ACTA ARITHMETICA
109.4 (2003)

Primitive free quartics with specified norm and trace

by

Stephen D. Cohen and Sophie Huczynska (Glasgow)

1. Introduction. Given q, a power of a prime p, denote by F the finite field $\mathrm{GF}(q)$ of order q and, for a given positive integer n, by E its extension $\mathrm{GF}(q^n)$ of degree n. A *primitive element* of E is a generator of the cyclic group E^*. Additively too, the extension E is cyclic when viewed as an FG-module, G being the Galois group of E over F, and a generator is called a *free element* of E over F. The core result linking additive and multiplicative structure—the *primitive normal basis theorem*—is that there exists $\alpha \in E$, simultaneously primitive and free over F. Existence of such an element for every extension was demonstrated by Lenstra and Schoof [9] (completing work by Carlitz ([1], [2]) and Davenport [7]). A computer-free proof of the primitive normal basis theorem is given in [6].

The result of the primitive normal basis theorem has been extended by Cohen and Hachenberger in two directions. In [4], it was shown that, given an arbitrary non-zero element $a \in F$, there exists a primitive element ω of E, free over F, such that ω has (E,F)-trace a in F, i.e. $\mathrm{Tr}_{E/F}(w) := \sum_{i=0}^{n-1} \omega^{q^i} = a$. Further, in [5] it was shown that, given an arbitrary primitive element b of F, there exists a primitive element ω of E, free over F, with (E,F)-norm b in F, i.e. $N_{E/F}(w) := \prod_{i=1}^{n-1} \omega^{q^i} = \omega^{(q^n-1)/(q-1)} = b$.

In [5], Cohen and Hachenberger posed the following question, known as the PFNT problem. (A similar description of the above problems would be as PFT, PFN respectively.)

Problem 1.1. 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*.

2000 *Mathematics Subject Classification*: Primary 11T06; Secondary 11A25, 11T24, 11T30.

In [3], Cohen showed (Theorem 1.1) that, for $n \geq 5$, every pair (q, n) is a PFNT-pair.

THEOREM 1.2. *Let q be a prime power and $n \geq 5$ an integer. Then (q, n) is a PFNT-pair.*

Note that, since w is effectively specified by its trace and norm for $n \leq 2$, we may suppose $n \geq 3$ for the problem to be meaningful. Since resolving the PFNT problem in the affirmative is equivalent to demonstrating the existence of a primitive free polynomial of degree n with two coefficients fixed, the cases with n small (i.e. $n = 3, 4$) are clearly the most challenging to tackle since the corresponding polynomials have fewest "degrees of freedom". In [3] it was suggested that the $n = 4$ case was soluble in principle by the methods outlined in the paper, whereas it might be impractical to expect any progress on the $n = 3$ case. In what follows, we solve the PFNT problem for $n = 4$, by identifying sets of elements whose cardinalities can be estimated with particular accuracy and using a sieving technique (on both the additive and multiplicative parts) designed to exploit these new estimates.

THEOREM 1.3. *Let q be a prime power and $n \geq 4$ an integer. Then (q, n) is a PFNT-pair.*

The basic technique ([5]) of expressing the number of elements with the desired properties in terms of Gauss sums over E yields, if applied directly, estimates in terms of the numbers of prime factors of $q^n - 1$ and irreducible factors of $x^n - 1$. This establishes the result for large n but is inadequate when n is small. In [3], use of a sieve on both the additive and multiplicative parts produces an expression in terms of the numbers of prime (resp. irreducible) factors of divisors of $q^n - 1$ (resp. $x^n - 1$), which are estimated as previously; this approach is more successful in dealing with small n but remains inappropriate for $n < 5$. The novel aspects of the approach to the PFNT problem which we take in this paper are our exploitation of the idiosyncrasies of the situation when $n = 4$, and the use of "external" results to estimate appropriate quantities (i.e. we no longer depend exclusively on the estimates derived from the initial Gauss sum formulation).

It transpires that when applying the sieve in the $n = 4$ case, it is sufficient to consider only linear factors of $x^n - 1$; specialising to the linear case when deriving the estimates allows improved precision (an extra G_1 term can be extracted and properties of additive characters with linear F-order can be used). Results from [8] provide estimates for the multiplicative quantities in the sieve which show an improvement, by a factor of $q^{1/2}$, on the estimates from Gauss sums obtained from [3]. The structure of the problem and the nature of our estimates then determine the optimal sieving approach, which is to treat the additive and multiplicative parts separately within the sieve,

and to take the linear factors of $x^n - 1$ individually. Applying this general strategy with a degree of flexibility (varying the choice of multiplicative divisors in the sieve and using some simplifying approximations which are once again specific to the $n = 4$ case) establishes the result for all odd q, with three exceptions. Finally, the exceptions are dealt with using the computer package MAPLE. For q a power of 2, the PFNT property follows from a solution of the non-zero PNT problem (in the obvious sense). This is treated in the final section: here there are two further values of q which must be dealt with numerically.

2. Preliminaries. We begin by making some reductions to the problem, and formulating the basic theory. The account will be as self-contained as possible, but to avoid excessive repetition, reference will be made to earlier work where appropriate.

By Proposition 4.1 of [5], which states that (q, n) is a PFNT-pair whenever $q - 1$ divides n, we may assume that $q > 2$. In fact, in the $n = 4$ case, this proposition establishes the result for $q = 2$, 3 and 5; so with the exception of $q = 4$ we may assume $q \geq 7$.

From now on, suppose that $a, b \in F$, with $a \neq 0$ and b a primitive element, are given.

Let $m = m(q, n)$ be the greatest divisor of $q^n - 1$ that is relatively prime to $q - 1$ (so in particular $m \mid \frac{q^n-1}{(q-1)(n,q-1)}$. In [3] it was demonstrated that, if $w \in E$ has (E, F)-norm b, then to guarantee that w is primitive it suffices to show that w is m-free in E (i.e. that $w = v^d$, where $v \in E$ and $d \mid m$, implies $d = 1$).

Analogously for the additive part: let $M = M(q, n)$ be the monic divisor of $x^n - 1$ (over F) of maximal degree that is prime to $x - 1$. So $M = (x^n - 1)/(x^{p^l} - 1)$ where $n = n_0 p^l$, $p = \operatorname{char} F$ and $p \nmid n_0$. It was shown in [3] that, if $w \in E$ has (non-zero) (E, F)-trace a, then to guarantee that w is free over F it suffices to show that w is M-free in E (i.e. that $w = h^\sigma(v)$, where $v \in E$ and h is an F-divisor of M, implies $h = 1$).

Define $N(t, T)$ to be the number of elements of E which

(i) are t-free ($t \in \mathbb{Z}$, $t \mid m$),
(ii) are T-free ($T(x) \in F[x]$, $T \mid x^n - 1$),
(iii) have norm b,
(iv) have trace a.

Write $\pi(t, T)$ for $q(q - 1)N(t, T)$.

We begin by expressing the characteristic functions of the four subsets of E (or E^*) defined by the conditions (i)–(iv) in terms of characters on E or F.

We suppose throughout that $t \mid m$, $T \mid x^n - 1$.

I. *The set of $w \in E^*$ with $N_{E/F}(w) = b$.* The characteristic function of the subset of E^* comprising elements with norm b is

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

where $\widehat{F}^*$ denotes the group of multiplicative characters of F^*, and $N_{E/F}$ is abbreviated to N.

II. *The set of $w \in E^*$ with $\mathrm{Tr}_{E/F}(w) = a$.* The characteristic function of the subset of E comprising elements with trace a is

$$\frac{1}{q} \sum_{c \in F} \lambda(c(\mathrm{Tr}(w) - a)),$$

where λ is the canonical additive character of F and $\mathrm{Tr}_{E/F}$ is abbreviated to Tr.

III. *The set of $w \in E^*$ that are t-free.* The characteristic function for the subset of t-free elements $(t \,|\, m)$ of E^* is

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

where $\theta(t) = \phi(t)/t$, η_d denotes a character of order d $(d \,|\, m)$ in $\widehat{E}^*$ and, using the notation introduced in [3], the integral notation is shorthand for a weighted sum:

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

IV. *The set of $w \in E$ that are T-free over F.* The characteristic function of the set of T-free elements of E takes the form

$$\Theta(T) \int_{D|T} \chi_{\delta_D}(w), \qquad w \in E,$$

where $\Theta(T) = \Phi(T)/T$, χ is the canonical additive character on E and, as defined in [3], $\{\chi_{\delta_D} : \delta_D \in \Delta_D\}$ (where $\chi_\delta(w) := \chi(\delta w)$, $w \in E$) is the set of all additive characters of E of order D $(D \,|\, x^n - 1)$. Again, the integral notation represents a weighted sum:

$$\int_{D|T} \chi_{\delta_D} := \sum_{D|T} \frac{\mu(D)}{\Phi(D)} \sum_{(\delta_D)} \chi_{\delta_D}.$$

Using these characteristic functions, we derive the following expression for $\pi(t, T)$:

$$\pi(t,T) = \theta(t)\Theta(T) \int_{d|t} \int_{D|T} \sum_{\nu \in \widehat{F}^*} \sum_{c \in F} \overline{\nu}(b)\overline{\lambda}(ac) \sum_{w \in E} (\eta_d \widetilde{\nu})(w) \chi((\delta_D + c)w) \tag{2.1}$$

where $\widetilde{\nu}(w) = \nu(N(w))$ and $\chi(cw) = \lambda(c\mathrm{Tr}(w))$ (cf. [3, (2.2)]).

We shall now specialise to the case when $n = 4$. Observe that, if $p \mid n$, then $q = 2^k$ where $k \geq 2$; in this case $M = 1$ and the PFNT problem reduces to the PNT problem (where the specified trace is non-zero). This takes a simpler form than the PFNT problem due to the absence of an additive component; we shall consider the $p = 2$ case in the final section. Hence in the main part of the paper (in particular in those sections dealing with the additive part of the problem) we may assume that $p = \operatorname{char} F \nmid n$, i.e. q is odd. With n equal to 4 and q odd,

$$m \,\Big|\, \frac{(q+1)(q^2+1)}{4} \quad \text{and} \quad M = \frac{x^4-1}{x-1}.$$

More precisely, if $q \equiv 1 \pmod 4$, then

$$m = \left(\frac{q+1}{2}\right)\left(\frac{q^2+1}{2}\right) \quad \text{and} \quad M = (x+1)(x-i)(x+i)$$

(where $i \in F$ is such that $i^2 = -1$); while if $q \equiv 3 \pmod 4$, then

$$m \,\Big|\, \left(\frac{q+1}{4}\right)\left(\frac{q^2+1}{2}\right) \quad \text{and} \quad M = (x+1)(x^2+1).$$

Note that in both cases $\frac{q^2+1}{2} \,\big|\, m$. Our strategy for proving the PFNT problem for $n = 4$ is to apply a sieving technique which treats the additive and multiplicative parts separately. In the next two sections, we establish estimates for $\pi(1, L)$ (L a linear factor of M) and $\pi(t, 1)$ ($t \mid m$).

