MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 217-231

Primitive Normal Bases for Finite Fields

By H. W. Lenstra, Jr. and R. J. Schoof

Dedicated to Daniel Shanks

Abstract. It is proved that any finite extension of a finite field has a normal basis consisting of primitive roots.

Introduction. Let q be a prime power, $q > 1$. We denote by $\mathbf{F}_q$ a finite field of q elements. It is well known that for every positive integer m there exists a *normal basis* of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$, i.e., a basis of the form

$$\left(\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}\right)$$

with $\alpha \in \mathbf{F}_{q^m}$. It is also well known that the multiplicative group $\mathbf{F}_{q^m}^*$ of $\mathbf{F}_{q^m}$ is cyclic, i.e., that for some $\alpha \in \mathbf{F}_{q^m}^*$ we have

$$\mathbf{F}_{q^m}^* = \{\alpha^n\colon n \in \mathbf{Z}\}.$$

Such an element α is called a *primitive root* of $\mathbf{F}_{q^m}$. Following Davenport [4] we call a normal basis $(\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}})$ of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$ a *primitive normal basis* if α is a primitive root of $\mathbf{F}_{q^m}$.

Carlitz [2], [3] proved in 1952 that for all sufficiently large q^m there exists a primitive normal basis of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$. Davenport [4] proved in 1968 that a primitive normal basis exists for all m if q is prime. In the present paper this result is extended to the general case.

THEOREM. *For every prime power $q > 1$ and every positive integer m there exists a primitive normal basis of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$.*

Section 1 contains an exposition of certain results due to Ore [7] concerning the Galois module structure of finite fields. These lead to an alternative formulation of the theorem. In Section 2 we describe an improved version of the method of Carlitz and Davenport, which handles all but finitely many pairs (q, m). In Section 3 we determine which are the remaining pairs, and they are dealt with in Section 4.

We denote the cardinality of a set S by $\#S$, and the group of units of a ring R with 1 by R^*. If f, g are polynomials in one variable, we mean by $g \mid f$ that g divides f and is *monic*, i.e., has leading coefficient one. The same notation for divisibility is used for *positive* integers.

Received March 5, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11T30, 12E20.
Key words and phrases. Finite field, normal basis, primitive root.

1. The Cyclic Structure of Finite Fields. Let q be a prime power, $q > 1$, and denote by $\overline{\mathbf{F}}_q$ an algebraic closure of $\mathbf{F}_q$. Let $\sigma\colon \overline{\mathbf{F}}_q \to \overline{\mathbf{F}}_q$ be defined by $\sigma(\alpha) = \alpha^q$ for all $\alpha \in \overline{\mathbf{F}}_q$. For $f = \sum_{i=0}^{n} a_i X^i \in \mathbf{F}_q[X]$ and $\alpha \in \overline{\mathbf{F}}_q$ we define

$$f \circ \alpha = \sum_{i=0}^{n} a_i \sigma^i(\alpha).$$

This makes the additive group of $\overline{\mathbf{F}}_q$ into a module over $\mathbf{F}_q[X]$. We shall see that many well-known properties of the multiplicative group of $\overline{\mathbf{F}}_q$ have analogues for the additive group when considered as an $\mathbf{F}_q[X]$-module.

For a positive integer m, let $\mathbf{F}_{q^m}$ be the unique subfield of $\overline{\mathbf{F}}_q$ of order q^m. For $\alpha \in \overline{\mathbf{F}}_q^*$ we have

$$\alpha \in \mathbf{F}_{q^m} \Leftrightarrow \sigma^m(\alpha) = \alpha \Leftrightarrow \alpha^{q^m-1} = 1.$$

It follows that the multiplicative order $\operatorname{ord}(\alpha)$ of α is finite and relatively prime to q, for each $\alpha \in \overline{\mathbf{F}}_q^*$. Also, we have

$$\alpha \in \mathbf{F}_{q^m} \Leftrightarrow \operatorname{ord}(\alpha) \mid q^m - 1.$$

