Publ. Math. Debrecen
56 / 3-4 (2000), 293–312

Gauss sums and a sieve for generators of Galois fields

By STEPHEN D. COHEN (Glasgow)

To Kálmán Győry on his 60th birthday, with respect and admiration

Abstract. Given the extension E of degree n of a Galois field $F = \mathrm{GF}(q)$, it is proved that, when $n \geq 5$, there is an element of E that simultaneously

(i) is a primitive element (i.e., a multiplicative generator) of E,
(ii) is free (i.e., an additive generator) in E over F,
(iii) has prescribed (non-zero) (E, F)-trace,
(iv) has prescribed (E, F)-norm, a primitive element of F.

The keys to the method are the derivation of relevant formulae involving Gauss sums, both over E and F, and a sieving technique that produces viable lower bounds and leads to a theoretical solution. The sieve is novel insofar as it is applied to the additive, as well as the multiplicative, structure. The method will be effective, in principle, also when $n = 4$.

1. Introduction

A *primitive element* of a finite field E is a generator of its (cyclic) multiplicative group. Given a prime power q and a positive integer n, we shall suppose E is the degree n extension $\mathrm{GF}(q^n)$ of the finite field $F = \mathrm{GF}(q)$. Additively too, the extension E, viewed as an FG-module is cyclic and a generator is called a *free element of E over F*. (Here G, a cyclic group generated by σ, say, is the Galois group of E over F.) The classical form of this statement – the *normal basis theorem* – is that E

Mathematics Subject Classification: 11T24, 11T30.
Key words and phrases: Gauss sum, finite field, primitive element, free element, normal basis.

contains an element w whose conjugates $\{w, w^q, \ldots, w^{q^{n-1}}\}$ constitute an F-basis of E: w is then free over F.

The terms *primitive* and *free* are correspondingly applied to the minimal polynomials M_w over F of appropriate elements w of E. Thus, a monic irreducible polynomial M of degree n over F is *primitive* if and only if it has (multiplicative) order $q^n - 1$: this means that $m = q^n - 1$ is minimal such that $M(x)$ divides $x^m - 1$. Further, M is free over F if and only if its roots constitute an F-basis of E. An equivalent formulation is that the (additive) F-order of M (necessarily a divisor of $x^n - 1$) is $x^n - 1$ itself. This means that, if $g(x)$ is a monic divisor of $x^n - 1$ over F such that M divides g^σ (the polynomial obtained from g by replacing x^i by x^{q^i}, $i \geq 0$), then $g(x) = x^n - 1$.

The distribution of elements of E that are both primitive and free over F can be expressed in terms of Gauss sums over E. Thus, Lenstra and Schoof [LeSc] (completing work of Davenport [Da] and Carlitz [Ca]) proved the existence of such elements for every pair (q, n). This result has recently been strengthened by Cohen and Hachenberger in two directions. In [CoHa1] it was shown that the primitive and free element w may have an arbitrary specified non-zero (E, F)-trace a in F, i.e., $\mathrm{Tr}_{E,F}(w) := \sum_{i=0}^{n-1} w^{q^i} = a$. (This established a conjecture of Morgan and Mullen [MoMu].) Further, in [CoHa2], it was shown that, given an arbitrary primitive element b of F, there exists a primitive element w of E, free over F, such that w has (E, F)-norm b, i.e., $\mathrm{N}_{E,F}(w) := \prod_{i=0}^{n-1} w^{q^i} = w^{\frac{q^n-1}{q-1}} = b$. Succinctly, these conclusions are that every pair (q, n) is both a PFT-pair and a PFN-pair.

Also introduced in [CoHa2] was the PFNT-problem that combines the requirements of the PFT- and PFN-problems featured above.

Problem PFNT. *Given a finite extension E/F of Galois fields, a primitive element b in F, and a non-zero element a in F, does there exist a primitive element w in E, free over F, whose (E, F)-norm and trace equal b and a, respectively?*

If so for each pair (a, b), then the pair (q, n) corresponding to E/F is called a PFNT-pair.

Note that, since for $n \leq 2$, w is prescribed by its trace and norm, we may suppose $n \geq 3$ for the PFNT-problem to be meaningful. Not only would a solution of the PFNT-problem be highly desirable in itself, it would also have significant implications for the construction of *universal generators* of closures of Galois fields, see [Ha2].

In [CoHa2], drawing on more widely applicable estimates based on Gauss sums from [Ha2] (whose proofs were therefore omitted in [CoHa2]), it was shown that, for $n \geq 9$, every pair (q, n) is a PFNT-pair: indeed, whenever $n \geq 7$, every pair, aside from at most 8 exceptions, is a PFNT-pair. The purpose of this paper is to refine radically the Gauss sum formulation of the PFNT-problem, employing Gauss sums both over E and over F, so that it becomes applicable whenever $n \geq 4$ (see Section 2), and to use sieving techniques (described in Section 3) to provide a complete theoretical solution for $n \geq 5$ (in Section 4). The innovative part of the sieve is that its thrust here is in regard to sifting in respect of additive orders; sieving with respect to multiplicative order has become already an established technique, see [Co1], [Co2], for example. We prove the following result.

Theorem 1.1. *Let q be a prime power and $n \geq 5$ an integer. Then (q, n) is a PFNT-pair.*

The PFNT-problem for $n = 4$ is soluble, in principle, by the same method. Nevertheless the details would be delicate for smaller values of q and direct verification in E is likely to be necessary in some cases. We exclude this case in order to focus here on the theoretical principles of the method. The estimates fail altogether when $n = 3$, and it may be impractical to expect progress on the PFNT-problem in this instance.

Finally, we observe that an affirmative solution of the PFNT-problem for (q, n) is equivalent to demonstrating the existence, for each $a, b \in F$ (as in its statement), of a primitive free polynomial $M(x) = x^n + M_{n-1}x^{n-1} + \cdots + M_0$ with $M_{n-1} = -a$, $M_0 = (-1)^n b$. In particular, Theorem 1.1 implies the solution of a case of a conjecture of Hansen and Mullen [HaMu] as follows.

Corollary 1.2. *Let q be a prime power and $n \geq 5$ an integer. Then, for any non-zero M_1 in $\mathrm{GF}(q)$, there exists a primitive free polynomial $x^n + M_{n-1}x^{n-1} + \cdots + M_1 x + M_0$ over $\mathrm{GF}(q)$.*

To derive Corollary 1.2 from Theorem 1.1, simply consider the monic form $M_0 x^n M(1/x)$ of the reciprocal polynomial of a primitive (free) polynomial postulated by the theorem. By a natural variation (simplification) of the method the same result holds with $M_1 = 0$; the restriction to $M_1 \neq 0$ only arises through the constraint of free-ness in Theorem 1.1.

