ABELIAN GROUPS, GAUSS PERIODS, AND NORMAL BASES

SHUHONG GAO

ABSTRACT. 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.

Dedicated to Professor Chao Ko on his 90th birthday.

1. Introduction and main results

We first prove a result on finite abelian groups. We use the standard notation $< S, K >$ 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 $G =< S, K >$. Then, for any direct product $G = G_1 \otimes G_2 \otimes \cdots \otimes G_t$, there is a subgroup H of the form*

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

such that

$$G =< S, H > \quad \text{and} \quad \frac{G}{H} \cong \frac{G}{K}.$$

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

---

Key words and phrases. Finite fields, finite abelian groups, Gauss periods, normal bases.

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

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, pp. 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 $\ell^v \mid r_2$. 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 say a Gauss period of type (n, k) instead of (n, K). To distinguish this case, we sometime call the Gauss periods defined above em general Gauss periods.

A *normal basis* for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ 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 $< q, K >= \mathbb{Z}_r^\times$.*

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 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, 9, 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, the 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 $< q, K >= \mathbb{Z}_r^\times$. It is possible that $< q, K >= \mathbb{Z}_r^\times$ for some subgroups K of order k in $\mathbb{Z}_r^\times$ while $< q, K >\neq \mathbb{Z}_r^\times$ 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 $< q, K >= \mathbb{Z}_r^\times$. Then n and k factor as*

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

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 $n \le 3000$ 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 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

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

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

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

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

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

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 $G_i =< \alpha_i >$ generated by α_i, $1 \le i \le t$. The number t is called the rank of G and $\alpha_1, \alpha_2, \dots, \alpha_t$ 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 $K \ne G$. Denote the elements of G/K by $\overline{a}$, $a \in G$. For convenience, we switch to the additive notation for the group operation of G. Then

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

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

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

Thus

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

The order of $\overline{a}$ is equal to the least common multiple of the orders of $a_i\overline{\alpha}_i$, $1 \le i \le t$. Since all the orders are powers of p, there is an i such that $a_i\overline{\alpha}_i$ has order p^e. Without loss of generality, we assume that $i = t$. Note that $p \nmid a_t$, since otherwise $\overline{\alpha}_t \in G$ would have order at least p^{e+1}, contradicting to the choice of $\overline{a}$ 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

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

where $\overline{a}$ and $\overline{\alpha}_t$ 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 $\alpha_1, \dots, \alpha_t$, 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

$$G =< S, \tilde{K} > . \tag{2}$$

We shall show later that

$$\overline{G} \cong \frac{\tilde{G}}{\tilde{K}} \otimes < \overline{\alpha}_t > . \tag{3}$$

Let $\tilde{S}$ be the subgroup consisting of all elements of S with t-th component zero. Since $G_t =< \alpha_t >$ is a component in the direct product of

G, (1) and (2) imply that $\tilde{G} =< \tilde{S}, \tilde{K} >$. Now $\tilde{G}/\tilde{K}$ has rank at most $t-1$, by 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

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

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

$$\frac{G}{H} \cong \frac{\tilde{G}}{\tilde{H}} \otimes \frac{G_t}{H_t} \cong \frac{\tilde{G}}{\tilde{K}} \otimes < \alpha_t > \cong \frac{G}{K}$$

and

$$\begin{aligned} < S, H > &= < \tilde{S}, a, \tilde{H}, p^e\alpha_t >=< \tilde{S}, \tilde{H}, a, p^e\alpha_t > \\ &= < \tilde{G}, a, p^e\alpha_t >=< \tilde{G}, \alpha_t, p^e\alpha_t >= G, \end{aligned}$$

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

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

$$\overline{G} \cong \frac{\tilde{G}}{< \overline{a} >} \otimes < \overline{a} > . \tag{4}$$

But $< \overline{a} >\cong< K, a > /K$. By the third isomorphism theorem of groups,

$$\frac{\overline{G}}{< \overline{a} >} \cong \frac{G/K}{< K, a > /K} \cong \frac{G}{< K, a >}. \tag{5}$$

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

$$< K, a >=< \tilde{K}, a >= \tilde{K}+ < a >$$

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

$$\frac{G}{< K, a >} = \frac{\tilde{G}+ < a >}{\tilde{K}+ < a >} \cong \frac{\tilde{G}}{\tilde{K}} \otimes \frac{< a >}{< a >} \cong \frac{\tilde{G}}{\tilde{K}}.$$

