Finite Fields and Their Applications **7**, 149–164 (2001)
doi.10.1006/ffta.2000.0304, available online at http://www.idealibrary.com on IDEAL®

Abelian Groups, Gauss Periods, and Normal Bases

Shuhong Gao[1]

Department of Mathematical Sciences, Clemson University, Clemson, South Carolina 29634–0975
E-mail: sgao@math.clemson.edu

Communicated by Daqing Wan

Received June 14, 2000; published online November 29, 2000

DEDICATED TO PROFESSOR CHAO KO ON HIS 90TH BIRTHDAY

A result on finite abelian groups is first proved and then used to solve problems in finite fields. Particularly, all finite fields that have normal bases generated by general Gauss periods are characterized and it is shown how to find normal bases of low complexity. © 2000 Academic Press

Key Words: finite fields; finite abelian groups; Gauss periods; normal bases.

1. INTRODUCTION AND MAIN RESULTS

We first prove a result on finite abelian groups. We use the standard notation $\langle S, K\rangle$ for the subgroup generated by the elements in S and K together, and G/K, or $\frac{G}{K}$, for the quotient group of G by K.

THEOREM 1.1. *Let G be any finite abelian group. Let S be a subset and K a subgroup of G such that $G = \langle S, K\rangle$. Then, for any direct product $G = G_1 \otimes G_2 \otimes \cdots \otimes G_t$, there is a subgroup H of the form*

$$H = H_1 \otimes H_2 \otimes \cdots \otimes H_t, \quad H_i \trianglelefteq G_i, \quad 1 \le i \le t,$$

such that

$$G = \langle S, H\rangle \quad \textit{and} \quad \frac{G}{H} \cong \frac{G}{K}.$$

[1] The author was supported in part by NSF grant #DMS9970637, NSA grant #MDA904-00-1-0048 and ONR grant #N00014-00-1-0565.

1071-5797/00 $35.00

Next we apply this theorem to some problems in finite fields that arise in the work of Feisel *et al.* [7] on constructing normal bases from Gauss periods.

Gauss periods were invented by C. F. Gauss in 1796 in his famous resolution of the problem of constructing regular polygons by straightedge and compass (see [21]) and have been very useful in studying algebraic structures and in number theory. In recent years, special Gauss periods have been successfully used to construct normal bases of low complexity [4, 7, 11, 17] and for implementation of finite fields [2, 3, 19]. While Gauss periods can be defined in any finite Galois extension of an arbitrary field (see Pohst and Zassenhaus [20, pp. 171–173] and van der Waerden [22, p. 169]), we only consider them in finite fields.

Definition 1.2 (Feisel *et al.*, 1999). Let q be a prime power and r a positive integer with $\gcd(r, q) = 1$. Let $\mathbb{Z}_r$ denote the ring of integers modulo r, $\mathbb{Z}_r^\times$ the multiplicative group of $\mathbb{Z}_r$ and $\phi(r) = |\mathbb{Z}_r^\times| = nk$. Write r as $r = r_1 r_2$ where r_1 is the squarefree part of r and set

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

where ℓ runs through all prime divisors of r_2 and $v_\ell(r_2)$ denotes the largest integer v such that $\ell^v | r_2$. For any subgroup K of $\mathbb{Z}_r^\times$ of order k, a *Gauss period* of type (n, K) over $\mathbb{F}_q$ is defined as

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

where β is a primitive rth root of unity in $\mathbb{F}_{q^{nk}}$.

When r is a prime (or squarefree), $r_2 = 1$ and $g(x) = x$. In this case, the above definition agrees with Gauss' original one [13, Article 356], and since there is only one subgroup K of order k in $\mathbb{Z}_r^\times$, we refer to a Gauss period of type (n, k) instead of (n, K). To distinguish this case, we sometime call the Gauss periods defined above *general Gauss periods.*

A *normal basis* for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}$ for some $\alpha \in \mathbb{F}_{q^n}$. Any such α is called a *normal element* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and the corresponding basis is said to be generated by α.

Theorem 1.3 (Feisel *et al.*, 1999). *A Gauss period of type* (n, K) over $\mathbb{F}_q$ *generates a normal basis for* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$ *iff* $\langle q, K \rangle = \mathbb{Z}_r^\times$.

The problem is to characterize the values of q and n for which there exist an integer r and a subgroup K as above such that a Gauss period of type (n, K) is normal. The experimental results in [7] indicate that such r may not exist for many values of q and n. For example, when $q = 2$ and n is divisible by 8, no such r were found by computers. Our Theorem 1.1 can now be applied to resolve this problem.

THEOREM 1.4. *Let $q = p^m$, where p is a prime. There exists an integer r such that a Gauss period of type (n, K) is normal for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ for some subgroup K of $\mathbb{Z}_r^\times$ iff* $\gcd(m, n) = 1$ *and if $p = 2$ then $8 \nmid n$.*

In the special case, when r is required to be a prime, the above theorem was previously proved by Wassermann (1993). Theorem 1.4 characterizes exactly which finite fields have normal bases generated by general Gauss periods. For more information on how to perform fast arithmetic under normal bases generated by Gauss periods, see [8–10, 12, 18].

In practice, the size of r is extremely important: smaller r results in smaller complexity for the normal bases. We present computational results on the size of r. We shall see from the proof of Theorem 1.4 that whenever the required r exist, one can find squarefree r. Hence, for simplicity, we only consider squarefree r. Note that there are some theoretical bounds on prime r in [1, 5], however, these bounds are quite bad compared to the experimental results presented in the tables below.

Suppose that r is given squarefree and $nk = \phi(r)$. The question is how to efficiently decide whether there is any subgroup K of order k in $\mathbb{Z}_r^\times$ such that $\langle q, K\rangle = \mathbb{Z}_r^\times$. It is possible that $\langle q, K\rangle = \mathbb{Z}_r^\times$ for some subgroups K of order k in $\mathbb{Z}_r^\times$ while $\langle q, K\rangle \neq \mathbb{Z}_r^\times$ for other subgroups K of the same cardinality. In general, if $r = nk + 1$ is not a prime then $\mathbb{Z}_r^\times$ may have many subgroups of order k. For instance, if $k = 2$ and r has t distinct odd prime factors then $\mathbb{Z}_r^\times$ has at least 2^t subgroups of order 2. Searching through all subgroups of order k is time consuming. We solve this problem by the next result.