As a paper in a collection dedicated to the distinguished number-theorist Kálmán Győry, it is intended to be relatively self-contained as regards its main number-theoretical ideas. Nevertheless, we draw on some results from previous items to avoid unnecessary duplication of detail.

I gladly acknowledge the assistance of Dirk Hachenberger (Augsburg) in the preparation of this article. Indeed, this paper was intended to form part of a collaborative sequence that began with [CoHa1] and [CoHa2], but Dirk has graciously declined the status of co-author on this occasion. Nonetheless, the work has evidently benefited from discussions we have held throughout our association.

2. Character sum formulation

From now on, suppose that $F = \mathrm{GF}(q)$, $E = \mathrm{GF}(q^n)$, $n \geq 4$, and a, b in F with $a \neq 0$ and b a primitive element, are given. We reformulate this specific case of the PFNT-problem in terms of characters and ultimately Gauss sums. Many texts such as [LiNi], Chapter 5, could be consulted for the general background, and [Ha1] for that on additive orders.

Let $m = m(q, n)$ be the greatest divisor of $q^n - 1$ that is relatively prime to $q-1$. Then, indeed, m divides $\frac{q^n-1}{(q-1)\cdot\gcd(n,q-1)}$, perhaps properly. Were it already known that $w \in E$ has (E, F)-norm b, then to guarantee that w be a primitive element of E, it would suffice to show that $w = v^d$ (where $v \in E$ and $d \mid m$) implies $d = 1$; in other words, in a rather inelegant phrase, w is *not any kind of* m*th power in* E.

The additive analogue of the above is as follows. Let $M = M(q, n)$ be the monic divisor of $x^n - 1$ (over F) of maximal degree that is prime to $x - 1$. Thus, defining $p := \operatorname{char} F$ and setting $n = p^l n_0$, where p does not divide n_0, we have $M = \frac{x^n-1}{x^{p^l}-1}$, a factor of $\frac{x^n-1}{x-1}$. The *(additive)* F*-order* of $w \in E$ is the monic divisor g (over F) of $x^n - 1$ of minimal degree such that $g^\sigma(w) = 0$. For a comprehensive account of this notion, see [Ha1], but, certainly, if w has F-order g, then $w = h^\sigma(v)$ for some $v \in E$, where $h = (x^n - 1)/g$. In particular, were it already known that $w \in E$ has (non-zero) (E, F)-trace a, then, to guarantee that w be free over F, it would suffice to show that $w = h^\sigma(v)$ (where $v \in E$ and h is an F-divisor of M) implies $h = 1$, i.e., in a loose imitation of a previous phrase, w is *not any kind of Mth power in E*.

Because of the above correspondence, it is convenient to present a (partially) unified treatment of the multiplicative and additive parts. To this end, define $\mathcal{T} = \mathcal{T}(q,n)$ as the set of formal products $\{\tau = tT : t \mid m, T \mid M\}$. For $\tau = tT \in \mathcal{T}$, let $\pi(\tau) = \pi(q,n,a,b;\tau)$ be the number (conveniently scaled (multiplied) by a factor $q(q-1)$) of elements w of E such that

(i) $\mathrm{N}_{E,F}(w) = b$;

(ii) $\mathrm{Tr}_{E,F}(w) = a$;

(iii) w is not any kind of tth power in E;

(iv) w is not any kind of Tth power in E.

(We remark that the use of the scaling factor $q(q-1)$ in $\pi(\tau)$ avoids repetition of this factor in formulae. It arises because of the potential $q-1$ values of $\mathrm{N}_{E,F}(w)$ and q values of $\mathrm{Tr}_{E,F}(w)$ for $w \in E^*$.)

We shall refer to the distinct prime or irreducible factors of $\tau \in \mathcal{T}$ as its *atoms*. Their significance is that $\pi(\tau)$ depends only on the atoms of τ, i.e., on its square-free part. Of course, to ensure a solution to the PFNT-problem for given parameters q, n, a, b, we need to show that $\pi(mM)$ is positive. Nevertheless, it is useful to study more general values of $\pi(\tau)$. A further incidental comment on the definition of $\pi(q,n,a,b;mM)$ is that the prescribed restrictions on a,b (for example, that b be primitive) are crucial in limiting the order criteria (iii), (iv) above to m, M, respectively, when applied to the PFNT-problem. From this point on, these restrictions do not feature prominently and formulae for $\pi(q,n,a,b;\tau)$ could be derived more generally, although for example, when $a = 0$, they would have a somewhat different shape.

The next stage is to express the characteristic functions of the four subsets of E (or E^*) defined by each of the conditions (i)–(iv) in terms of characters (whether multiplicative or additive) on E or F.

(i) $\underline{\mathrm{N}_{E,F}(w) = b, w \in E^*}$

Let $\widehat{F^*}$ denote the group of multiplicative characters of F^*. Abbreviating $\mathrm{N}_{E,F}$ to N, we have that the characteristic function of the subset of E^* comprising elements w satisfying (i) is

$$\frac{1}{q-1}\sum_{\nu\in\widehat{F^*}} \nu\left(N(w)b^{-1}\right), \quad w \in E^*.$$

(ii) $\underline{\mathrm{Tr}_{E,F}(w) = a,\ w \in E}$

Let λ be the canonical additive character of F. Thus, for $x \in F$,

$$\lambda(x) = \exp\left(2\pi i \,\mathrm{Tr}_{F,\mathrm{GF}(p)}(x)/p\right),$$

where $p = \operatorname{char} F$. Then the characteristic function of the subset of E prescribed by (ii) is

$$\frac{1}{q}\sum_{c\in F}\lambda(c(T(w)-a)), \quad w \in E,$$

where, here, T is an abbreviation for $\mathrm{Tr}_{E,F}$.

(iii) $\underline{w \text{ is not any kind of } t\text{th power in } E,\ t \mid m,\ w \in E^*}$

For any $d \mid m$, we write η_d for a typical character in $\widehat{E^*}$ of order d. In particular, η_1 is the trivial character. Observe that, since $d \mid \frac{q^n-1}{q-1}$, then the restriction of η_d to F^* is the trivial character ν_1 of $\widehat{F^*}$. We shall use a shorthand "integral" notation for certain weighted sums; namely, for $t \mid m$, define

$$\int_{d|t} \eta_d := \sum_{d|t}\frac{\mu(d)}{\phi(d)}\sum_{(d)}\eta_d,$$

where ϕ and μ denote the functions of Euler and Möbius, respectively, and the inner sum ranges over all $\phi(d)$ characters of order d. Then, according to a formula developed from one of Vinogradov (see [Ju], Lemma 7.5.3, and [Co1]), the characteristic function for the subset described by (iii) is

$$\Theta(t)\int_{d|t}\eta_d(w), \quad w \in E^*,$$

where $\Theta(t) := \phi(t)/t = \prod_{l|t}(1-l^{-1})$, the product running over all prime divisors of t.