It follows from (4) and (5) that

$$\overline{G} \cong \frac{\tilde{G}}{\tilde{K}} \otimes < \overline{a} > \cong \frac{\tilde{G}}{\tilde{K}} \otimes < \overline{\alpha_t} >,$$

as $\overline{\alpha}_t$ and $\overline{a}$ have the same order in $\overline{G}$. 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. $< p^m, K >= \mathbb{Z}_r^\times$ 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 $< p^m, K >= \mathbb{Z}_r^\times$ iff $< p, K >= \mathbb{Z}_r^\times$ and $\gcd(n,m) = 1$.

We prove that if $p = 2$ and $8|n$ then $< p, K >\neq \mathbb{Z}_r^\times$ 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 $< 2, K >= \mathbb{Z}_r^\times$. Let $K_1 =< 2^8, K >\subseteq \mathbb{Z}_r^\times$. 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 $< 2, K_1 >\neq \mathbb{Z}_r^\times$, 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 (1993) for each $1 \le i \le t$ there is a positive integer k_i such that $r_i = n_i k_i + 1$ is a prime and $< p, K_i >= \mathbb{Z}_{r_i}^\times$ 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, pp. 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

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

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

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

Note that

$$\frac{\mathbb{Z}_r^\times}{H} \cong \frac{\mathbb{Z}_{r_1}^\times}{H_1} \oplus \frac{\mathbb{Z}_{r_2}^\times}{H_2} \oplus \cdots \oplus \frac{\mathbb{Z}_{r_t}^\times}{H_t}. \tag{6}$$

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 $< q, H >= \mathbb{Z}_r^\times$ 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,

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

implies that $< q, H_i >= \mathbb{Z}_{r_i}^\times$ 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, pp. 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 $< q, K >= \mathbb{Z}_r^\times$ 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 $< q, K >= \mathbb{Z}_r^\times$. 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 don't 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 $\{(n_1, k_1), \dots, (n_t, k_t)\}$ of pairs, we say that it is of type $\{(n_1, k_1), \dots, (n_t, k_t)\}$. Define

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

where $\bar{k}_i$ is the same as defined in Theorem 1.5 and the minimum is taken over all the collections of pairs $\{(n_1, k_1), \dots, (n_t, k_t)\}$ 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 $n = n_1 n_2 \cdots n_t$ and positive integers $k_1, k_2, \ldots k_t$ 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

$$n = P_1 P_2 \cdots P_\ell$$

where P_i are prime powers and ℓ is the number of distinct prime factors of n. Then we partition $\{P_1, P_2, \ldots, P_\ell\}$ to form all possible factorizations $n = n_1 n_2 \cdots n_t$, $t \le \ell$, where $n_1, n_2, \ldots, n_t$ are pairwise relatively prime. For each factorization $n = n_1 n_2 \cdots n_t$ 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 $r = \prod_{i=1}^{t}(n_i k_i + 1)$ 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

$$p^{n/v} \not\equiv 1 \pmod{r} \text{ for each prime factor } v \text{ of } n.$$

When n and p are given, the smallest prime Gauss pair (n, k) is found by trying $k = 1, 2, 3, \ldots$. Adleman & Lenstra [1] and Bach & 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 $\{P_1, P_2, \ldots, P_\ell\}$. The number of partitions of a set with ℓ distinct elements is called a Bell number, denoted by $\mathrm{Bell}(\ell)$, which is exponential in ℓ. All the partitions of a set $\{1, 2, \ldots, \ell\}$ of ℓ distinct elements can be generated recursively as follows. Let $m = \mathrm{Bell}(i-1)$. Suppose that

$$S_1, S_2, \ldots, S_m$$

is a list of all partitions of $\{1, 2, \ldots, i-1\}$ 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 $\{1, 2, \ldots, i\}$:

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

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 $\{1, 2, \ldots, i\}$ is the union of (7) for $1 \le j \le m$. Since each partition of $\{1, 2, \ldots, i-1\}$ has at most $i-1$ parts, the above algorithm shows that $\mathrm{Bell}(i) \le i\,\mathrm{Bell}(i-1)$. So $\mathrm{Bell}(\ell) \le \ell!$. (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 $\mathrm{Bell}(\ell) < n$ for any positive integer n with ℓ distinct prime factors. Therefore one can generate all the partitions of $\{P_1, P_2, \ldots, P_\ell\}$ in time linear in n.

