ACTA ARITHMETICA
143.4 (2010)

The strong primitive normal basis theorem

by

Stephen D. Cohen (Glasgow) and Sophie Huczynska (St Andrews)

1. Introduction. Given q, a power of a prime p, denote by F the finite field $\mathrm{GF}(q)$ of order q, and 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. The classical form of this result, *the normal basis theorem*, is stated as follows:

Theorem 1.1 (Normal Basis Theorem). *There exists an element $\alpha \in E$ (an additive generator) whose conjugates $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ form a basis of E over F.*

Such an element α is a *free* (or *normal*) *element* of E over F, and a basis of this kind is a *normal basis* over F. The key existence result linking additive and multiplicative structure is *the primitive normal basis theorem*:

Theorem 1.2 (Primitive Normal Basis Theorem). *For every prime power q and $n \in \mathbb{N}$, there exists $\alpha \in E$ simultaneously primitive and free over F. Equivalently, there exists a primitive normal basis of E over F all of whose members are primitive and free.*

Existence of such a basis for every extension was first proved by Lenstra and Schoof [7], completing work by Carlitz [1], [2], and Davenport [6]. A computer-free proof of this result was produced by Cohen and Huczynska [5]. The key to the transition to the more theoretical and less computational approach realised in [5] was the introduction of sieving techniques (cf. Section 4 below). The question arises as to whether a yet stronger existence theorem concerning primitive and free elements can be proved unconditionally (or with very few exceptions) by means of such techniques. In this paper, we consider the following natural problem, first suggested to us by Robin J. Chapman (Exeter) (to whom we are grateful).

2010 *Mathematics Subject Classification*: Primary 11T30; Secondary 11T06, 12E20.
Key words and phrases: finite field extension, primitive element, normal basis.

DOI: 10.4064/aa143-4-1

Problem 1.3 (PFF problem). *Given a finite extension E/F of Galois fields, does there exist a primitive element α of E, free over F, such that its reciprocal $\alpha^{-1} \in E$ is also primitive and free over F? If so, then the pair (q, n) corresponding to E/F is called a* PFF pair.

Observe that, for $\alpha \in E$, α is a primitive element of E if and only if α^{-1} is primitive; hence the four conditions in Problem 1.3 effectively reduce to three (α *p*rimitive and *f*ree, α^{-1} *f*ree).

In this paper, we solve this problem completely: the answer is in the affirmative except for a small number of listed exceptions. We obtain the following strengthening of the primitive normal basis theorem.

Theorem 1.4 (Strong Primitive Normal Basis Theorem). *For every prime power q and $n \in \mathbb{N}$, there exists a primitive element α of E, free over F, such that its reciprocal $\alpha^{-1} \in E$ is also primitive and free over F unless the pair (q, n) is one of*

$$(2,3),\ (2,4),\ (3,4),\ (4,3),\ (5,4).$$

Towards Theorem 1.4, Tian and Qi [9] have given a proof for the case $n \geq 32$ (when there are no exceptions). They use an elaboration of the method of Lenstra and Schoof [7] but do not employ any of the sieving techniques that are a feature of the present article and appear to be necessary for completion, particularly for small values of n. Moreover, because of the demanding nature of the PFF condition, fields of smallest cardinality require individual treatment. Our consideration of the general problem therefore takes place in the setting where $q \geq 5$ (even here, special care is needed for $q = 5$ and 7), and we deal with the case $2 \leq q \leq 4$ in Section 7 "Very small fields". In what follows, all non-trivial computation is performed using MAPLE (Version 10). Aside from the five genuine exceptions listed in Theorem 1.4, there are 35 pairs (q, n) (with $q \leq 13$, $n \leq 16$) for which verification is by direct construction of a PFF polynomial; otherwise, the proof is purely theoretical.

2. Reductions.

In this section, we formulate the basic theory and perform some reductions to the problem. As much as possible, we aim to make this account self-contained.

We begin by extending the notions of primitivity and freeness. Let $w \in E^*$. Then w is a primitive element of E if and only if w has multiplicative order $q^n - 1$, i.e., $w = v^d$ ($w \in E$) implies $(d, q^n - 1) = 1$. We extend this concept as follows: for any divisor m of $q^n - 1$, we say that $w \in E^*$ is *m-free* if $w = v^d$ (where $v \in E$ and $d \mid m$) implies $d = 1$. Thus $w \in E^*$ is m-free if and only if w is an lth power for no prime l dividing m. It follows that w is m-free if and only if it is m_0-free, where m_0 is the *radical* of m, i.e., the product of its distinct prime factors. In the context of the PFF problem, observe that w is m-free if and only if w^{-1} is m-free since, if $w^{-1} = v^k$ for some $k \mid m$ and $v \in E^*$, then $w = (v^{-1})^k$ and $v^{-1} \in E^*$.

For $w \in E$, the F-*order* of w is defined to be the monic divisor g (over F) of $x^n - 1$ of minimal degree such that $g^\sigma(w) = 0$ (g^σ is the polynomial obtained from g by replacing each x^i with x^{q^i}). Clearly, w is free if and only if the F-order of w is $x^n - 1$. If $w \in E$ has F-order g, then $w = h^\sigma(v)$ for some $v \in E$, where $h = (x^n - 1)/g$. Let M be an F-divisor of $x^n - 1$. If $w = h^\sigma(v)$ (where $v \in E$ and h is an F-divisor of M) implies $h = 1$ we say that w is M-*free in* E. Again, M may be replaced by its radical. An important instance of this occurs when n is divisible by the characteristic p, say $n = p^b n^*$ (where $p \nmid n^*$), in which event w is $x^n - 1$-free if and only if it is $x^{n^*} - 1$-free. (The expansion of $n = p^b n^*$, as above, will be assumed throughout.)

We remark that, in the following, most arguments concerning divisors of a given integer divisor of $q^n - 1$, or polynomial divisors of a given factor of $x^n - 1$, depend only on the appropriate radicals so that the divisors may be assumed to be square-free. To avoid awkward qualifications to these arguments, the reader is requested throughout to interpret all relevant statements accordingly.

We make the following observation.

LEMMA 2.1. *Let $x^d - w$ be an F-divisor of $x^n - 1$ ($w \in F^*$, $d \mid n$). Then, for $\alpha \in E^*$,*

$$(x^d - w)^\sigma(\alpha) = 0 \ \Leftrightarrow\ (x^d - w^{-1})^\sigma(\alpha^{-1}) = 0.$$

In particular, if $w \in E^*$ has F-order $x + 1$ or $x - 1$, then so does w^{-1}.

If $n = 2$ and $w \in E^*$ is primitive, then neither w nor w^{-1} can have F-order $x \pm 1$ and so both are free over F. Henceforth, we assume $n \geq 3$.

LEMMA 2.2. *Let n (≥ 5) be prime. Suppose that q is such that $p \nmid n$ and $q \pmod{n}$ is a multiplicative generator of the cyclic group $(\mathbb{Z}/n\mathbb{Z})^*$. Then (q, n) is a PFF pair.*

Proof. Under the given circumstances, $(n, q^i - 1)$ is 1 for $i = 1, \dots, n-2$, and n for $i = n - 1$; so $x^n - 1$ factorises into irreducibles over F as $(x - 1) \cdot (x^{n-1} + x^{n-2} + \dots + x + 1)$. By Theorem 1.1 of [4], there exists a primitive element $w \in E$ such that its trace over F, $T(w)$, is not 0, and similarly, $T(w^{-1}) \neq 0$, i.e. neither w nor w^{-1} has F-order $x^{n-1} + x^{n-2} + \dots + x + 1$. Since w is primitive, neither w nor w^{-1} can have F-order $x - 1$. ∎

Observe that Lemma 2.2 applies to $\phi(n-1)$ of the n possible congruence classes for values of q. The next result demonstrates the application of the lemma to some small values of n.

Lemma 2.3. *For the following values of q and n, the pair (q,n) is a PFF pair:*

(i) $n=5$; $q\equiv 2$ *or* $3 \pmod 5$.
(ii) $n=7$; $q\equiv 3$ *or* $5 \pmod 7$.
(iii) $n=11$; $q\equiv 2$, 6, 7 *or* $8 \pmod{11}$.

For any $m \mid q^n-1$, and $g,h \mid x^n-1$, denote by $N(m,g,h)$ the number of non-zero elements $w\in E$ such that w is m-free and g-free, and w^{-1} is h-free (note that w^{-1} is automatically m-free). As a consequence of the earlier discussion, we may replace m, g or h by their radicals at any time. To solve the PFF problem it would suffice to show that $N(q^n-1,x^n-1,x^n-1)$ is positive for every pair (q,n); however, it is useful to refine this requirement.

For a given pair (q,n), define $Q:=Q(q,n)$ to be (the radical of)

$$\frac{q^n-1}{(q-1)\gcd(n,q-1)}.$$

As in [7] and [4], we now demonstrate that q^n-1 may be replaced by Q, i.e. it suffices to show that $N(Q,x^n-1,x^n-1)$ is positive. The following lemma, analogous to Lemma 2.1 of [5], makes this relationship explicit.

Lemma 2.4. *For any pair (q,n),*

$$N(Q,x^n-1,x^n-1)=\frac{R}{\phi(R)}N(q^n-1,x^n-1,x^n-1),$$

where ϕ denotes Euler's function, and R is the greatest divisor of q^n-1 coprime to Q.

Proof. Let $Q^*:=(q^n-1)/R$. Then Q^* is the greatest divisor of q^n-1 whose prime factors are those of Q. Moreover, $Q\mid Q^*$, $R\mid (q-1)(n,q-1)\mid (q-1)^2$, and $(R,Q^*)=1$. In particular, if γ $(\in E^*)$ is an Rth root of unity, then $c:=\gamma^{q-1}\in F^*$, and $\gamma^{q^i}=c^i\gamma$ for every i. It follows that, if $\alpha\in E$ and γ is any Rth root of unity, then α is x^n-1-free if and only if $\gamma\alpha$ is x^n-1-free. Indeed, for any k, with $0\le k<n$,

$$\sum_{i=0}^{k} a_i(\gamma\alpha)^{q^i}=0 \;\Leftrightarrow\; \sum_{i=0}^{k} a_i c^i\alpha^{q^i}=0, \qquad a_0,\dots,a_k,\, c\in F.$$

Now, any element $\alpha\in E^*$ can be expressed uniquely as the product of a Q^*th root of unity α_0 and an Rth root of unity (in E^*). By the above, if α is Q-free and both α and α^{-1} are x^n-1-free, then $\gamma\alpha_0$ is also Q-free with $\gamma\alpha_0$ and its inverse both x^n-1-free, for any Rth root of unity γ. If in fact α is primitive, then $\alpha=\gamma\alpha_0$ for some primitive Rth root of unity, γ. ∎

The following result will prove useful.

Lemma 2.5.

(i) *Assume $n = 4$ and $q \equiv 3 \pmod 4$. Then $N(Q, x^4 - 1, x^4 - 1) = N(Q, x^2 - 1, x^2 - 1)$.*

(ii) *Assume $n = 3$ and $q \equiv 2 \pmod 3$. Then $N(Q, x^3 - 1, x^3 - 1) = N(Q, x - 1, x - 1)$.*

Proof. Take the case with $n = 4$, so that $x^2 + 1$ is irreducible over F. Suppose that α is Q-free and $x^2 - 1$-free and α^{-1} is $x^2 - 1$-free, but α is not $x^4 - 1$-free. Then $\alpha = \beta^{q^2} + \beta$, and hence $\alpha^{q^2} = \alpha$, i.e., $\alpha^{q^2-1} = 1$. This implies that $\alpha = \gamma^{q^2+1}$, an evident contradiction (because α is Q-free). The same argument ensures that α^{-1} is also $x^4 - 1$-free. The "$n = 3$" case is exactly analogous. ∎

3. An expression for $N(m, g, h)$. In this section, we employ character sums to obtain expressions, and thence estimates, for the number of elements of the desired type. We suppose throughout that $m \mid Q$ and $g, h \mid x^n - 1$, where, if desired, these can be assumed to be square-free. We begin by establishing characteristic functions for those subsets of E comprising elements that are m-free, g-free or h-free.

I. *The set of $w \in E^*$ that are m-free.* Let $\hat{E}^*$ ($\cong E^*$) denote the group of multiplicative characters of E^*. For any $d \mid Q$, we write η_d for a typical character in $\hat{E}^*$ of order d. Thus η_1 is the trivial character. Notice that, since $d \mid \frac{q^n-1}{q-1}$, the restriction of η_d to F^* is the trivial character ν_1 of $\hat{F}^*$.

