmeticus* of Jacobi (1839) contains 240 pages of tables of primitive elements and discrete

[1] Methods for finding primitive roots are mainly reduced to trial and error. [...] The illustrious Euler admits that it is extremely difficult to find these numbers and that their nature is one of the deepest mysteries of numbers. But they can be determined easily enough by the following method. The experienced computer will know how to reduce the tediousness of the calculation by a variety of devices, but these are better taught by practice than by rules.

logarithms, one table for each prime number up to 1000. Euler had previously given such a table for $3 \le p \le 37$, and Crelle (1832) for $3 \le p \le 101$. The tables of Bussey (1906, 1910) give primitive elements in nonprime fields $\mathbb{F}_q$ for all relevant $q \le 1000$.

To test whether a given $\gamma \in \mathbb{F}_q^\times$ is primitive, we only have to check if $\gamma^{(q-1)/t} \neq 1$ for all prime divisors t of $q-1$. There are $\varphi(q-1)$ many primitive elements, so taking a random element of $\mathbb{F}_q^\times$ will give a primitive one with fairly high probability, namely $\varphi(q-1)/(q-1) \ge c/\operatorname{loglog} q$ for some absolute constant $c > 0$, see Theorem 5.1 in Chapter 1 of Prachar (1957).

Computationally, the bottleneck in this procedure is the prime factorization of $q-1$. No polynomial-time algorithm is known for this, where polynomial time means $(\log q)^{O(1)}$ operations, since the size of a reasonable representation of an element of $\mathbb{F}_q$ is proportional to $\log_2 q$. We have the following tasks:

1. test whether a given $\gamma \in \mathbb{F}_q^\times$ is primitive,
2. find a primitive element,
3. find an element of "large order".

To solve any of them in (random) polynomial time is an important open problem.

Now a further relaxation of our requirements allows a successful solution of the last problem. Namely, for a given N, we do not insist on finding a good element in $\mathbb{F}_{q^N}$, but are content if we find one in $\mathbb{F}_{q^n}$ for some n close to N, as in Theorem 1 below. A variation, mentioned at the end of this section, works when we want to work in a small extension of $\mathbb{F}_{q^N}$.

The progress here can be viewed as follows: finding a primitive element in polynomial time is a black and white question: either you have such an algorithm or you don't. Now we have a question with many shades of gray where incremental progress is possible: increase the order of the elements and decrease the degree of the field extension.

We will make use of the following famous conjecture.

Artin's conjecture: *For $a \in \mathbb{Z}$, not -1 or a square, there exists $c(a) > 0$ such that*

$$\#\{p \le x : (a \bmod p) \in \mathbb{Z}_p^\times \text{ is primitive } \} \sim c(a)\frac{x}{\log x}.$$

Hooley (1967) proved this under the Extended Riemann Hypothesis, and also determined $c(a)$ explicitly. Then Heath-Brown (1986) showed, without any assumption, that a slightly weaker lower bound of the form $c(a)x/\log^2 x$ for the cardinality of the above set holds for all prime powers a, except maybe powers of at most three primes. (It is conjectured that these three potential exceptions are an artifact of the proof and actually do not exist.) In fact, even more general results have been established in Heath-Brown (1986), but for our purposes prime powers are of primal interest. Furthermore, even a weaker version, say cardinality at least $c(a)x/\log^3 x$ for the set of prime powers a would be sufficient for our applications.

This question is already implicit in Jacobi's *Canon*, where he counts the primes modulo which 10 is primitive in the first 25 blocks of 100 integers each.

Theorem 1. *Suppose that Artin's conjecture holds for q. Then for any N there exists $n \geq N$ with $n \in O(N \log N)$ such that the Gauß period α in $\mathbb{F}_{q^n}$ of type $(n, \{\pm 1\})$ over $\mathbb{F}_q$ is normal and has order at least*

$$2^{(2n)^{1/2}-2}.$$

These n and α can be computed (probabilistically) in time polynomial in N and $\log q$.