Using the above algorithm, we computed $G_p(n)$ for $n \le 3000$ 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 $G_p(n) \le k$ for various small values of k. Note that for $p = 2$, the percentage is relatively small for $k > 2$ comparing to other p's. The reason is that whenever $8|n$, $\mathbb{F}_{2^n}$ has no normal bases from Gauss periods. For all $p \in \{3, 5, 7, 11, 13, 17, 19, 23\}$, $G_p(n) \le 10$ for more than 70% of $n \le 3000$, and $G_p(n) \le 20$ for more than 95% of $n \le 3000$. To see how much general Gauss periods improve over prime Gauss periods, we list in Tables 2, 3 and 4 the values of $n \le 2000$ for which $\kappa_p'(n) - G_p(n) \ge 20$ for $p \in \{2, 3, 5, 7, 11\}$, where "Cplex" denotes complexity, "Diff" is the difference of complexities divided by n. General Gauss periods indeed give many new normal bases of low complexity.

Acknowledgement. The author would like to thank 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

k\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 1. Percentages of $n \leq 3000$ with $G_p(n) \leq k$.

encouragement. The main results of the paper were reported at a Workshop on Finite fields: Theory and Computation, 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*, Proc. 18th Annual ACM Symp. on Theory of Computing (1986), 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. of Cryptology, **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. on Selected Areas in Communications, **11** (1993), 804–813.

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

[5] E. Bach and J. Shallit, *Factoring with cyclotomic polynomials*, Math. Comp., **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 Mathematics, *7* (1994), 499–512.

[7] S. Feisel, J. von zur Gathen and M.A. Shokrollahi, *Normal bases via general Gauss periods*, Math. Comp., **68** (1999), no. 225, 271–290.

	General				Prime			
n	Types	k	r	Cplex	k	r	Cplex	Diff
154	{(14, 2),(11, 2)}	4	667	567	25	3851	4003	22
415	{(5, 2),(83, 2)}	4	1837	1485	28	11621	11619	24
477	{(9, 2),(53, 2)}	4	2033	1785	46	21943	21941	42
514	{(2, 1),(257, 6)}	6	4629	4623	33	16963	17475	25
862	{(2, 1),(431, 2)}	2	2589	2583	31	26723	27583	29
884	{(4, 1),(221, 2)}	2	2215	3087	27	23869	24751	25
885	{(177, 4),(5, 2)}	8	7799	6363	28	24781	24779	21
954	{(106, 1),(9, 2)}	2	2033	3587	49	46747	47699	46
996	{(12, 1),(83, 2)}	2	2171	3795	43	42829	43823	40
1073	{(29, 2),(37, 4)}	8	8791	8379	30	32191	32189	22
1189	{(29, 2),(41, 2)}	4	4897	4617	24	28537	28535	20
1209	{(93, 4),(13, 4)}	16	19769	18921	38	45943	45941	22
1227	{(3, 2),(409, 4)}	8	11459	8175	34	41719	41717	27
1335	{(3, 2),(5, 2),(89, 2)}	8	13783	7965	44	58741	58739	38
1410	{(470, 2),(3, 2)}	4	6587	4695	42	59221	59219	39
1431	{(27, 6),(53, 2)}	12	17441	16905	40	57241	57239	28
1465	{(5, 2),(293, 2)}	4	6457	5265	30	43951	43949	26
1476	{(36, 1),(41, 2)}	2	3071	5751	25	36901	38375	22
1545	{(3, 2),(515, 2)}	4	7217	5145	28	43261	43259	25
1572	{(4, 1),(393, 2)}	2	3935	5495	25	39301	40871	23
1605	{(3, 2),(535, 4)}	8	14987	10695	32	51361	51359	25
1635	{(3, 2),(545, 2)}	4	7637	5445	38	62131	62129	35
1674	{(2, 1),(837, 6)}	6	15069	15063	33	55243	56915	25
1691	{(19, 10),(89, 2)}	20	34189	33453	42	71023	71021	22
1719	{(9, 2),(191, 2)}	4	7277	6477	24	41257	41255	20
1724	{(4, 1),(431, 2)}	2	4315	6027	27	46549	48271	25
1771	{(161, 6),(11, 2)}	12	22241	20265	40	70841	70839	29
1833	{(3, 2),(611, 2)}	4	8561	6105	26	47659	47657	23
1842	{(614, 2),(3, 2)}	4	8603	6135	25	46051	47891	23
1908	{(36, 1),(53, 2)}	2	3959	7455	25	47701	49607	22
1962	{(218, 5),(9, 2)}	10	20729	22219	50	98101	98099	39
1964	{(4, 1),(491, 2)}	2	4915	6867	29	56957	58919	27