We employ the following notation for weighted sums (cf. [5]). For $m \mid Q$, set

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

where ϕ and μ denote the functions of Euler and Möbius respectively and the inner sum runs through all $\phi(d)$ characters of order d. (Note that only square-free divisors d have any influence.) Then, according to a formula developed from one of Vinogradov, the characteristic function for the subset of m-free elements of E^* is

$$\theta(m) \int_{d|m} \eta_d(w), \qquad w \in E^*, \tag{3.1}$$

where

$$\theta(m) := \frac{\phi(m)}{m} = \prod_{l|m,\, l \text{ prime}} (1 - l^{-1}).$$

(In Vinogradov's original formula characterising primitive roots of a prime p, (3.1) holds with $m = p - 1$.)

II. *The set of $w \in E$ that are g-free or h-free over F.* Let λ be the canonical additive character of F. Thus, for $x \in F$,

$$\lambda(x) = \exp(2\pi i T_{F,\mathbb{F}_p}(x)/p),$$

where p is the characteristic of F and $T_{F,\mathbb{F}_p}$ denotes the trace function from F to $\mathbb{F}_p$.

Now let χ be the canonical additive character on E; it is simply the lift of λ to E, i.e., $\chi(w) = \lambda(T(w))$, $w \in E$. For any (monic) F-divisor D of $x^n - 1$, a typical character χ_D of F-order D is one such that $\chi_D \circ D^\sigma$ is the trivial character in E, and D is minimal (in terms of degree) with this property. For any $\delta \in E$, let χ_δ be the character defined by $\chi_\delta(w) = \chi(\delta w)$, $w \in E$. Define the subset Δ_D of E as the set of δ for which χ_δ has F-order D. So we may also write χ_{δ_D} for χ_D, where $\delta_D \in \Delta_D$; 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 $\Phi(D)$ characters χ_D, where Φ is the Euler function on $F[x]$ (Φ 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 **I**, for $g \mid x^n - 1$, define

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

where μ is the Möbius function on $F[x]$ and the inner sum runs through all $\Phi(D)$ elements δ_D of Δ_D (only square-free D matter). With the notation $\Theta(g) = \Phi(g)/|g|$, the characteristic function of the set of g-free elements of E correspondingly takes the form

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

Using these characteristic functions, we derive an expression for $N(m, g, h)$ in terms of Kloosterman and Gauss sums on E and F. For any $\alpha, \beta \in E$ and any multiplicative character $\eta \in \hat{E^*}$, we define the *generalised Kloosterman sum* $K(\alpha, \beta; \eta)$ $(= K_{q,n}(\alpha, \beta; \eta))$ by

$$K(\alpha, \beta; \eta) = \sum_{\zeta \in E^*} \chi(\alpha\zeta + \beta\zeta^{-1})\eta(\zeta).$$

In particular, we write $K(\alpha, \beta)$ for $K(\alpha, \beta; \eta_1)$, the (standard) Kloosterman sum.

For any $\eta \in \hat{E^*}$, we define the *Gauss sum* $G(\eta)$ $(= G_{n,q}(\eta))$ over E by

$$G(\eta) := \sum_{w \in E^*} \chi(w)\eta(w).$$

It is clear that some Kloosterman sums will reduce to Gauss sums.

In what follows, we will use the following properties of Kloosterman and Gauss sums. For further details, the reader is referred to [4] or a reference book such as [8].

LEMMA 3.1. *Let η be a multiplicative character of E. Then*

$$K(0,0;\eta)=\begin{cases} q^n-1 & \text{if } \eta=\eta_1,\\ 0 & \text{otherwise.}\end{cases}$$

Further, if either $\eta\neq\eta_1$ or $\alpha,\ \beta\in E$ are not both zero, then

$$|K(\alpha,\beta;\eta)|\le 2q^{n/2}.$$

LEMMA 3.2.

(i) *If $\alpha\ (\neq 0)$, $\beta\in E$, then*

$$K(\alpha,\beta;\eta)=\bar{\eta}(\alpha)K(1,\alpha\beta;\eta).$$

(ii) *If $\beta\neq 0$, then $K(0,\beta;\eta)=\eta(\beta)G(\bar{\eta})$.*
(iii) *If $\alpha\neq 0$, then $K(\alpha,0;\eta)=\bar{\eta}(\alpha)G(\eta)$.*

LEMMA 3.3.

(i) $G(\eta_1)=-1$.
(ii) *If $\eta\neq\eta_1$, then $|G(\eta)|=q^{n/2}$.*

PROPOSITION 3.4. *Assume that m is a divisor of Q, and g, h are divisors of x^n-1. Then*

$$N(m,g,h)=\theta(m)\Theta(g)\Theta(h)\int_{d\mid m}\int_{D_1\mid g}\int_{D_2\mid h}K(\delta_{D_1},\delta_{D_2};\eta_d).$$

Proof. Using the characteristic functions derived above, we have

$$\begin{aligned}(3.2)\qquad & N(m,g,h)\\ &=\sum_{w\in E^*}\Big(\theta(m)\int_{d\mid m}\eta_d(w)\Big)\Big(\Theta(g)\int_{D_1\mid g}\chi_{\delta_{D_1}}(w)\Big)\Big(\Theta(h)\int_{D_2\mid h}\chi_{\delta_{D_2}}(w^{-1})\Big).\end{aligned}$$

Thus

$$N(m,g,h)=\theta(m)\Theta(g)\Theta(h)\int_{d\mid m}\int_{D_1\mid g}\int_{D_2\mid h}\sum_{w\in E^*}\chi(\delta_{D_1}w+\delta_{D_2}w^{-1})\eta_d(w),$$

and the result follows from the definition of the generalised Kloosterman sum. ■

From this, we obtain the following expression.

PROPOSITION 3.5. *Assume that m and g are divisors of Q and x^n-1 respectively. Then*

$$
\begin{aligned}
(3.3)\quad & N(m,g,h) \\
&= \theta(m)\Theta(g)\Theta(h)\Big(q^n + \varepsilon + \int\limits_{\substack{d|m\\ d\neq 1}} \int\limits_{\substack{D_1|g\\ D_1\neq 1}} \bar{\eta}_d(\delta_{D_1})G(\eta_d) + \int\limits_{\substack{d|m\\ d\neq 1}} \int\limits_{\substack{D_2|h\\ D_2\neq 1}} \eta_d(\delta_{D_2})G(\bar{\eta}_d) \\
&\qquad + \int\limits_{\substack{D_1|g\\ D_1\neq 1}} \int\limits_{\substack{D_2|h\\ D_2\neq 1}} K(\delta_{D_1},\delta_{D_2}) + \int\limits_{\substack{d|m\\ d\neq 1}} \int\limits_{\substack{D_1|g\\ D_1\neq 1}} \int\limits_{\substack{D_2|h\\ D_2\neq 1}} K(\delta_{D_1},\delta_{D_2};\eta_d)\Big),
\end{aligned}
$$

where

$$
\varepsilon = \begin{cases} -1 & \text{if } g = h = 1, \\ +1 & \text{if } g \neq 1 \text{ and } h \neq 1, \\ 0 & \text{otherwise.} \end{cases}
$$

Proof. We combine the formulation of Proposition 3.4 with the results of Lemmas 3.1–3.3. If $d = 1$, then the Kloosterman sum takes the value $q^n - 1$ when $D_1 = D_2 = 1$, $\eta_1(\delta_{D_2})G(\bar{\eta}_1) = -1$ when $D_1 = 1$ and $D_2 \neq 1$, and $\bar{\eta}_1(\delta_{D_1})G(\eta_1) = -1$ when $D_2 = 1$ and $D_1 \neq 1$. If $d \neq 1$, then we obtain a contribution of 0 when $D_1 = D_2 = 1$, $\bar{\eta}_d(\delta_{D_1})G(\eta_d)$ when $D_1 \neq 1$ and $D_2 = 1$, and $\eta_d(\delta_{D_2})G(\bar{\eta}_d)$ when $D_1 = 1$ and $D_2 \neq 1$. Note that the ε term in the statement of the result arises from the situation when $d = 1$, $D_i = 1$ and $D_j \neq 1$ (where $\{i,j\} = \{1,2\}$); for example in the "$D_1 = 1$" case we have $\int_{D_2|h,\, D_2\neq 1}(-1) = -\sum_{D_2|h,\, D_2\neq 1}\mu(D_1)$, which takes value 0 when $h = 1$ and 1 when $h \neq 1$. ∎

From Proposition 3.5 and the size of the Kloosterman and Gauss sums, we immediately derive a lower bound for $N(m,g,h)$. Write $W(m) = 2^{\omega(m)}$ for the number of square-free divisors of m, where ω counts the number of distinct primes in m, and similarly define $W(g)$.

Corollary 3.6. *Under the conditions and with the notation of Proposition* 3.5,

$$
\begin{aligned}
N(m,g,h) \geq \theta(m)\Theta(g)\Theta(h)(q^n &+ \varepsilon \\
&- q^{n/2}[2W(m)W(g)W(h) - (W(m)+1)(W(g)+W(h)) + 2]).
\end{aligned}
$$

In the case when $g = h$, this inequality takes the form

$$
\begin{aligned}
(3.4)\quad & N(m,g,g) \\
&\geq \theta(m)\Theta(g)^2(q^n + \varepsilon_g - 2q^{n/2}(W(m)W(g) - 1)(W(g) - 1)),
\end{aligned}
$$

where

$$
\varepsilon_g = \begin{cases} -1 & \text{if } g = 1, \\ +1 & \text{if } g \neq 1. \end{cases}
$$

In particular,

$$
(3.5)\qquad N(m,g,h) \geq \theta(m)\Theta(g)\Theta(h)q^{n/2}(q^{n/2} - 2W(m)W(g)W(h)).
$$

Proof. The bounds of Lemmas 3.1 and 3.2 yield for the sum of the "integrals" in the identity (3.3) the absolute bound

$$\begin{aligned}2(W(m)-1)(W(g)-1)(W(h)-1)\\ +2(W(g)-1)(W(h)-1)+(W(m)-1)(W(g)+W(h)-2).\end{aligned}$$

Rearrangement gives the result. ∎

The following simple bound for $W(m)$, the number of square-free divisors of $m\in\mathbb{N}$, will be useful in what follows. The proof is immediate using multiplicativity.

Lemma 3.7. *For any positive integer m,*

$$W(m)\le c_m m^{1/4}, \tag{3.6}$$

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, $c_m<2.9$.

In what follows, we recall the notation n^* defined by $n=p^bn^*$, $p\nmid n^*$.

Proposition 3.8. *Let q be a prime power and let n $(\ge 3)\in\mathbb{N}$ with $n^*\le 4$. Suppose, in addition, $q\equiv 2 \pmod 3$ if $n^*=3$, and $q\equiv 3\pmod 4$ if $n^*=4$. The pairs $(q,n)=(2,3)$, $(2,4)$ and $(3,4)$ are not PFF. Otherwise, (q,n) is a PFF pair.*

Proof. We have $Q(q,n)<q^n/\gcd(n,q-1)$, where, under the given conditions,

$$\gcd(n,q-1)=\begin{cases}1 & \text{if } n^*=1 \text{ or } 3,\\ 2 & \text{if } n^*=2 \text{ or } 4.\end{cases}$$

Moreover, $N(Q,x^n-1,x^n-1)=N(Q,g(x),g(x))$, where g factorises into F-irreducibles as

$$g(x)=\begin{cases}x-1 & \text{if } n^*=1 \text{ or } n^*=n=3,\\ (x-1)(x+1) & \text{if } n^*=2 \text{ or } n^*=n=4,\\ (x-1)(x^2+x+1) & \text{if } n^*=3<n,\\ (x-1)(x+1)(x^2+1) & \text{if } n^*=4<n,\end{cases}$$

using Lemma 2.5 when $n=3$ or 4. It follows from Corollary 3.6 and Lemma 3.7 that $N:=N(Q,x^n-1,x^n-1)$ is positive whenever

$$q^{n/2}>2(W(Q)W(g)-1)(W(g)-1)-\varepsilon_g q^{-n/2}, \tag{3.7}$$

and hence whenever

$$(q^n(q-1))^{1/4}>Ac_Q, \tag{3.8}$$

where

$$A = \begin{cases} 4 & \text{if } n^* = 1 \text{ or } n^* = n = 3, \\ 2^{11/4} \cdot 3 & \text{if } n^* = 2 \text{ or } n^* = n = 4, \\ 24 & \text{if } n^* = 3 < n, \\ 2^{15/4} \cdot 7 & \text{if } n^* = 4 < n. \end{cases}$$

We now consider when (3.8) holds for each of the values of A, using an appropriate bound for c_Q. We use notation like (q_0+, n_0+) to signify any pair (q, n) with $q \geq q_0,\ n \geq n_0$.