3. Estimates for linear polynomial factors. In this section, we derive estimates for the number $N(1, L)$ of L-free elements of E with prescribed norm and trace, where L is a linear divisor of M. (We assume that q is an odd prime power.)

For economy of calculation, it is in fact desirable to consider the difference between $\pi(1, L)$ and $\theta(L)\pi(1, 1)$ (in some sense the "error term"). We will prove the following lemma, whose bounds will play a key role in our sieve. (As will be shown later, it is sufficient to obtain bounds for only those factors of $x^4 - 1$ which are linear over F.)

LEMMA 3.1. (i) *When* $q \equiv 1 \pmod 4$,

$$|\pi(1, x+1) + \pi(1, x+i) + \pi(1, x-i) - 3(1-1/q)\pi(1, 1)| < q^3(3 - 11/q)(1 + 1/\sqrt{q}). \tag{3.1}$$

(ii) *When* $q \equiv 3 \pmod 4$,

$$|\pi(1, x+1) - (1-1/q)\pi(1, 1)| \leq q^3(1 - 3/q)(1 + 1/\sqrt{q}). \tag{3.2}$$

These bounds represent an improvement by a factor of order $q^{1/2}$ over those derivable from Theorem 2.1 of [3].

Denote by L a linear factor of M; L may take the value $x+1$ or, in the case when $q \equiv 1 \pmod 4$, the values $x \pm i$.

First, we establish some results about δ_L. For a polynomial $f(x)$, let f^σ denote the polynomial obtained from f by replacing x^i by x^{q^i}.

LEMMA 3.2. (i) *If* $D \mid x^{n/k}-1$ $(k \mid n)$, *then* δ_D *is a root of* $(x^{n/k}-1)^\sigma$, *i.e.* $\delta_D \in \mathrm{GF}(q^{n/k})$.

(ii) *If* $D \mid x^{n/k}+1$ $(k \mid n)$, *then* δ_D *is a root of* $(x^{n/k}+1)^\sigma$, *i.e.* $\delta_D^{q^{n/k}} = -\delta_D$.

Proof. (i) Set $R = q^{n/k}$. So for the canonical character χ_1 of E, $\chi_1(w) = \lambda(\mathrm{Tr}_{R^k/p}(w))$ $(w \in E)$, where $\lambda(x) = e^{2\pi i x/p}$ and $\mathrm{Tr}_{\mathrm{GF}(R^k)/\mathrm{GF}(p)}$ is abbreviated to $\mathrm{Tr}_{R^k/p}$. Let $\chi(w) = \chi_\delta(w) = \lambda(\mathrm{Tr}_{R^k/p}(\delta w))$ and suppose $\delta \in \mathrm{GF}(R)$, so $\delta^R = \delta$. Then

$$\begin{aligned}\chi(w^R) &= \lambda(\mathrm{Tr}_{R^k/p}(\delta w^R)) = \lambda(\mathrm{Tr}_{R/p}(\mathrm{Tr}_{R^k/R}(\delta^R w^R)))\\ &= \lambda(\mathrm{Tr}_{R/p}(\mathrm{Tr}_{R^k/R}(\delta w))) = \lambda(\mathrm{Tr}_{R^k/p}(\delta w)) = \chi(w).\end{aligned}$$

Hence $\chi(w^R - w) = 1$ for all $w \in E$. So for any $D \mid x^{n/k}-1$, i.e. $D^\sigma \mid x^R - x$, $\chi_\delta(D^\sigma(w)) = 1$. Thus $\delta = \delta_D$ for some $D \mid x^{n/k}-1$. Letting δ vary in $\mathrm{GF}(R)$ accounts for all R characters of order dividing $x^{n/k}-1$.

(ii) Suppose δ is a root of $x^{q^{n/k}} + x$, so $\delta^R = -\delta$. Proceed as in part (i).

LEMMA 3.3. *Suppose* $q \equiv 1 \pmod 4$, *and let* $i \in \mathrm{GF}(q)$ *be such that* $i^2 = -1$.

(i) *Let* $D = x + i$. *Then* $(x-i)^\sigma(\delta_D) = 0$, *i.e.* $\delta_D^q = i\delta_D$.
(ii) *Let* $D = x - i$. *Then* $(x+i)^\sigma(\delta_D) = 0$, *i.e.* $\delta_D^q = -i\delta_D$.

Proof. (i) Suppose $\delta^q = i\delta$. Define $\chi(w) = \chi_1(\delta w) = \lambda(\mathrm{Tr}_{q^4/p}(\delta w))$, $w \in E = \mathbb{F}_{q^4}$. Then

$$\begin{aligned}\chi(w^q + iw) &= \lambda(\mathrm{Tr}_{q/p}[\mathrm{Tr}_{q^4/q}(\delta(w^q + iw))])\\ &= \lambda(\mathrm{Tr}_{q/p}[\mathrm{Tr}_{q^4/q}(-i((\delta w)^q - \delta w))])\\ &= \lambda(\mathrm{Tr}_{q/p}[-i\mathrm{Tr}_{q^4/q}((\delta w)^q - \delta w)]) = 1,\end{aligned}$$

since $\mathrm{Tr}_{q^4/q}((\delta w)^q - \delta w) \equiv 0$. So the F-order of χ is $x+i$. This accounts for all characters with F-order $x+i$.

(ii) Replace i by $-i$ in (i).

We are now ready to prove Lemma 3.1. Throughout this discussion, $G_n(\nu)$ (where ν is a multiplicative character on $\mathbb{F}_{q^n}^*$) will denote a Gauss sum in $\mathbb{F}_{q^n}^*$. We will use the notation $J_a(\nu_1, \ldots, \nu_k)$ (where $a \in F$, $\nu_1, \ldots, \nu_k$ are multiplicative characters of F, $k \in \mathbb{N}$) to denote the Jacobi sum

$$\sum_{c_1+\ldots+c_k=a} \nu_1(c_1)\ldots\nu_k(c_k).$$

For extra background material, the reader may consult texts such as [10].

Proof of Lemma 3.1. By equation (2.1), since $\Theta(L) = 1 - 1/q$,

$$\begin{aligned}(3.3)\qquad &\pi(1,L) - \Theta(L)\pi(1,1)\\ &\quad = \Theta(L)\Big(-\frac{1}{q-1}\Big)\sum_{\nu\in\widehat{F}^*}\sum_{c\in F}\sum_{(\delta_L)}\overline{\nu}(b)\overline{\lambda}(ac)\sum_{w\in E}\widetilde{\nu}(w)\chi((\delta_L+c)w),\end{aligned}$$

where δ_L runs through all $\Phi(L)$ elements of Δ_L (i.e. χ_{δ_L} runs through all additive characters of E of order L). Separating the term for which $c = 0$, we have

$$\begin{aligned}(3.4)\qquad &\pi(1,L) - \Theta(L)\pi(1,1)\\ &\quad = -\frac{1}{q}\Big(\sum_{\nu\in\widehat{F}^*}\sum_{(\delta_L)}\overline{\nu}(b)\sum_{w\in E}\widetilde{\nu}(w)\chi(\delta_L w)\\ &\qquad + \sum_{\nu\in\widehat{F}^*}\sum_{c\in F^*}\sum_{(\delta_L)}\overline{\nu}(b)\overline{\lambda}(ac)\sum_{w\in E}\widetilde{\nu}(w)\chi((\delta_L+c)w)\Big).\end{aligned}$$

For the first term on the right side of (3.4), using the fact that $\delta_L \neq 0$, replace w by w/δ_L to obtain

$$\sum_{\nu\in\widehat{F}^*}\nu(1/b)G_4(\widetilde{\nu})\sum_{(\delta_L)}\overline{\widetilde{\nu}}(\delta_L).$$

Since $F^*\Delta_D = \Delta_D$,

$$\sum_{(\delta_L)}\overline{\widetilde{\nu}}(\delta_L) = \frac{1}{q-1}\sum_{(\delta_L)}\sum_{c\in F^*}\overline{\widetilde{\nu}}(c\delta_L) = \frac{1}{q-1}\sum_{(\delta_L)}\overline{\widetilde{\nu}}(\delta_L)\Big(\sum_{c\in F^*}\overline{\widetilde{\nu}}(c)\Big)$$

and the inner sum equals 0 unless ν^* ($:= \widetilde{\nu}|_F$) is trivial, when it equals $q-1$. Note that, for $k \in F$, $\nu^*(k) = \widetilde{\nu}(k) = \nu(N(k)) = \nu(k^4)$, i.e. $\nu^* = \nu^4$. So the first term of (3.4) can be simplified to

$$\sum_{\substack{\nu\in\widehat{F}^*\\ \nu^4=\nu_1}}\sum_{(\delta_L)}\nu(1/b)G_4(\widetilde{\nu})\overline{\widetilde{\nu}}(\delta_L).$$

For the second term on the right side of (3.4) (i.e. the part for which $c \neq 0$), replace δ_L by $c\delta_L$, then w by $w/(c(\delta_L+1))$ to get

$$\sum_{\nu\in\widehat{F}^*}\nu(1/b)G_4(\widetilde{\nu})\sum_{(\delta_L)}\overline{\widetilde{\nu}}(\delta_L+1)\sum_{c\in F^*}\overline{\lambda}(ac)\overline{\widetilde{\nu}}(c).$$

Consider the inner sum $\sum_{c\in F^*}\overline{\lambda}(ac)\overline{\widetilde{\nu}}(c)$. In the case when $\nu^4 = \nu_1$, this reduces to a sum over additive characters of F, while for $\nu^4 \neq \nu_1$, a Gauss sum over F is obtained. Thus the second term of (3.4) may be expanded as

$$- \sum_{\substack{\nu\in\widehat{F}^*\\ \nu^4=\nu_1}} \nu(1/b)G_4(\widetilde{\nu})\sum_{(\delta_L)}\overline{\widetilde{\nu}}(\delta_L+1) + \sum_{\substack{\nu\in\widehat{F}^*\\ \nu^4\neq\nu_1}} \nu^*(a)\nu(1/b)G_4(\widetilde{\nu})\overline{G}_1(\nu^*)\sum_{(\delta_L)}\overline{\widetilde{\nu}}(\delta_L+1).$$

Hence,

$$\begin{aligned}(3.5)\qquad \pi(1,L)-\Theta(L)\pi(1,1) &= -\frac{1}{q}\Big(\sum_{\substack{\nu\in\widehat{F}^*\\ \nu^4\neq\nu_1}} \nu(a^4/b)G_4(\widetilde{\nu})\overline{G}_1(\nu^*)\Big(\sum_{(\delta_L)}\overline{\widetilde{\nu}}(\delta_L+1)\Big)\\ &\quad + \sum_{\substack{\nu\in\widehat{F}^*\\ \nu^4=\nu_1\\ \overline{\nu}\neq\eta_1}} \nu(1/b)G_4(\widetilde{\nu})\sum_{(\delta_L)}(\overline{\widetilde{\nu}}(\delta_L)-\overline{\widetilde{\nu}}(\delta_L+1))\Big)\\ &= \frac{1}{q}\Big(\sum_{\substack{\nu\in\widehat{F}^*\\ \nu^4\neq\nu_1}}\sum_{(\delta_L)} \nu(a^4/b)\overline{\nu}(N(\delta_L+1))\overline{G}_1(\nu^4)G_1^4(\nu)\\ &\quad + \sum_{\substack{\nu\in\widehat{F}^*\\ \nu^4=\nu_1\\ \nu\neq\nu_1}} \nu(1/b)G_1^4(\nu)\sum_{(\delta_L)}[\overline{\nu}(N(\delta_L))-\overline{\nu}(N(\delta_L+1))]\Big)\end{aligned}$$

since $G_4(\widetilde{\nu}) = -G_1^4(\nu)$ by the Davenport–Hasse Theorem ([10, Theorem 5.14]).