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

[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. Comp., **67** (1998), no. 221, 343–352.

[10] S. Gao, J. von zur Gathen, D. Panario and V. Shoup, *Algorithms for exponentiation in finite fields*, J. of Symbolic Computation, **29** (2000), 879-889.

		General				Prime			
p	n	Types	k	r	Cplex	k	r	Cplex	Diff
3	159	{(3, 2),(53, 2)}	4	749	1264	34	5407	5564	27
3	415	{(5, 2),(83, 2)}	4	1837	3472	30	12451	12449	22
3	450	{(50, 2),(9, 2)}	4	1919	3874	33	14851	14849	24
3	495	{(99, 2),(5, 2)}	4	2189	4144	30	14851	14849	22
3	534	{(6, 1),(89, 2)}	2	1253	2926	27	14419	14417	22
3	942	{(6, 1),(157, 10)}	10	10997	18986	43	40507	41447	24
3	1078	{(98, 2),(11, 2)}	4	4531	9376	34	36653	37729	26
3	1189	{(29, 2),(41, 2)}	4	4897	10492	30	35671	35669	21
3	1195	{(5, 2),(239, 2)}	4	5269	10024	28	33461	34654	21
3	1220	{(4, 1),(305, 6)}	6	9155	12803	29	35381	36599	20
3	1375	{(125, 2),(11, 2)}	4	5773	11968	34	46751	48124	26
3	1438	{(2, 2),(719, 2)}	4	7195	10780	57	81967	81965	50
3	1498	{(2, 2),(749, 2)}	4	7495	11230	40	59921	61417	34
3	1592	{(8, 2),(199, 4)}	8	13549	22862	35	55721	57311	22
3	1710	{(18, 1),(95, 2)}	2	3629	9940	27	46171	46169	21
3	1771	{(161, 6),(11, 2)}	12	22241	30880	40	70841	72610	24
3	1815	{(363, 4),(5, 2)}	8	15983	25396	44	79861	81674	31
5	407	{(11, 2),(37, 4)}	8	3427	5888	36	14653	15058	23
5	415	{(5, 2),(83, 2)}	4	1837	3472	42	17431	17844	35
5	693	{(9, 2),(77, 6)}	12	8797	13988	52	36037	36728	33
5	836	{(4, 3),(209, 2)}	6	5447	9390	36	30097	30931	26
5	917	{(7, 4),(131, 2)}	8	7627	13328	36	33013	33928	22
5	1105	{(5, 2),(221, 2)}	4	4873	9268	30	33151	33149	22
5	1107	{(27, 4),(41, 2)}	8	9047	16348	40	44281	44279	25
5	1122	{(102, 1),(11, 2)}	2	2369	6496	46	51613	52733	41
5	1242	{(46, 1),(27, 4)}	4	5123	12194	41	50923	52163	32
5	1488	{(16, 1),(93, 4)}	4	6341	14384	34	50593	52079	25
5	1496	{(136, 1),(11, 2)}	2	3151	8672	36	53857	55351	31
5	1497	{(3, 2),(499, 4)}	8	13979	19952	56	83833	85328	44
5	1524	{(12, 3),(127, 4)}	12	18833	29798	44	67057	68579	25
5	1558	{(2, 1),(779, 2)}	2	4677	7008	34	52973	54529	31
5	1586	{(2, 1),(793, 6)}	6	14277	16650	32	50753	52337	23
5	1605	{(3, 2),(535, 4)}	8	14987	21392	32	51361	52964	20
5	1908	{(36, 1),(53, 2)}	2	3959	11218	32	61057	62963	27

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

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

[12] S. Gao and S.A. Vanstone, *On orders of optimal normal basis generators*, Math. Comp., **64** (1995), 1227–1233.