• Assume $A = 4$. Then (3.8) holds with $c_Q < 4.9$ for $(3+, 11+)$, $(4+, 8+)$, $(5+, 7+)$, $(7+, 6+)$, $(8+, 5+)$, $(13+, 4+)$, $(23+, 3+)$; with $c_Q < 2.9$ for $(2, 15+)$; and with $c_Q < 3.2$ for $(3, 9)$ (when $3 \nmid Q$). For $n^* = 1$, direct application of inequality (3.7) establishes the result for $(5, 5)$, $(8, 4)$, $(4, 4)$ (for this, (3.7) reduces to $16 > 14$) and $(9, 3)$, leaving only the pairs $(2, 4)$, $(2, 8)$ and $(3, 3)$. When $q = 2$, one of the sole reciprocal pair of primitive quartics has zero trace so there does not exist a PFF polynomial. Otherwise, a PFF polynomial for the case $(2, 8)$ is given in Section 7.3; one for $(3, 3)$ is in Section 7.2. For the case $n = n^* = 3$, inequality (3.7) establishes the result for $(17, 3)$, $(11, 3)$, $(8, 3)$ and $(5, 3)$. When $q = 2$ one of the pair of primitive cubics has zero trace so there does not exist a PFF polynomial.

• Assume $A = 2^{11/4} \cdot 3$. Then (3.8) holds with $c_Q < 4.9$ for $(3+, 17+)$, $(4+, 13+)$, $(5+, 11+)$, $(6+, 10+)$, $(7+, 9+)$, $(8+, 8+)$, $(11+, 7+)$, $(14+, 6+)$, $(22+, 5+)$, $(40+, 4+)$; and with $c_Q < 3.2$ for $(3, 15+)$. For the case $n^* = 2$, direct application of inequality (3.7) establishes the result for $(5, 10)$ and $(9, 6)$, leaving only the pair $(3, 6)$: a PFF polynomial for this case is given in Section 7.2. When $n^* = n = 4$, inequality (3.7) establishes the result for $(31, 4)$, $(27, 4)$ and $(23, 4)$ (for which $W(Q) \leq 16$) and $(19, 4)$ ($W(Q) \leq 8$). This leaves the pairs $(11, 4)$ and $(7, 4)$, $(3, 4)$. When $q = 3$, there are four primitive quartics with non-zero traces, namely $f(\pm x)$ where $f(x) = x^4 + x^3 + x^2 - x - 1$, together with their reciprocals. None is a PFF polynomial. On the other hand, direct verification yields PFF polynomials as follows:

(q, n)	PFF polynomial
$(11, 4)$	$x^4 + x^3 - 5x + 2$
$(7, 4)$	$x^4 + x^3 - x^2 - x - 2$

• Assume $A = 24$. Then (3.8) holds with $c_Q < 4.9$ for $(16+, 6+)$ and $(5+, 12+)$, and with $c_Q < 2.9$ for $(2, 25+)$. Inequality (3.7) establishes the result for $(8, 6)$: for $q = 2$, degrees $6, 12$ and 24 are treated in Section 7.3.

• Assume $A = 2^{15/4} \cdot 7$. Then (3.8) holds with $c_Q < 4.9$ for $(7+, 12+)$, $(4+, 20+)$ and $(3+, 22+)$. This leaves the pair $(3, 12)$, which is treated in Section 7.2. ■

4. The sieve. In this section, we introduce our key tool: a sieve with both additive and multiplicative components. For a given pair (q,n), let $m \mid Q$, $f \mid x^n - 1$ and $g \mid y^n - 1$. Let $m_1, \ldots, m_r$ be factors of m, for some $r \geq 1$, and let $f_1, \ldots, f_r$ and $g_1, \ldots, g_r$ be factors of f and g respectively. We call $\{(m_1, f_1, g_1), \ldots, (m_r, f_r, g_r)\}$ a set of *complementary divisor triples* of (m, f, g) with common divisor triple (m_0, f_0, g_0) if the primes in $\operatorname{lcm}\{m_1, \ldots, m_r\}$ are precisely those in m, the irreducibles in $\operatorname{lcm}\{f_1, \ldots, f_r\}$ are precisely those in f, the irreducibles in $\operatorname{lcm}\{g_1, \ldots, g_r\}$ are precisely those in g and, for any distinct pair (i,j), the primes and irreducibles in $\gcd(m_i, m_j)$, $\gcd(f_i, f_j)$ and $\gcd(g_i, g_j)$ are precisely those in m_0, f_0 and g_0 respectively. Observe that the value of $N(m, f, g)$ depends only on the primes and irreducibles present in m, f and g. The following result extends Theorem 3.1 of [3].

PROPOSITION 4.1 (Sieving inequality). *For divisors m of Q, f of $x^n - 1$ and g of $y^n - 1$, let $\{(m_1, f_1, g_1), \ldots, (m_r, f_r, g_r)\}$ be a set of complementary divisor triples of (m, f, g) with common divisor triple (m_0, f_0, g_0). Then*

$$N(m,f,g) \geq \sum_{i=1}^{r} N(m_i, f_i, g_i) - (r-1)N(m_0, f_0, g_0). \tag{4.1}$$

Proof. When $r = 1$, the result is trivial. For $r = 2$, denote by $\mathcal{S}_{m,f,g}$ the set of elements $w \in E^*$ such that w is m-free and f-free and w^{-1} is g-free. Then $\mathcal{S}_{m_1,f_1,g_1} \cup \mathcal{S}_{m_2,f_2,g_2} \subseteq \mathcal{S}_{m_0,f_0,g_0}$, while $\mathcal{S}_{m_1,f_1,g_1} \cap \mathcal{S}_{m_2,f_2,g_2} = \mathcal{S}_{m,f,g}$, and the inequality holds by consideration of cardinalities. For $r \geq 2$, use induction on r. ■

We observe that, in Proposition 4.1, mfg can be regarded as a formal product whose "atoms" are either prime factors of Q or irreducible factors of $x^n - 1$ or $y^n - 1$. Write k for (the radical of) mfg and k_0 for (that of) $m_0 f_0 g_0$; we shall refer to k_0 as the *core* of k. Also write $N(k)$ for $N(m,f,g)$ (so that, in a natural sense, $W(k) = W(m)W(f)W(g)$). Consider an application of the sieve in which, for each $i = 1, \ldots, r$, $m_i f_i g_i$ runs through the values of $k_0 p_i$ as p_i runs through atoms of k not in k_0. We shall call this a (k_0, r) *decomposition* of k. Given a (k_0, r) decomposition, define $\delta = 1 - \sum_{i=1}^{r} 1/|p_i|$ with $|p| = p$ when p is a prime (integer) and $|p| = q^{\deg p}$ when p is an irreducible polynomial, and set $\Delta = (r-1)/\delta + 2$. As we shall see, *it is crucial that δ is positive* for the (k_0, r) decomposition selected. In particular, when $r = 1$ (the *non-sieving situation*), then (4.1) is a trivial equality, $W(k) = 2W(k_0)$ and $\Delta = 2$.

PROPOSITION 4.2. *In the above notation, for a given pair (q,n), let k denote the formal product mfg, where $m \mid Q$, $f \mid x^n - 1$ and $g \mid y^n - 1$. Suppose* *that*

$$q > (2W(k))^{2/n}. \tag{4.2}$$

Then $N(k)$ is positive.

More generally, for a (k_0, r) decomposition as described above, suppose that δ is positive and

$$q > (2W(k_0)\mathit{\Delta})^{2/n}. \tag{4.3}$$

Then $N(k)$ is positive.

Proof. The non-sieving criterion (4.2) follows immediately from (3.5) of Corollary 3.6.

For (4.3), define $\mathit{\Theta}(k) = \theta(m)\mathit{\Theta}(f)\mathit{\Theta}(g)$ and write (4.1) in the form

$$\begin{aligned} N(k) &\ge \delta N(k_0) + \sum_{i=1}^{r}\Big(N(k_0 p_i) - \Big(1 - \frac{1}{|p_i|}\Big)N(k_0)\Big) \\ &= \delta\mathit{\Theta}(k_0)\Big(q^n - 1 + \sum_{\substack{d \mid k_0 \\ d \ne 1}} U(d)\Big) + \mathit{\Theta}(k_0)\sum_{i=1}^{r}\Big(1 - \frac{1}{|p_i|}\Big)\sum_{\substack{d \mid k_0 p_i \\ d \nmid k_0}} U_i(d), \end{aligned}$$

where the sums over d are over "square-free" formal factors of the formal products k_0 and $k_0 p_i$ and, by the estimates of Lemmas 3.1 and 3.3 (as already used in Corollary 3.6), each of the expressions $U(d)$ and $U_i(d)$ does not exceed $2q^{n/2}$ in absolute value. Granted that $\delta > 0$, it follows that $N(k)$ is positive whenever

$$\delta q^{n/2} > 2\delta W(k_0) + 2\sum_{i=1}^{r}(W(k_0 p_i) - W(k_0))\Big(1 - \frac{1}{|p_i|}\Big).$$

The result follows since $W(k_0 p_i) - W(k_0) = W(k_0)$ and

$$\sum_{i=1}^{r}\Big(1 - \frac{1}{|p_i|}\Big) = r - 1 + \delta. \ ■$$

In applying (4.3) to the PFF problem, k is taken to be $Q(x^n - 1)(y^n - 1)$; in fact, by the discussion in Section 2 we may take $k = Q(x^{n^*} - 1)(y^{n^*} - 1)$. Generally, we take $g_0(x) = f_0(x)$, although if necessary, a more general set of "complementary divisor triples" or the full form of Corollary 3.6 can be used.

We illustrate the direct use of the sieve in dealing with the case when $n^* = q - 1$.

Proposition 4.3. *Let q (≥ 4) be a prime power and n $(\ge 3) \in \mathbb{N}$. Suppose $n^* = q - 1 > 2$. The pairs $(q, n) = (5, 4)$ and $(4, 3)$ are not PFF. Otherwise, (q, n) is a PFF pair.*

Proof. We use a (k_0, r) decomposition of $k = Q(x^{n^*} - 1)(y^{n^*} - 1)$. Here $Q = (q^n - 1)/(q-1)^2$ and all polynomial atoms are linear. Take $f_0(x) = g_0(x)$ and suppose that $(x^{n^*} - 1)/f_0(x)$ is chosen to be a product of t (say) linear polynomial atoms.

As a first step, we use the additive sieve (alone). To ensure that δ is positive, of necessity $2t < q$. Specifically, for q odd (whence n^* even) take $t = n^*/2$. Then $\delta = 1 - n^*/q = 1/q$ and $\Delta = (n^* - 1)/\delta + 2 = n^{*2} + 1$. Moreover, $W(f_0) = W(g_0) = 2^{n^*/2}$. Thus (4.3) becomes

$$q^{n/2} > 2^{n^*+1}(n^{*2} + 1)W(Q). \tag{4.4}$$

Otherwise, for q even (whence n^* odd) take $t = (n^* - 1)/2$. Then $\delta = 2/q$ and

$$\Delta = \frac{n^* - 2}{\delta} + 2 = \frac{(n^* - 2)(n^* + 1)}{2} + 2 = \frac{n^{*2} - n^* + 2}{2} < \frac{n^{*2} + 1}{2}.$$

Now, $W(f_0) = W(g_0) = 2^{(n^*+1)/2}$. Accordingly, (4.4) remains a valid sufficient condition.

By Lemma 3.7, $W(Q) < c_Q q^{n/4}/\sqrt{q-1}$. Hence we obtain the sufficient condition

$$q^{n/4} > \frac{c_Q 2^q((q-1)^2 + 1)}{\sqrt{q-1}}. \tag{4.5}$$

First assume that $n = n^*$. Then inequality (4.5) is satisfied whenever $n = q - 1 \geq 37$. Therefore we can suppose $q \leq 37$. Next, since $q = n + 1 \leq 37$, factorising yields $\omega(Q) \leq 15$ (with equality only when $q = 37$). With this bound for $\omega(Q)$, (4.4) is satisfied for $q \geq 23$. Further, with the exact values $\omega(Q)$, (4.4) is also satisfied for $q = 19$ ($\omega(Q) = 8$) and $q = 17$ ($\omega(Q) = 6$).

Next, suppose $q = 16$ so that $Q = 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41 \cdot 61 \cdot 151 \cdot 331 \cdot 1321$ and $\omega(Q) = 9$. Introduce a non-trivial multiplicative component to the sieve by taking $m_0 = 7 \cdot 11 \cdot 13$. This time select $t = 6$. Then $r = 6 + 12 = 18$ and

$$\delta = 1 - \tfrac{1}{31} - \tfrac{1}{41} - \tfrac{1}{61} - \tfrac{1}{151} - \tfrac{1}{331} - \tfrac{1}{1321} - \tfrac{12}{16} > 0.1665\ldots,$$

$\Delta = 104.06\ldots$ and $W(k_0) = W(m_0)W(g)^2 = 2^3 \cdot 2^{18} = 2^{21}$. Hence

$$(2W(k_0)\Delta)^{2/n} < 14.2 < q.$$

Direct verification deals with five of the seven remaining cases ($7 \leq q \leq 13$): see table below. On the other hand, when $q = 5$, given a root α of any of the 32 primitive quartics over $F = \mathrm{GF}(5)$ for which the coefficients of x^3 and x are both non-zero, either α or $1/\alpha$ is *not* free over F. Hence $(5, 4)$ is not a PFF pair. Similarly, when $q = 4$, none of the 12 primitive cubics is a PFF polynomial.