Let the *degree* $\deg(\alpha)$ of an element $\alpha \in \overline{\mathbf{F}}_q$ be the degree of the irreducible polynomial of α over $\mathbf{F}_q$. Clearly, $\deg(\alpha)$ is the smallest m with $\alpha \in \mathbf{F}_{q^m}$, which, for $\alpha \neq 0$, is the smallest m with $q^m \equiv 1 \bmod \operatorname{ord}(\alpha)$. This proves

(1.1) *Let* $\alpha \in \overline{\mathbf{F}}_q^*$, $\operatorname{ord}(\alpha) = n$. *Then* $\deg(\alpha)$ *equals the multiplicative order of* $(q \bmod n)$ *in the group* $(\mathbf{Z}/n\mathbf{Z})^*$.

To obtain the additive analogue, we start from

$$\alpha \in \mathbf{F}_{q^m} \Leftrightarrow \sigma^m(\alpha) = \alpha \Leftrightarrow (X^m - 1) \circ \alpha = 0,$$

for $\alpha \in \overline{\mathbf{F}}_q$. It follows that for any $\alpha \in \overline{\mathbf{F}}_q$ the annihilator of α in $\mathbf{F}_q[X]$ is nonzero. Let the unique monic polynomial in $\mathbf{F}_q[X]$ generating this annihilator as an ideal be called the *Order* of α; notation: $\operatorname{Ord}(\alpha)$. We have

$$\alpha \in \mathbf{F}_{q^m} \Leftrightarrow \operatorname{Ord}(\alpha) \mid X^m - 1, \tag{1.2}$$

so that $\operatorname{Ord}(\alpha)$ is relatively prime to X. As above, we obtain

(1.3) *Let* $\alpha \in \overline{\mathbf{F}}_q$, $\operatorname{Ord}(\alpha) = f$. *Then* $\deg(\alpha)$ *equals the multiplicative order of* $(X \bmod f)$ *in the group* $(\mathbf{F}_q[X]/f\mathbf{F}_q[X])^*$.

We give a picturesque application.

(1.4) LEMMA. *If* $X^p + X + 1$ *is irreducible in* $\mathbf{F}_2[X]$, *and* $2^p - 1$ *is prime, then* $X^{2^p-1} + X + 1$ *is irreducible in* $\mathbf{F}_2[X]$.

Proof. Take $q = 2$, and let $\alpha \in \overline{\mathbf{F}}_2$ satisfy $\alpha^{2^p-1} + \alpha + 1 = 0$. It suffices to show that $\deg(\alpha) = 2^p - 1$. We have $(X^p + X + 1) \circ \alpha = \alpha(\alpha^{2^p-1} + \alpha + 1) = 0$, so $\operatorname{Ord}(\alpha)$ divides $X^p + X + 1$. But $X^p + X + 1$ is irreducible, and $1 \circ \alpha \neq 0$, so in fact $\operatorname{Ord}(\alpha)$ *equals* $X^p + X + 1$. By (1.3) the degree of α equals the order of the residue class of X in the group $(\mathbf{F}_2[X]/(X^p + X + 1)\mathbf{F}_2[X])^*$. Denote by β a zero of $X^p + X + 1$ in $\overline{\mathbf{F}}_2$; then this order is just $\operatorname{ord}(\beta)$. The group $\mathbf{F}_2(\beta)^* = \mathbf{F}_{2^p}^*$ has prime order $2^p - 1$, and $\beta \neq 1$, so we conclude that $\deg(\alpha) = \operatorname{ord}(\beta) = 2^p - 1$, as required. □

Starting from the observation that $X^2 + X + 1$ is irreducible over $\mathbf{F}_2$, we find by successive applications of (1.4):

since $2^2 - 1 = 3$ is prime, $X^3 + X + 1$ is irreducible over $\mathbf{F}_2$;
since $2^3 - 1 = 7$ is prime, $X^7 + X + 1$ is irreducible over $\mathbf{F}_2$;
since $2^7 - 1 = 127$ is prime, $X^{127} + X + 1$ is irreducible over $\mathbf{F}_2$;

and finally, since

$$2^{127} - 1 = 170141183460469231731687303715884105727$$

was proved to be prime by Lucas in 1876 (see [5, Section 2.5]), the polynomial

$$X^{2^{2^{2^{2^2-1}-1}-1}-1} + X + 1$$

is irreducible over $\mathbf{F}_2$; cf. [10]. We conjecture that the next polynomial in this sequence is also irreducible over $\mathbf{F}_2$, but that its degree is not prime.