We shall consider the various specific values that may be taken by L in (3.5); we begin by assuming that $L = x+1$. By Lemma 3.2, $\delta_L^q = -\delta_L$. Hence $\delta_L^2 = c$, where c is a non-square in F. Indeed, $\{\delta_L\} = \{\pm\sqrt{c}\colon c \text{ a non-square in } F\}$, a set of cardinality $q-1$ as required. Moreover, $\{\delta_L\} = \{1/\delta_L\}$. Hence $N(\delta_L) = c^2$, while $N(1+\delta_L) = (1+\delta_L)(1+\delta_L^q)(1+\delta_L^{q^2})(1+\delta_L^{q^3}) = (1+\delta_L)^2(1-\delta_L)^2 = (1-c)^2$.

Writing ν_2 for the quadratic character on F, we have

$$\begin{aligned}&\pi(1,x+1)-(1-1/q)\pi(1,1)\\ &\quad= \frac{1}{q}\Big(\sum_{\substack{\nu\in\widehat{F}^*\\ \nu^4\neq\nu_1}} \nu(a^4/b)\overline{G}_1(\nu^4)G_1^4(\nu)\sum_{c\in F^*}(1-\nu_2(c))\overline{\nu}((1-c)^2)\\ &\qquad + \sum_{\substack{\nu\in F^*\\ \nu^4=\nu_1\\ \nu\neq\nu_1}} \nu(1/b)G_1^4(\nu)\sum_{c\in F^*}(1-\nu_2(c))(\overline{\nu}(c^2)-\overline{\nu}((1-c)^2))\Big)\\ &\quad= \frac{1}{q}\{S_1+S_2\}, \quad \text{say.}\end{aligned}$$

The quadratic character satisfies the condition "$\nu^4 = \nu_1$, $\nu \neq \nu_1$", but contributes zero to S_2. In particular, when $q \equiv 3 \pmod 4$, there are no further contributions, whence $S_2 = 0$.

In the case when $q \equiv 1 \pmod 4$, there are also two characters of degree 4, which (may) give non-zero contributions. Thus

$$S_2 = -\sum_{\substack{\nu \in \widehat{F}^* \\ \operatorname{ord}\nu = 4}} \nu(1/b) G_1^4(\nu) \Big(\sum_{c \in \widehat{F}^*} (1 - \nu_2(c))(1 + \nu_4^2(1-c)) \Big),$$

since only non-square $c \in F^*$ contribute to the inner sum. The latter has the form

$$\begin{aligned}\sum_{c \in F^*} &(1 - \nu_2(c) + \overline{\nu}_4^2(1-c) - \nu_2(c)\overline{\nu}_4^2(1-c)) \\ &= (q-1) - \sum_{c \in F^*} \nu_2(c) + \sum_{c \in F^*} \nu_2(1-c) - \sum_{c \in F^*} \nu_2(c)\nu_2(1-c) \\ &= (q-1) - 0 + (0-1) - J_1(\nu_2, \nu_2) = (q-1) - 1 - (-1) = q - 1.\end{aligned}$$

Thus

$$S_2 = -(q-1) \sum_{\substack{\nu \in F^* \\ \operatorname{ord}\nu = 4}} \nu(1/b) G_1^4(\nu), \tag{3.6}$$

i.e. $|S_2| \leq 2q^2(q-1)$ and hence $q^{-1}|S_2| \leq 2q(q-1)$ when $q \equiv 1 \pmod 4$.

Next, consider S_1:

$$S_1 = \sum_{\substack{\nu \in \widehat{F}^* \\ \nu^4 \neq \nu_1}} \nu(a^4/b) \overline{G}_1(\nu^4) G_1^4(\nu) \sum_{c \in F^*} (1 - \nu_2(c)) \overline{\nu}(1-c)^2. \tag{3.7}$$

The inner sum of (3.7) has the following form (note that $\overline{\nu}^2 \neq \nu_1, \nu_2$):

$$\sum_{c \in F^*} \overline{\nu}^2(1-c) - \sum_{c \in F^*} \nu_2(c)\overline{\nu}^2(1-c) = -1 - J_1(\nu_2, \overline{\nu}^2).$$

Since the Jacobi sum has absolute value $\sqrt{q}$, the inner sum has absolute value at most $1 + \sqrt{q}$. Hence

$$\frac{1}{q}\,|S_1| \leq \frac{1}{q}\,((q-1) - e)\sqrt{q}\,q^2(1 + \sqrt{q}) = q^3 \left(1 - \frac{e+1}{q}\right)\left(1 + \frac{1}{\sqrt{q}}\right),$$

where $e = \gcd(q-1, 4)$.

In conclusion, in the case $q \equiv 3 \pmod 4$,

$$|\pi(1, x+1) - (1 - 1/q)\pi(1,1)| \leq (q^3 + q^{5/2})(1 - 3/q), \tag{3.8}$$

while in the case $q \equiv 1 \pmod 4$,

$$\begin{aligned}&|\pi(1, x+1) - (1 - 1/q)\pi(1,1)| \\ &\leq (q^3 + q^{5/2})(1 - 5/q) + 2q(q-1) = q^3(1 - 3/q - 2/q^2) + q^{5/2}(1 - 5/q).\end{aligned} \tag{3.9}$$

In particular, this establishes part (ii) of Lemma 3.1, i.e. the case when $q \equiv 3 \pmod 4$.

In the case when $q \equiv 1 \pmod 4$, there are two more linear factors to be considered, namely $L = x + i$ and $L = x - i$. Since these L are divisors of $x^2 + 1$, $\delta_L^{q^2} = -\delta_L$ by Lemma 3.2; thus $\delta_L^2 \in \mathbb{F}_{q^2}^*$ but $\delta_L^2 \notin \mathbb{F}_q^*$, and so $\delta_L^4 = c$, where c is a non-square in F. In fact, $\{\delta_{x-i}\} \cup \{\delta_{x+i}\} = \{4\text{th roots of } c,\ c \text{ a non-square in } F\}$, a set of cardinality $2(q-1)$.

In the case when $L = x + i$ in (3.5), by Lemma 3.3, $N(\delta_L) = \delta_L \delta_L^q \delta_L^{q^2} \delta_L^{q^3}$ $= \delta_L(i\delta_L)(-\delta_L)(-i\delta_L) = -\delta_L^4 = -c$ and $N(1 + \delta_L) = (1 - \delta_L^2)(1 + \delta_L^2) = 1 - \delta_L^4 = 1 - c$. The same values are obtained when $L = x - i$. Denote $x + i$ and $x - i$ by L_1 and L_2 respectively. Then (3.5) yields

$$\pi(1, L_1) + \pi(1, L_2) - 2\Theta(L)\pi(1, 1) = \frac{2}{q}\{S_1 + S_2\}$$

where

$$S_1 := \sum_{\substack{\nu \in \widehat{F}^* \\ \nu^4 \neq \nu_1}} \nu(a^4/b)\overline{G}_1(\nu^4)G_1^4(\nu) \sum_{c \in F^*} (1 - \nu_2(c))\overline{\nu}(1 - c), \tag{3.10}$$

$$S_2 := \sum_{\substack{\nu \in \widehat{F}^* \\ \nu^4 = \nu_1 \\ \nu \neq \nu_1}} \nu(1/b)G_1^4(\nu) \sum_{c \in F^*} [\overline{\nu}(-c) - \overline{\nu}(1 - c)](1 - \nu_2(c)). \tag{3.11}$$

Consider S_1. It may be written in the form

$$S_1 = \sum_{\substack{\nu \in \widehat{F}^* \\ \nu^4 \neq \nu_1}} \nu(a^4/b)\overline{G}_1(\nu^4)G_1^4(\nu)\sigma_1, \quad \text{say,}$$

where $\sigma_1 := \sum_{c \in F^*}(1 - \nu_2(c))\overline{\nu}(1 - c)$. Then

$$\sigma_1 = \sum_{c \in F^*} \overline{\nu}(1 - c) - \sum_{c \in F^*} \nu_2(c)\overline{\nu}(1 - c) = -1 + J_1(\nu_2, \overline{\nu}).$$

As before, the Jacobi sum has absolute value $\sqrt{q}$. Thus

$$|S_1| \leq (q - 1 - e)\sqrt{q}\, q^2(1 + \sqrt{q})$$

where $e = \gcd(q - 1, 4)$, i.e.

$$\frac{2}{q}|S_1| \leq 2q^3(1 - 5/q)(1 + 1/\sqrt{q}).$$

Now consider S_2 in (3.11). For a given ν with $\nu^4 = \nu_1$, $\nu \neq \nu_1$, the inner sum σ_2 satisfies

$$\begin{aligned}\sigma_2 &= \sum_{c \in F^*} \overline{\nu}(-c) - \sum_{c \in F^*} \overline{\nu}(1 - c) - \sum_{c \in F^*} \overline{\nu}(-c)\nu_2(c) + \sum_{c \in F^*} \overline{\nu}(1 - c)\nu_2(c) \\ &= 0 - (-1) - J_0(\nu_2, \overline{\nu}) + J_1(\nu_2, \overline{\nu}) = 1 - J_0(\nu_2, \overline{\nu}) + J_1(\nu_2, \overline{\nu}).\end{aligned}$$

If $\nu = \nu_2$, then

$$\sigma_2 = 1 - J_0(\nu_2, \nu_2) + J_1(\nu_2, \nu_2) = 1 - (q-1) + (-1) = -(q-1)$$