(q,n)	PFF polynomial	Polynomial for u
$(13,12)$	$x^{12}+x^{11}-3x+2$	
$(11,10)$	$x^{10}+x^{9}-2x+2$	
$(9,8)$	$x^8-(u-1)x^7-x^6-x^5-(u+1)x^4+(u-1)x^3+(u+1)x^2-x-u$	u^2-u-1
$(8,7)$	$x^7+x^6+(u+1)x^5+(u^2+1)x^4+(u^2+u+1)x^3+u^2x^2+ux+u^2+u$	u^3+u+1
$(7,6)$	$x^6+x^5+x^2-x+3$	

When $n > n^*$, condition (4.5) is satisfied for $q > 11$ with $n \ge 2n^*$, for $q > 7$ with $n \ge 3n^*$, for $q > 4$ with $n \ge 5n^*$, and for $q = 4$ (whence $c_Q = 2.9$) with $n \ge 8n^* = 24$. The only pairs not covered are $(8,14)$, $(4,12)$ and $(4,6)$. For $(8,14)$ direct substitution in condition (4.4) yields the result. For $(4,12)$, use (4.3) with multiplicative sieving alone. Specifically, $Q = 5\cdot 7\cdot 13\cdot 17\cdot 241$. Take the core to be $(x^3-1)(y^3-1)$ and let all the $r = 5$ primes in Q be sieving primes. Then $\delta > 0.5172$ and $(2W(k_0)\varDelta)^{2/n} < 3.29 < 4$. Finally, a PFF polynomial of degree 6 is given in Section 7.1. ∎

4.1. Key strategy: applying the sieve in the general case. In this section, we derive an inequality which provides a sufficient condition for a pair (q,n) to be a PFF pair in the general case, by considering a specific factorisation of $x^{n^*}-1$ followed by a “core-atom” application of the sieve. The universal value of this strategy can be judged from the fact that, in what follows, only a single case, namely $(2,21)$, arose for which another factorisation succeeded where the key strategy failed. While the sieve has both an additive and a multiplicative component, we note that it is often possible to obtain our desired result by using the additive part alone; correspondingly, we state two versions of our main inequality. The multiplicative part of the sieve is a useful tool in dealing with cases where the value of q is small.

Denote by s the positive integer $\operatorname{ord}_{n^*} q$, i.e., $n^* \mid q^s-1$ with s minimal; then every irreducible factor of $x^{n^*}-1$ over F has degree dividing s. Write $x^{n^*}-1$ as $g(x)G(x)$, where G is the product $\prod_{i=1}^{r} G_i$ of the (r, say) irreducible factors ($G_1,\ldots,G_r$, say) of degree s, and g is the product of those with degree less than s (with $g=1$ if $s=1$). Let $m := \deg g$. Note that $r = (n^*-m)/s$. For the next result suppose that the set of $\omega(Q)$ distinct prime divisors of Q is partitioned into a set of t “sieving” primes $\{l_1,\ldots,l_t\}$ and a set of u primes whose product is the multiplicative core m_0. Thus $t+u = \omega(Q)$; in particular $u = \omega(Q)$ when there is no multiplicative sieving.

Proposition 4.4. *Assume the notation defined above. Then $N(Q, x^n-1, y^n-1) > 0$ whenever*

$$q^{n/2} > 2^{1-t}W(Q)W(g)^2\biggl(\frac{q^s(2(n^*-m)+s(t-1))}{sq^s(1-\sum_{i=1}^{t}1/l_i)-2(n^*-m)}+2\biggr), \tag{4.6}$$

provided the displayed denominator in the right side of (4.6) *is positive.*

In the case of additive sieving only, we have the sufficient condition

$$q^{n/2} > 2W(Q)W(g)^2\biggl(\frac{q^s(2(n^*-m)-s)}{sq^s-2(n^*-m)}+2\biggr), \tag{4.7}$$

provided the denominator in (4.7) *is positive.*

Note. Since $n^* \mid q^s-1$ the denominator in (4.7) is always positive unless $s=1$ and $n^*=n=q-1$ (which case is covered by Proposition 4.3).

Proof of Proposition 4.4. Take $2r+t$ complementary divisors with core $k_0=m_0g(x)g(y)$, namely $\{k_0G_i(x): i=1,\dots,r\}$, $\{k_0G_i(y): i=1,\dots,r\}$ and $\{k_0l_i : i=1,\dots,t\}$.

Then $N(Q,x^n-1,y^n-1)$ is positive, by (4.3), if

$$q^{n/2} > 2W(m_0)W(g)^2\biggl(\frac{2r+t-1}{1-\sum_{i=1}^t 1/l_i-\sum_{i=1}^{2r}1/q^s}+2\biggr),$$

i.e., if

$$q^{n/2} > 2\cdot 2^uW(g)^2\biggl(\frac{2rs+s(t-1)}{s(1-\sum_{i=1}^t 1/l_i)-2rs/q^s}+2\biggr),$$

i.e., since $rs=n^*-m$, if (4.6) holds. ■

We conclude this section with some remarks which deal with the relationship of the case in which $n^*<n=p^bn^*$ with the (more demanding) one in which $n^*=n$. The condition (4.7) may be written in the form $q^{n/2}/W(Q) > H(n^*)$, say, where the quantity $H(n^*)$ depends only on n^*. Suppose that we are in a situation where it may be assumed that $W(Q)<\kappa q^{\varepsilon n}$ for positive constants κ,ε with $\varepsilon\le 1/4$. For example, for any pair (q,n), $W(Q)\le c_QQ^{1/4}<\frac{c_Q}{(q-1)^{1/4}}q^{n/4}<4.9q^{n/4}$, by Lemma 3.7. Then (4.7) is satisfied whenever the stronger condition

$$q > (\kappa H(n^*))^{2/(n(1-2\varepsilon))} = (\kappa H(n^*)^{2/(n^*(1-2\varepsilon))})^{1/p^b} \tag{4.8}$$

holds. The main burden of the proof of Theorem 1.4 is to divide the pairs (q,n) into infinite classes and show, theoretically using the additive sieve alone, that such a condition holds for all but relatively few pairs. Of course, if $n^*<n$, then $b\ge 1$ and it turns out that often (4.8) is satisfied for all relevant pairs without much need for further investigation. Sometimes even taking $b=1$ is sufficient for all cases.

5. Some special cases. First we treat some special cases, where the values of q and n are related, or when n is of a distinguished type (e.g., prime).

Proposition 5.1. *Let q (≥ 5) be a prime power and let n $(\ge 3)\in\mathbb{N}$. Suppose that n^* (>2) divides $q-1$ but $n^*\ne q-1$. Then (q,n) is a PFF pair.*

Proof. Here we have $G(x) = x^{n^*} - 1$, $g(x) = 1$ and, since $(n, q-1) = n^*$, we have $Q = (q^n - 1)/(n^*(q-1))$. Moreover $s = 1$ and $m = 0$. Note that here $3 \le n^* \le (q-1)/2$; if $n^* < (q-1)/2$, then $n^* \le (q-1)/3$.

Inequality (4.7) yields the sufficient condition

$$q^{n/2} > 2W(Q)\left(\frac{2n^*(q-2)+q}{q-2n^*}\right). \tag{5.1}$$

Using the basic bound $W(Q) < c_Q q^{(n-1)/4}/(n^*(1-1/q))^{1/4}$ we obtain the sufficient condition

$$q > \left(2c_Q \frac{2n^*(q-2)+2}{q-2n^*}\right)^{4/(n+1)} \left(\frac{1}{n^*(1-1/q)}\right)^{1/(n+1)} =: T_1, \tag{5.2}$$

say. Clearly, $T_1 \to \infty$ as n^* approaches $q/2$. We shall show that an appropriate upper bound T_2 for T_1 decreases in the range $3 \le n^* \le (q-1)/3$.

Since $q - 2n^* \ge 1$ and $n^*(1-1/q) > 1$, to begin to analyse (5.2), we can replace it by the weaker sufficient condition

$$q > (2c_Q q(2n^*+1))^{4/(n+1)} =: T_2, \tag{5.3}$$

say.

We first consider the case when $n = n^*$. We begin by assuming that $n \ge 10$: thus $q \ge 23$. Taking natural logarithms, we get

$$\log T_2 = \frac{4}{n+1}(\log(2c_Q q) + \log(2n+1)).$$

For fixed q, differentiating with respect to n we obtain

$$\frac{d}{dn}\log T_2 = -\frac{4}{(n+1)^2}\left(\log(2c_Q q(2n+1)) - \left(1 + \frac{1}{2n+1}\right)\right),$$

which is negative since $\log(4n+2) > 1 + 1/(2n+1)$ for all $n \ge 1$. So, in the range $10 \le n \le (q-1)/2$, the maximal value of T_2 is attained at $n = 10$: it is certainly less than q for $q \ge 23$.

Now assume $3 \le n \le 9$. Since $q - 2n \ge q - 18$, we can replace (5.2) by

$$q > \left(\frac{2c_Q q(2n^*+1)}{q-18}\right)^{4/(n+1)} =: T_3,$$

say. Taking logarithms and differentiating, we find that T_3 is a decreasing function if

$$\log\frac{14c_Q q}{q-18} > \frac{8}{7},$$

which holds for $q > 18$ (since $\log 14 > 8/7$). The maximum value of T_3 occurs when $n = 3$; it is less than q for $q > 14c_Q + 18$, i.e., $q > 86$. This establishes the result except when $q < 87$ and $3 \le n \le \min(9, (q-1)/2)$.

Using (5.1), with the c_Q bound, we find from a computational check that the result holds for all remaining (q, n) except $(19, 9)$, $(17, 8)$, $(19, 6)$,

$(13,6)$, $(16,5)$, $(11,5)$ and appropriate values of $(q,4)$, $q \leq 29$ (5 values), and $(q,3)$, $q \leq 49$ (9 values). For all remaining values, $\omega(Q) \leq 4$; taking exact values deals (via (5.1)) with all pairs except $(7,3)$, $(16,3)$, $(9,4)$, $(13,4)$, $(11,5)$, $(13,6)$. Invoking the multiplicative part of the sieve also, i.e., using inequality (4.6), yields the result for $(13,6)$ ($Q = 7 \cdot 61 \cdot 157$, $m_0 = 7$) and $(16,3)$ ($Q = 7 \cdot 13$, $m_0 = 7$). Direct verification establishes the other four cases (see table below).

(q,n)	PFF polynomial	Polynomial for u
$(13,4)$	$x^4 + x^3 - x - 2$	
$(11,5)$	$x^5 + x^4 + 3x - 2$	
$(9,4)$	$x^4 - x^3 + x^2 + x - u + 1$	$u^2 - u - 1$
$(7,3)$	$x^3 + x^2 + 2x - 3$	

Now suppose $n > n^*$, and replace $n+1$ by $2n^*+1$ in (5.3) to obtain the sufficient condition

$$q > (2c_Q q(2n^*+1))^{4/(2n^*+1)} =: T_4, \tag{5.4}$$

say. We begin by assuming that $n^* \geq 5$ and $q > 13$. Taking logarithms and differentiating, we get

$$\frac{d}{dn^*} \log T_4 = \frac{8}{(2n^*+1)^2}(1 - \log(2c_Q q(2n^*+1))),$$

clearly negative. So, in the range $5 \leq n^* \leq (q-1)/2$, the maximum value of T_4 is attained at $n^* = 5$, and this is less than q for $q > 13$. When $n^* = (q-1)/2$, we note that $n \geq 3n^*$; using this in condition (5.4), we find the result holds for $q \geq 9$ (and so in every case).

Finally we consider $3 \leq n^* \leq 4$. Since $n^* \leq 4$, we can use a final sufficient criterion, namely

$$q > \left(\frac{2c_Q q(2n^*+1)}{q-8}\right)^{4/(n+1)} =: T_5,$$

say. Again by differentiation, we can check that T_5 is a decreasing function when $q > 8$. The maximum value of T_5 occurs when $n^* = 3$. Indeed, $T_5 < q$ in the following circumstances:

- $q \leq 17$ (using $c_Q < 4.9$ except as noted),
- $q = 16$, $n^* = 3$ (using $c_Q < 2.9$),
- $q = 13$, $n^* = 3, 4$ (using $n \geq 13n^*$),
- $q = 9$, $n^* = 4$ (using $c_Q < 3.2, n \geq 3n^*$).