We sketch the idea of the *proof*. Under the assumptions, we can find a prime r so that $n = (r-1)/2$ is sufficient and q is primitive in $\mathbb{Z}_r^\times$. We take a primitive rth root of unity β in $\mathbb{F}_{q^{2n}}$; then β has degree $r-1$ over $\mathbb{F}_q$. Furthermore, we consider the quantities

$$\begin{aligned}
&\alpha = \beta + \beta^{-1},\\
&h = \lfloor r^{1/2} \rfloor - 1,\\
&S = \{i : 0 \leq i \leq r-1 \text{ and } 1 \leq (q^i \text{ rem } r) \leq h\} \subseteq \mathbb{F}_r^\times,\\
&U \neq U' \subseteq S,\\
&u = \sum_{s \in U} q^s, \quad u' = \sum_{s \in U'} q^s.
\end{aligned}$$

We now claim that $\alpha^u \neq \alpha^{u'}$. If the claim is true, then we have at least 2^h different powers of α, and the lower bound on the order of α follows with an easy calculation.
If the claim is false, the following calculation yields a nonzero $f \in \mathbb{F}_q[x]$ of degree less than $r-1$ with $f(\beta) = 0$. This contradiction to the fact that β has degree $r-1$ over $\mathbb{F}_q$ proves the claim.
We may suppose that $U \cap U' = \emptyset$. We assume that $\alpha^u = \alpha^{u'}$, and thus

$$\begin{aligned}
0 = \alpha^u - \alpha^{u'} &= \prod_{s \in U} (\beta + \beta^{-1})^{q^s} - \prod_{s \in U'} (\beta + \beta^{-1})^{q^s}\\
&= \beta^{-u} \prod_{s \in U} (\beta^{2q^s} + 1) - \beta^{-u'} \prod_{s \in U'} (\beta^{2q^s} + 1).
\end{aligned}$$

Since β is an rth root of unity, we may reduce the exponents modulo r. We define

$$E = \{q^s \text{ rem } r : s \in U\}, E' = \{q^s \text{ rem } r : s \in U'\} \subseteq \{1, \ldots, r-1\},$$

$$e = \sum_{t \in E} t, \quad e' = \sum_{t \in E'} t.$$

Then $E \cap E' = \emptyset$, and

$$0 = \beta^{-e} \prod_{t \in E} \left(\beta^{2t} + 1\right) - \beta^{-e'} \prod_{t \in E'} \left(\beta^{2t} + 1\right).$$

We may assume that $e' \geq e$, and let

$$f(x) = x^{e'-e} \prod_{t \in E} \left(x^{2t} + 1\right) - \prod_{t \in E'} \left(x^{2t} + 1\right) \in \mathbb{F}_q[x].$$

Then $f(\beta) = 0$, and

$$\deg f \leq 2e' \leq 2 \sum_{1 \leq j \leq h} j = h(h+1) \leq r - \sqrt{r} < r - 1.$$

If $e' > e$, then $f(0) = -1$. Thus $e' = e$. But then the monomial $x^{2\tau}$ occurs in f with nonzero coefficient, where $\tau = \min(E \cup E')$, and we have the desired contradiction. □

Similar arguments yield:

- a denser sequence of n in Theorem 1,
- for each $\mathbb{F}_q$, a small extension $\mathbb{F}_{q^n}$ and an element of exponential order in it,
- unconditional results,
- deterministic algorithms.

These results have appeared, with complete proofs, in von zur Gathen & Shparlinski (1998, 1999).

4 A new lower bound on multiplicative orders

Applying the same method as in the previous section, we obtain a new result which is of independent interest, while its proof exhibits the main tool of our method—information about the distribution of exponential functions in residue classes.

Let $\beta \in \mathbb{F}_{q^n}^{\times}$ be a root of an irreducible polynomial in $\mathbb{F}_q[x]$ of degree $n \geq 2$. For the order t of β, we obviously have $t \geq n$. In fact, this can be strengthened a little as $\varphi(t) \geq n$. This bound is tight, since it is attained if $t = n + 1$ is prime, q is a primitive root modulo t, and β is a primitive tth root of unity. Below we show that for any $\varepsilon > 0$ there is a constant $c > 0$ such that among the q shifts $\beta + a$, with $a \in \mathbb{F}_q$, at most one is of order less than $c \cdot n^{4/3-\varepsilon}$.

We need some results about exponential sums and their distribution in residue classes of exponential functions.

Lemma 2. *Let q and r be positive integers with $\gcd(q, r) = 1$, and let τ be the order of q modulo r. Then for any integer c we have*

$$\left| \sum_{1 \leq k \leq \tau} \exp(2\pi i c q^k / r) \right| \leq \delta^{1/2} r^{1/2},$$

where $\delta = \gcd(c, r)$.