THEOREM 1.5. *Suppose that r is squarefree, $n|\phi(r)$ and there is a subgroup $K \subseteq \mathbb{Z}_r^\times$ of order $k = \phi(r)/n$ with $\langle q, K\rangle = \mathbb{Z}_r^\times$. Then n and k factor as*

$$n = n_1 n_2 \cdots n_t, \quad k = k_1 k_2 \cdots k_t, \quad n_i \geq 2, k_i \geq 1$$

such that

(i) *$n_1, n_2, \ldots, n_t$ are pairwise relatively prime;*

(ii) *for each $1 \leq i \leq t$, (n_i, k_i) is a prime Gauss pair for q, and $r = \prod_{i=1}^t r_i$ where $r_i = n_i k_i + 1$, $1 \leq i \leq t$, are distinct.*

Conversely, if (i) and (ii) are satisfied then there is a Gauss period of type (n, H) that generates a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ of complexity at most $\prod_{i=1}^t (n_i \bar{k}_i - 1)$ with $\bar{k}_i = k_i$ if $p|k_i$, and $\bar{k}_i = k_i + 1$ otherwise where p is the characteristic of $\mathbb{F}_q$.

Here and hereafter (n, k) is called a *prime Gauss pair* if $r = nk + 1$ is a prime and a Gauss period of type (n, k) is normal. The proof of Theorem 1.5 also shows how to find a subgroup H of order k such that a Gauss period of type (k, H) generates a normal basis of the required complexity in the theorem.

The remainder of the paper is organized as follows. Theorem 1.1 is first proved in Section 2. Theorems 1.4 and 1.5 are proved in Sections 3 and 4, respectively. In Section 5, we discuss how to efficiently search for low-complexity normal bases generated by Gauss periods for any given n and q. We give a table of percentages of $n \leq 3000$ for which $\mathbb{F}_{q^n}$ has a normal basis from Gauss periods with small complexity for $q \in \{2, 3, 5, 7, 11, 13, 17, 19, 23\}$. Our computation shows that general Gauss periods do yield many new normal bases of low complexity.

2. PROOF OF THEOREM 1.1

The properties we use on Abelian groups can be found in any standard textbook on modern algebra; see, for example, [14].

Without loss of generality, we may assume that S is a subgroup of G. We first reduce the proof to the case where the order of G is a prime power. Let n be the order of G. For a prime divisor p of n, let $G^{(p)}$ denote the p-Sylow subgroup of G; similarly for $G_i^{(p)}$, $S^{(p)}$, $K^{(p)}$, etc. Then

$$G = \prod_{p|n} G^{(p)}, \quad \langle S, K \rangle = \prod_{p|n} \langle S^{(p)}, K^{(p)} \rangle,$$

where p runs through all distinct prime divisors of n. Also, $G^{(p)}$ has order a power of p and

$$G^{(p)} = G_1^{(p)} \otimes G_2^{(p)} \otimes \cdots \otimes G_t^{(p)}.$$

Suppose that there is a subgroup of $G^{(p)}$ of the form

$$H^{(p)} = H_1^{(p)} \otimes H_2^{(p)} \otimes \cdots \otimes H_t^{(p)}, \quad H_i^{(p)} \trianglelefteq G_i^{(p)},$$

such that

$$G^{(p)} = \langle S^{(p)}, H^{(p)} \rangle \quad \text{and} \quad \frac{G^{(p)}}{H^{(p)}} \cong \frac{G^{(p)}}{K^{(p)}}$$

for each prime divisor p of n. Let $H_i = \prod_{p|n} H_i^{(p)}$ and

$$H = \prod_{p|n} H^{(p)} = H_1 \otimes H_2 \otimes \cdots \otimes H_t.$$

Then H satisfies the requirement of Theorem 1.1, since

$$\langle S, H\rangle = \prod_{p|n} \langle S^{(p)}, H^{(p)}\rangle = \prod_{p|n} G^{(p)} = G$$

and

$$\frac{G}{H} \cong \prod_{p|n} \frac{G^{(p)}}{H^{(p)}} \cong \prod_{p|n} \frac{G^{(p)}}{K^{(p)}} \cong \frac{G}{K}.$$

So we may assume that G is a p-group; i.e., G has order a power of p. In this case, it suffices to prove the theorem when all the subgroups G_i are cyclic, since we can always decompose G_i into a direct product of cyclic groups and combine subgroups of the components to get the required H_i of G_i for all $1 \le i \le t$.

Henceforth, we assume that G is a p-group and $G_i = \langle \alpha_i \rangle$ generated by α_i, $1 \le i \le t$. The number t is called the rank of G and $\alpha_1, \alpha_2, \ldots, \alpha_t$ form a basis for G. We prove by induction on the rank t of G. When $t = 1$, the theorem holds trivially. Suppose that the theorem is true for any p-group of rank at most $t - 1$. We prove it for G of rank t.

If $K = G$, the theorem holds trivially. So assume that $K \neq G$. Denote the elements of G/K by $\bar{a}, a \in G$. For convenience, we switch to the additive notation for the group operation of G. Then

$$G = S + K \quad \text{and} \quad \bar{G} = \{\bar{a}: a \in S\}.$$

As $\bar{G}$ is finite, there is an element of largest order in $\bar{G}$. Let $\bar{a}$ be any such element with order p^e. Then $p^e > 1$, as $\bar{G}$ is not the identity group. There are integers $a_1, a_2, \ldots, a_t$ such that

$$a = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_t\alpha_t.$$

Thus

$$\bar{a} = a_1\bar{\alpha}_1 + a_2\bar{\alpha}_2 + \cdots + a_t\bar{\alpha}_t.$$

The order of $\bar{a}$ is equal to the least common multiple of the orders of $a_i\bar{\alpha}_i$, $1 \le i \le t$. Since all the orders are powers of p, there is an i such that $a_i\bar{\alpha}_i$ has order p^e. Without loss of generality, we assume that $i = t$. Note that $p \nmid a_t$, since otherwise $\bar{\alpha}_t \in \bar{G}$ would have order at least p^{e+1}, contradicting to the choice of $\bar{a}$ whose order p^e is the largest. Suppose that G_t has order p^r. Then the coefficient of α_t is computed modulo p^r. As $p \nmid a_t$, an appropriate multiple of a will make the coefficient of α_t into 1. So we may assume that a is of the form

$$a = \beta + \alpha_t \in S, \quad \text{for some} \quad \beta \in G_1 \otimes \cdots \otimes G_{t-1}, \tag{1}$$

where $\bar{a}$ and $\bar{\alpha}_t$ have the same order p^e.