(using the fact that $\nu_2(-1) = 1$). If $\nu^2 = \nu_2$ (write $\nu = \nu_4$, since ν must be one of the two characters of order 4), then

$$\sigma_2 = 1 - J_0(\nu_2, \overline{\nu}_4) + J_1(\nu_2, \overline{\nu}_4) = 1 - 0 + J_1(\nu_2, \overline{\nu}_4).$$

Once again, $|\sigma_2| \le 1 + \sqrt{q}$. Hence

$$\begin{aligned} S_2 &= \nu_2(1/b)G_1^4(\nu_2)[-(q-1)] + \sum_{\substack{\nu \in F^* \\ \operatorname{ord}\nu = 4}} \nu(1/b)G_1^4(\nu)(1 + J_1(\nu_2, \overline{\nu})) \\ &= q^2(q-1) + \sum_{\substack{\nu \in F^* \\ \operatorname{ord}\nu = 4}} \nu(1/b)G_1^4(\nu)(1 + J_1(\nu_2, \overline{\nu})), \end{aligned} \tag{3.12}$$

since b is primitive and hence a non-square, and $G_1^4(\nu_2) = q^2$. Thus

$$|S_2| \le q^2(q-1) + 2q^2(1 + \sqrt{q}) = q^3(1 + 1/\sqrt{q})^2 \tag{3.13}$$

and so

$$\frac{2}{q}\,|S_2| \le 2q^2(1 + 1/\sqrt{q})^2.$$

Hence,

$$\begin{aligned} &|\pi(1, L_1) + \pi(1, L_2) - 2(1 - 1/q)\pi(1, 1)| \\ &\qquad \le 2q^3(1 - 4/q + 1/q^2) + 2q^{5/2}(1 - 3/q). \end{aligned} \tag{3.14}$$

Combining (3.9) and (3.14) proves Lemma 3.1(i) as follows:

$$\begin{aligned} &|\pi(1, x+1) + \pi(1, x+i) + \pi(1, x-i) - 3(1 - 1/q)\pi(1, 1)| \\ &\quad < (q^3 + q^{5/2})(1 - 5/q) + 2q(q-1) + 2q^3(1 - 4/q + 1/q^2) + 2q^{5/2}(1 - 3/q) \\ &\quad = (q^3 + q^{5/2})(3 - 11/q) = q^3(3 - 11/q)(1 + 1/\sqrt{q}). \end{aligned}$$

4. Estimates for integer factors. In this section we obtain new estimates for the number $N(t, 1)$ of t-free elements of E with prescribed norm and trace, where $t \in \mathbb{N}$ is a divisor of m. We improve upon the estimates of [3] by applying some deep results of Katz arising from the study of Soto–Andrade sums [8].

LEMMA 4.1 ([8, Theorem 4]). *Suppose that $n \ge 2$. Then*

$$\left| N(1, 1) - \frac{q^n - 1}{q(q-1)} \right| \le n q^{(n-2)/2}, \tag{4.1}$$

i.e.

$$|\pi(1, 1) - (q^n - 1)| \le n(1 - 1/q)q^{(n+2)/2}. \tag{4.2}$$

In particular, for $n = 4$, Lemma 4.1 has the form

$$|\pi(1,1) - (q^4 - 1)| \le 4(1 - 1/q)q^3.$$

Note that this is an improvement, by a factor of approximately $q^{1/2}/4$, on the estimate

$$|\pi(1,1) - q^4| \le (1 - (e+1)/q)q^{7/2},$$

obtained from Corollary 2.2 of [3].

Next, we estimate $N(t,1)$ where $t \mid m$, $t > 1$.

LEMMA 4.2 ([8, Corollary of Theorem 3 bis]). *Let η be a character of E of order d, where $d \mid m$, $d > 1$. Set*

$$M(\eta) = \sum_{\substack{x \in E \\ N(x)=b \\ \mathrm{Tr}(x)=a}} \eta(x).$$

In the special cases when η^{q-1} is trivial, or when n is odd, n is prime to p, η^{q-1} has exact order n, the characters η^{q^i-1} are all distinct for $i = 0, \dots, n-1$ and $d^n = n^n b$,

$$|M(\eta) - q^{(n-1)/2}| \le nq^{(n-2)/2}.$$

Otherwise, in the general case,

$$|M(\eta)| \le nq^{(n-2)/2}.$$

Note that the general case of this lemma is applicable when $n = 4$ to all $\eta_d \in \widehat{F}^*$ $(d \mid m)$, since $(d, q-1) = 1$ for all such d by the definition of m.

COROLLARY 4.3. *Let $t \mid m$, $t > 1$ and $t_0 \mid t$, $t_0 \ge 1$. Then*

$$\left|\pi(t,1) - \frac{\theta(t)}{\theta(t_0)}\,\pi(t_0,1)\right| \le \theta(t)n(W(t) - W(t_0))(1 - 1/q)q^{(n+2)/2}. \tag{4.3}$$

Proof. By definition,

$$N(t,1) = \theta(t) \sum_{\substack{w \in E \\ N(w)=b \\ \mathrm{Tr}(w)=a}} \int_{d \mid t} \eta_d(w) = \theta(t) \int_{d \mid t} M(\eta_d),$$

and so

$$N(t,1) - \frac{\theta(t)}{\theta(t_0)}\,N(t_0,1) = \theta(t) \int_{\substack{d \mid t \\ d \nmid t_0}} M(\eta_d).$$

By Lemma 4.2,

$$\left|N(t,1) - \frac{\theta(t)}{\theta(t_0)}\,N(t_0,1)\right| \le \theta(t)(W(t) - W(t_0))nq^{(n-2)/2}$$

and hence

$$\left|\pi(t,1) - \frac{\theta(t)}{\theta(t_0)}\,\pi(t_0,1)\right| \le \theta(t)n(W(t)-W(t_0))(1-1/q)q^{(n+2)/2}.$$

In particular, for $n=4$,

$$\left|\pi(t,1) - \frac{\theta(t)}{\theta(t_0)}\,\pi(t_0,1)\right| \le 4\theta(t)(W(t)-W(t_0))(1-1/q)q^3. \tag{4.4}$$

5. The proof for general prime powers. Having established bounds for $\pi(1,L)$ ($L \mid M$, L linear) and $\pi(t,1)$ ($t \mid m$), as the next step, we develop a sieving technique.

We shall use the basic sieving inequality introduced in Theorem 3.1 of [3]. Let $d \mid m$ and $f \mid x^n - 1$. Then (d_i, f_i) ($i = 1, \dots, r$ for $r \in \mathbb{N}$) will be called *complementary divisor pairs* with *common divisor pair* (d_0, f_0) if the primes in $\operatorname{lcm}\{d_1, \dots, d_r\}$ are precisely those in d, the irreducibles in $\operatorname{lcm}\{f_1, \dots, f_r\}$ are precisely those in f, and for any distinct pair (i,j), the primes and irreducibles in $\gcd(d_i, d_j)$ and $\gcd(f_i, f_j)$ are precisely those in d_0 and f_0 respectively. Observe that the value of $\pi(d,f)$ will depend only on which "atoms" (primes/irreducibles) are present in d and f, not on the power to which the atoms occur.

LEMMA 5.1 (Sieving inequality). *For divisors d of m and f of x^n-1, let $\{(d_1,f_1), \dots, (d_r,f_r)\}$ be complementary divisor pairs of (d,f) with common divisor (d_0,f_0). Then*

$$\pi(d,f) \ge \sum_{i=1}^{r} \pi(d_i,f_i) - (r-1)\pi(d_0,f_0). \tag{5.1}$$

The following lemma allows us to make a simplification in the case when $q \equiv 3 \pmod 4$.

LEMMA 5.2. *For $q \equiv 3 \pmod 4$,*

$$N\left(m, \frac{x^4-1}{x-1}\right) = N(m, x+1).$$

Proof. Suppose that α is both m-free and $x+1$-free, but not $\frac{x^4-1}{x-1}$-free. (Note that in this case x^2+1 is irreducible over F.) Then $\alpha = \beta^{q^2} + \beta$, and hence $\alpha^{q^2} = \alpha$, i.e. $\alpha^{q^2-1} = 1$. This implies that $\alpha = \gamma^{q^2+1}$ for some $\gamma \in E$, an evident contradiction since α is m-free. Observe that the norm/trace restrictions do not affect the argument here.

The following are sufficient conditions for $(q,4)$ to be a PFNT-pair.

LEMMA 5.3. (i) *When $q \equiv 1 \pmod 4$, $(q,4)$ is a PFNT-pair if*

$$\begin{aligned}\pi(1,1)(\theta(m) - 3/q) \\ > 4\theta(m)(W(m)-1)(1-1/q)q^3 + (3-11/q)q^3 + (3-11/q)q^{5/2}.\end{aligned} \tag{5.2}$$

(ii) *When* $q \equiv 3 \pmod 4$, $(q, 4)$ *is a PFNT-pair if*

$$\pi(1,1)(\theta(m) - 1/q) \geq 4\theta(m)(W(m) - 1)(1 - 1/q)q^3 + (1 + 1/\sqrt{q})(1 - 3/q)q^3. \tag{5.3}$$

Proof. (i) Apply the sieve in the following form:

$$\pi(m, M) \geq \pi(m, 1) + \pi(1, x + 1) + \pi(1, x - i) + \pi(1, x + i) - 3\pi(1, 1). \tag{5.4}$$

Using the lower bounds for $\pi(m, 1)$ and the $\pi(1, L_i)$ $(i = 1, 2, 3)$ from inequalities (4.4) and (3.1), we see that $\pi(m, M) > 0$ whenever the stated condition holds.

(ii) Apply the sieve in the form

$$\pi(m, M) \geq \pi(m, 1) + \pi(1, x + 1) - \pi(1, 1). \tag{5.5}$$

As in the proof of part (i), the result follows using the lower bounds for $\pi(m, 1)$ and $\pi(1, x + 1)$ given by inequalities (4.4) and (3.2).

The following lemmas provide easy, but useful, lower bounds for $\theta(m)$ and $W(m)$.

LEMMA 5.4. (i) *For all odd* $r \in \mathbb{N}$ $(\neq 1, 3, 9, 15, 21, 105)$,

$$\theta(r) > 1/r^{1/6}.$$

(ii) *Let* q *be an odd prime power, and let* m *be the greatest divisor of* $q^4 - 1$ *coprime to* $q - 1$. *Then*

$$\theta(m) > 1/\sqrt{q}.$$

Proof. (i) Exploit the multiplicativity of the function $r^{1/6}\theta(r)$ by breaking r (not one of the exceptions) into coprime factors ϱ of the following types and applying the result to each factor.