At this point we append the following related material for later use. Any character $\nu \in \widehat{F^*}$ can be lifted to a character $\tilde\nu \in \widehat{E^*}$ by defining $\tilde\nu(w) = \nu(N(w))$, $w \in E$. We may then restrict $\tilde\nu$ to F^* to obtain ν^* in $\widehat{F^*}$. It need not be that $\nu = \nu^*$: indeed, if ν has order e (a divisor of $q-1$), then ν^* has order $\frac{e}{\gcd(e,n)}$. In particular, $\nu^* = \nu_1$ if and only if the order of ν divides n.

(iv) w is not any kind of Tth power in E, $T \mid M$, $w \in E$

Let χ be the canonical additive character on E: it is just the lift of λ to E, i.e., $\chi(w) = \lambda(T(w))$, $w \in E$. For any (monic) F-divisor D of M, a typical character χ_D of order D is one such that $\chi_D \circ D^\sigma$ is the trivial character in E, and D is minimal (in respect of degree) with this property. Further, let Δ_D be the subset of $\delta \in E$ such that χ_δ has F-order D if and only if $\delta \in \Delta_D$, where $\chi_\delta(w) := \chi(\delta w)$, $w \in E$. (Here we are using the assumption that $D \mid M$, a divisor of $x^n - 1$; if this did not hold, some adjustments would be necessary.) Thus, we may also write χ_{δ_D} for χ_D, where δ_D is some element of Δ_D; moreover $\{\chi_{\delta_D}, \delta_D \in \Delta_D\}$ is the set of all characters of order D. Note that Δ_D is invariant under multiplication by F^*, and that, if $D = 1$, then $\delta_1 = 0$ and $\chi_D = \chi_0$, the trivial character. There are, in fact, $\Phi(D)$ characters χ_D, where Φ is the Euler function on $F[x]$: the latter is multiplicative and is given by the formula $\Phi(D) = |D| \prod_{P|D}(1 - |P|^{-1})$, where the product is over all monic irreducible F-divisors of D and $|D| = q^{\deg(D)}$.

In analogy to (iii), for $T \mid M$, define

$$\int\limits_{D|T} \chi_{\delta_D} := \sum_{D|T} \frac{\mu(D)}{\Phi(D)} \sum_{(\delta_D)} \chi_{\delta_D},$$

where μ is the Möbius function on $F[x]$ and the inner sum runs over all $\Phi(D)$ elements δ_D of Δ_D. Then the characteristic function of the subset of E described by (iv) is

$$\Theta(T) \int\limits_{D|T} \chi_{\delta_D}(w), \quad w \in E,$$

where $\Theta(T) := \Phi(T)/|T|$.

For later use, note that, because M and $x - 1$ are co-prime, then, for any divisor D ($\neq 1$) of T, Δ_D has empty intersection with F.

Using the above characteristic functions, we derive an expression for $\pi(\tau)$ in terms of Gauss sums on E and F.

For any $\eta \in \widehat{E^*}$, set

$$G_n(\eta) := \sum_{w \in E} \chi(w)\eta(w)$$

with the convention that $\eta_1(0) = 1$, but $\eta(0) = 0$ for $\eta \neq \eta_1$. Similarly, the Gauss sum over F corresponding to $\nu \in \widehat{F^*}$ is denoted by $G_1(\nu)$. The key fact is that $|G_1(\nu)| = \sqrt{q}$ for $\nu \neq \nu_1$, and hence $|G_n(\eta)| = q^{\frac{n}{2}}$ for $\eta \neq \eta_1$. Of course, $G_1(\eta_1) = G_n(\eta_1) = 0$.

In the theorem which follows we establish a new type of formula for $\pi(\tau)$ that combines products of Gauss sums over E and over F. In its statement we draw on notation introduced above, though some summations will be modified as indicated. For example, $\sum_{\nu \in \widehat{F^*}, \nu^* \neq \nu_1}$ means that the sum will be restricted to characters ν for which ν^* (defined in (iii)) is non-trivial: there are $q - 1 - e$ such characters, where $e = \gcd(n, q-1)$. We shall also use bars over symbols to denote complex conjugation.

Theorem 2.1. *Let the prime power q, the integer n (≥ 4) and elements $a \in F^*$ and b, a primitive element of F, be given. Then, for any $\tau = tT \in \mathcal{T}$, where $t \mid m$ and $T \mid M$, we have*

$$\pi(\tau) = \Theta(\tau) \cdot (q^n + A + B - C)\,, \tag{2.1}$$

where

$$A = \int_{d|t} \int_{D|T} \sum_{\substack{\nu \in \widehat{F^*} \\ \nu^* \neq \nu_1}} \nu^*(a)\overline{\nu}(b)\overline{(\eta_d\tilde{\nu})}(\delta_D + 1)\overline{G_1}(\nu^*)G_n(\eta_d\tilde{\nu}),$$

$$B = \int_{d|t} \int_{\substack{D|T \\ D\neq 1}} \sum_{\substack{\nu \in \widehat{F^*} \\ \nu^* = \nu_1,\, \eta_d\tilde{\nu} \neq \eta_1}} \overline{\nu}(b) \left(\overline{(\eta_d\tilde{\nu})}(\delta_D) - \overline{(\eta_d\tilde{\nu})}(\delta_D + 1)\right) G_n(\eta_d\tilde{\nu}),$$

$$C = \int_{d|t} \sum_{\substack{\nu \in \widehat{F^*} \\ \nu^* = \nu_1,\, \eta_d\tilde{\nu} \neq \eta_1}} \overline{\nu}(b)G_n(\eta_d\tilde{\nu}),$$

and where Θ is extended to $\mathcal{T}$ by multiplicativity.

Proof. From the characteristic functions (i)–(iv), taking into account the scaling factor $q(q-1)$, we have

$$\pi(\tau) = \Theta(\tau) \int_{d|t} \int_{D|T} \sum_{\nu \in \widehat{F^*}} \sum_{c \in F} \overline{\nu}(b)\overline{\lambda}(ac) \sum_{w \in E} (\eta_d\tilde{\nu})(w)\chi((\delta_D + c)w). \tag{2.2}$$

To see this, recall that $\tilde{\nu}(w) = \nu(N(w))$ and $\chi(cw) = \lambda(cT(w))$. Moreover, because the characteristic function under (ii) scores 0 when $w = 0$, it is safe to extend the definition of the characteristic functions under (i) and (iii) to $w = 0$, using our conventions on the values of $\nu(0)$ and $\eta_d(0)$.