Proof. If $\delta = 1$, then this bound is essentially Theorem 10 in Chapter 1 of Korobov (1992); see also the proof of Lemma 2 in Korobov (1972). For $\delta > 1$, we denote by τ_ρ the order of q modulo $\rho = r/\delta$, and we also put $c/\delta = \gamma$. Thus $\gcd(\gamma, \rho) = 1$ and we obtain

$$\left| \sum_{1 \le k \le \tau} \exp(2\pi i c q^k / r) \right| \le \frac{\tau}{\tau_\rho} \left| \sum_{1 \le k \le \tau_\rho} \exp\left(2\pi i \gamma q^k / \rho\right) \right| \le \frac{\tau}{\tau_\rho} \rho^{1/2}.$$

Finally, we have $\tau \le \delta \tau_\rho$ by Lemma 3 of Shparlinski (1988). □

We also need the following well-known identity (see Problem 11.a of Chapter 3 of Vinogradov (1954))

$$\sum_{0 \le c < r} \exp(2\pi i c u / r) = \begin{cases} 0 \text{ if } u \not\equiv 0 \bmod r, \\ r \text{ if } u \equiv 0 \bmod r, \end{cases} \tag{1}$$

and the bound

$$\sum_{1 \le c < r} \left| \sum_{0 \le u \le h} \exp\left(2\pi i c u / r\right) \right| = O(r \log r), \tag{2}$$

which hold for any integers $r \ge 1$ and $h \ge 0$; see Problem 11.c of Chapter 3 of Vinogradov (1954).

Lemma 3. *Let q, h, and r be positive integers, τ the order of q modulo r, and T be the number of elements in $\{0, 1, \ldots, h-1\}$ that are powers of q modulo r. Then for any $\varepsilon > 0$, we have*

$$T = \frac{\tau h}{r} + O\left(r^{1/2+\varepsilon}\right).$$

Proof. From (1) we derive

$$\begin{aligned} T &= \frac{1}{r} \sum_{1 \le k \le \tau} \sum_{0 \le x < h} \sum_{0 \le c < r} \exp\left(2\pi i c (q^k - x)/r\right) \\ &= \frac{1}{r} \sum_{0 \le c < r} \sum_{1 \le k \le \tau} \exp\left(2\pi i c q^k / r\right) \sum_{0 \le x < h} \exp\left(-2\pi i c x / r\right). \end{aligned}$$

The contribution of the term corresponding to $c = 0$ is $\tau h / m$. Therefore, from Lemma 2 and the bound (2), we obtain

$$\left| T - \frac{\tau h}{r} \right| \le \frac{1}{r} \sum_{1 \le c < r} \left| \sum_{1 \le k \le \tau} \exp\left(2\pi i c q^k / r\right) \right| \cdot \left| \sum_{0 \le x < h} \exp\left(2\pi i c x / r\right) \right|$$

$$\leq \frac{1}{r} \sum_{\substack{\delta \mid r \\ \delta < r}} \sum_{\substack{1 \leq c < r \\ \gcd(c,r)=\delta}} \left| \sum_{1 \leq k \leq \tau} \exp\left(2\pi i c q^k / r\right) \right| \left| \sum_{0 \leq x < h} \exp\left(-2\pi i c x / r\right) \right|$$

$$\leq \frac{1}{r^{1/2}} \sum_{\substack{\delta \mid r \\ \delta < r}} \delta^{1/2} \sum_{\substack{1 \leq c < r \\ \gcd(c,r)=\delta}} \left| \sum_{0 \leq x < h} \exp\left(2\pi i c x / r\right) \right|$$

$$\leq \frac{1}{r^{1/2}} \sum_{\substack{\delta \mid r \\ \delta < r}} \delta^{1/2} \sum_{1 \leq c < r/\delta} \left| \sum_{0 \leq x < h} \exp\left(2\pi i c \delta x / r\right) \right|$$

$$\in O\left(r^{1/2} \log r \sum_{\substack{\delta \mid r \\ \delta < r}} \delta^{-1/2} \right).$$

Taking into account that

$$\sum_{\substack{\delta \mid r \\ \delta < r}} \delta^{-1/2} \leq \sum_{\delta \mid r} 1 \in O(r^{\varepsilon/2}),$$

by Theorem 5.2 in Chapter 1 in Prachar (1957), we obtain the desired result. □

Now we are prepared to establish the main result of this section.