- $\varrho = p^k$ $(p \geq 5,\ k \geq 1)$. Since $x - x^{5/6} - 1 > 0$ for $x \geq 5$, it follows that
$$\theta(\varrho) = \theta(p) = 1 - \frac{1}{p} > \frac{1}{p^{1/6}} \geq \frac{1}{\varrho^{1/6}}.$$
- $\varrho = 3^k$ $(k \geq 3)$. Then
$$\theta(\varrho) = \theta(3) = \frac{2}{3} > \frac{1}{\sqrt{3}} = \frac{1}{27^{1/6}} \geq \frac{1}{\varrho^{1/6}}.$$
- $\varrho = 9p^k$ $(k \geq 1)$ or $\varrho = 3p^k$ $(k \geq 2)$, with $p \geq 5$. Then
$$\theta(\varrho) = \frac{2}{3}\left(1 - \frac{1}{p}\right) \geq \frac{8}{15} > \frac{1}{45^{1/6}} \geq \frac{1}{\varrho^{1/6}}.$$
- $\varrho = 3p$ $(p > 11)$. Then
$$\theta(p) = \frac{2}{3}\left(1 - \frac{1}{p}\right) \geq \frac{20}{33} > \frac{1}{33^{1/6}} \geq \frac{1}{\varrho^{1/6}}.$$

(ii) Since $4m < (q^4 - 1)/(q - 1) < (q + 1)^3$, $q > 4^{1/3}m^{1/3} - 1$ and so $q \geq m^{1/3}$ for all q. Hence, $\sqrt{q} \geq m^{1/6}$, i.e. $1/\sqrt{q} \leq 1/m^{1/6}$. From part (i),

$\theta(m) > 1/m^{1/6} \geq 1/\sqrt{q}$. (Observe that, because $\frac{q^2+1}{2} \mid m$, m is not one of the exceptional values in (i).)

LEMMA 5.5 ([6, Lemma 3.3]). *For any positive integer* m,

$$W(m) \leq c_m m^{1/4}, \tag{5.6}$$

where $c_m = 2^s/(p_1 \dots p_s)^{1/4}$, *and* $p_1, \dots, p_s$ *are the distinct primes less than* 16 *which divide* m. *In particular, for all* $m \in \mathbb{N}$, $c_m < 4.9$, *and for all odd* m, $c_m < 2.891 < 2.9$.

(The proof is obvious using multiplicativity.)

PROPOSITION 5.6. *Let* $q \equiv 1 \pmod 4$ *be a prime power. Then* $(q, 4)$ *is a PFNT-pair for all* $q \geq 6217$.

Proof. By Lemma 5.3,

$$\begin{aligned}\pi(1,1)(\theta(m) - 3/q) \\ > 4\theta(m)(W(m)-1)(1-1/q)q^3 + (3-11/q)q^3 + (3-11/q)q^{5/2}.\end{aligned} \tag{5.7}$$

Then by Lemma 4.1, $\pi(m, M) > 0$ if

$$\begin{aligned}\theta(m)(q^4 - 4W(m)(1-1/q)q^3 - 1) \\ > q^3(6 + 1/q - 12/q^2) + q^{5/2}(3 - 11/q) - 3/q.\end{aligned} \tag{5.8}$$

By Lemma 5.5, $W(m) \leq c_m q/(4^{1/4}(q-1)^{1/4})$, where $c_m < 2.9$ since m is odd. Set $d := 4^{3/4}c_m$; then $4W(m) \leq dq/(q-1)^{1/4}$ and so $4W(m)((q-1)/q)q^3 \leq d(q-1)^{3/4}q^3$. Using this result and the second part of Lemma 5.4, $\pi(m, M) > 0$ certainly if

$$\begin{aligned}\frac{1}{\sqrt{q}}\{q^4 - d(q-1)^{3/4}q^3 - 1\} \\ > q^3(6 + 1/q - 12/q^2) + q^{5/2}(3 - 11/q) + 3/q,\end{aligned} \tag{5.9}$$

i.e. if

$$q > d(q-1)^{3/4} + \sqrt{q}\,(6 + 1/q - 12/q^2) + (3 - 11/q) + 1/q^3. \tag{5.10}$$

Take $c_m = 2.891$ and set $d = 8.2$ in inequality (5.10). Then (5.10) holds for all $q \geq 6217$; the largest prime power $q \equiv 1 \pmod 4$ for which the inequality fails is $q = 6197$.

PROPOSITION 5.7. *Let* $q \equiv 3 \pmod 4$ *be a prime power. Then* $(q, 4)$ *is a PFNT-pair for all* $q \geq 2659$.

Proof. By Lemma 5.3, $\pi(m, M) > 0$ if

$$\begin{aligned}\pi(1,1)(\theta(m) - 1/q) \\ \geq 4\theta(m)(W(m)-1)(1-1/q)q^3 + (1 + 1/\sqrt{q})(1-3/q)q^3.\end{aligned} \tag{5.11}$$

Then by Lemma 4.1, $\pi(m, M) > 0$ if

$$\begin{aligned}\theta(m)\{q^4 - 4W(m)(1-1/q)q^3 - 1\} \\ \geq q^3(2 - 7/q + 4/q^2) + (1 - 3/q) - 1/q,\end{aligned} \tag{5.12}$$

i.e. certainly if

$$q \geq d(q-1)^{3/4} + \sqrt{q}\,(2 - 7/q + 4/q^2) + (1 - 3/q) + 1/q^3, \tag{5.13}$$

where in this case $d := 4^{5/8} c_m$, since $8 \,|\, (q+1)(q^2+1)$ and so $W(m) \leq c_m q/(8^{1/4}(q-1)^{1/4})$. Take $c_m = 2.9$ and $d = 6.90$ in (5.13). Then inequality (5.13) holds for $q \geq 2659$; the largest prime power $q \equiv 3 \pmod 4$ for which the inequality fails is $q = 2647$.

5.1. *Sieving with atomic divisors.* In order to establish the result for smaller prime powers q, we will use the following sufficient conditions, which arise from the application of the sieve with atomic divisors.

In order to simplify notation, from this point onwards we shall adopt the convention that all unmarked summation signs have index i running from $i = 1$ to s.

LEMMA 5.8. *Let s denote the number of distinct prime factors of m. Then the following are sufficient conditions for $(q, 4)$ to be a PFNT-pair.*

(i) *When $q \equiv 1 \pmod 4$,*

$$q \geq \frac{(3+4s) - \frac{11+4s}{q} - 4\big(1-\frac{1}{q}\big)\sum \frac{1}{p_i} + \frac{1}{\sqrt{q}}\big(3 - \frac{11}{q}\big)}{1 - \sum \frac{1}{p_i} - \frac{3}{q}} + 4\left(1 - \frac{1}{q}\right) + \frac{1}{q^3}. \tag{5.14}$$

(ii) *When $q \equiv 3 \pmod 4$,*

$$q \geq \frac{(1+4s) - \frac{3+4s}{q} - 4\big(1-\frac{1}{q}\big)\sum \frac{1}{p_i} + \frac{1}{\sqrt{q}}\big(1 - \frac{3}{q}\big)}{1 - \sum \frac{1}{p_i} - \frac{1}{q}} + 4\left(1 - \frac{1}{q}\right) + \frac{1}{q^3}. \tag{5.15}$$

Proof. (i) Let $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, where $p_1, \dots, p_s$ are distinct primes and $s \in \mathbb{N}$ (recall that the values of the α_i will be irrelevant here). Apply the sieve in the form

$$\pi(m, M) \geq \pi(p_1, 1) + \dots + \pi(p_s, 1) + \pi(1, x+1) + \pi(1, x+i) + \pi(1, x-i) - (s+2)\pi(1, 1). \tag{5.16}$$

Using the results of inequalities (3.1) and (4.4), $\pi(m, M) > 0$ if

$$\pi(1,1)\left(1 - \sum \frac{1}{p_i} - \frac{3}{q}\right) - q^3\left(3 - \frac{11}{q}\right) - q^{5/2}\left(3 - \frac{11}{q}\right) - 4q^3\left(1 - \frac{1}{q}\right)\sum\left(1 - \frac{1}{p_i}\right) \geq 0, \tag{5.17}$$

i.e. if

$$\pi(1,1) \geq \frac{q^3\big((3+4s) - \frac{11+4s}{q} - 4\big(1-\frac{1}{q}\big)\sum \frac{1}{p_i}\big) + q^{5/2}\big(3-\frac{11}{q}\big)}{1-\sum \frac{1}{p_i} - \frac{3}{q}} \tag{5.18}$$

and so, using Lemma 4.1, certainly if

$$q \geq \frac{(3+4s) - \frac{11+4s}{q} - 4\big(1-\frac{1}{q}\big)\sum \frac{1}{p_i} + \frac{1}{\sqrt{q}}\big(3-\frac{11}{q}\big)}{1-\sum \frac{1}{p_i} - \frac{3}{q}} + 4\left(1-\frac{1}{q}\right) + \frac{1}{q^3}. \tag{5.19}$$

(ii) Let $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$. Then, applying the sieve with atomic divisors,

$$\pi(m, x+1) \geq \pi(p_1,1) + \dots + \pi(p_s,1) + \pi(1,x+1) - s\pi(1,1). \tag{5.20}$$

Using the results of inequalities (3.2) and (4.4), $\pi(m,M) > 0$ if

$$\pi(1,1)\left(1-\sum\frac{1}{p_i}-\frac{1}{q}\right) - q^3\left(1-\frac{3}{q}\right)\left(1+\frac{1}{\sqrt{q}}\right) - 4q^3\left(1-\frac{1}{q}\right)\sum\left(1-\frac{1}{p_i}\right) \geq 0, \tag{5.21}$$

i.e. if

$$\pi(1,1) \geq \frac{q^3\big((1+4s) - \frac{3+4s}{q} - 4\big(1-\frac{1}{q}\big)\sum \frac{1}{p_i}\big) + q^{5/2}\big(1-\frac{3}{q}\big)}{1-\sum \frac{1}{p_i} - \frac{1}{q}}, \tag{5.22}$$

and so, using Lemma 4.1, certainly if

$$q \geq \frac{(1+4s) - \frac{3+4s}{q} - 4\big(1-\frac{1}{q}\big)\sum \frac{1}{p_i} + \frac{1}{\sqrt{q}}\big(1-\frac{3}{q}\big)}{1-\sum \frac{1}{p_i} - \frac{1}{q}} + 4\left(1-\frac{1}{q}\right) + \frac{1}{q^3}. \tag{5.23}$$

This completes the proof.