Denote $\tilde{G} = G_1 \otimes \cdots \otimes G_{t-1}$. For any element $g \in G$ represented under the basis $\alpha_1, \ldots, \alpha_t$, we define the projection of g via a into $\tilde{G}$ to be the element $g - ua$ where u is the coefficient of α_t in g. Let $\tilde{K}$ be the set of elements of K projected into $\tilde{G}$ via a. Then $\tilde{K}$ is a subgroup of $\tilde{G} \subset G$. As $a \in S$, we still have

$$G = \langle S, \tilde{K} \rangle. \tag{2}$$

We shall show later that

$$\bar{G} \cong \frac{\tilde{G}}{\tilde{K}} \otimes \langle \bar{\alpha}_t \rangle. \tag{3}$$

Let $\tilde{S}$ be the subgroup consisting of all elements of S with tth component zero. Since $G_t = \langle \alpha_t \rangle$ is a component in the direct product of G, (1) and (2) imply that $\tilde{G} = \langle \tilde{S}, \tilde{K} \rangle$. Now $\tilde{G}/\tilde{K}$ has rank at most $t - 1$. By the induction hypothesis, there is a subgroup $\tilde{H}$ of $\tilde{G}$ of the form

$$\tilde{H} = H_1 \otimes \cdots \otimes H_{t-1}, \quad H_i \trianglelefteq G_i,$$

such that

$$\tilde{G} = \langle \tilde{S}, \tilde{H} \rangle \quad \text{and} \quad \frac{\tilde{G}}{\tilde{K}} \cong \frac{\tilde{G}}{\tilde{H}}.$$

Since p^e is the order of $\bar{\alpha}_t$ in G/K, $p^e \alpha_t \in K$ and the order p^r of G_t is at least p^e. Let $H_t = \langle p^e \alpha_t \rangle$. Then G_t/H_t is cyclic of order p^e. So $\langle \bar{\alpha}_t \rangle \cong G_t/H_t$. Take $H = \tilde{H} \otimes H_t$. Then, by (3),

$$\frac{G}{H} \cong \frac{\tilde{G}}{\tilde{H}} \otimes \frac{G_t}{H_t} \cong \frac{\tilde{G}}{\tilde{K}} \otimes \langle \alpha_t \rangle \cong \frac{G}{K}$$

and

$$\langle S, H \rangle = \langle \tilde{S}, a, \tilde{H}, p^e \alpha_t \rangle = \langle \tilde{S}, \tilde{H}, a, p^e \alpha_t \rangle$$
$$= \langle \tilde{G}, \beta + \alpha_t, p^e \alpha_t \rangle = \langle \tilde{G}, \alpha_t, p^e \alpha_t \rangle = G,$$

as $-\beta \in \tilde{G}$ and $-\beta + a = \alpha_t$. So the theorem follows by induction.

It remains to prove (3). Since $\bar{a} \in \bar{G}$ is of maximum order, $\langle \bar{a} \rangle$ is a direct summant of $\bar{G}$. Hence

$$\bar{G} \cong \frac{\tilde{G}}{\langle \bar{a} \rangle} \otimes \langle \bar{a} \rangle. \tag{4}$$

But $\langle \bar{a} \rangle \cong \langle K, a \rangle / K$. By the third isomorphism theorem of groups,

$$\frac{\bar{G}}{\langle \bar{a} \rangle} \cong \frac{G/K}{\langle K, a \rangle / K} \cong \frac{G}{\langle K, a \rangle}. \tag{5}$$

Note that the elements of $\tilde{K}$ are linear combinations of a and elements of K. We have

$$\langle K, a \rangle = \langle \tilde{K}, a \rangle = \tilde{K} + \langle a \rangle$$

where the sum is direct as $\tilde{K}$ has no common elements with $\langle a \rangle$. Since $G = \tilde{G} + \langle a \rangle$ is also a direct sum, we have

$$\frac{G}{\langle K, a \rangle} = \frac{\tilde{G} + \langle a \rangle}{\tilde{K} + \langle a \rangle} \cong \frac{\tilde{G}}{\tilde{K}} \otimes \frac{\langle a \rangle}{\langle a \rangle} \cong \frac{\tilde{G}}{\tilde{K}}.$$

It follows from (4) and (5) that

$$\bar{G} \cong \frac{\tilde{G}}{\tilde{K}} \otimes \langle \bar{a} \rangle \cong \frac{\tilde{G}}{\tilde{K}} \otimes \langle \bar{\alpha}_t \rangle,$$

as $\bar{\alpha}_t$ and $\bar{a}$ have the same order in $\bar{G}$. Hence (3) holds, and the proof is complete. ■

3. PROOF OF THEOREM 1.4

Denote the elements of $\mathbb{Z}_r^\times / K$ by $\bar{a}, a \in \mathbb{Z}_r^\times$. Since $\# \mathbb{Z}_r^\times = \phi(r) = nk$, $\mathbb{Z}_r^\times / K$ has order n. $\langle p^m, K \rangle = \mathbb{Z}_r^\times$ iff $\bar{p}^m$ has order n in $\mathbb{Z}_r^\times / K$. The latter happens iff $\gcd(n, m) = 1$ and $\bar{p}$ has order n. Therefore $\langle p^m, K \rangle = \mathbb{Z}_r^\times$ iff $\langle p, K \rangle = \mathbb{Z}_r^\times$ and $\gcd(n, m) = 1$.

We prove that if $p = 2$ and $8 | n$ then $\langle p, K \rangle \neq \mathbb{Z}_r^\times$ for any odd r with $\phi(r) = nk$ and any subgroup K of order k in $\mathbb{Z}_r^\times$. The following argument is due to H. W. Lenstra, Jr. Suppose on the contrary that $\langle 2, K \rangle = \mathbb{Z}_r^\times$. Let $K_1 = \langle 2^8, K \rangle \subseteq \mathbb{Z}_r^\times$. Then K_1 has order $nk/8$, and $\mathbb{Z}_r^\times / K_1$ is cyclic of order 8 generated by $\bar{2}$. Suppose that $r = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ where $p_1, p_2, \ldots, p_t$ are distinct odd primes. Consider the natural homomorphism

$$\mathbb{Z}_r^\times \cong \prod_{i=1}^{t} \mathbb{Z}_{p_i^{e_i}}^\times \xrightarrow{\sigma} \mathbb{Z}_r^\times / K_1.$$

If $p_i \not\equiv 1 \bmod 8$, then $\#\mathbb{Z}_{p_i^{e_i}}^\times = (p_i - 1)p_i^{e_i - 1} \not\equiv 0 \bmod 8$, so $\sigma(\mathbb{Z}_{p_i^{e_i}}^\times)$ and thus $\sigma(2 \bmod p_i^{e_i})$ is in the subgroup of order 4 in $\mathbb{Z}_r^\times / K_1$. If $p_i \equiv 1 \bmod 8$, then 2 is a quadratic residue mod p_i and thus a square mod $p_i^{e_i}$, so $\sigma(2 \bmod p_i^{e_i})$ is again in the subgroup of order 4 in $\mathbb{Z}_r^\times / K_1$. Therefore $\langle 2, K_1 \rangle \neq \mathbb{Z}_r^\times$, a contradiction.