Accordingly, the contribution to the right side of (2.2) of the terms with $d = 1$ and $\nu = \nu_1$, or $D = 1$ ($\delta_D = 0$) and $c = 0$ (or both) is simply $\Theta(\tau)q^n$. (Note, in particular, that $\delta_D + c = 0$ implies $D = 1$ and $c = 0$.)

Next, the contribution of the terms in (2.2) with $c = 0$ and $D \neq 1$ ($\delta_D \neq 0$), on replacing w by w/δ_D, yields

$$\Theta(\tau) \int\limits_{d|t} \sum_{\substack{\nu \in \widehat{F^*} \\ \eta_d\tilde{\nu} \neq \eta_1}} \overline{\nu}(b) G_n(\eta_d\tilde{\nu}) \int\limits_{\substack{D|T \\ D\neq 1}} (\overline{\eta_d\tilde{\nu}})(\delta_D).$$

Now, $F^*\Delta_D = \Delta_D$ and η_d is trivial on F^*. Hence the inner sum

$$\begin{aligned}
\int\limits_{\substack{D|T \\ D\neq 1}} (\overline{\eta_d\tilde{\nu}})(\delta_D) &= \frac{1}{q-1} \int\limits_{\substack{D|T \\ D\neq 1}} \sum_{c\in F^*} (\overline{\eta_d\tilde{\nu}})(c\delta_D) \\
&= \frac{1}{q-1} \int\limits_{\substack{D|T \\ D\neq 1}} (\overline{\eta_d\tilde{\nu}})(\delta_D) \sum_{c\in F^*} \nu^*(c) = 0,
\end{aligned}$$

unless $\nu^* = \nu_1$. Consequently, the terms under consideration yield the first part of the term B in (2.1), i.e., the part involving $\overline{\eta_d\tilde{\nu}}(\delta_D)$. Again, since $\Delta_D = c\Delta_D$ for $c \in F^*$, when $c \neq 0$, we may replace δ_D in (2.2) by $c\delta_D$ and then w by $w/(c(\delta_D + 1))$. As $\eta_d(c) = 1$, the contribution of the remaining terms is therefore

$$\Theta(\tau) \int\limits_{d|t} \int\limits_{D|T} \sum_{\substack{\nu \in \widehat{F^*} \\ \eta_d\tilde{\nu} \neq \eta_1}} \overline{\nu}(b) \overline{(\eta_d\tilde{\nu})}(\delta_D + 1) G_n(\eta_d\tilde{\nu}) \sum_{c\in F^*} \overline{\lambda}(ac)\overline{\nu}^*(ac).$$

The latter is equal to $\Theta(\tau)(A - Y)$, where A is as in (2.1) and

$$Y = \int\limits_{d|t} \int\limits_{D|T} \sum_{\substack{\nu \in \widehat{F^*} \\ \nu^* = \nu_1,\, \eta_d\tilde{\nu} \neq \eta_1}} \overline{\nu}(b) \overline{(\eta_d\tilde{\nu})}(\delta_D + 1) G_n(\eta_d\tilde{\nu}).$$

The expression for Y yields (through those terms with $D \neq 1$) the balance of the part B in (2.1) as well as the part C (through the terms with $D = 1$). $\square$

From Theorem 2.1, we derive a lower bound for $\pi(\tau)$. We write $W(\tau) = W(t)W(T) = 2^{\omega(\tau)}$ for the number of square-free divisors of τ, where ω counts the atoms in τ. Note that $W(T) \leq 2^{n-1}$.

Corollary 2.2. *Under the conditions of* Theorem 2.1, *we have*

$$\pi(\tau) \geq \Theta(\tau)\left(q^n - (q-1-e)W(\tau)q^{\frac{n+1}{2}} - (eW(t)-1)(2W(T)-1)q^{\frac{n}{2}}\right),$$

where $e = \gcd(n, q-1)$.

Corollary 2.3. *Under the conditions of* Theorem 2.1, $\pi(\tau)$ *is positive whenever*

$$q^{\frac{n-3}{2}} > \left(1 - \frac{e+1}{q}\right)W(\tau) + \frac{1}{q^{3/2}}(eW(t)-1)(2W(T)-1), \tag{2.3}$$

and so certainly whenever

$$q^{\frac{n-3}{2}} > \left(1 - \frac{1}{q}\right)W(\tau), \quad q \geq 4. \tag{2.4}$$

For the case in which $\tau = mM$, Corollary 2.3 represents an improvement by a factor of approximately $\sqrt{q}$ over the criterion in [CoHa2].

3. Sieving inequalities

To establish Theorem 1.1 for arbitrary large values of q and n, it is necessary first to employ Corollary 2.3 (or a weaker variant) with $\tau = mM$. With the aid of some supplementary facts (such as Lemma 3.3, below), the theorem was thereby justified in [CoHa2] for $n \geq 7$, save for a few exceptional values of q when $n = 7$ or 8. But for smaller values of n, it is hopeless to contemplate a complete proof solely by these means. To overcome the considerable obstacles in these cases, we have devised a sieving process. (Actually, use of this device would have reduced the effort of [CoHa2].)

Let $\tau = tT \in \mathcal{T}$. Given $r \geq 1$, divisors $\tau_1 = m_1 M_1, \ldots, \tau_r = m_r M_r$[1] of τ will be called *complementary divisors* of τ with common divisor τ_0, if the atoms (i.e., distinct primes and irreducibles) in $\operatorname{lcm}\{\tau_1, \ldots, \tau_r\}$ are precisely those in τ and, for any distinct pair (i, j), the atoms of $\gcd(\tau_i, \tau_j)$ are precisely those of τ_0. (The point is that the value of $\pi(\tau)$ depends only on the atoms of τ.) When $r = 1$, take $\tau_1 = \tau_0 = \tau$ and recover the situation of Section 2.

The novel feature of the basic sieving inequality which follows is its applicability with $M_1, \ldots, M_r$ proper divisors of M, i.e., to the component relating to F-order, cf. [Co2].