In the last remaining case when $q = 7$ and $n^* = 3$, since $n \geq 7n^*$ it follows that $T_2 < q$. ■

The following simple lemma improves Lemma 3.7 under the stated conditions.

Lemma 5.2. *Let $n \geq 5$ be prime, and let $h \in \mathbb{N}$ be square-free with each prime divisor of h congruent to 1 modulo $2n$. Then*

$$W(h) < h^{1/4},$$

except when $n = 5$ and $h = 11$.

Proposition 5.3. *Let q (≥ 5) be a prime power and let $n \in \mathbb{N}$. Suppose n^* (≥ 5) does not divide $q-1$ and either n^* is prime or $n^* = q+1$ with q even. Then (q, n) is a PFF pair.*

Proof. In this case, $x^{n^*} - 1$ factors as $(x-1)G(x)$ where G is a product of $(n^*-1)/s$ factors of degree s. We have $s \geq 2$ $(s = 2$ if $n^* = q+1)$, $m = 1$, $(n, q-1) = 1$ and $Q = (q^n - 1)/(q-1)$ odd.

By inequality (4.7) of Proposition 4.4, we have the sufficient condition (for $N(Q, x^n - 1, y^n - 1) > 0$)

$$q^{n/2} - 8W(Q)\left(\frac{2(n^*-1)}{s - 2(n^*-1)/q^s} + 1\right) > 0; \tag{5.5}$$

this certainly holds if

$$\varDelta = \varDelta(q, n, s) := (q^n(q-1))^{1/4} - 8c_Q\left(\frac{2(n^*-1)}{s - 2(n^*-1)/q^s} + 1\right) > 0.$$

Concentrating on the "worst-case scenario" when $n = n^*$, we require

$$\varDelta(q, n^*, s) = (q^{n^*}(q-1))^{1/4} - 8c_Q\left(\frac{2(n^*-1)}{s - 2(n^*-1)/q^s} + 1\right) > 0. \tag{5.6}$$

In (5.6) we can take $c_Q < 2.9$ since Q is odd. In fact, when q and n are odd and n is an odd prime, Lemma 5.2 applies and we can take $c_Q = 1$.

Evidently, $\varDelta(q, n^*, s)$ is an increasing function of q (with n^*, s fixed) and of s (with q, n^* fixed). It is also increasing with respect to n^* with some qualification as regards small values of q, s. In fact, with $c_Q = 1$, by differentiation, for given odd q and $s = 2$, $\varDelta$ is an increasing function of n^* in the range $(q, n^*) = (5+, 9+), (7+, 6+), (9+, 5+)$. For even q (take $c_Q = 2.9$), the corresponding pairs are $(8+, 6+), (16+, 5+)$. For $s = 3$, the pairs need to be $(5+, 6+), (7+, 5+)$, q odd; $(8+, 7+), (16+, 5+)$, q even. For $s \geq 4$, any pair $(5+, 5+)$ (q odd) or $(8+, 6+)$ is in a region of increasing $\varDelta$. Within the above framework, it suffices to establish the result for smallest q and n. It also suffices to take least s, i.e., $s = 2$.

In the general case, by computation, the result holds for $(25+, 5+)$, $(16+, 7+)$, $(9+, 9+)$, $(7+, 11+)$ and $(5+, 17+)$, in each case within the range of increasing $\varDelta$.

Suppose first that $n = n^*$. For the pairs (q, n) not covered by the above list, a number are simply excluded by Lemma 2.3. For all but two remaining pairs, $\Delta(q, n, s)$ is quickly calculated to be positive; specifically, when $(q, n, s) = (19, 5, 2), (13, 7, 2), (11, 7, 3), (9, 7, 3), (5, 11, 5), (5, 13, 4)$. The final two pairs are $(9, 5)$ and $(8, 9)$; in each case $s = 2$. For these, $W(Q) = 4$ and the sufficient condition (5.5) holds.

Finally, suppose $n > n^*$. In the definition of Δ and in condition (5.6), replace in the first term $q^{n^*}(q-1)$ by $q^{3n^*}(q-1)$ (q odd) and by $q^{2n^*}(q-1)$ (q even). Also, set $c_Q = 1$ or 2.9 according as q is odd or even. Then, easily, $\Delta(5, n^*, 2)$ and $\Delta(8, n^*, 2)$ are increasing and positive in the respective cases. This completes the proof. ■

Proposition 5.4. *Let q (≥ 5) be an odd prime power and let $n \in \mathbb{N}$. Suppose $n^* = 2l \geq 6$, where either l is a prime not dividing $q-1$ or $l = \frac{1}{2}(q+1)$ with $q \equiv 3 \pmod 4$. Then (q, n) is a PFF pair.*

Proof. When l is prime then $2 \leq s \mid l-1$ (since $q^s \equiv 1 \pmod{l}$), whence $n^* - 2 = 2(l-1)$ is divisible by s. The same conclusion holds when $l = \frac{1}{2}(q+1)$, in which case $s = 2$. Indeed, in both cases, $x^{n^*} - 1$ factors into two linear factors and $(n^* - 2)/s$ factors of degree s. (Note that $(n^*, q-1) = 2$.) Let $\gamma_s = 1$ if s is even, or 2 if s is odd: thus, since n^* divides $\gamma_s(q^s - 1)/(q-1)$, we have $n^* < \gamma_s q^s/(q-1)$. Apply Proposition 4.4 with $m = 2$. By inequality (4.7), we have the sufficient condition

$$q^{n/2} - 64W(Q)\left(\frac{n^* - 2}{s - 2(n^* - 2)/q^s} + 1\right) > 0, \tag{5.7}$$

which, as before, is certainly implied by

$$\Delta(q, n, s) := (q^n(q-1))^{1/4} - \frac{64}{2^{1/4}} c_Q \left(\frac{n^* - 2}{s - 2\gamma_s/(q-1)} + 1\right) > 0.$$

Concentrating on the "worst-case scenario" when $n = n^*$, we require

$$\Delta(q, n^*, s) > 0. \tag{5.8}$$

As in Proposition 5.3, it suffices to establish the result for smallest q and n. We take $s = 2$, $\gamma_s = 2$ and $c_Q < 4.9$.

By computation, the result holds for $(47+, 6+)$, $(23+, 8+)$, $(16+, 10+)$, $(11+, 12+)$, $(9+, 14+)$, $(7+, 16+)$ and $(5+, 21+)$. We may now assume that $q \leq 43$.

Suppose first that $n = n^*$. Note that, for $n \geq 14$, the only case which remains is $(5, 14)$. When $n = 6$, we find that $W(Q) \leq 2^5$ for all $q < 47$ with $q \not\equiv 1 \pmod 6$. Using this, (5.7) gives the result for $q \geq 19$. Indeed, for $q < 19$, all except $q = 11$ have $W(Q) \leq 2^4$, which gives the result for $q = 17$. This leaves just $q \leq 13$ when $n = 6$; in fact, only $(5, 6)$ ($Q = 2 \cdot 3^2 \cdot 7 \cdot 19 \cdot 37$) and $(11, 6)$ ($Q = 3^2 \cdot 7 \cdot 31$). Using both the additive and multiplicative power of the sieve, i.e., using inequality (4.6), gives the sufficient condition

$$q^{n/2} > 2^{1-t}16W(Q)\biggl(\frac{n^*+t-3}{(1-\sum 1/l_i)-(n^*-2)/q^2}+2\biggr).$$

With $t=3$, this yields the result for $q=11$ ($l_1=7$, $l_2=19$ and $l_3=37$). This leaves just $q=5$. When $n=8$, using the additive-only estimate with $W(Q)=2^3$ and $\gamma_s=1$ gives the result for $(7,8)$. When $n=10$, all valid $q<16$ have $W(Q)=2^4$; using this value in the additive-only inequality yields the result for all $q\geq 7$. Finally, using $W(Q)\leq 2^5$ deals with $(5,14)$. Direct verification deals with the remaining case: the pair $(5,6)$ has PFF polynomial $x^6+x^5+x^3+x^2-x-2$. When $n>n^*$, taking $3n^*$ in place of n^* in the first term of condition (5.8) yields the result for all pairs. ∎

6. Larger fields and degrees. It is necessary to deal individually with fields of smallest cardinality, namely $2,3$ and 4, and their treatment is deferred to Section 7. Here we suppose $q\geq 5$. Even so, it turns out that $\mathbb{F}_5$ and $\mathbb{F}_7$ require closer attention. From what has been accomplished so far we may also assume that $n^*\geq 8$.

We make the following definitions. For g as defined in Section 4.1, $\omega=\omega(q,n)=\omega(q,n^*)$ is the number of distinct irreducible factors of g (so $W(g)=2^\omega$), and $\rho=\rho(q,n)=\rho(q,n^*)=\omega(q,n)/n^*$. As in Section 4.1, s denotes the degree of the irreducible factors of G. We can suppose that $s\geq 2$. Also set $n_1:=\gcd(n,q-1)$.

Lemma 6.1 ([5]). *Assume that $n>4$ with $p\nmid n$ and $q>4$. Then the following hold:*

(i) *If $n=2n_1$ with q odd, then $s=2$ and $\rho=1/2$.*
(ii) *If $n=4n_1$ with $q\equiv 1 \pmod 4$, then $s=4$ and $\rho=3/8$.*
(iii) *If $n=6n_1$ with $q\equiv 1 \pmod 6$, then $s=6$ and $\rho=13/36$.*
(iv) *Otherwise, $\rho\leq 1/3$.*

Because the bounds of Lemma 6.1 (taken from [5]) are insufficient for our purposes when $q=5$ or 7, there is some difficulty for these field cardinalities. We overcome the obstacle by a numerical result related to Lemma 3.7; bounds of similar type (such as Lemma 7.5) will occur in Section 7.

Lemma 6.2. *Suppose $\omega(h)\geq 49$. Then*

$$W(h)<h^{1/6}.$$

Proof. By calculation the result holds when $\omega(h)=49$, since then h is at least the product of the first 49 primes. The result follows since the 50th prime is $229>2^6$. ∎

Write the radical of Q as $m_0p_1\dots p_t$, where m_0 is the core and $p_1,\dots,p_t$ are the (multiplicative) sieving primes. When $t=0$ there is no multiplicative sieving. Set $u := \omega(m_0)$; thus, often $u = \omega(Q)$. In this context, the basic form of (4.6) in Proposition 4.4 takes the shape (6.1) with (6.2) or (6.3) below (because $n^* - m \leq (1-\rho)n^*$).

PROPOSITION 6.3. *Suppose that*

$$q > R(n), \tag{6.1}$$

where

$$R(n) = R(n;q) = \left\{2^{2\rho n^*+u+1}\left(\frac{\frac{2(1-\rho)n^*}{s} + t - 1}{\delta - \frac{2(1-\rho)n^*}{sq^s}} + 2\right)\right\}^{2/n} \tag{6.2}$$

and $\delta = 1 - \sum_{i=1}^t 1/p_i$ *(with* $\delta = 1$ *when* $t = 0$*). Then* (q,n) *is a PFF pair.*

In particular, when additive sieving alone is being used (i.e., $t = 0$*), then* $R(n)$ *takes the form*

$$R(n) = R(n;q) = \left\{2^{2\rho n^*+u+1}\left(\frac{\frac{2(1-\rho)n^*}{s} - 1}{1 - \frac{2(1-\rho)n^*}{sq^s}} + 2\right)\right\}^{2/n}. \tag{6.3}$$

Note also that $R(n;q)$ depends on q (as well as n). Inasmuch as it is obviously a decreasing function of q (for fixed values of the other parameters), we shall apply it either when q has a specified value or when $q \geq q_0$ with q_0 specified. In what follows we shall, for convenience of calculation, use alternative weaker (i.e., larger) forms of $R(n)$ (to be denoted by $R_1(n)$, $R_2(n)$, etc): it will be sufficient to show that (6.1) holds for the relevant form.

We divide the discussion into two categories broadly according to whether $\rho > 1/3$ or $\rho \leq 1/3$ as described in Lemma 6.1.

PROPOSITION 6.4. *Suppose* $q \geq 5$ *and* $n^* \geq 8$ *with* $n^* \nmid q-1$*. Suppose also that* $\rho(q,n) > 1/3$*. Then* (q,n) *is a PFF pair.*

Proof. The circumstances where $\rho > 1/3$ are delineated in Lemma 6.1. Suppose first that $n = n^*$ and put $n = dn_1$, where $d = 2, 4$ or 6. Then $Q = d(q^n-1)/(n(q-1))$ and $n^* = n < qd$. By means of the simple bound (3.6) for $W(Q)$ and without multiplicative sieving, we obtain (as an alternative to $R(n)$)

$$R_1(n) := \left\{c2^{2\rho n+1}\left(\frac{d}{n(q_0-1)}\right)^{1/4}\left(\frac{\frac{2(1-\rho)n}{s} - 1}{1 - \frac{2d(1-\rho)}{sq_0^{s-1}}} + 2\right)\right\}^{4/n} \tag{6.4}$$

(with $c < 4.9$ and $q \geq q_0$) for use in (6.1).