It remains to show that if $p > 2$, or $p = 2$ but $8 \nmid n$, then there is a positive integer k such that (n, k) is a Gauss pair over $\mathbb{F}_p$, thus over $\mathbb{F}_{p^m}$ when $\gcd(m, n) = 1$. Suppose that $n = n_1 n_2 \cdots n_t$ where $n_1, n_2, \ldots, n_t$ are prime powers of distinct primes. By Wassermann [24], for each $1 \leq i \leq t$ there is a positive integer k_i such that $r_i = n_i k_i + 1$ is a prime and $\langle p, K_i \rangle = \mathbb{Z}_{r_i}^\times$ where K_i is the unique subgroup of order k_i in $\mathbb{Z}_{r_i}^\times$. If some of $r_1, r_2, \ldots, r_t$ are equal, say $r_1 = r_2$, then $r_1 = n_1 n_2 k_1' + 1$ for some integer k_1', and (n_1', k_1') is a prime Gauss pair where $n_1' = n_1 n_2$. So we can drop the pair (n_2, k_2) and r_2. Now $n = n_1' n_3 \cdots n_t$ with $n_1', n_3, \ldots, n_t$ pairwise relatively prime. We can repeat this process until all the r's are distinct. Without loss of generality, we may assume that $r_1, r_2, \ldots, r_n$ are already distinct and $n_1, n_2, \ldots, n_t$ are pairwise relatively prime.

Let $\alpha_i = \sum_{a \in K_i} \beta_i^a$ be a Gauss period of type (n_i, k_i) over $\mathbb{F}_p$ where β_i is a primitive r_ith root of unity in some extension of $\mathbb{F}_p$. Then α_i is a normal element in $\mathbb{F}_{p^{n_i}}$ over $\mathbb{F}_p$. As $n_1, n_2, \ldots, n_t$ are pairwise relatively prime, by Theorem 4.3 in [16, p. 72], $\alpha = \alpha_1 \alpha_2 \cdots \alpha_t$ is a normal element in $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. It suffices to show that α is a Gauss period. Let $r = r_1 r_2 \cdots r_t$. Since $r_1, r_2, \ldots, r_n$ are distinct primes, by the Chinese remainder theorem,

$$\mathbb{Z}_r = \mathbb{Z}_{r_1} \oplus \mathbb{Z}_{r_2} \oplus \cdots \oplus \mathbb{Z}_{r_t}, \quad \text{and} \quad \mathbb{Z}_r^\times = \mathbb{Z}_{r_1}^\times \oplus \mathbb{Z}_{r_2}^\times \oplus \cdots \oplus \mathbb{Z}_{r_t}^\times$$

where we identify $\mathbb{Z}_{r_i}$ with its embedding in $\mathbb{Z}_r$ (similarly for $\mathbb{Z}_{r_i}^\times$, and K_i below) and the sums are internal. Let

$$K = K_1 \oplus K_2 \oplus \cdots \oplus K_t \subset \mathbb{Z}_r^\times.$$

Then

$$\sum_{a \in K} \beta^a = \sum_{a_i \in K_i,\ 1 \leq i \leq t} \beta_1^{a_1} \beta_2^{a_2} \cdots \beta_t^{a_t} = \prod_{i=1}^{t} \sum_{a_i \in K_i} \beta_i^{a_i} = \prod_{i=1}^{t} \alpha_i = \alpha.$$

Therefore α is a Gauss period of type (n, K). ■

4. PROOF OF THEOREM 1.5

Let $r = r_1 r_2 \cdots r_t$ where $r_1, r_2, \ldots, r_t$ are distinct primes. By the Chinese remainder theorem,

$$\mathbb{Z}_r^\times = \mathbb{Z}_{r_1}^\times \oplus \mathbb{Z}_{r_2}^\times \oplus \cdots \oplus \mathbb{Z}_{r_t}^\times,$$

here again we identify $\mathbb{Z}_{r_i}$ with its embedding in $\mathbb{Z}_r$ and the sum is internal. By Theorem 1.1 with $S = \{q\}$, there exists a subgroup $H = H_1 \oplus H_2 \oplus \cdots \oplus H_t$, where H_i is a subgroup of $\mathbb{Z}_{r_i}^\times$, such that

$$\mathbb{Z}_r^\times = \langle q, H > \quad \text{and} \quad \frac{\mathbb{Z}_r^\times}{K} \cong \frac{\mathbb{Z}_r^\times}{H}.$$

Note that

$$\frac{\mathbb{Z}_r^\times}{H} \cong \frac{\mathbb{Z}_{r_1}^\times}{H_1} \oplus \frac{\mathbb{Z}_r^\times}{H_2} \oplus \cdots \oplus \frac{\mathbb{Z}_{r_t}^\times}{H_t}. \tag{6}$$

Let $n_i = \# \mathbb{Z}_{r_i}^\times / H_i$ and $k_i = \# H_i$ for $1 \le i \le t$. Then $r_i = n_i k_i + 1$, $1 \le i \le t$, and $n = \# \mathbb{Z}_r^\times / K = \# \mathbb{Z}_r^\times / H = n_1 n_2 \cdots n_t$. Now $\langle q, H \rangle = \mathbb{Z}_r^\times$ implies that $\mathbb{Z}_r^\times / H$ is cyclic. It follows from (6) that $n_1, n_2, \ldots, n_t$ are pairwise relatively prime. Also,

$$\mathbb{Z}_r^\times = \langle q, H \rangle = \langle q, H_1 \rangle \oplus \langle q, H_2 \rangle \oplus \cdots \oplus \langle q, H_t \rangle$$

implies that $\langle q, H_i \rangle = \mathbb{Z}_{r_i}^\times$ for $1 \le i \le t$. Hence (n_i, k_i) is a Gauss pair over $\mathbb{F}_q$ for $1 \le i \le t$. Obviously $k = |K| = |H| = k_1 \cdots k_t$.