Observe that the inequalities of Lemma 5.8 are meaningful only when the denominator $1 - \sum 1/p_i - 3/q$ is greater than 0; in particular it is necessary to have $\sum 1/p_i < 1$. Note that, taking $\{p_1, p_2, p_3, \dots\}$ to be the odd primes $\{3, 5, 7, \dots\}$, we have $\sum_{i=1}^{s} 1/p_i > 1$ for $s \geq 9$. Hence this approach is practical only for those q for which m has fewer than 9 distinct prime factors. All prime powers q which are congruent to 1 modulo 4 and less than 6217 have $s < 9$; in fact, with the exception of $q = 2309$ and $q = 5813$ ($s = 7$) and $q = 4217$ and $q = 6089$ ($s = 8$), all have $s \leq 6$. Note that $s \geq 2$ for all relevant q in this case. All prime powers $q \equiv 3 \pmod 4$ such that $q \leq 2659$ have $s \leq 6$. There are 2 values of q with $s = 1$, $q = 3$ and $q = 7$; however the $q = 3$ case has already been dealt with.

PROPOSITION 5.9. *Let $q \equiv 1 \pmod 4$, $q \leq 6197$, $q \notin \{9, 13, 17, 29\}$. Then $(q, 4)$ is a PFNT-pair.*

Proof. First, observe that $\sum 1/p_i \geq 2/q$, since

$$\sum \frac{1}{p_i} \geq \frac{2}{q+1} + \frac{2}{q^2+1} = 2\left(\frac{1}{q} + \frac{q-1}{q(q+1)(q^2+1)}\right).$$

If we use this lower bound in Lemma 5.8, the desired result holds if

$$q \geq \frac{(3+4s) - \frac{19+4s}{q} + \frac{8}{q^2} + \frac{3}{\sqrt{q}} - \frac{11}{q^{3/2}}}{1 - \sum \frac{1}{p_i} - \frac{3}{q}} + 4\left(1 - \frac{1}{q}\right) + \frac{1}{q^3}. \tag{5.24}$$

An upper bound is required for $\sum 1/p_i$, say $\sum 1/p_i \leq K(q)$ for some function K. In general, to simplify calculations, the crude estimate

$$\sum_{i=1}^{s} \frac{1}{p_i} \leq \sum_{j=1}^{s} \frac{1}{p[j+1]} \tag{5.25}$$

will be used, where $p[n]$ is the nth prime ($n \in \mathbb{N}$). (More precise values may be taken in specific cases.)

Observe that the desired result certainly holds when

$$q \geq \frac{(3+4s) + \frac{3}{\sqrt{q}} + \frac{8}{q^2}}{1 - \sum \frac{1}{p[i]} - \frac{3}{q}} + 4 + \frac{1}{q^3}, \tag{5.26}$$

and, for fixed s, the function of q on the right side of (5.26) clearly decreases as q increases. Hence to prove for a given s that the result is true for $q \geq q_0$, with some $q_0 \in \mathbb{N}$, it is sufficient to show that inequality (5.26) holds for $q = q_0$. (Observe that for individual q, the more precise inequality (5.24) is to be preferred.)

The smallest prime power $q \equiv 1 \pmod 4$ with $s = 6$ is $q = 853$. The basic estimate (5.25) yields

$$\sum \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} < 0.90285;$$

inequality (5.26) holds for $q = 853$ (right-hand side of (5.26) equals 293.46) and hence for all $q \geq 853$. In the $s = 5$ case, the smallest relevant q is $q = 173$; taking

$$\sum \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} < 0.84403$$

shows that the result holds for $q = 173$ ($173 > 171.56$) and thus for all $q \geq 173$. The first values of q for which $s = 4$ are $q = 73, 89, 109, 113, \ldots$; however the smallest of these q for which inequality (5.26) holds in view of

$$\sum \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} < 0.76710$$

is $q = 109$ ($109 > 97.92$). Clearly a more precise estimate is required for $\sum 1/p_i$ than that of equation (5.25). For $q = 73$, the prime factors of m are $\{5, 13, 37, 41\}$; the use of the exact value

$$\sum \frac{1}{p_i} = \frac{1}{5} + \frac{1}{13} + \frac{1}{37} + \frac{1}{41} < 0.32835$$

yields inequality (5.24) (with the right side equal to 33.85). For $q = 89$, m has prime factors $\{3, 5, 17, 233\}$ and, using the exact value of $\sum 1/p_i$, we find that the right side of inequality (5.24) has value 55.10. So the result holds in all cases when $s = 4$.

When $s = 3$, inequality (5.26) holds with approximation (5.25) for $q \geq 61$, i.e. for all prime powers $q \equiv 1 \pmod 4$ with the exception of $q \in \{13, 17, 29, 37, 41, 53\}$. The use of exact values of $\sum 1/p_i$ in (5.24) proves the result for $q = 53$ (primes $\{3, 5, 281\}$ divide m), $q = 41$ (primes $\{3, 7, 29\}$) and $q = 37$ (primes $\{5, 19, 137\}$). For the remaining 3 values of q, even the use of exact values in inequality (5.14) fails; clearly another approach is required here.

For $s = 2$, inequality (5.26) with estimate (5.25) holds for all $q \geq 35$, leaving only the exceptions $q = \{9, 25\}$. Use of the exact value $\sum 1/p_i = 1/13 + 1/313 < 0.08012$ establishes the result for $q = 25$. However, for $q = 9$ (primes $\{5, 41\}$), even the use of exact values in inequality (5.14) fails ($9 < 22.30$).

Lastly, consider the 4 values of q less than 6217 with $s > 6$. When $s = 7$, use of the estimate

$$\sum \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} < 0.95548$$

in inequality (5.26) shows that the result holds for $q = 2309$ (right side of inequality has value 722.69) and hence for $q = 5813$ also. For $s = 8$, exact values are required. For $q = 4217$ (prime factors of m are $\{3, 5, 13, 19, 29, 37, 53, 89\}$), $\sum 1/p_i < 0.75451$, and the right side of inequality (5.24) takes value $147.12 < 4217$. For $q = 6089$ (primes $\{3, 5, 7, 13, 29, 61, 97, 241\}$), use of the exact value $\sum 1/p_i < 0.81845$ yields the result (right side < 194).

Hence the desired result has been established for all $q \equiv 1 \pmod 4$ with the exception of $q \in \{9, 13, 17, 29\}$.

PROPOSITION 5.10. *Let* $q \equiv 3 \pmod 4$, $q \leq 2659$, $q \notin \{7, 11, 23, 47, 83\}$. *Then* $(q, 4)$ *is a PFNT-pair.*

Proof. First observe that, except in the case when $s = 1$ ($q = 7$) (which will be treated separately), $\sum 1/p_i > 4/q - 2/q^2$, since

$$\sum \frac{1}{p_i} \geq \frac{2}{q^2+1} + \frac{4}{q+1} = \frac{4}{q} - \frac{2}{q^2} + \frac{2}{q^2}\left(\frac{2q^2 - q + 1}{(q+1)(q^2+1)}\right).$$

So $4(1 - 1/q)\sum 1/p_i$ may be replaced by $16/q - 24/q^2 + 8/q^3$; then clearly $\pi(m, M) > 0$ whenever

$$q \geq \frac{(1+4s) - \frac{19+4s}{q} + \frac{24}{q^2} + \frac{1}{\sqrt{q}} - \frac{3}{q^{3/2}}}{1 - \sum \frac{1}{p_i} - \frac{1}{q}} + 4\left(1 - \frac{1}{q}\right) + \frac{1}{q^3}. \tag{5.27}$$

A sufficient condition with an obviously decreasing function on the right-hand side is given by: $\pi(m, M) > 0$ whenever

$$q \geq \frac{(1+4s) + \frac{1}{\sqrt{q}} + \frac{24}{q^2}}{1 - \sum \frac{1}{p_i} - \frac{1}{q}} + 4 + \frac{1}{q^3}. \tag{5.28}$$

As in the proof of Proposition 5.9, the $\sum 1/p_i$ term in the denominator will usually be replaced by the upper bound given by inequality (5.25). Once again, to prove for a given s that the result is true for $q \geq q_0$, it is sufficient to prove that inequality (5.28) holds for $q = q_0$.

When $s = 6$, the smallest relevant q is 659. Use of the estimate

$$\sum \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} < 0.90285$$

in inequality (5.28) proves the desired result for $q = 659$ ($659 > 286.74$) and thus for all $q \geq 659$.

The smallest prime powers $q \equiv 3 \pmod 4$ with $s = 5$ are $\{83, 307, 419, \ldots\}$; however the first such q for which inequality (5.28) holds with approximation (5.25) is $q = 307$. To deal with $q = 83$, more precise estimates are required. The prime factors of m when $q = 83$ are $\{3, 5, 7, 13, 53\}$; however, even using the exact value

$$\sum \frac{1}{p_i} = \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{13} + \frac{1}{53} < 0.77198$$

in inequality (5.15) is insufficient to prove the result ($83 < 86.27$).

For $s = 4$, the first few $q \equiv 3 \pmod 4$ are $\{47, 167, 179, \ldots\}$; inequality (5.28) holds with the approximation

$$\sum \frac{1}{p_i} \leq \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} < 0.76710$$

for all such q except for $q = 47$ ($47 < 81.42$). For $q = 47$ (primes dividing $m = \{3, 5, 13, 17\}$), use of the exact value

$$\sum \frac{1}{p_i} = \frac{1}{3} + \frac{1}{5} + \frac{1}{13} + \frac{1}{17} < 0.66908$$

in inequality (5.15) just fails ($47 < 49.49$).

When $s = 3$, inequality (5.27) holds with approximation (5.25) for values of $q \geq 48$; since the first few q with $s = 3$ are $\{23, 27, 43, 59, \ldots\}$, this leaves $q = \{23, 27, 43\}$ still to be dealt with. Use of exact values of $\sum 1/p_i$ in inequality (5.27) proves the result for $q = 43$ (primes $\{5, 11, 37\}$ divide m) and $q = 27$ (primes $\{5, 7, 73\}$). However, for $q = 23$ (primes $\{3, 5, 53\}$), even use of the exact value

$$\sum \frac{1}{p_i} = \frac{1}{3} + \frac{1}{5} + \frac{1}{53} < 0.55221$$

in inequality (5.15) fails ($23 < 29.59$).

When $s = 2$ the first few values of q are $\{11, 19, 31, 71, \ldots\}$; inequality (5.28) with estimate (5.25) holds for all except $q = \{11, 19\}$. For $q = 19$

(primes $\{5, 181\}$), use of the exact value $1/5 + 1/181 < 0.20553$ in (5.27) establishes the result; however for $q = 11$ (primes $\{3, 61\}$), even use of exact values in (5.15) fails ($11 < 16.06$).

Returning to the $s = 1$ case mentioned earlier, the only prime power $q \equiv 3 \pmod 4$, $q > 3$, with $s = 1$ is $q = 7$ ($m = 25$). If we set $1/p_i = 1/5$ in inequality (5.15), the inequality fails ($7 < 8.86$), suggesting that another approach is appropriate in this case.