Because $n^{1/n}$ decreases as n increases, it is seen (with a little effort) that $R_1(n)$ decreases as $n \geq 8$ increases under the given conditions.

From Lemma 6.1, suppose first that $\rho = 1/2$ (with $s = 2$ and $d = 2$). Then $R_1(8;59) < 57$. Hence (q,n) is a PFF pair whenever $q \geq 59$. Indeed, $R_1(12;43) < 41.6$, and $R_1(16;37) < 34.7$, etc., thus reducing further the list of possible exceptional pairs. Since $n < 2q$, it can thus be quickly checked (using R_1 for R in (6.1)) that the only pairs not shown to be PFF pairs are $(5,8)$, $(7,12)$, $(9,16)$, $(11,20)$, $(13,8)$, $(13,24)$, $(17,32)$, $(19,12)$, $(19,36)$, $(25,16)$, $(29,8)$, $(31,12)$, $(37,8)$, $(53,8)$.

These 14 pairs were then tested using (6.3), with u calculated by factorising Q. This was successful except for $(5,8)$, $(7,12)$, $(9,16)$, $(13,8)$. The final stage for these pairs was to sieve multiplicatively, also. Thus, for $(9,16)$, $Q = 2\cdot 5\cdot 17\cdot 41\cdot 193\cdot 21523361$, the largest four primes being the sieving ones. With $u = 2$ this yields $R(16) < 7.4$ and hence a PFF pair. Similarly, for $(13,8)$, $Q = 2\cdot 5\cdot 7\cdot 17\cdot 14281$, and, again with four sieving primes, this yields $R(8) < 11$ and another PFF pair. This process fails, however, for the two pairs $(5,8)$ and $(7,12)$. For these we give an explicit PFF polynomial as follows: for $(7,12)$, a PFF polynomial is $x^{12} + x^{11} - 3x - 2$; for $(5,8)$, one is $x^8 + x^7 - x^2 - x - 2$.

Next, suppose from Lemma 6.1 that $\rho = 3/8$ (with $s = 4$ and $d = 4$). This implies that $n \geq 16$. We calculate $R_1(16;19) < 17$ and $R_1(13;13) < 13$. This excludes only the pairs $(5,16)$, $(9,32)$ and $(13,16)$. In all these cases, $\omega(Q) \leq 7$. Using this in (6.3) with $u = 7$, we see that $(13,16)$ and $(9,32)$ are (comfortably) PFF pairs. For $(5,16)$, use multiplicative sieving. Here $Q = 2^2\cdot 3\cdot 13\cdot 17\cdot 313\cdot 11489$ and we take $u = 2$, $t = 4$ to yield $\delta = 0.8610$ and $R(16;5) < 5$.

Lastly, when $n^* = n$, suppose from Lemma 6.1 that $\rho = 13/36$ (with $s = 6$ and $d = 6$). This implies that $n \geq 36$ and $R_1(36;11) < 10.9$. This does leave the pair $(7,36)$ but an application of (6.3) with $u = 11$ yields $R(36;7) < 5$.

Finally, all pairs (q,n) with $n^* < n$ can be shown to be PFF pairs by using the principle of (4.8) with $b = 1$. Thus, instead of (6.4) a sufficient condition to guarantee a PFF pair is

$$q > R_2(n;q) := \left\{ c2^{2\rho n^*+1}\left(\frac{d}{n(q-1)}\right)^{1/4}\left(\frac{\frac{2(1-\rho)n^*}{s} - 1}{1 - \frac{2d(1-\rho)}{sq^{s-1}}} + 2\right)\right\}^{4/pn^*}.$$

For example, take $\rho = 1/2$ with n^* as in Lemma 6.1(i). Then q is odd ($p \geq 3$) and $R_2(n;q) \leq R_2(8;9) < 5$. The other cases are similar. ∎

For the remainder of this section we assume $\rho \leq 1/3$. Consider the function $R(n;q)$ defined by (6.3). In the situation to which it applies, s and ρ are determined by q and n. Nevertheless it is useful sometimes to consider $R(n;q)$ (and similar expressions) as functions of n, q, s and ρ, more loosely related. (For instance, since $s \geq 2$ is the least integer for which n^* divides $q^s - 1$, we have $n^* < q^s$ and $s \leq \phi(n^*) < n^*$.) It is important to ensure that $sq^s > 2(1-\rho)n^*$ so that the right side of (6.3) is a well-defined positive quantity. It is a consequence of the next lemma that, for given n, q, s with

$2 \le s < n^*$ and $8 \le n^* < q^s$ (indeed $n^* < q^2/2$ when $s = 2$), $R(n^*; q)$ is an increasing function of ρ for $0 \le \rho \le 1/3$.

LEMMA 6.5. *For fixed positive integers n, q, s with $2 \le s < n$ and $8 \le n < q^s$ (indeed with $n < q^2/2$ when $s = 2$), set*

$$\tau(\rho) = 2^{2\rho n} \frac{\frac{2(1-\rho)n}{s} - 1}{1 - \frac{2(1-\rho)n}{sq^s}}.$$

Then $\tau(\rho)$ is an increasing function for $0 \le \rho \le 1/3$.

Proof. Differentiate to obtain

$$(6.5) \qquad \tau'(\rho) = K \cdot [(\log 2)(2(1-\rho)n - s)(sq^s - 2(1-\rho)n) - s(q^s - 1)],$$

where $K = 2nq^s 2^{2\rho n}/(sq^s - 2(1-\rho)n)^2$ is a positive function (of all the variables).

If $s = 2$ then, since $0 \le \rho \le 1/3$ and $8 \le n < q^2/2$,

$$\tau'(\rho)/K \ge (\log 2)\left(\frac{4n}{3} - 2\right)(2q^2 - q^2) - 2q^2 = q^2\left(\left(\frac{4n}{3} - 2\right)\log 2 - 2\right) > 0.$$

If $3 \le s < n/2$, then, by (6.5), for $0 \le \rho \le 1/3$,

$$\begin{aligned}\tau'(\rho)/K &\ge n(\log 2)\left(\frac{4}{3} - \frac{1}{2}\right)(s-2)q^s - sq^s \\ &= q^s\left(s\left(\frac{5n}{6}\log 2 - 1\right) - \frac{5n}{3}\log 2\right) \\ &\ge q^s\left(3\left(\frac{5n}{6}\log 2 - 1\right) - \frac{5n}{3}\log 2\right) = q^s\left(\frac{5n}{6}\log 2 - 3\right) > 0,\end{aligned}$$

since $n \ge 8$.

Finally, if $n/2 \le s \le n$ $(< q^s)$, then, again by (6.5), and since $q^s \ge n + 1$ (q^s being an integer),

$$\begin{aligned}\tau'(\rho)/K &\ge \frac{n}{3}(sq^s - 4s)\log 2 - sq^s = s\left\{\left(\frac{n}{3}\log 2 - 1\right)q^s - \frac{4n}{3}\log 2\right\} \\ &\ge s\left[(n+1)\left(\frac{n}{3}\log 2 - 1\right) - \frac{4n}{3}\log 2\right] \\ &= \frac{ns}{3}\left[(n-3)\log 2 - 3\left(1 + \frac{1}{n}\right)\right] > 0,\end{aligned}$$

again since $n \ge 8$. ∎

In practice, when $n = n^*$ it is convenient to employ a larger "starter" function $\bar{R}(n; q)$,

$$(6.6) \qquad (R(n;q) <)\ \bar{R}(n) = \bar{R}(n;q) := \{2^{(2/3)n+u+1}(2n-1)\}^{2/n},$$

derived from $R(n)$ by taking $\rho = 1/3$, and then using the facts that $n < q^s$ and $s \geq 2$. In the result which follows we employ suitable modifications of these ideas.

PROPOSITION 6.6. *Suppose $q \geq 5$ and $n^* \geq 8$ with $n^* \nmid q - 1$. Suppose also that $\rho(q, n) \leq 1/3$. Then (q, n) is a PFF pair.*

Proof. We concentrate on the case when $n = n^*$ in the theoretical discussion. But recall (4.8) with $b \geq 1$ for the relevant modification in the (computationally less demanding) case $n^* < n$ and observe that Lemma 6.5 (with $n = n^*$) is then also applicable. For an example of how to proceed when $n^* < n$, see Case I below.

CASE O: $n^* = q^2 - 1$. In this situation, the argument about $R(n)$ increasing with ρ (to be used elsewhere) fails. Here $\rho = 1/(q + 1)$ and $R(n) = R(q^2 - 1)$ (see (6.3)), using $W(Q) < q^{(q^2-1)/4}$ (by Lemma 3.7), has the form

$$R(q^2 - 1) = (c2^{2q-1}(q^3 - q^2 - q + 2))^{4/(q^2-1)}.$$

With $c = 4.9$, it is quickly seen that $R(q^2 - 1)$ decreases and is less than 5.2 for $q \geq 6$. This leaves only the pair $(5, 24)$, discussion of which is incorporated with the figures for the most delicate cases in Case II below. Aside from this, in what follows we assume (as we may) $n^* < q^2/2$ when $s = 2$.

CASE I: $q \geq 8$. Since the conditions of Lemma 6.5 with $n = n^*$ are satisfied, replace ρ by 1/3 and use Lemma 3.7 in (6.1) and (6.3). It therefore suffices that $q > R_3(n)$, where

$$(6.7)\quad R_3(n) = R_3(n; q, s) = \left\{ c2^{(2/3)n^*+1} \frac{1}{(q-1)^{1/4}} \left(\frac{\frac{4n^*}{3s} - 1}{1 - \frac{4n^*}{3sq^s}} + 2 \right) \right\}^{4/n},$$

where $c < 4.9$. Here a suitable starter form, derived from (6.7) by using $s \geq 2$ and $n^* < q^s$, is

$$(6.8)\qquad \bar{R}_3(n) = \bar{R}_3(n; q) = \left\{ c2^{(2/3)n^*+1} \frac{(2n^* - 1)}{(q-1)^{1/4}} \right\}^{4/n}.$$

To eliminate at the outset the case in which $n^* < n$, suppose this holds so that $n \geq 2n^*$. Then, in accordance with (4.8), the exponent of the right side of (6.8) may be replaced by $2/n^*$ to yield a function which evidently increases as n^* or q decreases and whose numerical value when $n^* = q = 8$ and $c = 4.9$ is less than 7.1. It follows that $\bar{R}_3(n) < q$ and (q, n) is a PFF pair.

From now on suppose $n^* = n$. Again $\bar{R}_3(n; q)$ increases as n or q decreases. With $c = 4.9$, we have $\bar{R}_3(8; 49) < 47.5$. Hence the result holds for $q \geq 49$.

We treat prime powers $q \le 47$ first by $\bar{R}_3(n)$, to establish the result for (potentially) large values of n and s, and then by $R_3(n)$ for more critical values of n, with s (close to) 2. Indeed, to begin, suppose $37 \le q \le 47$. Take $c = 4.9$. Since $\bar{R}_3(10; 37) < 36$ the result holds for this range of q, provided $n \ge 10$. But also $R_3(8; 37, 2) < 32.1$. Hence the result holds unconditionally.

Finally suppose $8 \le q \le 32$. Since $\bar{R}_3(130; 8) < 8$ it can be assumed $8 \le n < 130$. Excluding pairs covered by previous results (such as Propositions 5.1, 5.3 and 5.4) there are 124 pairs left. For these, evaluate $R_3(n; q, s)$ using the relevant precise value of s. Many of them are such that $R_3(8) < q$: these yield PFF pairs. For the remaining 64 pairs evaluate $R(n)$ given by (6.3) using the exact values of $u = \omega(Q)$ and s but with $\rho = 1/3$. In each case $R(n) < q$ so that (q, n) is a PFF pair. Some of the smaller cases are summarised as follows. Take $q = 11$. Then, with $c = 4.45$, we have $R(8) < 9.6$ and $R(15) < 10.7$ (with $(s = 2, u = 4)$ in each case). Take $q = 9$ (so that $n \ge 20$). Then indeed, with $c = 3.2$, $R(20) < 5.5$ (with $u = 6$). Take $q = 8$ so that $n \ge 15$. Then, with $c = 2.9$, $R(15) < 5.6$ (with $u = 5$). Thus Case I has been completed simply by additive sieving with $\rho = 1/3$.

Case II: $q = 5$ or 7. Take $n = n^*$. (The modifications when $n^* < n$ are similar to the treatment of (6.8) but more immediate because we can assume $p \ge 5$ in (4.8).)