Finally, for the last claim of the theorem, taking the subgroup $H = H_1 \oplus H_2 \oplus \cdots \oplus H_t$ in $\mathbb{Z}_r^\times$ where H_i is the unique subgroup of order k_i in $\mathbb{Z}_{r_i}^\times$, let $\alpha = \alpha_1 \alpha_2 \cdots \alpha_t$ where α_i is a Gauss period of type (n_i, k_i) over $\mathbb{F}_q$, $1 \le i \le t$. Then α is a Gauss period of type (n, H) by the proof of Theorem 1.4. Since α_i is normal in $\mathbb{F}_{q^{n_i}}$ over $\mathbb{F}_q$ and the n_i's are pairwise relatively prime, α is normal in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ By Exercise 4.2 in [16, p. 73], the complexity of the normal basis generated by α is equal to the product of those generated by α_i for $\mathbb{F}_{q^{n_i}}$, $1 \le i \le t$. The claim follows. ■

5. NORMAL BASES OF LOW COMPLEXITY

Let n be a positive integer and $q = p^m$ where p is a prime and m is a positive integer. We want to construct a normal basis of low complexity for $\mathbb{F}_{q^n}$ over

$\mathbb{F}_q$. Theorem 1.4 says that if $\gcd(m, n) = 1$ then a normal basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ can always be constructed from Gauss periods except for $p = 2$ and $8|n$. Since any basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is still a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ when $\gcd(m, n) = 1$, we will concentrate only on the fields $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. To the author's knowledge, there is currently no known construction of normal bases of low complexity for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ when $8|n$, and little is known for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ when $\gcd(m, n) > 1$; see Blake *et al.* [6] for a construction of normal bases with complexity $3n - 2$ for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ when $n|(q-1)$ or $n = p$.

Recall that (n, k) is a prime Gauss pair if $r = nk + 1$ is a prime and $\langle q, K\rangle = \mathbb{Z}_r^\times$ where K is the unique subgroup of $\mathbb{Z}_r^\times$ of order k. We call (n, k) a *Gauss pair* over $\mathbb{F}_q$ if $nk = \phi(r)$ for some squarefree integer r with $\gcd(r, q) = 1$ and if there is a subgroup K in $\mathbb{Z}_r^\times$ of order k such that $\langle q, K\rangle = \mathbb{Z}_r^\times$. Define

$$\kappa'_q(n) = \begin{cases} \min\{k : (n, k) \text{ is a prime Gauss pair over } \mathbb{F}_q\}, & \text{if } k \text{ exists,} \\ \infty, \text{ if no such } k \text{ exists;} \end{cases}$$

and

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

As a prime Gauss pair is always a Gauss pair, $\kappa_q(n) \le \kappa'_q(n)$.

In the prime case, $\kappa'_q(n)$ measures the complexity of the corresponding normal basis. In the general case, however, we do not know the precise relationship between $\kappa_q(n)$ and the complexity of the normal basis. We introduce another measure. By Theorem 1.5, if the conditions (i) and (ii) are satisfied then there is a Gauss period that generates a normal basis of complexity at most $\prod_{i=1}^t (n_i\bar{k}_i - 1)$. When a Gauss period comes from the set $\{(n_1, k_1), \ldots, (n_t, k_t)\}$ of pairs, we say that it is of type $\{(n_1, k_1), \ldots, (n_t, k_t)\}$. Define

$$G_q(n) = \frac{1}{n} \min\left\{1 + \prod_{i=1}^{t} (n_i\bar{k}_i - 1)\right\},$$

where $\bar{k}_i$ is the same as defined in Theorem 1.5 and the minimum is taken over all the collections of pairs $\{(n_1, k_1), \ldots, (n_t, k_t)\}$ that satisfy the conditions (i) and (ii) in Theorem 1.5. $G_q(n)$ is approximately the same as $\kappa_p(n)$ but $G_q(n)$ measures more accurately the complexity of normal bases. For example, when $n = 15$ and $p = 2$, a Gauss period of type $(15, 4)$ yields a normal basis of complexity $15 \cdot 4 - 1 = 59$, and a Gauss period of type $\{(3, 2), (5, 2)\}$ yields a normal basis complexity $(3\cdot 2-1)(5\cdot 2-1)=45$; both have the same k but with different complexities. In fact, $G_2(15)=46/15\approx 3.07$ but $\kappa_2(15)=4$.

Given a prime p and a positive integer n, we want to compute $G_p(n)$. We need to search for an appropriate factorization $n=n_1n_2\cdots n_t$ and positive integers $k_1,k_2,\dots,k_t$ such that (i) and (ii) are satisfied and such that $\prod_{i=1}^t(n_i\bar{k}_i-1)$ is minimized. To do this we first factor n as

$$n=P_1P_2\cdots P_\ell,$$

where P_i are prime powers and ℓ is the number of distinct prime factors of n. Then we partition $\{P_1,P_2,\dots,P_\ell\}$ to form all possible factorizations $n=n_1n_2\cdots n_t$, $t\le\ell$, where $n_1,n_2,\dots,n_t$ are pairwise relatively prime. For each factorization $n=n_1n_2\cdots n_t$ and for each $1\le i\le t$, find the smallest positive integer k_i such that (n_i,k_i) is a prime Gauss pair. If $r=\prod_{i=1}^t(n_ik_i+1)$ is squarefree then we have a normal basis of complexity at most $\prod_{i=1}^t(n_i\bar{k}_i-1)$. Take the smallest complexity among all such factorizations of n. For example, if $n=154=2\cdot 7\cdot 11$ then we can factor n as

$$(2)(7)(11),\ (2\cdot 11)(7),\ (2)(7\cdot 11),\ (2\cdot 7)(11),\ (2\cdot 7\cdot 11).$$

For $p=2$ and for $m\in\{2,7,11,14,22,77,154\}$, the smallest prime Gauss pairs (m,k) are

$$(2,1),\ (7,4),\ (11,2),\ (14,2),\ (22,3),\ (77,6),\ (154,25).$$

The optimal combination is $\{(11,2),(14,2)\}$. So there is a Gauss period of type $\{(11,2),(14,2)\}$ that generates a normal basis for $\mathbb{F}_{2^{154}}$ of complexity $(11\cdot 2-1)(14\cdot 2-1)=567$, and $G_2(154)=568/154\approx 3.69$. Note that $\kappa_2'(154)=25$, and the smallest complexity of normal bases from prime Gauss periods is $154\cdot(25+1)-1=4003$. In this case general Gauss periods yield normal bases with much smaller complexity.

To test if any given pair (n,k) is a prime Gauss pair for p, we check if the following conditions are satisfied, $r=nk+1$ must be a prime and $\gcd(e,n)=1$ where e is the index of p modulo r. The latter condition is equivalent to

$$p^{n/v}\not\equiv 1\,(\mathrm{mod}\,r) \text{ for each prime factor } v \text{ of } n.$$

When n and p are given, the smallest prime Gauss pair (n,k) is found by trying $k=1,2,3,\dots$. Adleman and Lenstra [1] and Bach and Shallit [5] prove under the extended Riemann hypothesis that $\kappa_p'(n)\le cn^3\log^2(np)$ for some absolute constant c. But our computer experiment shows that such k is much smaller. For example, $\kappa'_2(3^i) < 6i$ and $\kappa'_3(2^i) < 6i$ for all $1 \le i \le 1000$. It would be interesting to have a better theoretical bound for $\kappa_p(n)$.