Thus the result has been established for all prime powers $q \equiv 3 \pmod 4$ with the exception of $q \in \{7, 11, 23, 47, 83\}$.

6. The proof for some special prime powers. In this section, we employ various devices to prove the result for odd q by theoretical means in as many cases as possible.

6.1. *The case when* $\frac{1}{2}(q^2+1)$ *is prime.* The following simplification applies for odd q whenever $(q^2 + 1)/2$ is prime.

LEMMA 6.1. *Let q be an odd prime power. Suppose that $m_0 := (q^2 + 1)/2$ is prime. Then*

$$N(m, x^4 - 1) = N(m/m_0, x^4 - 1).$$

In particular, $N(m, x^4 - 1) = N((q + 1)/2, x^4 - 1)$ if $q \equiv 1 \pmod 4$.

Proof. Suppose $\alpha \in E$ is both m/m_0-free and $x^4 - 1$-free, but $\alpha = \beta^{m_0}$. Then $\alpha^2 \in \mathrm{GF}(q^2)$, whence $\alpha^{q^2} = \gamma\alpha$, where $\gamma^2 = 1$, $\gamma \in \mathrm{GF}(q^2)$. However, this means that either $(x^2 - 1)^\sigma(\alpha) = 0$ or $(x^2 + 1)^\sigma(\alpha) = 0$, in both cases contradicting the fact that α is $x^4 - 1$-free.

Applying Lemma 6.1 establishes the result for $q = 29$ (primes $\{3, 5, 421\}$); using inequality (5.14), $29 > 28.01$. Note incidentally that in the case $q = 9$, we may replace $N(5 \cdot 41, M)$ by $N(5, M)$.

6.2. *The case when* $15 \mid m$. In this section, we increase the precision of the sieve in a special case, namely when $15 \mid m$.

In the original derivation of the sieving inequality (see [3] for details), the following (fairly crude) estimate is used: if p_1 and p_2 are primes dividing m, then the number of elements of E which are "either p_1-free or p_2-free" is bounded above by $N(1, 1)$. However, it is clear that this upper bound can be replaced by $N(1, 1) - R(p_1p_2)$ where $R(p_1p_2)$ is the set of p_1p_2th powers in E. Thus the sieving inequality may be adjusted by the addition of a $R(p_1p_2)$ term to the right-hand side. This approach may of course be generalised to more than one pair of primes; however for our purposes it suffices to consider the pair of primes $p_1 = 3$, $p_2 = 5$.

LEMMA 6.2. *Let $q \equiv 3 \pmod 4$ be a prime power such that $15 \mid m$. Then $(q,4)$ is a PFNT-pair if*

$$q \ge \frac{\left(4s-\frac{3}{5}\right) - \frac{4s+7/5}{q} - 4\left(1-\frac{1}{q}\right)\sum_{i=3}^{s}\frac{1}{p_i} + \frac{1}{\sqrt{q}}\left(1-\frac{3}{q}\right)}{\frac{8}{15} - \sum_{i=3}^{s}\frac{1}{p_i} - \frac{1}{q}} + 4\left(1-\frac{1}{q}\right) + \frac{1}{q^3}. \tag{6.1}$$

Proof. Denote by $R(r)$ the set of rth powers in E ($r \in \mathbb{N}$), and here set $\varrho(r) := q(q-1)R(r)$. A more precise sieving inequality than that of Lemma 5.1 is given by the following:

$$\begin{aligned}\pi(m,M) &\ge \pi(3,1) + \pi(5,1) + \sum_{i=3}^{s}\pi(p_i,1) + \varrho(15) + \pi(x+1) - s\pi(1,1)\\ &= [\pi(3,1) - \theta(3)\pi(1,1)] + [\pi(5,1) - \theta(5)\pi(1,1)]\\ &\quad + \sum_i [\pi(p_i,1) - \theta(p_i)\pi(1,1)] + \left[\varrho(15) - \frac{1}{15}\,\pi(1,1)\right]\\ &\quad + [\pi(1,x+1) - \theta(x+1)\pi(1,1)] + \left[\frac{8}{15} - \sum_{i=3}^{s}\frac{1}{p_i} - \frac{1}{q}\right]\pi(1,1).\end{aligned}$$

Using the bounds of Katz, each character sum involving a cubic character occurs with coefficient $-1/3 + 1/15 = -4/15$ in the above, and so the contribution to the total from cubic characters is bounded absolutely by $\frac{8}{15}\cdot 4q(q-1)$, rather than $\frac{2}{3}\cdot 4q(q-1)$ as previously. Similarly, the contribution from quintic sums is also bounded by $\frac{8}{15}\cdot 4q(q-1)$, and sums involving characters of order 15 contribute another $\frac{8}{15}\cdot 4q(q-10)$ term. Hence the bounds contributed by

$$|\pi(3,1) - \theta(3)\pi(1,1)| + |\pi(5,1) - \theta(5)\pi(1,1)| + \left|\varrho(15) - \tfrac{1}{15}\pi(1,1)\right|$$

are $\frac{24}{15}\cdot 4q(q-1)q^3$, instead of $\frac{22}{15}\cdot 4q(q-1)q^3$. Then we may replace (5.15) by

$$q \ge \frac{\left(4s-\frac{3}{5}\right) - \frac{4s+7/5}{q} - 4\left(1-\frac{1}{q}\right)\sum_{i=3}^{s}\frac{1}{p_i} + \frac{1}{\sqrt{q}}\left(1-\frac{3}{q}\right)}{\frac{8}{15} - \sum_{i=3}^{s}\frac{1}{p_i} - \frac{1}{q}} + 4\left(1-\frac{1}{q}\right) + \frac{1}{q^3}. \tag{6.2}$$

By means of this lemma, the result is established for $q = 83$ ($83 > 68.44$) and $q = 47$ ($47 > 42.80$).

6.3. *The use of the Cohen bound.* When q is small, it is preferable in some cases to use the bounds of Cohen ([3]) to estimate integer factors rather than those of Katz ([8]).

LEMMA 6.3. *Let $q \equiv 3 \pmod 4$ be a prime power. Then $(q,4)$ is a PFNT-pair if*

$$q \geq \frac{\left(1+\frac{2s-3}{q}\right)+\sqrt{q}\left(s-\frac{3s-1}{q}-\frac{3}{q^2}\right)-\sqrt{q}\left(\sum\frac{1}{p_i}\right)\left(1-\frac{3}{q}+\frac{2}{q^{3/2}}\right)}{1-\sum\frac{1}{p_i}-\frac{1}{q}} + \sqrt{q}\left(1-\frac{3}{q}\right). \tag{6.3}$$

Proof. Analogous to the proof of Proposition 5.10, but with the bounds of [8] replaced by those of [3] to estimate integer factors. Hence $4(1-1/q)$ is replaced by $\sqrt{q}\,(1-(e+1)/q+e/q^{3/2})$ (this latter bound may be derived from Theorem 3.2 of [3]), and Katz's bound $|\pi(1,1)-(q^4-1)| < 4(1-1/q)q^3$ is replaced by Cohen's bound $|\pi(1,1)-q^4| \leq q^{7/2}(1-(e+1)/q)$.

Through this lemma, the result is established for $q = 7$ ($7 > 3.39$) and $q = 11$ ($11 > 5.46$).

6.4. *The case when $q = 9$.* In order to establish the result in the case when $q = 9$, we derive more precise versions of the bounds in Sections 3 and 4 for this special case. Write $q = q_0^2$, so that $q_0 = 3$. Consider the expression for S_2 given by equation (3.6). Since, for $\nu \in \widehat{F}^*$ occurring in the sum, $\operatorname{ord}\nu = 4 = q_0+1$, Stickelberger's Theorem (see [10, Theorem 5.16]) applies to give $G_1(\nu_4)$ $(= G_1(\overline{\nu}_4)) = -3$ (where ν_4 denotes one of the two characters of order 4). Hence

$$S_2 = -8 \cdot 81(\nu_4(1/b)+\overline{\nu}_4(1/b)) = 0,$$

since b is a non-square and so $\nu_4(1/b) = \pm i$. Thus the bound of inequality (3.9) may be replaced, for $q = 9$, by

$$\left|\pi(1,x+1)-\left(1-\frac{1}{q}\right)\pi(1,1)\right| \leq \frac{1}{q}\,|S_1| \leq \frac{16}{3}\,q^2. \tag{6.4}$$

Next, consider S_2 as defined in equation (3.12). Again, $G_1^4(\nu_4) = 81$, while

$$1+J_1(\nu_2,\overline{\nu}_2) = 1+\frac{G_1(\nu_2)G_1(\overline{\nu}_4)}{G_1(\nu_2\overline{\nu}_4)} = 1+\frac{G_1(\nu_2)G_1(\overline{\nu}_4)}{G_1(\nu_4)} = 1+G_1(\nu_2) = 4 \tag{6.5}$$

since $G_1(\nu_4) = G_1(\overline{\nu}_4) = -3$, as before. So

$$S_2 = q^2(q-1)+4\cdot 81(\nu_4(1/b)+\overline{\nu}_4(1/b)) = q^2(q-1).$$

Hence

$$|\pi(1,L_1)+\pi(1,L_2)-2(1-1/q)\pi(1,1)-2(1-1/q)q^2| \leq \frac{2}{q}\,|S_1| = \frac{32}{3}\,q^2. \tag{6.6}$$

For the multiplicative part of the sieve, we employ the Cohen bound in preference to the Katz bound; then

$$|\pi(1,1)-q^4| \leq 12q^2 \tag{6.7}$$

and

$$\left|\pi(5,1) - \tfrac{4}{5}\,\pi(1,1)\right| \le \tfrac{4}{5}\cdot 16q^2. \tag{6.8}$$

Applying the sieve in the form (5.4) with the bounds derived above yields the following (recall that, by Lemma 6.1, we may take $m = 5$):

$$\begin{aligned}\pi(5,M) &\ge q^2\left\{\left(1-\frac{1}{5}-\frac{3}{q}\right)(q^2-12) - \left(\frac{64}{5}+\frac{16}{3}+\frac{32}{3}\right) + 2\left(1-\frac{1}{q}\right)\right\}\\ &= q^2\left(\frac{7}{15}\cdot 69 - \frac{144}{5} + \frac{16}{9}\right) \ge 5.178q^2 > 0.\end{aligned}$$

6.5. *The case when direct computation is required.* To deal with the remaining cases ($q = 13$, 17 and 23), we use the computer package MAPLE (version 6). The field E is searched explicitly for elements satisfying the PFNT problem; in all cases, the desired result holds without exception.