Theorem 3.1. *Let $\tau_1, \ldots, \tau_r$ be complementary divisors of $\tau \in \mathcal{T}$ with common divisor τ_0. Then*

$$\pi(\tau) \geq \left(\sum_{i=1}^{r} \pi(\tau_i) \right) - (r-1)\pi(\tau_0).$$

Proof. When $r = 1$, the result is trivial. For $r = 2$, denote the set of elements of E^* that satisfy (i)–(iv) of Section 2 by $\mathcal{A}_\tau$, where $\tau = tT$, etc. Then

$$\mathcal{A}_{\tau_1} \cup \mathcal{A}_{\tau_2} \subseteq \mathcal{A}_{\tau_0}, \quad \mathcal{A}_{\tau_1} \cap \mathcal{A}_{\tau_2} = \mathcal{A}_\tau,$$

and the inequality holds by consideration of cardinalities. For $r \geq 2$, use induction on r. Write $\tau' = \tau_2 \ldots \tau_r$, apply the result for $r = 2$ to τ, τ', and then apply the induction hypothesis to τ'. The result follows. $\square$

To state an inequality extending Corollary 2.3, we require the definition of a crucial parameter: it is a generalization of the quantity $\Theta(\tau)$. Given complementary divisors $\tau_1, \ldots, \tau_r$ of τ with common divisor τ_0, set

$$\Theta = \Theta(\tau_1, \ldots, \tau_r) := \left(\sum_{i=1}^{r} \Theta(\tau_i) \right) - (r-1)\Theta(\tau_0).$$

To illustrate, suppose that $q \equiv 1 \pmod{n}$ (so that p does not divide n). Thus $M = \frac{x^n - 1}{x - 1} = M_1 \ldots . M_{n-1}$, a product of $n - 1$ distinct linear factors over F. Then, for the indicated set of complementary divisors with common divisor m,

$$\Theta(mM_1, \ldots, mM_{n-1}) = \Theta(m)\left(1 - \frac{n-1}{q}\right), \tag{3.1}$$

[1]We use $m_1, M_1, \ldots$ rather than $t_1, T_1, \ldots$ because in all applications we will have $\tau = mM$, where m, M are as in Section 2.

whereas, for another set with common divisor 1,

$$\Theta(M_1,\dots,M_{n-1},m)=\Theta(m)-\frac{n-1}{q}. \tag{3.2}$$

To be useful in a given situation it is essential that Θ is positive. Indeed, the ratio $\Theta/\Theta(\tau_0)$, which we will denote by Θ_0, should not be too small.

Theorem 3.2. *Assume that q is a prime power and n (≥ 4) is an integer, and that a in F^* and b, a primitive element of F, are given. Suppose that $\tau_1=m_1M_1,\dots,\tau_r=m_rM_r$ are complementary divisors of $\tau=mM$ with common divisor $\tau_0=m_0M_0$. Suppose also that $\Theta:=\Theta(\tau_1,\dots,\tau_r)$ is positive. Then $\pi(\tau)$ is positive whenever*

$$q^{\frac{n-3}{2}}\geq R-S+\Theta^{-1}\sum_{i=1}^{r}\Theta(\tau_i)(U_i-V_i), \tag{3.3}$$

where, with $e=\gcd(n,q-1)$,

$$R=\left(1-\frac{e+1}{q}+\frac{2e}{q^{3/2}}\right)W(\tau_0),$$

$$S=\frac{1}{q^{3/2}}\left(eW(m_0)+2W(M_0)-1\right),$$

$$U_i=\left(1-\frac{e+1}{q}+\frac{2e}{q^{3/2}}\right)(W(\tau_i)-W(\tau_0)),$$

$$V_i=\frac{1}{q^{3/2}}\left(e(W(m_i)-W(m_0))+2(W(M_i)-W(M_0))\right).$$

In particular, it suffices that

$$q^{\frac{n-3}{2}}>\left(1-\frac{1}{q}\right)\left(W(\tau_0)+\Theta^{-1}\sum_{i=1}^{r}\Theta(\tau_i)(W(\tau_i)-W(\tau_0))\right),\quad q\geq 4. \tag{3.4}$$

Proof. From Theorems 3.1 and 2.1,

$$\pi(\tau)\geq\Theta_0\pi(\tau_0)+\sum_{i=1}^{r}\Theta(\tau_i)S_i,$$

where S_i is equal to

$$\int_{d|m_i}\int_{\substack{D|M_i\\ dD\nmid\tau_0}}\sum_{\substack{\nu\in\widehat{F^*}\\ \nu^*\neq\nu_1}} A_i+\int_{d|m_i}\int_{\substack{D|M_i\\ dD\nmid\tau_0,\,D\neq 1}}\sum_{\substack{\nu\in\widehat{F^*}\\ \nu^*=\nu_1,\,\eta_d\tilde{\nu}\neq\eta_1}} B_i-\int_{\substack{d|m_i\\ d\nmid m_0}}\sum_{\substack{\nu\in\widehat{F^*}\\ \nu^*=\nu_1,\eta_d\tilde{\nu}\neq\eta_1}} C_i,$$

with A_i, B_i and C_i being as in the corresponding expressions in (2.1). The bound (3.3) now follows by applying Corollary 2.3 to $\pi(\tau_0)$ and similar estimates used in its derivation for the remaining terms. As at (2.4), (3.4) follows since $\frac{e}{\sqrt{q}}\leq 2e$ for $q\geq 4$. □

In this paper, two types of complementary divisors suffice for the most part. (But note that for the case of $n=4$, greater ingenuity in the selection of complementary divisors will be required and therefore the flexibility offered by these detailed results will be useful.) Given that we may assume $n\leq 8$, the first use of Theorem 3.2 will be to sieve wholly on the additive part (i.e., with $\tau_0=m$) to deal with large values of q. For smaller values of q, we generally take the atoms of τ as complementary divisors. In the former of these applications, the inequality (3.4) takes the form

$$q^{\frac{n-3}{2}}>Q_M W(m), \tag{3.5}$$

where $Q_M=Q_M(q)$, a rational function of q, converges rapidly to $\omega(M)+1$. The following illustration serves as a model.

Corollary 3.3. *Under the assumption of* Theorem 3.2*, suppose that* $q\equiv 1 \pmod n$*, so that* $M=M_1\dots M_{n-1}$*, a product of linear factors over* F*. Then* $\pi(mM)$ *is positive whenever* (3.5) *holds, where*

$$Q_M(q)=\frac{(q-1)(nq-2(n-1))}{q(q-n+1)}.$$

Proof. Take complementary divisors $\tau_1,\dots,\tau_{n-1}$ as in (3.1). Thus $W(\tau_i)-W(\tau_0)=W(\tau_0)=W(m)$. Hence, from (3.4) and (3.1) it suffices that

$$q^{\frac{n-3}{2}}>\left(1-\frac{1}{q}\right)\left(1+\frac{(n-1)\left(1-\frac{1}{q}\right)}{1-\frac{n-1}{q}}\right)W(m),$$

which is equivalent to the stated result. □

Note that a stronger version of Corollary 3.3 would be obtained if we used (3.3), with $e = n$, instead of (3.4). Indeed, if $q-1$ divides n, so that $e = q-1$, the main terms on the right side of (3.3) disappear, leaving only the $q^{-3/2}$-terms. This is consistent with Proposition 4.1 of [CoHa2] which reduced the PFNT-problem in this case to the PFN-problem which was solved completely in that paper.