[13] C.F. Gauss, *Disquisitiones Arithmeticae*, Braunschweig, 1801.

[14] N. Jacobson, *Basic Algebra I*, 2nd ed., W.H. Freeman, New York, 1985.

		General				Prime			
p	n	Types	k	r	Cplex	k	r	Cplex	Diff
7	276	{(4, 1),(69, 2)}	2	695	1442	41	11317	11591	37
7	415	{(5, 2),(83, 2)}	4	1837	3472	28	11621	11619	20
7	1004	{(4, 1),(251, 2)}	2	2515	5264	24	24097	25099	20
7	1166	{(106, 1),(11, 2)}	2	2461	6752	32	37313	38477	27
7	1194	{(2, 2),(597, 4)}	8	11945	14920	63	75223	75221	51
7	1275	{(51, 2),(25, 4)}	8	10403	18848	40	51001	52274	26
7	1386	{(126, 1),(11, 2)}	2	2921	8032	25	34651	36035	20
7	1545	{(309, 2),(5, 2)}	4	6809	12964	30	46351	47894	23
7	1662	{(554, 2),(3, 4)}	8	14417	23254	48	79777	81437	35
7	1664	{(128, 2),(13, 4)}	8	13621	24512	48	79873	81535	34
7	1771	{(161, 6),(11, 2)}	12	22241	36032	40	70841	72610	21
7	1794	{(78, 1),(23, 2)}	2	3713	10540	48	86113	87905	43
7	1826	{(22, 1),(83, 2)}	2	3841	10664	38	69389	71213	33
7	1855	{(5, 2),(371, 2)}	4	8173	15568	40	74201	76054	33
7	1986	{(2, 2),(993, 2)}	4	9935	14890	26	51637	53621	20
7	1996	{(4, 1),(499, 4)}	4	9985	17458	40	79841	81835	32
7	2000	{(16, 1),(125, 2)}	2	4267	11594	48	96001	97999	43
11	106	{(2, 1),(53, 2)}	2	321	474	28	2969	3073	25
11	334	{(2, 1),(167, 14)}	14	7017	7512	45	15031	15363	24
11	375	{(3, 2),(125, 2)}	4	1757	2992	38	14251	14624	31
11	750	{(250, 1),(3, 2)}	2	1757	3992	28	21001	21749	24
11	805	{(35, 2),(23, 2)}	4	3337	7072	28	22541	23344	20
11	1054	{(2, 1),(527, 8)}	8	12651	14226	34	35837	36889	22
11	1300	{(100, 1),(13, 4)}	4	5353	12736	52	67601	68899	43
11	1431	{(27, 4),(53, 2)}	8	11663	21172	36	51517	52946	22
11	1476	{(36, 2),(41, 2)}	4	6059	13054	30	44281	45755	22
11	1728	{(64, 3),(27, 4)}	12	21037	34170	45	77761	79487	26
11	1810	{(2, 1),(905, 2)}	2	5433	8142	24	43441	45249	21
11	1833	{(3, 2),(611, 2)}	4	8561	14656	34	62323	64154	27
11	1887	{(3, 2),(629, 2)}	4	8813	15088	28	52837	54722	21
11	1902	{(2, 1),(951, 10)}	10	28533	31380	41	77983	79883	26
11	1908	{(36, 2),(53, 2)}	4	7811	16906	30	57241	59147	22

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

[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, 1993.

[17] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone and R.M. Wilson, *Optimal normal bases in $GF(p^n)$*, Discrete Applied 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 #4,745,568, May 1988.
[20] M. Pohst and H. Zassenhaus, *Algorithmic Algebraic Number Theory*, Cambridge University Press, 1989.
[21] I. Stewart, *Gauss*, Scientific American, **237** (1977), July, 123–131.
[22] B. van der Waerden, *Algebra*, vol. 1, Springer-Verlag, Berlin, 1966.
[23] A. Wassermann, *Konstruktion von Normalbasen*, Bayreuther Mathematische Schriften, **31** (1990), 155–164.
[24] A. Wassermann, *Zur Arithmetik in endlichen Körpern*, Bayreuther Mathematische Schriften, **44** (1993), 147–251.

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975 USA, sgao@@math.clemson.edu