As an illustration, we display the relevant quartic polynomials for the smallest case, i.e. when $q = 13$. The following simplification shows that 12 polynomials will suffice (compared to the expected $12 \cdot \phi(12) = 48$).

LEMMA 6.4. *Let $q = 13$. Suppose that there exist free, primitive $\alpha \in E$ such that $\mathrm{Tr}_{E/F}(\alpha) = a$ and $N_{E/F}(\alpha) = b$ for all pairs (a,b) where $a \in \{1,2,4\}$ and $b \in \{2,6,7,11\}$. Then there exist free, primitive $\alpha \in E$ such that $\mathrm{Tr}_{E/F}(\alpha) = a$ and $N_{E/F}(\alpha) = b$ for all pairs (a,b) where a is a non-zero element of F and b is a primitive element of F.*

Proof. The result follows upon observing that $F^* = \{j, 2j, 4j : j \in F, j^4 = 1\}$, and that $\mathrm{Tr}_{E/F}(j\gamma) = j\mathrm{Tr}_{E/F}(\gamma)$, $N_{E/F}(j\gamma) = j^4 N_{E/F}(\gamma)$ for all $\gamma \in E$, $j \in F$.

The following table lists twelve quartic polynomials over $F = \mathrm{GF}(13)$ whose roots $\alpha \in E = \mathrm{GF}(13^4)$ are primitive and free with norm and trace equal to b and a respectively.

$(a,\ b)$	Relevant PFNT quartic
$(1,2)$	$x^4 - x^3 + 3x^2 + 2$
$(1,6)$	$x^4 - x^3 + 11x^2 - 10x + 6$
$(1,7)$	$x^4 - x^3 + 10x^2 - 6x + 7$
$(1,11)$	$x^4 - x^3 + 5x^2 - 4x + 11$
$(2,2)$	$x^4 - 2x^3 + x^2 - 11x + 2$
$(2,6)$	$x^4 - 2x^3 + 8x^2 - 2x + 6$

$(a,\ b)$	Relevant PFNT quartic
$(2,7)$	$x^4 - 2x^3 + 11x^2 - 9x + 7$
$(2,11)$	$x^4 - 2x^3 - x + 11$
$(4,2)$	$x^4 - 4x^3 + 8x^2 - 10x + 2$
$(4,6)$	$x^4 - 4x^3 + 9x^2 - 11x + 6$
$(4,7)$	$x^4 - 4x^3 + 6x^2 + 7$
$(4,11)$	$x^4 - 4x^3 + 4x^2 - 7x + 11$

7. The non-zero PNT problem for fields of even order. Recall that, in the case when $\mathrm{char}\, F = 2$, the PFNT problem reduces to the non-zero PNT problem. Hence, to establish the result, it suffices to show that $\pi(m,1) > 0$.

The following simplification applies in the case when q^2+1 is prime.

LEMMA 7.1. *Let $q = 2^k$, $k \in \mathbb{N}$. Suppose that q^2+1 is prime. Then*

$$N(m,1) = N(q+1,1),$$

where $N(t,1)$ $(t \mid m)$ is the number of t-free elements of E with trace and norm equal to a and b respectively $(a, b \in F,\ a \neq 0,\ b$ primitive$)$.

Proof. In this case, $m = (q+1)(q^2+1)$. Suppose that $\alpha \in E$ is $q+1$-free, with $\mathrm{Tr}(\alpha) = a$, $N(\alpha) = b$, but $\alpha = \beta^{q^2+1}$. Then $\alpha \in \mathrm{GF}(q^2)$, i.e. $\alpha^{q^2} = \alpha$. Hence, $\mathrm{Tr}_{E/F}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \alpha^{q^3} = 2(\alpha + \alpha^q)$, which equals 0 since $\mathrm{char}\, F = 2$—a contradiction as $a \neq 0$.

PROPOSITION 7.2. *Suppose $q = 2^k$ $(k \in \mathbb{N},\ k \neq 3, 5)$. Then $(q,4)$ is a PFNT-pair.*

Proof. We may assume that either $k = 2$, $k = 4$ or $k \geq 6$.

As a first step, apply the bounds of Lemma 4.1 and Corollary 4.3 directly, without sieving. Then

$$\pi(m,1) \geq \theta(m)\{(q^4-1) - 4(1-1/q)q^3\} - 4\theta(m)(W(m)-1)(1-1/q)q^3,$$

and so $\pi(m,1) > 0$ whenever

$$q > 4W(m)(1-1/q) + 1/q^3. \tag{7.1}$$

Using the approximation of Lemma 5.5 for $W(m)$, $(q,4)$ is a PFNT-pair whenever

$$q > 4c_m(q-1)^{3/4} + 1/q^3, \tag{7.2}$$

where $c_m = 2.9$. This inequality holds for integers $q \geq 18106$, and so establishes the result for $q = 2^k$, $k \geq 15$.

To deal with the smaller powers, apply the sieve with atomic divisors. Let $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$. For all $q = 2^k$ with $2 \leq k \leq 14$, $s \leq 6$. Using the results of Corollary 4.3 shows that $\pi(m,1) > 0$ whenever

$$\pi(1,1)\left\{1 - \sum \frac{1}{p_i}\right\} - 4\left(1 - \frac{1}{q}\right)q^3 \sum \left(1 - \frac{1}{p_i}\right) > 0.$$

By Lemma 4.1, $\pi(m,1) > 0$ if

$$q > 4\left(1 - \frac{1}{q}\right)\left(1 + \frac{\sum\left(1 - \frac{1}{p_i}\right)}{1 - \sum \frac{1}{p_i}}\right) + \frac{1}{q^3}. \tag{7.3}$$

The desired result certainly holds when

$$q > C_s, \quad \text{where} \quad C_s := 4\left(2 + \frac{s-1}{1 - \sum \frac{1}{p[i+1]}}\right) + \frac{1}{64}.$$

Clearly C_s is a constant for fixed s, and increases as s increases $(1 \leq s \leq 9)$. Since $C_6 < 213.9 < 2^8$, the result holds for $q = 2^k$, $k \geq 8$. The result is established for $k = 7$ $(s = 5)$ since $2^7 > 110.6 > C_5$; for $k = 6$ $(s = 4)$ since

$2^6 > 59.6 > C_4$; and for $k = 4$ ($s = 2$) using exact values in inequality (7.3) ($m = 17 \cdot 257$, $2^4 > 11.51$).

By Lemma 7.1, when $q = 4$ we may replace $N(5 \cdot 17, 1)$ by $N(5, 1)$. Using the bounds of Cohen, we find that generally

$$\begin{aligned}\pi(m,1) &\geq \theta(m)\pi(1,1) - q^{7/2}(1 - 2/q + 1/q^{3/2})\theta(m)(W(m) - 1)\\ &\geq \theta(m)(q^4 - q^{7/2}(1 - 2/q) - q^{7/2}(1 - 2/q + 1/q^{3/2})(W(m) - 1)).\end{aligned}$$

Hence, in the case when $q = 4$,

$$\pi(5,1) \geq \frac{4}{5}\left(4^4 - 4^{7/2}\left(1 - \frac{1}{2}\right) - 4^{7/2}\left(1 - \frac{1}{2} + \frac{1}{4^{3/2}}\right)\right) = \frac{2^9}{5}\left(2 - \frac{9}{8}\right) > 0,$$

and this establishes the desired result.

7.1. *Computational strategy for remaining cases.* To deal with the remaining cases ($q = 8$ and 32), we use the computer package MAPLE (version 6) to search the field E for m-free elements with norms and traces equal to the required values. The following lemma allows us to simplify our computational strategy.

LEMMA 7.3. *Let $q = 2^k$ be such that $q - 1$ is a Mersenne prime. Let $a, b \in F$ ($a \neq 0$, b primitive) be given. Denote by $Z_{\alpha,\beta}(m)$ the number of elements $w \in E$ which are m-free and have $\mathrm{Tr}_{E/F}(w) = \alpha$, $N_{E/F}(w) = \beta$ ($\alpha, \beta \in F$). Suppose*

$$Z_{1,b}(m) > 0 \quad \forall b \in F^*.$$

Then $(q, 4)$ is a PNT-pair.

Proof. To prove that $(q, 4)$ is a PNT-pair, we must show that $N(m, 1) > 0$, i.e. that $Z_{a,b}(m) > 0$ for all $a, b \in F$, $a \neq 0$, $b \neq 0, 1$. We prove the (stronger) result

$$Z_{a,b}(m) > 0 \quad \forall a, b \in F^*.$$

If $a = 1$, there is nothing to prove. Otherwise, set $b^* := b/a^4 \in F^*$. Since $Z_{1,b^*}(m) > 0$, there exists an element $\zeta \in E$ such that ζ is m-free, $\mathrm{Tr}_{E/F}(\zeta) = 1$, and $N_{E/F}(\zeta) = b^*$. Then $\alpha := a\zeta$ is also m-free, and has $\mathrm{Tr}_{E/F}(\alpha) = a$ and $N_{E/F}(\alpha) = b$.

The use of Lemma 7.3 reduces the number of necessary tests from $(q - 1)(q - 2)$ (testing each pair (a, b), b primitive) to $q - 1$ (testing each pair $(1, b)$, b non-zero). This improves economy and speed of computation. In both cases, the desired result holds without exception.

References

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

[2] L. Carlitz, *Some problems involving primitive roots in a finite field*, Proc. Nat. Acad. Sci. U.S.A. 38 (1952), 314–318, 618.
[3] S. D. Cohen, *Gauss sums and a sieve for generators of Galois fields*, Publ. Math. Debrecen 56 (2000), 293–312.
[4] S. D. Cohen and D. Hachenberger, *Primitive normal bases with prescribed trace*, Appl. Algebra Engrg. Comm. Comput. 9 (1999), 383–403.
[5] —, —, *Primitivity*, *freeness*, *norm and trace*, Discrete Math. 214 (2000), 135–144.
[6] S. D. Cohen and S. Huczynska, *The primitive normal basis theorem—without a computer*, J. London Math. Soc. 67 (2003), 41–56.
[7] H. Davenport, *Bases for finite fields*, ibid. 43 (1968), 21–39; 44 (1969), 378.
[8] N. M. Katz, *Estimates for Soto–Andrade sums*, J. Reine Angew. Math. 438 (1993), 143–161.
[9] H. W. Lenstra, Jr. and R. J. Schoof, *Primitive normal bases for finite fields*, Math. Comput. 48 (1987), 217–231.
[10] R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA, 1983; 2nd ed.: Cambridge Univ. Press, Cambridge, 1997.

Department of Mathematics
University of Glasgow
Glasgow G12 8QW, Scotland
E-mail: sdc@maths.gla.ac.uk
sh@maths.gla.ac.uk

Received on 18.6.2002
and in revised form on 3.1.2003 (4311)