We still need to generate all the partitions of $\{P_1, P_2, \dots, P_\ell\}$. The number of partitions of a set with ℓ distinct elements is called a Bell number, denoted by Bell(ℓ), which is exponential in ℓ. All the partitions of a set $\{1, 2, \dots, \ell\}$ of ℓ distinct elements can be generated recursively as follows. Let $m =$ Bell $(i-1)$. Suppose that

$$S_1, S_2, \dots, S_m$$

is a list of all partitions of $\{1, 2, \dots, i-1\}$ for some $i > 1$. For each partition $S_j = s_{j1} \cup s_{j2} \cup \cdots \cup s_{jv}$ with v parts, $1 \le j \le m$, form $v + 1$ partitions of $\{1, 2, \dots, i\}$:

$$s_{j1} \cup s_{j2} \cup \cdots \cup s_{jv} \cup \{i\}, \quad S_{jw}, \ 1 \le w \le v, \tag{7}$$

where S_{jw} is the partition S_j with its wth part s_{jw} replaced by s_{jw} with i added. Then all the partitions of $\{1, 2, \dots, i\}$ is the union of (7) for $1 \le j \le m$. Since each partition of $\{1, 2, \dots, i-1\}$ has at most $i - 1$ parts, the above algorithm shows that Bell$(i) \le i$ Bell$(i-1)$. So Bell$(\ell) \le \ell!$. (Of course, the number of partitions is at most the number of permutations.) Note that the ith prime is at least $i + 1$. We have Bell$(\ell) < n$ for any positive integer n with ℓ distinct

TABLE 1
Percentages of $n \le 3000$ with $G_p(n) \le k$

$k\backslash p$	2	3	5	7	11	13	17	19	23
2	20.2	5.67	6.00	5.37	5.47	5.50	5.30	5.50	5.37
3	22.8	28.0	21.4	20.0	20.0	20.0	19.8	20.3	20.1
4	48.6	28.0	28.1	26.3	26.3	26.5	25.7	26.3	26.2
5	48.6	40.0	41.7	37.7	39.7	37.6	39.1	38.0	39.6
6	61.2	59.1	45.8	45.4	46.2	44.8	47.0	45.3	46.5
7	62.7	59.1	58.0	60.4	58.6	57.0	59.5	58.2	59.1
8	69.4	65.2	62.3	61.4	63.6	60.4	64.0	61.5	63.9
9	70.2	76.5	71.2	71.5	71.4	69.6	72.4	70.1	70.6
10	75.7	77.6	78.2	74.2	74.6	72.6	76.0	73.5	73.7
15	81.9	92.2	91.7	90.8	90.6	89.0	90.8	89.8	90.2
20	85.3	95.8	96.6	96.0	95.7	95.1	95.4	95.0	95.8
25	86.6	98.3	98.1	98.5	98.1	98.1	97.9	97.6	98.2
30	87.0	99.2	99.2	99.2	99.2	98.7	98.8	98.4	98.9
35	87.2	99.5	99.6	99.6	99.7	99.6	99.5	99.2	99.6
40	87.4	99.8	99.7	99.8	99.8	99.8	99.6	99.3	99.7
50	87.5	99.9	99.8	100.0	100.0	99.9	99.9	99.8	99.9

TABLE 2
Values of $n \leq 2000$ Where $\kappa_2'(n) - G_2(n) \geq 20$

	General				Prime			
n	Types	k	r	Cplex	k	r	Cplex	Diff
154	$\{(14, 2), (11, 2)\}$	4	667	567	25	3,851	4,003	22
415	$\{(5, 2), (83, 2)\}$	4	1,837	1,485	28	11,621	11,619	24
477	$\{(9, 2), (53, 2)\}$	4	2,033	1,785	46	21,943	21,941	42
514	$\{(2, 1), (257, 6)\}$	6	4,629	4,623	33	16,963	17,475	25
862	$\{(2, 1), (431, 2)\}$	2	2,589	2,583	31	26,723	27,583	29
884	$\{(4, 1), (221, 2)\}$	2	2,215	3,087	27	23,869	24,751	25
885	$\{(177, 4), (5, 2)\}$	8	7,799	6,363	28	24,781	24,779	21
954	$\{(106, 1), (9, 2)\}$	2	2,033	3,587	49	46,747	47,699	46
996	$\{(12, 1), (83, 2)\}$	2	2,171	3,795	43	42,829	43,823	40
1073	$\{(29, 2), (37, 4)\}$	8	8,791	8,379	30	32,191	32,189	22
1189	$\{(29, 2), (41, 2)\}$	4	4,897	4,617	24	28,537	28,535	20
1209	$\{(93, 4), (13, 4)\}$	16	19,769	18,921	38	45,943	45,941	22
1227	$\{(3, 2), (409, 4)\}$	8	11,459	8,175	34	41,719	41,717	27
1335	$\{(3, 2), (5, 2), (89, 2)\}$	8	13,783	7,965	44	58,741	58,739	38
1410	$\{(470, 2), (3, 2)\}$	4	6,587	4,695	42	59,221	59,219	39
1431	$\{(27, 6), (53, 2)\}$	12	17,441	16,905	40	57,241	57,239	28
1465	$\{(5, 2), (293, 2)\}$	4	6,457	5,265	30	43,951	43,949	26
1476	$\{(36, 1), (41, 2)\}$	2	3,071	5,751	25	36,901	38,375	22
1545	$\{(3, 2), (515, 2)\}$	4	7,217	5,145	28	43,261	43,259	25
1572	$\{(4, 1), (393, 2)\}$	2	3,935	5,495	25	39,301	40,871	23
1605	$\{(3, 2), (535, 4)\}$	8	14,987	10,695	32	51,361	51,359	25
1635	$\{(3, 2), (545, 2)\}$	4	7,637	5,445	38	62,131	62,129	35
1674	$\{(2, 1), (837, 6)\}$	6	15,069	15,063	33	55,243	56,915	25
1691	$\{(19, 10), (89, 2)\}$	20	34,189	33,453	42	71,023	71,021	22
1719	$\{(9, 2), (191, 2)\}$	4	7,277	6,477	24	41,257	41,255	20
1724	$\{(4, 1), (431, 2)\}$	2	4,315	6,027	27	46,549	48,271	25
1771	$\{(161, 6), (11, 2)\}$	12	22,241	20,265	40	70,841	70,839	29
1833	$\{(3, 2), (611, 2)\}$	4	8,561	6,105	26	47,659	47,657	23
1842	$\{(614, 2), (3, 2)\}$	4	8,603	6,135	25	46,051	47,891	23
1908	$\{(36, 1), (53, 2)\}$	2	3,959	7,455	25	47,701	49,607	22
1962	$\{(218, 5), (9, 2)\}$	10	20,729	22,219	50	98,101	98,099	39
1964	$\{(4, 1), (491, 2)\}$	2	4,915	6,867	29	56,957	58,919	27

prime factors. Therefore one can generate all the partitions of $\{P_1, P_2, \dots, P_\ell\}$ in time linear in n.