Theorem 4. *For any positive integers d and n and real $\varepsilon > 0$, there exists $c > 0$ such that for any nonconstant rational function R over $\mathbb{F}_q$ of the form*

$$R = \sum_{-d \leq \nu \leq d} R_\nu x^\nu \in \mathbb{F}_q(x),$$

with all R_ν in $\mathbb{F}_q$, and for any root β of an irreducible polynomial of degree n with $R(\beta) \neq 0$, at least one of the elements β and $R(\beta)$ has order at least $cn^{4/3-\varepsilon}$.

Proof. Let r be the order of β. Because β is a root of an irreducible polynomial of degree n, the order of q modulo r is n. Indeed, if $q^k \equiv 1 \bmod r$ for some positive integer k, then $\beta^{q^k} = \beta$ and thus $\beta \in \mathbb{F}_{q^k}$, which is true for $k = n$ and false for $k < n$.
We consider the set K of integers $k \in \{1, \ldots, n\}$ such that the remainders $e = q^k \text{ rem } r$ with $0 \leq e < r$ satisfy $e < n/8d$. We denote by $M = \#K$ its size, and claim that the $M(M+1)/2$ powers

$$R(\beta)^{q^k + q^{k'}} \qquad \text{with } k, k' \in K \text{ and } k \leq k'$$

are pairwise distinct. Indeed

$$R(\beta)^{q^k+q^{k'}} = R(\beta)^{q^k} R(\beta)^{q^{k'}} = R\left(\beta^{q^k}\right) R\left(\beta^{q^{k'}}\right) = R\left(\beta^e\right) R\left(\beta^{e'}\right),$$

where $e = q^k$ rem r and $e' = q^{k'}$ rem r. We take two pairs (s,t) and (u,v) of integers with $0 \le s \le t < n/8d$, $0 \le u \le v < n/8d$, and $R(\beta^s)\,R(\beta^t) = R(\beta^u)\,R(\beta^v)$, and claim that $(s,t) = (u,v)$. We write $R = f \cdot x^l$ with some integer l, where $|l| \le d$ and the polynomial $f \in \mathbb{F}_q[x]$ satisfies $\deg f \le 2d$ and $f(0) \ne 0$. Then the above equation implies that

$$f(\beta^s)\,f\left(\beta^t\right)\beta^{-l(s+t)} = f(\beta^u)\,f(\beta^v)\,\beta^{-l(u+v)}.$$

If $l \ge 0$, we consider the polynomial

$$G = f(x^s)\,f\left(x^t\right)x^{l(u+v)} - f(x^u)\,f(x^v)\,x^{l(s+t)} \in \mathbb{F}_q[x]$$

of degree

$$\deg G \le 2d \cdot (s+t+u+v) < n.$$

Furthermore, $G(\beta) = 0$, and hence $G = 0$. This implies that $s + t = u + v$, and thus $F = f(x^s)\,f(x^t) - f(x^u)\,f(x^v)$ is the zero polynomial.
If $l < 0$, we consider the polynomial

$$G = f(x^s)\,f\left(x^t\right)x^{-l(s+t)} - f(x^u)\,f(x^v)\,x^{-l(u+v)}$$

to derive that $s + t = u + v$ and $F = 0$.
Since $s + t = u + v$, we may assume that $s \ne u$, because otherwise $(s,t) = (u,v)$. Without loss of generality we may assume that $s < u$. We let $a_m x^m$ be the term of smallest degree in $f - f(0)$ with $a_m \ne 0$. Then the first product contains the term $a_m f(0) x^{ms} \ne 0$. Moreover, this term is unique and does not cancel with any other term unless $s = u$. So we conclude that $s = u$ and $t = v$.
This proves our claim about the existence of $M(M+1)/2$ pairwise distinct powers of $R(\beta)$, and thus the order of $R(\beta)$ is at least $M(M+1)/2$.
From Lemma 3, we know that for any $\varepsilon > 0$

$$M = \frac{n^2}{8dr} + O(r^{1/2+\varepsilon/2}).$$

We let c_1 be the constant implicit in the "O", and set $c_2 = (8c_1 d)^{-2/(3+\varepsilon)}$. Then for $r \le c_2 \cdot n^{4/3-\varepsilon/2}$ we have

$$c_1 r^{(1+\varepsilon)/2} \le \frac{n^2}{8dr},$$

$$M \ge \frac{n^2}{8dr} - c_1 r^{1/2+\varepsilon/2} \ge \frac{n^2}{16dr} \ge (16c_2 d)^{-1} n^{2/3-\varepsilon/2}.$$