Lemma 3.4. *Let q be a prime power and n a positive integer. Assume that $q-1$ divides n. Then (q,n) is a PFNT-pair.*

For example, Lemma 3.4 applies whenever $q = 2$ or when $q = 3$ and n is even. One further simplification is the following.

Lemma 3.5. *Suppose that, for a given pair (q,n), M is irreducible. Then $\pi(mM)$ is positive if and only if $\pi(m)$ is positive.*

Proof. If w (with the prescribed non-zero trace and norm) is not any kind of mth power, then $w \notin F$. In particular, it does not have F-order $x-1$ and so must be free. $\square$

4. Proof Theorem 1.1

We deal mainly with the cases $n = 5, 6$. After that, it will be seen that further cases ($n = 7, 8, \dots$) are a formality. For a given pair (q,n) let ω or ω_q denote $\omega(m)$. We can suppose that $q > 2$: indeed $q > 3$ if n is even.

As a preliminary to a case by case discussion when $n = 5$, note that $m \mid \frac{q^5-1}{q-1}$ and the latter is divisible by 5 if and only if $q \equiv 1 \pmod 5$: even then $5 \nmid m$. Hence, in every case, all primes that are candidates to be factors of m lie in the set $\mathcal{S}_5 = \{11, 31, 41, 61, 71, 101, \dots\}$ comprising primes $l \equiv 1 \pmod{10}$. Denote by P_r ($r = 1, 2, \dots$) the product of the first r primes in $\mathcal{S}_5$.

(i) $\underline{n = 5,\ q \equiv 1 \pmod 5}$

Since $m \le \frac{q^5-1}{5(q-1)}$, then $q > (5m)^{1/4} - 1 \ge (5P_\omega)^{1/4} - 1 =: R_\omega$, say. Now, Corollary 3.3 (in this situation) offers the sufficient condition

$$q > 2^\omega Q_M(q), \tag{4.1}$$

where $Q_M(q) = \frac{(q-1)(5q-8)}{q(q-4)}$, a function which decreases to 5 (being less than 5.1 for $q \geq 81$, say). Thus, it suffices to show that

$$R_\omega > 2^\omega Q_M(q), \quad q \geq R_\omega. \tag{4.2}$$

As ω increases it is evident that, because further primes taken into R_ω exceed $2^4 = 16$, the function $R_\omega/(2^\omega Q_M(R_\omega))$ is increasing. Hence, if (4.2) is established for $\omega = \omega_0$, say, it will hold for $\omega \geq \omega_0$.

Now, $R_6 > 417 > 322 > 64Q_M(417)$ and hence (4.1) holds whenever $\omega \geq 6$. Next, $R_5 > 130$. On the other hand, $32Q_M(165) < 162$, so that (4.1) holds when $\omega = 5$, unless $131 \leq q < 165$. There are, however, no prime powers q in this range with $\omega_q = 5$. The story is similar for $\omega = 4$. For $\omega = 3$, $R_\omega > 15$, so that $q \geq 16$. (Indeed, $m(16,5) = (P_3^5 - 1)/(5(P_3 - 1))$, the minimal theoretical value.) We have $8Q_5(43) < 42$, so that $16 \leq q \leq 43$ but there are no further relevant prime powers in this range.

For $q = 16$, $m = 11 \cdot 31 \cdot 41$, so that $\omega(mM) = 7$ and we take atomic complementary divisors, i.e., $M_1, \dots, M_4, 11, 31, 41$. This gives $\Theta_0 := \Theta/\Theta(m) = 4(1 - \frac{1}{16}) + \frac{10}{11} + \frac{30}{31} + \frac{40}{41} - 6 = 0.6024\dots$. Thus, using the abbreviation $RS_{(3.4)}$ to denote the right side of (3.4), we have

$$RS_{(3.4)} \leq \frac{15}{16} \cdot \left(1 + \Theta_0^{-1}(\Theta_0 + 6)\right) < 11.3 < q.$$

Hence, (3.4) is satisfied.

The only prime power that remains to be dealt with is $q = 11$, in which case m is prime. We use complementary divisors with common divisor m (as in Corollary 3.3) but in respect of the inequality (3.3) with $e = 5$. We have $\Theta_0 = \frac{7}{11}$ and

$$RS_{(3.3)} = \frac{10}{11} + \frac{9}{11^{3/2}} + \Theta_0^{-1}\left(4 \cdot \frac{10}{11} \cdot \left(\frac{10}{11} + \frac{18}{11^{3/2}}\right)\right) < 9.2 < q.$$

Thus the result holds in this case.

(ii) $\underline{n = 5,\ q \equiv -1 \pmod 5}$

Now $M = M_1 M_2$, where M_1, M_2 are irreducible quadratic polynomials. Hence, in Corollary 3.3 we have $\Theta_0 = 1 - \frac{2}{q^2}$ and $Q_M(q) = \frac{(q-1)(3q^2-4)}{q(q^2-2)} < 3$. Indeed, we may take $Q_M = 3$ in (3.5). Since $m \leq (q^5 - 1)/(q - 1)$, we redefine $R_\omega := P_\omega^{1/4} - 1$ and then $q > R_\omega$. Now, $R_6 > 278 > 192 \geq 64Q_M$, and hence the result holds for $\omega \geq 6$. For $\omega = 3, 4, 5$ there are no relevant prime powers between R_ω and $3 \cdot 2^\omega$. Further, since $4Q_M(11) < 11$, only the prime powers $q = 4, 9$ remain: these have $\omega_q = 2$ and we take atomic complementary divisors. For $q = 4$, these are M_1, M_2, 11, 31 so that $\Theta = 2 \cdot \frac{15}{16} + \frac{10}{11} + \frac{30}{31} - 3 = 0.7518\ldots$. Then, in (3.3), $e = 1$ and

$$RS_{(3.3)} = \frac{7}{8} + \Theta^{-1}\left(2 \cdot \frac{1}{2} \cdot \frac{9}{10} + \frac{7}{8}\left(\frac{10}{11} + \frac{30}{31}\right)\right) < 3.89 < q.$$

For $q = 9$, $m = 11 \cdot 671$, $\Theta_0 = 0.8829\ldots$, and

$$RS_{(3.4)} = \frac{8}{9}\left(1 + \Theta^{-1}(3 + \Theta_0)\right) < 4.8 < q.$$

Thus a sufficient condition is satisfied in every case.