Using the above algorithm, we computed $G_p(n)$ for $n \leq 3000$ and $p \in \{2, 3, 5, 7, 11, 13, 17, 19, 23\}$. In Table 1, we tabulated the percentages of the values of n with $G_p(n) \leq k$ for various small values of k. Note that for $p = 2$, the percentage is relatively small for $k > 2$ compared to other p's. The reason is that whenever $8|n$, $\mathbb{F}_{2^n}$ has no normal bases from Gauss periods. For all $p \in \{3, 5, 7, 11, 13, 17, 19, 23\}$, $G_p(n) \leq 10$ for more than 70% of $n \leq 3000$,

TABLE 3
Values of $n \leq 2000$ Where $\kappa'_p(n) - G_p(n) \geq 20$

		General				Prime			
p	n	Types	k	r	Cplex	k	r	Cplex	Diff
3	159	{(3, 2), (53, 2)}	4	749	1,264	34	5,407	5,564	27
3	415	{(5, 2), (83, 2)}	4	1,837	3,472	30	12,451	12,449	22
3	450	{(50, 2), (9, 2)}	4	1,919	3,874	33	14,851	14,849	24
3	495	{(99, 2), (5, 2)}	4	2,189	4,144	30	14,851	14,849	22
3	534	{(6, 1), (89, 2)}	2	1,253	2,926	27	14,419	14,417	22
3	942	{(6, 1), (157, 10)}	10	10,997	18,986	43	40,507	41,447	24
3	1078	{(98, 2), (11, 2)}	4	4,531	9,376	34	36,653	37,729	26
3	1189	{(29, 2), (41, 2)}	4	4,897	10,492	30	35,671	35,669	21
3	1195	{(5, 2), (239, 2)}	4	5,269	10,024	28	33,461	34,654	21
3	1220	{(4, 1), (305, 6)}	6	9,155	12,803	29	35,381	36,599	20
3	1375	{(125, 2), (11, 2)}	4	5,773	11,968	34	46,751	48,124	26
3	1438	{(2, 2), (719, 2)}	4	7,195	10,780	57	81,967	81,965	50
3	1498	{(2, 2), (749, 2)}	4	7,495	11,230	40	59,921	61,417	34
3	1592	{(8, 2), (199, 4)}	8	13,549	22,862	35	55,721	57,311	22
3	1710	{(18, 1), (95, 2)}	2	3,629	9,940	27	46,171	46,169	21
3	1771	{(161, 6), (11, 2)}	12	22,241	30,880	40	70,841	72,610	24
3	1815	{(363, 4), (5, 2)}	8	15,983	25,396	44	79,861	81,674	31
5	407	{(11, 2), (37, 4)}	8	3,427	5,888	36	14,653	15,058	23
5	415	{(5, 2), (83, 2)}	4	1,837	3,472	42	17,431	17,844	35
5	693	{(9, 2), (77, 6)}	12	8,797	13,988	52	36,037	36,728	33
5	836	{(4, 3), (209, 2)}	6	5,447	9,390	36	30,097	30,931	26
5	917	{(7, 4), (131, 2)}	8	7,627	13,328	36	33,013	33,928	22
5	1105	{(5, 2), (221, 2)}	4	4,873	9,268	30	33,151	33,149	22
5	1107	{(27, 4), (41, 2)}	8	9,047	16,348	40	44,281	44,279	25
5	1122	{(102, 1), (11, 2)}	2	2,369	6,496	46	51,613	52,733	41
5	1242	{(46, 1), (27, 4)}	4	5,123	12,194	41	50,923	52,163	32
5	1488	{(16, 1), (93, 4)}	4	6,341	14,384	34	50,593	52,079	25
5	1496	{(136, 1), (11, 2)}	2	3,151	8,672	36	53,857	55,351	31
5	1497	{(3, 2), (499, 4)}	8	13,979	19,952	56	83,833	85,328	44
5	1524	{(12, 3), (127, 4)}	12	18,833	29,798	44	67,057	68,579	25
5	1558	{(2, 1), (779, 2)}	2	4,677	7,008	34	52,973	54,529	31
5	1586	{(2, 1), (793, 6)}	6	14,277	16,650	32	50,753	52,337	23
5	1605	{(3, 2), (535, 4)}	8	14,987	21,392	32	51,361	52,964	20
5	1908	{(36, 1), (53, 2)}	2	3,959	11,218	32	61,057	62,963	27

and $G_p(n) \leq 20$ for more than 95% of $n \leq 3000$. To see how much general Gauss periods improve over prime Gauss periods, we list in Tables 2, 3, and 4 the values of $n \leq 2000$ for which $\kappa'_p(n) - G_p(n) \geq 20$ for $p \in \{2, 3, 5, 7, 11\}$, where "Cplex" denotes complexity and "Diff" is the difference of complexities divided by n. General Gauss periods indeed give many new normal bases of low complexity.