The argument follows broadly the same pattern as Case I, except that, because $2^{8/3} > 6.34$, the expression $R_3(n)$ is useless when $q = 5$ and ineffective when $q = 7$. We therefore proceed as follows. Suppose $n > q^2$ so that $s \ge 3$. Suppose first that also $\omega(Q) \ge 49$. By Lemma 6.2 and the fact that $n/2 - n/6 = n/3$, we obtain as an alternative to (6.7) the equation

$$(6.9) \qquad R_4(n) = R_4(n; q, s) = \left\{ 2^{(2/3)n+1} \frac{1}{(q-1)^{1/6}} \left(\frac{\frac{4n}{3s} - 1}{1 - \frac{4n}{3sq^s}} + 2 \right) \right\}^{3/n}.$$

Here the starter form, derived from (6.9) using $s \ge 3$ and $n < q^s$, is

$$(6.10) \qquad \bar{R}_4(n) = \bar{R}_4(n; q) = \left\{ 2^{(2/3)n+1} \frac{(4n+1)}{5(q-1)^{1/6}} \right\}^{3/n}.$$

Now $\bar{R}_4(58; 5) < 4.998$ and $\bar{R}_4(16; 7) < 6.98$. Summarising, whenever $\omega(Q) \ge 49$, we have shown that necessarily $n \le 57$ $(q = 5)$ and $n \le 15$ $(q = 7)$. But, easily, if $n \le 57$ (say), then $\omega(Q) < 49$.

Hence we may suppose that $\omega(Q) \le 48$. Since $s \ge 3$ the appropriate starter form for $R(n)$ itself (in place of (6.6)) is

$$\bar{R}(n) = \bar{R}(n; 5, u) := \{2^{(2/3)n+u+1}(4n+1)/5\}^{2/n}.$$

For the rest, we focus almost exclusively on the more delicate case when $q = 5$. Then $\bar{R}(113; 5, 48) < 4.98$. So assume $n \le 112$, in which case since $Q \le (5^n - 1)/4$, necessarily $\omega(Q) \le 45$. Moreover, since in (6.3), $R(106; 5) <$

4.991 (with $u = 44$, $\rho = 1/3$, $s = 3$), we can suppose that $n \le 105$. Indeed, by repetition of this argument using $R(n;5)$ and smaller values of u, we conclude that we can suppose $n \le 90$.

The next stage for $n \le 90$ is to calculate the true value of $\omega(Q)$ and s and use $R(n;5)$. We find that each relevant $(5,n)$ ($n \ne 12$) is a PFF pair. The smallest (most delicate) values are tabulated below. When the same exercise is applied to $\mathbb{F}_7$, the only outstanding degree is $n = 9$, in which case apply Proposition 6.3 in full, using the form (6.2) for $R(n)$. We tabulate the outcome below.

q	n	s	ρ	Q	u	t	δ	$R(n)$
5	9	6	2/9	$19 \cdot 31 \cdot 829$	3	0	1	4.49
5	18	6	2/9	$3^3 \cdot 7 \cdot 19 \cdot 31 \cdot 829 \cdot 5167$	4	0	1	3.85
5	24	2	1/6	$2 \cdot 3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 313 \cdot 601 \cdot 390001$	8	0	1	3.91
7	9	3	1/3	$3 \cdot 19 \cdot 37 \cdot 1063$	1	3	0.919	4.82

For the pair $(5,12)$, Proposition 6.3 fails: in that case we have the explicit PFF polynomial $x^{12} + x^{11} + x^3 - x^2 - 2x - 2$.

As a consequence, Proposition 6.6 is established. ∎

7. Very small fields. In this section, we study the smallest fields $\mathbb{F}_q$ when $2 \le q \le 4$. For these it is imperative to use a smaller value of ρ than provided by Lemma 6.1.

Lemma 7.1 ([5]). *Assume that $n > 4$ ($p \nmid n$). Then the following hold:*

(i) *Suppose $q = 4$. Then $\rho(4,9) = 1/3$; $\rho(4,45) = 11/45$; otherwise $\rho(4,n) \le 1/5$.*
(ii) *Suppose $q = 3$. Then $\rho(3,16) = 5/16$; otherwise $\rho(3,n) \le 1/4$.*
(iii) *Suppose $q = 2$. Then $\rho(2,5) = 1/5$; $\rho(2,9) = 2/9$; $\rho(2,21) = 4/21$; otherwise $\rho(2,n) \le 1/6$.*

When $n = n^*$, i.e., $p \nmid n$, variations of Lemma 6.2 are also invoked where appropriate. When $n > n^*$, i.e., $p \mid n$, although, in the main, Lemma 3.7 suffices, more attention has to be paid than heretofore. Thus, with $n = p^b n^*$, a combination of (6.3) and (3.6) (in the spirit of (4.8)) yields the criterion

$$q > R_5(n) := \left(c 2^{2\rho n^* + 1} \left(\frac{\frac{2n^*(1-\rho)}{s} - 1}{1 - \frac{2n^*(1-\rho)}{sq^s}} + 2 \right) \right)^{\frac{4}{p^b n^*}} \tag{7.1}$$

for (q,n) to be a PFF pair. Here $c = 2.9$ if $q = 2$ or 4 whereas $c = 3.2$ if $q = 3$. Moreover, although we can assume $n^* > 4$ (by Propositions 3.8 and 4.3), note that Lemma 6.5 does not apply if $n^* = 5$ or 7 and we address these cases first (when, as it happens, always $\rho = 1/n^*$). Note that, for other variables fixed, R_5 decreases as b increases. Further, the least values of b satisfying (7.1) can be tabulated as follows:

n^*	q	s	b	$R(n)$	q	s	b	$R(n)$	q	s	b	$R(n)$
5	4	2	2	2.68	3	4	2	1.47	2	4	3	1.53
7	4	3	1	3.94	3	6	1	2.28	2	3	3	1.45

It follows that, when $n > n^*$, only the pairs $(q,n)=(4,10),(3,15),(2,10),(2,20),(2,14),(2,28)$ remain. Otherwise we may assume $n^* \geq 8$.

7.1. The field $\mathbb{F}_4$. Here $n^* = n$ if and only if n is odd, whereas Q, a divisor of $4^n - 1$, is always odd.

PROPOSITION 7.2. *Suppose $q = 4$ and $n \neq 3$. Then (q,n) is a PFF pair.*

Proof. For the main working suppose $n^* \geq 8$ and $s > 1$. By Lemma 7.1, $\rho(n) \leq 1/5$, except when $n^* = 9$ ($\rho = 1/3$) or $n^* = 45$ ($\rho = 11/45$). Further, $s = 2$ when $n^* = 15$; $s = 3$ when n^* divides 63; otherwise $s \geq 4$.

Start from the sufficient condition (6.1) with $R(n)$ given by (6.3) and $u = \omega(Q)$. It involves the expression

$$E := \frac{\frac{2n^*(1-\rho)}{s} - 1}{1 - \frac{2n^*(1-\rho)}{sq^s}} + 2, \tag{7.2}$$

for which $2^{\rho n^*}E$ is increasing with ρ in conformity with Lemma 6.5.

First suppose $n^* = 15$ (the only situation in which Lemma 6.5 does *not* apply); thus $\rho = 1/5$. Since here $E = 46$ and the (crude) bound $W(Q) < 2.9 \cdot 4^{n/4}$ holds (by Lemma 3.7), it follows from (4.8) with $b = 1$ that, when $n^* < n$, then inequality (6.1) certainly holds whenever

$$4 > (2.9 \cdot 2 \cdot 46)^{2/n^*} = (266.8)^{2/15} = 2.106\ldots,$$

which leaves only the case $n = 15$ itself.

Now suppose that $n^* \neq 15$. Indeed, first assume $n > 63$ is odd, i.e., $n = n^*$ and $s \geq 4$. In order to construct a suitable starter function for larger values of n, by Lemma 6.5 replace ρ by 1/5. By Lemma 3.7, $W(Q) < 2.9q^{n/4}$. Using $n < q^s$ and $s/(s-2(1-\rho)) > 1$, we see that, by (4.8) with $b = 0$, the condition $4 > R_6(n)$ suffices, where

$$R_6(n) \ = R_6(n;s) = \left\{5.8\left(\frac{8n}{5s-8} + 1\right)\right\}^{20/n}.$$

Here $R_6(n)$ decreases both as a function of s and as a function of n. Hence, for $n > 83$, $R_6(n) \leq R_6(84,4) < 4$ and (q,n) is a PFF pair.

Assume n is even so that $n = 2^b n^*$ with $b \geq 1$ and $s \geq 3$. By Lemma 6.5, replace ρ by 1/3 so that by (7.1) we can use

$$R_7(n) \; = R_7(n;s,b) = \left\{5.8\left(\frac{4n^*}{3s-4}+1\right)\right\}^{\frac{12}{n^*(3\cdot 2^b-4)}}.$$

In fact, $R_7(42;3,1)$, $R(16;3,2)$ and $R_7(7;3,3)$ are each less than 4 so that (q,n) is a PFF pair for $n \geq 84$.

It follows that for a putative exception n to Proposition 7.2 we may assume $n \leq 83$. For the remaining possibilities, we evaluate $R(n)$ given by (6.3) with precise values for s, ρ and $u = \omega(Q)$: if it is less than $q = 4$ then there *does* exist a PFF polynomial for that value of n. For larger values of n and those for which n^* is prime (in which case $\rho = 1/n$), comfortably $R(n) < 4$. We tabulate the outcome in the more delicate cases with $n \geq 10$: in particular, the column headed R lists $R(n)$ truncated to three decimal places.

n	s	ρ	u	R	n	s	ρ	u	R
45	6	11/45	11	3.187	25	10	1/5	4	3.238
36	3	1/3	12	2.277	21	3	1/7	6	3.063
35	6	1/7	9	2.532	18	3	1/3	8	3.815
33	5	1/11	8	2.195	15	2	1/5	6	**5.539**
30	2	1/5	11	2.965	11	5	1/11	4	3.238
27	9	5/27	6	2.729	10	2	1/5	5	**4.337**

We conclude that if there is no PFF polynomial of degree n, then $n \in \{15, 10, 9, 7, 5\}$. For the values $n = 10, 7$, using also multiplicative sieving yields the result. Specifically, suppose $n = 10$. Then $Q = 3^2 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41$, which has 5 prime factors. In (6.2), take $u = 1$, $t = 4$. Then $\delta > 0.6524$, which yields $R(10) < 3.73 < 4$. For $n = 7$, $Q = 3^2 \cdot 43 \cdot 127$. In this case, take $u = 1$, $t = 2$, so that $\delta > 0.9688$ and $R(7) < 3.93 < 4$.

Finally, we exhibit explicit PFF polynomials for the remaining degrees (including $n = 6$, held over from Proposition 4.3).

n	PFF polynomial
15	$x^{15} + x^{14} + (u+1)x^{12} + (u+1)x^{10} + x^9 + x^8 + x^7$ $+ ux^6 + ux^5 + ux^4 + x^2 + ux + u + 1$
9	$x^9 + (u+1)x^8 + ux^7 + (u+1)x^6 + ux^5 + ux^3 + (u+1)x + u$
6	$x^6 + ux^5 + (u+1)x^4 + (u+1)x^3 + ux + u + 1$
5	$x^5 + ux^4 + ux^3 + x + u + 1$

For these, we use $\mathbb{F}_4 = \mathbb{F}_2(u)$, where $u^2 + u + 1 = 0$. ■

7.2. The ternary field $\mathbb{F}_3$. For the main part, again suppose $n^* \geq 8$ and $s \geq 2$. Here any version of Lemma 3.7 valid for all integers is inadequate: the following numerical bound for large integers will be needed.

Lemma 7.3. *Suppose h is indivisible by* 3 *and $\omega(h) \geq 52$. Then*

$$W(h) < h^{4/25}.$$

Proposition 7.4. *Suppose $q = 3$ and $n \neq 4$. Then (q, n) is a PFF pair.*

Proof. By Lemma 7.1, unless $n^* = 16$, we have $\rho(n) \leq 1/4$, whereas $\rho(16) = 5/16$. Again, start from the sufficient condition (6.1) with $R(n)$ given by (6.3) and $u = \omega(Q)$.

Suppose $3 \mid n$ (i.e., $n > n^*$). By Lemma 6.5 we may replace ρ in E (given by (7.2)) by 5/16 and then use the facts that $n^* < q^s$ and $s \geq 2$ to yield $E < 3n - 2$. Since $c_Q < 3.2$ and $p = 3$ it follows from Lemma 3.7 and (4.8) that $(3, n)$ is a PFF pair whenever

$$3/2^{5/(2\cdot 3^b)} > (6.4(3n-2))^{4/(3^b n^*)}$$

and this holds if $n^* \geq 11$ for $b = 1$ and $n^* \geq 3$ for $b \geq 2$. Hence when $3 \mid n$, we can assume $n = 3n^* \leq 30$.