(iii) $\underline{n = 5,\ q \equiv \pm 2 \pmod 5 \text{ or } q \text{ a power of } 5}$

If $q \equiv \pm 2 \pmod 5$, then M is an irreducible quartic, so that, by Lemma 3.5 it suffices to show that $\pi(1)$ is positive. Since $M = 1$ when q is a power of 5, the same conclusion can be drawn in that case, too. Hence, for $q \geq 4$, by (2.4) it suffices to show that

$$q > \left(1 - \frac{1}{q}\right) W(m).$$

This inequality easily holds by the method of (i), (ii) for $\omega \geq 3$ or $q \geq 13$ (since R_3 (defined as in (ii)) exceeds 9). It also holds for $q = 5, 7, 8$, since $\omega_q \leq 2$ for these. Finally, for $q = 3$, $\omega_3 = 1$, and with $\tau = m$, $RS_{(2.3)} = \frac{2}{3} + \frac{1}{3^{3/2}} < 0.86 < q$.

We now suppose $n = 6$. Here, the extra $\sqrt{q}$ that appears on the left sides of (3.3) and (3.4) is offset by the fact that any odd prime is a candidate for a factor of m. For example, 3 is always a factor if $q \equiv 2 \pmod 3$. As m is a divisor of $(q+1)(q^2+q+1)(q^2-q+1)$ and the primes l (> 3) dividing the quadratic factors have $l \equiv 1 \pmod 6$, such primes must predominate the factorisation of m. Nevertheless, we do not exploit this fact here, but simply take $\mathcal{S}_6$ to be the set of odd primes, possibly omitting 3 (depending on the case). By Lemma 3.4 we may assume $q > 4$.

(iv) $\underline{n = 6,\ q \equiv 1 \pmod 6}$

We follow case (i). Since 3 does not divide m, the prime 3 can be excluded from $\mathcal{S}_6$ and we let P_r be the product of the first r odd primes (> 3). Moreover, $m \le \frac{q^6-1}{6(q-1)}$, and hence $q > (6m)^{1/5} - 1 \ge (6P_\omega)^{1/5} - 1 =: R_\omega$. Thus, by Corollary 2.5 with $Q_M(q) = \frac{2(q-1)(3q-5)}{q(q-5)} < 6$, it suffices to show specifically that

$$q^{\frac{3}{2}} > 6 \cdot 2^\omega, \tag{4.3}$$

or, more generally, that

$$R_\omega^{\frac{3}{2}} > 6 \cdot 2^\omega. \tag{4.4}$$

Now, $R_{10} > 374$ and $R_{10}^{3/2} > 7234 > 6144 = 6 \cdot 2^{10}$. Hence, (4.4) holds for $\omega \ge 10$ or $q > 374$. In fact, for $q < 374$, $\omega_q \le 6$. For $\omega = 6, 5, 4$, the values of q for which $R_\omega^{3/2} < q^{3/2} < 6 \cdot 2^\omega$ (so that (4.3) would fail) lie in the intervals $[25, 53]$, $[13, 34]$, $[7, 21]$, respectively. Yet, these intervals contain no relevant prime powers. For $\omega \le 3$, there remains $q = 7$ or 13. But $(7, 6)$ is a PFNT-pair by Lemma 3.4. For $q = 13$, use the complementary divisors of Corollary 3.3 (so that $\Theta_0 = 8/13$) but employ (3.3) with $e = 6$. Then

$$RS_{(3.3)} = 8 \cdot \left(\frac{6}{13} + \frac{5}{13^{3/2}}\right) + \Theta_0^{-1}\left(5 \cdot \frac{12}{13} \cdot \left(\frac{48}{13} + \frac{94}{13^{3/2}}\right)\right) < 24.7,$$

which is less than $q^{3/2} = 48.8\ldots$ and so the result holds in every case.

(v) $\underline{n = 6,\ q \equiv -1 \pmod 6}$

Now, $M = M_1 M_2 M_3$, where $M_1 = x + 1$ and M_2, M_3 are irreducible quadratics. Hence, in the analogue of Corollary 3.3, we have $\Theta_0 = 1 - \frac{1}{q} + \frac{2}{q^2}$ and (3.5) holds with $Q_M(q) = \frac{(3q+2)(q-1)^2}{q(q-2)(q+2)} < 3$. This time 3 is always a factor of m so that certainly $3 \in \mathcal{S}_6$ and we define $R_\omega := P_\omega^{1/3} - 1$. In like fashion to case (ii) (say) above, we find that (3.5) holds whenever $\omega \ge 11$ or $q > 374$. For lesser values of q, the maximum value of ω_q is 7. For $\omega = 7, 6$ or 5, there are no relevant prime powers in the range $R_\omega^{3/2} < q^{3/2} < 3 \cdot 2^\omega$ (cf. case (iv)). For $\omega \le 4$, by (3.5), we can assume $q < (48)^{2/3} < 14$, which implies $q = 5$ or 11. For $q = 11$, use the atomic complementary divisors

M_1, M_2, M_3, 3, 7, 19, 37. Then $\Theta = \frac{10}{11} + 2 \cdot \frac{120}{121} + \frac{2}{3} + \frac{6}{7} + \frac{18}{19} + \frac{36}{37} = 0.3367$ and

$$RS_{(3.4)} = \frac{10}{11}\left(1 + \Theta^{-1}(\Theta + 6)\right) < 18.1 < q^{3/2}.$$

For $q = 5$, $m = 3^2 \cdot 7 \cdot 31$, more care is needed. Take complementary divisors $3M_1$, $3M_2$, $3M_3$, $3 \cdot 7$ and $3 \cdot 31$ with common divisor $\tau_0 = 3$. Then $\Theta_0 = \Theta/\Theta(\tau_0) = \frac{4}{5} + 2 \cdot \frac{24}{25} + \frac{6}{7} + \frac{30}{31} - 4 = 0.54488\ldots$. Note that for each complementary divisor τ_i, $W(\tau_i) - W(\tau_0) = W(\tau_0) = 2$. Then, $e = 1$ in (3.3), and

$$RS_{(3.3)} = \frac{4}{5} + \frac{3}{5^{3/2}} + \Theta_0^{-1}\left(\left(\frac{4}{5} + \frac{4}{5^{3/2}}\right)\left(3 - \frac{1}{5} - \frac{2}{5^2} + \frac{6}{7} + \frac{30}{31}\right)\right).$$

Thus, $RS_{(3.3)} < 10.6 < q^{3/2} = 11.18\ldots$ and the result holds in every case.