Thus in this case the order of $R(\beta)$ is at least $(16c_2 d)^{-2} n^{4/3-\varepsilon}$. Otherwise the order of β is r larger than $c_2 \cdot n^{4/3-\varepsilon/2}$. □

Corollary 5. *For any $\varepsilon > 0$ there exists $c > 0$ such that for any root β of an irreducible polynomial of degree n, at most one of the shifts $\beta + a$ with $a \in \mathbb{F}_q$ is of order less than $cn^{4/3-\varepsilon}$.*

We see from the proof of Theorem 4 that the more information about the order r of β, the order n of q modulo r and the distribution of powers of q modulo r is available, the stronger are the results produced by this method. In particular, this explains how Artin's conjecture comes into play: if q is a primitive root modulo r, then we have full control over the distribution of powers of q modulo r and, as we have seen in Section 3, this implies much stronger results about the order of $R(\beta)$. Another case when we have good information about this distribution is the case when r is a product of large powers of small primes, see Korobov (1972; 1992). Accordingly, these two cases are the main sources of the results in von zur Gathen & Shparlinski (1998; 1999).

5 Exponentiation in finite fields

We consider the following task: Given are finite fields $\mathbb{F}_q \subseteq \mathbb{F}_{q^n}$, an integer e with $1 \leq e < q^n$, and $u \in \mathbb{F}_{q^n}$. The objective is to compute $u^e \in \mathbb{F}_{q^n}$. An important special case is $q = 2$. This is a basic operation in several cryptosystems: Diffie-Hellman and ElGamal.
The "classical" method is to use repeated squaring, with at most $2\log_2 e \leq 2n\log_2 q$ multiplications in $\mathbb{F}_{q^n}$, and classical multiplication, with $O(n^2)$ operations in $\mathbb{F}_q$. This gives a total of $O(n^3 \log q)$ operations in $\mathbb{F}_q$ for one exponentiation in $\mathbb{F}_{q^n}$.
In the *polynomial representation*, we write $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(\varphi)$, where $\varphi \in \mathbb{F}_q[x]$ is irreducible of degree n, and use the basis $(1, x \bmod \varphi, \ldots, x^{n-1} \bmod \varphi)$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Table 1. Multiplication in $\mathbb{F}_{q^n}$

	time
classical	$O(n^2)$
FFT (Schönhage & Strassen (1971))	$O(n \log n \operatorname{loglog} n)$
additive subspaces (Cantor (1989))	$O(n \log^2 n)$

Three multiplication algorithms are given in Table 1. The running time is the number of operations in $\mathbb{F}_q$. Using the fastest method, the cost for one exponentiation in $\mathbb{F}_{q^n}$ becomes $O(n^2 \log n \operatorname{loglog} n \log q)$ operations in $\mathbb{F}_q$.
A faster method is obtained from the *polynomial representation* of the Frobenius map, using *modular composition*, as introduced in von zur Gathen & Shoup (1992). Then exponentiation can be performed with $O(n^2 \operatorname{loglog} n \log q)$ operations in $\mathbb{F}_q$, as proved in Gao *et al.* (2000).
Now we consider a normal basis $(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and the coordinates $u_0, \ldots, u_{n-1} \in \mathbb{F}_q$ of a general element $\sum_{0 \leq i < n} u_i \alpha^{q^i}$ of $\mathbb{F}_{q^n}$.