TABLE 4
Values of $n \leq 2000$ Where $\kappa'_p(n) - G_p(n) \geq 20$

		General				Prime			
p	n	Types	k	r	Cplex	k	r	Cplex	Diff
7	276	{(4, 1), (69, 2)}	2	695	1,442	41	11,317	11,591	37
7	415	{(5, 2), (83, 2)}	4	1,837	3,472	28	11,621	11,619	20
7	1004	{(4, 1), (251, 2)}	2	2,515	5,264	24	24,097	25,099	20
7	1166	{(106, 1), (11, 2)}	2	2,461	6,752	32	37,313	38,477	27
7	1194	{(2, 2), (597, 4)}	8	11,945	14,920	63	75,223	75,221	51
7	1275	{(51, 2), (25, 4)}	8	10,403	18,848	40	51,001	52,274	26
7	1386	{(126, 1), (11, 2)}	2	2,921	8,032	25	34,651	36,035	20
7	1545	{(309, 2), (5, 2)}	4	6,809	12,964	30	46,351	47,894	23
7	1662	{(554, 2), (3, 4)}	8	14,417	23,254	48	79,777	81,437	35
7	1664	{(128, 2), (13, 4)}	8	13,621	24,512	48	79,873	81,535	34
7	1771	{(161, 6), (11, 2)}	12	22,241	36,032	40	70,841	72,610	21
7	1794	{(78, 1), (23, 2)}	2	3,713	10,540	48	86,113	87,905	43
7	1826	{(22, 1), (83, 2)}	2	3,841	10,664	38	69,389	71,213	33
7	1855	{(5, 2), (371, 2)}	4	8173	15,568	40	74,201	76,054	33
7	1986	{(2, 2), (993, 2)}	4	9,935	14,890	26	51,637	53,621	20
7	1996	{(4, 1), (499, 4)}	4	9,985	17,458	40	79,841	81,835	32
7	2000	{(16, 1), (125, 2)}	2	4,267	11,594	48	96,001	97,999	43
11	106	{(2, 1), (53, 2)}	2	321	474	28	2,969	3,073	25
11	334	{(2, 1), (167, 14)}	14	7,017	7,512	45	15,031	15,363	24
11	375	{(3, 2), (125, 2)}	4	1,757	2,992	38	14,251	14,624	31
11	750	{(250, 1), (3, 2)}	2	1,757	3,992	28	21,001	21,749	24
11	805	{(35, 2), (23, 2)}	4	3,337	7,072	28	22,541	23,344	20
11	1054	{(2, 1), (527, 8)}	8	12,651	14,226	34	35,837	36,889	22
11	1300	{(100, 1), (13, 4)}	4	5,353	12,736	52	67,601	68,899	43
11	1431	{(27, 4), (53, 2)}	8	11,663	21,172	36	51,517	52,946	22
11	1476	{(36, 2), (41, 2)}	4	6,059	13,054	30	44,281	45,755	22
11	1728	{(64, 3), (27, 4)}	12	21,037	34,170	45	77,761	79,487	26
11	1810	{(2, 1), (905, 2)}	2	5,433	8,142	24	43,441	45,249	21
11	1833	{(3, 2), (611, 2)}	4	8,561	14,656	34	62,323	64,154	27
11	1887	{(3, 2), (629, 2)}	4	8,813	15,088	28	52,837	54,722	21
11	1902	{(2, 1), (951, 10)}	10	28,533	31,380	41	77,983	79,883	26
11	1908	{(36, 2), (53, 2)}	4	7,811	16,906	30	57,241	59,147	22

ACKNOWLEDGMENT

The author thanks Hendrik W. Lenstra, Jr., for sharing his proof of part of Theorem 1.4. Many thanks also go to Joel Brawley and Jenny Key for their useful comments and encouragement. The main results of the paper were reported at a workshop on Finite Fields: Theory and Computation at the Mathematical Research Institute at Oberwolfach, Germany, January 19–25, 1997.

REFERENCES

1. L. M. Adleman and H. W. Lenstra, Jr., Finding irreducible polynomials over finite fields, *in* "Proc. 18th Annual ACM Symp. on Theory of Computing, 1986," pp. 350–355.
2. G. B. Agnew, R. C. Mullin, I. M. Onyszchuk, and S. A. Vanstone, An implementation for a fast public key cryptosystem, *J. Cryptolo.* **3** (1991), 63–79.
3. G. B. Agnew, R. C. Mullin, and S. A. Vanstone, An implementation of elliptic curve cryptosystems over $F_{2^{155}}$, *IEEE J. Select. Areas Commun.* **11** (1993), 804–813.
4. D. W. Ash, I. F. Blake, and S. A. Vanstone, Low complexity normal bases, *Discrete Appl. Math.* **25** (1989), 191–210.
5. E. Bach and J. Shallit, Factoring with cyclotomic polynomials, *Math. Comput.* **52** (1989), 201–219 (previous version *in* "Proc. 26th Annual ACM Symp. on Foundations of Computer Science, 1985," pp. 443–450).
6. I. F. Blake, S. Gao, and R. C. Mullin, Normal and self-dual normal bases from factorization of $cx^{q+1} + dx^q - ax - b$, *SIAM J. Discrete Math.* **7** (1994), 499–512.
7. S. Feisel, J. von zur Gathen, and M. A. Shokrollahi, Normal bases via general Gauss periods, *Math. Comput.* **68**, No. 225 (1999), 271–290.
8. S. Gao, J. von zur Gathen, and D. Panario, Gauss periods and fast exponentiation in finite fields, [extended abstract], *in* Lecture Notes in Computer Science, Vol. 911, Springer-Verlag, 1995, 311–322.
9. S. Gao, J. von zur Gathen, and D. Panario, Gauss periods: Orders and cryptographical applications, *Math. Comput.* **67**, No. 221 (1998), 343–352.
10. S. Gao, J. von zur Gathen, D. Panario, and V. Shoup, Algorithms for exponentiation in finite fields, *J. Symbol. Comput.* **29** (2000), 879–889.
11. S. Gao and H. W. Lenstra, Jr., Optimal normal bases, *Des. Codes Cryptogr.* **2** (1992), 315–323.
12. S. Gao and S. A. Vanstone, On orders of optimal normal basis generators, *Math. Comput.* **64** (1995), 1227–1233.
13. C. F. Gauss, "Disquisitiones Arithmeticae," Braunschweig, 1801.
14. N. Jacobson, "Basic Algebra I," 2nd ed., Freeman, New York, 1985.
15. D. Jungnickel, "Finite Fields: Structure and Arithmetics," Bibliographisches Institut, Mannheim, 1993.
16. A. J. Menezes (Ed.), I. F. Blake, X. H. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, "Applications of Finite Fields," Kluwer, Academic, Dordrecht, 1993.
17. R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson, Optimal normal bases in $GF(p^n)$, *Discrete Appl. Math.* **22** (1988/1989), 149–161.
18. M. Nöcker, Normal bases, Gauss periods, and fast arithmetic, preprint, 1999.
19. I. M. Onyszchuk, R. C. Mullin, and S. A. Vanstone, "Computational Method and Apparatus for Finite Field Multiplication," U.S. Patent No. 4,745,568, May 1988.
20. M. Pohst and H. Zassenhaus, Algorithmic Algebraic Number Theory, Cambridge Univ. Press, Cambridge, UK, 1989.
21. I. Stewart, "Gauss," *Sci. Am.* **237** (July 1977), 123–131.
22. B. van der Waerden, "Algebra," Vol. 1, Springer-Verlag, Berlin, 1966.
23. A. Wassermann, Konstruktion von Normalbasen, *Bayreuth. Math. Schr.* **31** (1990), 155–164.
24. A. Wassermann, Zur Arithmetik in endlichen Körpern, *Bayreuth. Math. Sch.* **44** (1993), 147–251.