(vi) $\underline{n = 6,\ q \text{ a power of } 3,\ q \geq 9}$

Now, M has a single irreducible factor $x + 1$, and, by Corollary 2.3, it suffices to show that

$$q^{3/2} > \left(1 - \frac{1}{q}\right) W(m). \tag{4.5}$$

In this case, 3 is not a member of $\mathcal{S}_6$ and $m \leq \frac{q^6-1}{2(q-1)}$, so that $q > (2P_\omega)^{1/5} - 1 =: R_\omega$. The method used in previous cases quickly yields the result whenever $\omega_q \geq 6$ or $q > R_6 > 19$. This leaves only $q = 9$, in which case (4.5) holds because $\omega_q = 4$.

(vii) $\underline{n = 6,\ q = 2^s,\ s \geq 3}$

Here $M = (x^2 + x + 1)^2$, so that M has a simple irreducible factor, if s is odd, and a pair of distinct linear factors, if s is even. (From Lemma 3.4 comes the restriction to $s \geq 3$.)

Suppose s is odd. Then, by Corollary 2.3, it suffices to satisfy (4.5). Since $3 \mid m$, then $3 \in \mathcal{S}_6$ and $q > R_\omega := P_\omega^{1/5} - 1$. As in case (vi), the result holds whenever $\omega_q \geq 7$ and $q > R_7 > 20$ (which implies $q \geq 32$) or $\omega_q \leq 6$ and $q > R_6 > 10$. This leaves only $q = 8$. But $\omega_8 = 3$ and therefore (4.5) holds in this case.

Suppose s is even. Then 3 does not divide m and $q > R_\omega := (3P_\omega)^{1/5} - 1$. We have to satisfy (3.5) with $Q_M = \frac{(q-1)(3q-4)}{q(q-2)} < 3$. If $\omega \geq 10$, then $q > 261$ and (3.5) holds. Thus $\omega_{256} \leq 9$ and therefore (3.5) is satisfied for

$q = 256$. Finally, $\omega_{64} = 6$ and $\omega_{16} = 4$, so that (3.5) holds also for $q = 64$ or 16.

(viii) $\underline{n = 7 \text{ or } 8}$

For $n = 7$, only members of $\mathcal{S}_7 = \{29, 43, 71, \dots\}$ comprising primes $l \equiv 1 \pmod{14}$ are candidates to be divisors of m. Thus, it is plain that the method of the previous cases will quickly yield success and only very small values of q could be in doubt. We check only the case $q = 4$ (unsettled in Theorem 1.2 of [CoHa2]). For this, M is a product of two irreducible cubics and $m = 43 \cdot 127$. Thus, $\omega(mM) = 4$ and, with $\tau = mM$,

$$RS_{(2.4)} = \frac{48}{49} \cdot 16 < q^2 = 16;$$

therefore (4,7) is a PFNT-pair. Easily, so also is $(64, 7)$, the other pair left unsettled in [CoHa2].

Finally, when $n = 8$, although any odd prime may be a divisor of m, the power $q^{5/2}$ on the left side of (3.3) or (3.4) is decisive. Moreover, $q = 2, 3, 5$ all yield to Lemma 3.4 and $M = 1$ for $q = 4$ or 8. We therefore simply check the cases $q = 7, 13, 17$ (unsettled in [CoHa2]). From these, the other cases $q = 25, 41, 89$, unsettled in [CoHa2], will also be clear. For $q = 7, 13, 17$ we have $\omega(M) = 4, 5, 7$ and $\omega(m) = 2, 4, 4$, respectively. For $q = 7$ or 13, we have $q^{5/2} > W(mM)$ and so the result holds by (2.4). For $q = 17$, by Corollary 3.3, we have to satisfy

$$1191.5\ldots = q^{5/2} > 16 \cdot \frac{2(q-1)(4q-7)}{q(q-7)} = 183.7\ldots\ .$$

From the above and [CoHa2], the proof of Theorem 1.1 is complete. $\square$

References

[Ca] L. Carlitz, Primitive roots in a finite field, *Trans. Amer. Math. Soc.* **73** (1952), 373–382.

[Co1] S. D. Cohen, Pairs of primitive roots, *Mathematika* **32** (1985), 276–285.

[Co2] S. D. Cohen, Primitive elements and polynomials: existence results, in: Proceedings of the First International Conference on Finite Fields and Applications (Mullen, G.L. and Shiue, P.J.-S., eds.), Lecture Notes in Pure and Applied Mathematics **141**, *Dekker*, 1993, 43–55.

[CoHa1] S. D. Cohen and D. Hachenberger, Primitive normal bases with prescribed trace, *Applic. Alg. Engin. Comm. Comp.* **9** (1999), 383–403.

[CoHa2] S. D. Cohen and D. Hachenberger, Primitivity, freeness, norm and trace, *Discrete Math.* (*to appear*).

[Da] H. Davenport, Bases for finite fields, *J. London Math. Soc.* **43** (1968), 21–49.

[Ha1] D. Hachenberger, Finite fields: normal bases and completely free elements, *Kluwer Academic Publishers*, *Boston*, 1997.

[Ha2] D. Hachenberger, Universal generators for primary closures of Galois fields, (*submitted*).

[HaMu] T. Hansen and G. L. Mullen, Primitive polynomials over finite fields, *Math. Comp.* **59** (1992), 639–643.

[Ju] D. Jungnickel, Finite fields, Structure and arithmetics, *BI-Wissenschaftsverlag*, *Mannheim*, 1993.

[LeSc] H. W. Lenstra, Jr. and R. J. Schoof, Primitive normal bases for finite fields, *Math. Comp.* **48** (1987), 217–231.

[LiNi] R. Lidl and H. Niederreiter, Finite Fields, *Addison-Wesley*, *Reading, Massachusetts*, 1983; 2nd edn: *Cambridge University Press*, *Cambridge,* 1997.

[MoMu] I. H. Morgan and G. L. Mullen, Primitive normal polynomials over finite fields, *Math. Comp.* **63** (1994), 759–765.

STEPHEN D. COHEN
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF GLASGOW
GLASGOW G12 8QW
SCOTLAND

E-mail: sdc@maths.gla.ac.uk

(Received February 4, 1999; revised August 30, 1999)