Then

$$\left(\sum_{0\le i<n} u_i \alpha^{q^i}\right)^q = \sum_{0\le i<n} u_i \alpha^{q^{i+1}} = \sum_{0\le i<n} u_{i-1}\alpha^{q^i},$$

where $u_{-1} = u_{n-1}$. Thus a qth power corresponds to a cyclic shift of coordinates, and has no arithmetic cost. It is plausible that when a specific power, as the qth one here, becomes cheaper, then this may also reduce the cost of a general exponentiation. Indeed, the number of multiplications in $\mathbb{F}_{q^n}$ becomes

$$\begin{aligned} &\text{at most } \Big(1+o(1)\Big)\frac{n}{\log_q n} && \text{for any } e,\\ &\text{at least } \Big(\frac{1}{3}+o(1)\Big)\frac{n}{\log_q n} && \text{for most } e \end{aligned}$$

(von zur Gathen (1991)). The crucial question now is: How expensive is one multiplication in $\mathbb{F}_{q^n}$?
We begin by considering multiplication via linear algebra in general. Given any basis $\alpha_0, \ldots, \alpha_{n-1}$ of $\mathbb{F}_{q^n}$ as vector space over $\mathbb{F}_q$, we can represent "multiplication by α_i" by an $n \times n$ matrix A_i. This yields the *multiplication tensor* $(A_0, \ldots, A_{n-1})$. We then have the following estimates:

- cost for multiplication by A_i : $O(n^2)$,
- cost for a general multiplication: $O(n^3)$,
- cost for exponentiation: $O(n^4 \log q)$.

In a normal basis $\alpha_i = \alpha^{q^i}$, each matrix A_i is a shift of A_0. This corresponds to the *Massey-Omura multiplier*. The time for a multiplication is still $O(n^3)$, but the storage requirement is only $O(n^2)$, rather than $O(n^3)$. An exponentiation costs $O(n^4 \log q)$ operations in $\mathbb{F}_q$.
Mullin *et al.* (1989) proved that A_0 has at least $2n-1$ nonzero entries. A fruitful suggestion of theirs was to consider *"optimal" normal basis*, which have exactly this minimal number $2n-1$ of nonzero entries. Then the costs drop by a factor of n:

- cost for one multiplication: $O(n^2)$,
- cost for exponentiation: $O(n^3/\log n)$.

They had actually rediscovered a special case of Gauß periods. Namely, Gao & Lenstra (1992) showed that optimal normal bases correspond to Gauß periods of type $(n, \mathcal{K})$ with $\#\mathcal{K} = 1$ or $\#\mathcal{K} = 2$, for $q = 2$.
But even in this improved situation, the computation is slower by a factor of almost n than those discussed in the above. The question is: can we reconcile the advantages of normal bases with those of fast multiplication? Gao *et al.* (1995) have shown that this is indeed possible. In the notation from Section 2, we have the tower of fields:

$$\mathbb{F}_q \subseteq \mathbb{F}_{q^n} = \mathbb{F}_q(\alpha) \subseteq \mathbb{F}_q(\beta).$$

We can represent the right hand field in a polynomial basis, using an appropriate polynomial which vanishes at β, and for the left hand extension we have the advantages of the normal basis. Now the algorithms become quite efficient:

- cost for one multiplication: $O(kn \log n \operatorname{loglog} n)$,
- cost for exponentiation: $O(kn^2 \operatorname{loglog} n \log q)$

operations in $\mathbb{F}_q$, with k as in Section 2.
The algorithms mentioned here work very well also in practice, as reported in the experimental results of von zur Gathen & Nöcker (1997, 1999).

Table 2. Cost of exponentiation algorithms, for $q = 2$

classical	n^3
fast multiplication	$n^2 \log n \operatorname{loglog} n$
optimal normal basis	$n^3 / \log n$
modular composition	$n^2 \operatorname{loglog} n$
optimal normal basis plus fast multiplication	$n^2 \operatorname{loglog} n$

6 Construction of Gauß periods

When do optimal normal bases exist? Or, more generously, when do we have Gauß periods with k "small"? Or any Gauß period at all? In the terminology of Section 2, we have r prime and $\varphi(r) = nk$, and want k as small as possible. Thus we study the following function.

$$\kappa_p(q,n) = \begin{cases} \min \#\mathcal{K} & \text{prime Gauß period of type } (n,\mathcal{K}) \text{ over } \mathbb{F}_q \text{ exists,} \\ \infty & \text{if none exists.} \end{cases}$$

Wassermann (1993), Theorem 3.3.4, showed that if $p = \operatorname{char}(\mathbb{F}_q)$, $q = p^m$ and $n \in \mathbb{N}$ is positive, then $\kappa_p(q,n) < \infty$ if and only if the following conditions hold:

(i) $\gcd(m,n) = 1$,
(ii) $2p \nmid n$, if $p \equiv 1 \bmod 4$, and $4p \nmid n$, if $p = 2$ or $p \equiv 3 \bmod 4$.