Now suppose $3 \nmid n$ (so that $n^* = n$). With Lemma 7.3 in view, suppose $\omega(Q) \geq 52$ so that certainly $\rho \leq 1/4$ and $s \geq 4$. Moreover, $n = n^* \neq 8$; so in $R(n)$ replace ρ by 1/4 by Lemma 6.5. From (6.3) and Lemma 7.3, we derive the sufficient condition

$$3^{17/25}/2 > \left(\frac{2(3n+2)}{5}\right)^{2/n},$$

which holds whenever $n \geq 205$ and therefore whenever $\omega(Q) \geq 52$.

Continue to suppose $3 \nmid n$ with $n \geq 55$ and $n \neq 80$ (so that $\rho \leq 1/4$ and $s \geq 5$) but assume now that $\omega(Q) \leq 51$. We introduce a multiplicative aspect to the sieve by invoking $R(n)$ as in (6.2). To show that $R(n)$ is increasing with ρ, analogously to Lemma 6.5 consider

$$\tau(\rho) = \log\left[2^{2\rho n}\left(\frac{2(1-\rho)(n/s) + t - 1}{\delta - 2(1-\rho)n/(sq^s)}\right)\right], \tag{7.3}$$

with $q = 3$. Here we suppose δ is bounded below by 0.42, an assumption that will be realised in applications. (In the first place, since $\rho > 0$ and $s \geq 5$, this guarantees that $\delta - 2(1-\rho)/s$ and so $\delta - 2(1-\rho)n/(sq^s)$ are positive.) For fixed s, differentiate $\tau(\rho)$ to obtain

$$\tau'(\rho) = 2n\log 2 - \frac{1}{(1-\rho) + s(t-1)/(2n)} - \frac{1}{\delta sq^s/(2n) - (1-\rho)}, \tag{7.4}$$

with $q = 3$. Since $0 < \rho \leq 1/4$, $n < 3^s$, $s \geq 5$ and $\delta \geq 0.42$ it follows that $\tau'(\rho) \geq 2n\log 2 - 4/3 - 3.4$, which is positive.

Granted that $\delta \geq 0.42$ it can be concluded that, for a given n and t, $\tau(n)$ and so $R(n)$ are maximised when $s = 5$ and $\rho = 1/4$. This yields the condition $3 > R_6(n)$, where

$$R_6(n) = 2\left(2^{1+u}\left(\frac{3n+10(t-1)}{10\delta-3}+2\right)\right)^{2/n}, \tag{7.5}$$

with t denoting the number of multiplicative sieving primes and u those of the multiplicative core m_0 (which divides Q). To use (7.5), let the least $u = 6$ primes in Q contribute to the core m_0. Then $t \le 45$ is the number of sieving primes and

$$\delta \ge 1 - \left(\tfrac{1}{19} + \tfrac{1}{23} + \cdots + \tfrac{1}{239}\right) = 0.42734\ldots.$$

Since $R_6(55.4) < 3$ there exists a PFF polynomial of degree n whenever $n \ge 55$ ($n \ne 80$).

Next, for values of $n \le 53$ (indeed ≤ 30 if $3 \mid n$) and $n = 80$ calculate $R(n)$ given by (6.3). Only those degrees which produce a value of $R(n) > 2.2$ are tabulated; none has $n^* < n$.

n	s	ρ	u	R	n	s	ρ	u	R
52	6	11/52	6	2.403	14	6	1/7	3	2.780
44	10	7/44	8	2.273	13	3	1/13	1	2.243
32	8	7/32	6	2.811	11	5	1/11	2	2.520
28	6	3/28	6	2.234	10	4	1/5	3	**4.208**
24	2	1/4	7	2.532	8	2	1/4	3	**8.122**
22	5	1/11	5	2.298	7	6	1/7	1	**3.023**
20	4	3/20	5	2.903	5	4	1/5	1	**4.720**
16	4	5/16	4	**5.085**					

To supplement this table note that when $n = 7$ we can successfully use (6.2) by sieving also with the single prime divisor of $Q = 1093$: this yields $R(7) < 2.694 < 3$. Including cases held over from Proposition 3.8, this leaves $n \in \{16, 12, 10, 8, 6, 5, 3\}$, for which we obtain a PFF polynomial in every case by direct verification of the properties.

n	PFF polynomial
16	$x^{16} - x^{15} + x^7 - x - 1$
12	$x^{12} + x^{11} + x^3 + x^2 + x - 1$
10	$x^{10} + x^9 + x^7 + x^3 - x - 1$
8	$x^8 + x^7 + x^4 - x^3 - x^2 + x - 1$
6	$x^6 + x^5 + x^3 + x^2 + x - 1$
5	$x^5 + x^4 - x + 1$
3	$x^3 + x^2 - x + 1$

In fact when $n = 3$ there is only one pair of PFF polynomials. ■

We remark that we incorporated multiplicative sieving as a device to treat general values of $n \geq 55$ (with $3 \nmid n$) in Proposition 7.4. Nevertheless, it is likely that, for any *specific* value of $n \geq 55$, additive sieving using (6.3) would suffice. A similar remark would apply to the proof of Proposition 7.6 below.

7.3. The binary field $\mathbb{F}_2$. A suitable numerical result on $W(h)$ here is the following.

LEMMA 7.5. *Suppose the* odd *integer h is such that $\omega(h) \geq 175$. Then $W(h) < h^{3/25}$.*

PROPOSITION 7.6. *Suppose $q = 2$ and $n \neq 3, 4$. Then (q, n) is a PFF pair.*

Proof. The cases $(2, n)$, $n = 6, 10, 14, 12, 14, 20, 24, 28$, have been held over. Otherwise, suppose that $n^* \geq 8$, so that $s \geq 4$. Here $Q = 2^n - 1$. By Lemma 7.1, if $n^* > 21$, then $\rho \leq 1/6$.

Suppose first that n is *even*. If $n^* = 21$, then $\rho = 5/21$, $s = 6$ and (7.1) holds for $b = 2$. This leaves $n = 42$. The same occurs if $n^* = 9$; then $\rho = 2/9$, $s = 6$, and only $n = 18$ is left. For other values of n, by Lemma 6.5, increase ρ in $R_5(n)$ to $1/6$. Then as before use $n^* < q^s$ and $s/(s - 2(1 - \rho)) > 1$ (where $s \geq 4$) to obtain the starter function

$$R_8(n) = R_8(n; b) := \left(\frac{5.8(5n^* + 7)}{7}\right)^{\frac{12}{n^*(3\cdot 2^b - 4)}}. \tag{7.6}$$

Then $R_8(n; 1) < 2$ whenever $n^* \geq 46$ and $R_8(n; 2) < 2$ whenever $n^* \geq 8$. It follows that except possibly for (relevant) values of $n = 2n^* \leq 90$ there is a PFF polynomial of given even degree n.

Now suppose n (> 64) is *odd*, so that $n^* = n$, $\rho \leq 1/6$ and $s \geq 7$. By Lemma 6.5 we can replace ρ by $1/6$ in $R(n)$ given by (6.3). In order to apply Lemma 7.5 suppose (temporarily) that additionally $\omega(Q) \geq 175$. Since $1/2 - 1/3 - 3/25 = 7/150$, $n < q^s$ and $s \geq 7$ we deduce that there is a PFF polynomial of degree n whenever

$$2 > R(n) = \left(\frac{2(5n + 11)}{16}\right)^{150/(7n)}$$

and so whenever $n \geq 139$. Easily, this is implied by $\omega(Q) \geq 175$.

Accordingly, we can now suppose $\omega(Q) \leq 174$. Introduce a multiplicative dimension to the sieve by applying the criterion of Proposition 6.3 with $R(n)$ given by (6.2). By (7.3) with $q = 2$ and provided $\delta > 0.42$, $\tau(n)$ is increasing for $0 < \rho \leq 1/6$, since $\tau'(\rho) \geq 2n \log 2 - 7/6 - 100/47 \geq 2n \log 2 - 4$ is positive. Hence in $R(n)$ we may replace ρ by $1/6$ and s by 7, to obtain the sufficient condition

$$2 > R_9(n) := \left\{ 2^{u+1} \left(\frac{5n + 21(t-1)}{21\delta - 5} + 2 \right) \right\}^{6/n},$$

provided $\delta > 0.42$, where u is the number of prime integers in the multiplicative core.

First take $u = 13$ so that $t \le 161$. Then $\delta > 0.4354$ and $R_9(144) < 2$. Hence we can suppose $n \le 143$. This implies $\omega \le 27$. Thus $u + t \le 28$. Repeat the above process with $u = 4$, $t \le 23$ and so $\delta > 0.4353$. Then $R_9(77) < 2$ and we can suppose $n \le 75$. Then $\omega(Q) \le 16$. Repeat once more with $u = 3$, $\delta > 0.4787$ to yield $R_9(66) < 2$.

Consequently, for the last stage, assume $n \le 65$ (n odd) or $n \le 90$ ($n = 2n^*$ even), and calculate $R(n)$ given by (6.3). The table lists the outcome for values of n with $n \ge 11$ which produce a value of $R(n)$ exceeding 1.8. Also included are the even values of n held over (as listed at the start of this proof).

n	s	ρ	u	R	n	s	ρ	u	R
45	12	1/9	6	1.963	21	6	4/21	3	**2.662**
42	6	4/21	6	1.801	20	4	1/5	5	1.952
35	12	4/35	4	1.856	18	6	1/9	4	**2.290**
30	4	2/15	6	1.953	15	4	2/15	3	**2.892**
28	3	1/7	6	1.811	14	3	1/7	3	**2.438**
27	3	1/9	3	1.839	13	12	1/13	1	1.814
24	2	1/3	6	1.887	11	10	1/11	2	**2.293**

Beyond this table, degrees $n = 11$, 18 and 21 can be treated theoretically. For $n = 11$ use (6.2) by sieving also with the two prime divisors of $Q = 23{\cdot}89$. This yields $R(11) = 1.968\ldots < 2$. Similarly, when $n = 18$, sieve also with the 4 prime divisors of $Q = 3^3 \cdot 7 \cdot 19 \cdot 73$. This yields $R(18) = 1.980\ldots < 2$. Finally when $n = 21$, for this occasion only, modify the key strategy for the additive sieve as follows. Over $\mathbb{F}_2$, we have $x^{21} - 1 = P_1 \cdot P_2 \cdot P_{31} \cdot P_{32} \cdot P_{61} \cdot P_{62}$, where the P's are distinct irreducible polynomials of degree indicated by the first subscript. For the sieve take the "core" to be $P_1 P_2$ and the sieving irreducibles to be those of degrees 3 and 6 together with the three prime factors of $Q = 7^2{\cdot}127{\cdot}337$. The crucial denominator satisfies $\delta - 4/2^3 - 4/2^6 = 0.2838\ldots$, and $R(21) = 1.963\ldots < 2$.

A final table of PFF polynomials is as follows.

n	PFF polynomial
15	$x^{15}+x^{14}+x^4+x+1$
14	$x^{14}+x^{13}+x^5+x^3+x^2+x+1$
12	$x^{12}+x^{11}+x^9+x^4+x^3+x+1$
10	$x^{10}+x^9+x^4+x+1$
9	$x^9+x^8+x^5+x^4+x^3+x+1$
8	$x^8+x^7+x^2+x+1$
7	$x^7+x^6+x^3+x+1$
6	$x^6+x^5+x^2+x+1$
5	$x^5+x^4+x^2+x+1$

We remark that, for $n = 6$ and $n = 5$, there is a single pair of reciprocal PFF polynomials. ■

Acknowledgements. The second author is supported by a Royal Society Dorothy Hodgkin Fellowship.

We thank the referee for his extremely careful and meticulous reading of successive versions of the manuscript. This has extended far beyond the normal call of duty and we are both appreciative of and grateful for all his efforts.

References

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

[2] —, *Some problems involving primitive roots in a finite field*, Proc. Nat. Acad. Sci. USA 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] —, *Kloosterman sums and primitive elements in Galois fields*, Acta Arith. 94 (2000), 173–201.

[5] S. D. Cohen and S. Huczynska, *The primitive normal basis theorem—without a computer*, J. London Math. Soc. 67 (2003), 41–56.

[6] H. Davenport, *Bases for finite fields*, ibid. 43 (1968), 21–39; 44 (1969), 378.

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

[8] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge Univ. Press, 1986.

[9] T. Tian and W. F. Qi, *Primitive normal element and its inverse in finite fields*, Acta Math. Sinica (Chin. Ser.) 49 (2006), 657–668 (in Chinese; English summary).

Stephen D. Cohen
Department of Mathematics
University of Glasgow
Glasgow, G12 8QW, UK
E-mail: sdc@maths.gla.ac.uk

Sophie Huczynska
School of Mathematics and Statistics
University of St Andrews
St Andrews, Fife, KY16 9SS, UK
E-mail: sophieh@mcs.st-and.ac.uk

Received on 7.5.2007
and in revised form on 12.3.2010 (5441)