The "prime" (and the index p of κ) refers to the fact that r is prime in the above construction. Gauß (1801) suggested in article 356 of his *Disquisitiones Arithmeticae* to remove this condition: *Haecce theoremata salva vel potius aucta elegantia sua etiam ad valores quosvis compositos ipsius n extendi posse: sed de his rebus, quae altioris sunt indaginis, hoc loco tacere*

earumque considerationem ad aliam occasionem nobis reservare oportet.[2] It seems that the other occasion never arose.
Following Gauß' suggestion, we now drop this requirement, and take positive integers n, k, and r, with $nk = \varphi(r)$, a subgroup $\mathcal{K} \subseteq \mathbb{Z}_r^\times$ of order k, a primitive rth root of unity $\beta \in \mathbb{F}_{q^{\varphi(r)}}$, and $\alpha = \sum_{i \in \mathcal{K}} \beta^i$.

Theorem 6. *The* Gauß period α *is normal in* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$ *if and only if* r *is squarefree,* $\gcd(r, q) = 1$, *and* $\langle q, \mathcal{K} \rangle = \mathbb{Z}_r^\times$.

For arbitrary r, the expression for α reads as follows. For a prime divisor ℓ of r, we let $\nu_\ell(r)$ be the multiplicity of ℓ in r. We write $r = r_1 r_2$ where r_2 is the product of all primes ℓ such that $\nu_\ell(r) = 1$. For any prime ℓ dividing r, let $\ell' = r/\ell^{\nu_\ell(r)}$, and set

$$g = x^{r_1} \prod_{\ell \mid r_1} \sum_{0 \le i < \nu_\ell(r_1)} x^{\ell' \ell^i} \in \mathbb{Z}[x].$$

The *general Gauß period of type* $(n, \mathcal{K})$ is defined as

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

If r is squarefree, then a general Gauß period is given by the same formula as a Gauß period. Theorem 6, without the squarefreeness condition, also holds for these Gauß periods (Feisel *et al.* (1999)). The proof argues mainly in algebraic number fields, which is of course Gauß' original setting. It would be nice to have an argument working just in finite fields.
The corresponding variant of $\kappa_p(q, n)$ is the following:

$$\kappa_g(q, n) = \begin{cases} \min \#\mathcal{K} & \text{general Gauß period of type } (n, \mathcal{K}) \\ & \quad \text{over } \mathbb{F}_q \text{ exists,} \\ \infty & \text{if none exists.} \end{cases}$$

Then $\kappa_g(q, n) \le \kappa_p(q, n)$.
There are considerably more of these general Gauß periods than of the ones with r prime, and the smallest value of k often gets reduced. For $q = 2$, this is illustrated in Table 3, where the "□" means that r has a square factor.
Fast arithmetic can also be used with these more general Gauß periods; see von zur Gathen & Nöcker (1999).
From an different point of view, von zur Gathen & Pappalardi (2000) have determined the density of primes $r = nk + 1$ that yield a Gauß period over $\mathbb{F}_q$, in terms of n and q.

[2] These theorems can be extended to arbitrary composite values of n [in our notation: r], retaining or even enhancing their elegance; but these matters, which are at a higher level of research, are best left unsaid in this place, and we reserve their consideration for another occasion.

Table 3. Improvements for $q = 2$ and $2 \leq n \leq 156$:

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

Acknowledgements

We thank Michael Nüsken for help with the typesetting.

Bibliography

W. H. Bussey (1906). Galois field tables for $p^n \leq 169$. *Bulletin of the American Mathematical Society* **12**, 22–38.

W. H. Bussey, Tables of Galois fields of order less than $1,000$. *Bulletin of the American Mathematical Society* **16** (1910), 188–206.

David G. Cantor, On arithmetical algorithms over finite fields. *Journal of Combinatorial Theory, Series A* **50** (1989), 285–300.

August L. Crelle, Table des racines primitives etc. pour les nombres premiers depuis 3 jusqu'à 101, precédée d'une note sur le calcul de cette table. *Journal für die Reine und Angewandte Mathematik* **9** (1832), 27–53.

Sandra Feisel, Joachim von zur Gathen, and M. Amin Shokrollahi, Normal bases via general Gauß periods. *Mathematics of Computation* **68**(225) (1999), 271–290.

S. Gao and H. W. Lenstra, Jr., Optimal normal bases. *Designs, Codes, and Cryptography* **2** (1992), 315–323.

Shuhong Gao, Joachim von zur Gathen, and Daniel Panario, Gauss periods and fast exponentiation in finite fields. In *Proceedings of LATIN '95*, Valparaíso, Chile, Lecture Notes in Computer Science **911**. Springer-Verlag, 1995, 311–322.

Shuhong Gao, Joachim von zur Gathen, Daniel Panario, and Victor Shoup, Algorithms for exponentiation in finite fields. *Journal of Symbolic Computation* **26**(6) (2000), 879–889.

Joachim von zur Gathen, Efficient and optimal exponentiation in finite fields. *computational complexity* **1** (1991), 360–394.

Joachim von zur Gathen and Michael Nöcker, Exponentiation in finite fields: Theory and practice. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: AAECC-12*, Toulouse, France, ed. Teo Mora and Harold Mattson, Lecture Notes in Computer Science **1255**. Springer-Verlag, 1997, 88–113.

Joachim von zur Gathen and Michael Nöcker, Normal bases, Gauss periods, and fast arithmetic. In *Abstracts of the Fifth International Conference on Finite Fields and Applications, August 2-6, 1999, University of Augsburg*, 1999, p. 70.

Joachim von zur Gathen & Francesco Pappalardi (2000). Density estimates for Gauß periods. In *Proc. Workshop on Cryptography and Computational Number Theory*. Birkhäuser Verlag. To appear.

Joachim von zur Gathen and Victor Shoup, Computing Frobenius maps and factoring polynomials. *computational complexity* **2** (1992), 187–224.

Joachim von zur Gathen and Igor Shparlinski, Orders of Gauss periods in finite fields. *Applicable Algebra in Engineering, Communication and Computing* **9** (1998), 15–24.

Joachim von zur Gathen and Igor Shparlinski, Constructing elements of large order in finite fields. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: AAECC-13*, Hawaii, Lecture Notes in Computer Science **1719**, Springer-Verlag, 1999, 404–409.

Carl Friedrich Gauss, *Disquisitiones Arithmeticae*. Gerh. Fleischer Iun., Leipzig, 1801. English translation by Arthur A. Clarke, Springer-Verlag, New York, 1986.

D. R. Heath-Brown, Artin's conjecture for primitive roots. *Quarterly Journal of Mathematics* **37** (1986), 27–38.
C. Hooley, On Artin's conjecture. *Journal für die Reine und Angewandte Mathematik* **225** (1967), 209–220.
C. G. J. Jacobi, *Canon Arithmeticus sive tabulae quibus exhibentur pro singulis numeris primis vel primorum potestatibus infra 1000 numeri ad datos indices et indices ad datos numeros pertinentes.* Typus Academicus, Berlin, 1839.
Nikolai M. Korobov, On the distribution of digits in periodic fractions. *Math. USSR – Sbornik* **18** (1972), 659–676. (In Russian).
Nikolai M. Korobov, *Exponential sums and their applications.* Kluwer Acad. Publ., Dordrecht, 1992.
R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson, Optimal normal bases in GF(p^n). *Discrete Applied Mathematics* **22** (1989), 149–161.
K. Prachar, *Primzahlverteilung.* Springer-Verlag, Berlin, 1957.
A. Schönhage and V. Strassen, Schnelle Multiplikation großer Zahlen. *Computing* **7** (1971), 281–292.
Igor E. Shparlinski, On the dimension of BCH codes. *Problemy Peredachi Inform.* **25**(1) (1988), 100–103. (In Russian).
I. M. Vinogradov, *Elements of number theory.* Dover Publications, Inc., New York, 1954.
Alfred Wassermann, Konstruktion von Normalbasen. *Bayreuther Math. Schriften* **31** (1990), 155–164.
Alfred Wassermann, Zur Arithmetik in endlichen Körpern. *Bayreuther Math. Schriften* **44** (1993), 147–251.