It is well known that for any positive integer n that is relatively prime to q the number of $\alpha \in \overline{\mathbf{F}}_q^*$ with $\operatorname{ord}(\alpha) = n$ equals $\varphi(n)$, where φ denotes the Euler function. In particular, with $n = q^m - 1$ one finds that elements α with order $q^m - 1$ do exist; these are precisely the primitive roots of $\mathbf{F}_{q^m}$. The additive analogue is as follows.

For a monic $f \in \mathbf{F}_q[X]$, let

$$\Phi(f) = \#\big(\mathbf{F}_q[X]/f\mathbf{F}_q[X]\big)^*,$$

the analogue of the Euler function. With

$$N(f) = \#\big(\mathbf{F}_q[X]/f\mathbf{F}_q[X]\big) = q^{\deg(f)}$$

we have the following analogues of well-known properties of the Euler function:

$$(1.5) \qquad \sum_{g|f} \Phi(g) = N(f),$$

$$(1.6) \qquad \Phi(f) = N(f) \cdot \prod_{g|f,\, g\,\mathrm{irr.}} \left(1 - \frac{1}{N(g)}\right),$$

the product ranging over the *irreducible* monic factors g of f in $\mathbf{F}_q[X]$. The proofs of (1.5) and (1.6) are left to the reader.

For a polynomial $f = \sum_{i=0}^n a_i X^i \in \mathbf{F}_q[X]$ we define

$$(1.7) \qquad f^* = \sum_{i=0}^{n} a_i X^{q^i}.$$

Clearly, $f^*(\alpha) = f \circ \alpha$ for any $\alpha \in \overline{\mathbf{F}}_q$, so the number of $\alpha \in \overline{\mathbf{F}}_q$ having an Order dividing f is equal to the number of distinct zeros of f^* in $\overline{\mathbf{F}}_q$. Assuming that $\gcd(f, X) = 1$ we have $df^*/dX = a_0 \neq 0$, so that f^* has only simple zeros; their number is then $\deg(f^*) = q^{\deg(f)} = N(f)$, and we obtain

$$\sum_{g|f} \#\left\{\alpha \in \overline{\mathbf{F}}_q : \operatorname{Ord}(\alpha) = g\right\} = N(f).$$

Comparing this with (1.5) and applying induction on $\deg(f)$ we find the expected result, due to Ore [7]:

(1.8) *Let $f \in \mathbf{F}_q[X]$ be monic and relatively prime to X. Then the number of $\alpha \in \overline{\mathbf{F}}_q$ with* $\operatorname{Ord}(\alpha) = f$ *equals* $\Phi(f)$.

For $\alpha \in \mathbf{F}_{q^m}$ the family $(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}})$ is a basis of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$ if and only if there is no nonzero $f \in \mathbf{F}_q[X]$ of degree less than m with $f \circ \alpha = 0$. With (1.2) this leads to

(1.9) *Let* $\alpha \in \overline{\mathbf{F}}_q$. *Then* $(\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}})$ *is a basis of* $\mathbf{F}_{q^m}$ *over* $\mathbf{F}_q$ *if and only if* $\mathrm{Ord}(\alpha) = X^m - 1$, *and if and only if the* $\mathbf{F}_q[X]$*-submodule of* $\overline{\mathbf{F}}_q$ *generated by* α *equals* $\mathbf{F}_{q^m}$.

Combining (1.8) and (1.9) we see that normal bases of $\mathbf{F}_{q^m}$ over $\mathbf{F}_q$ do exist. This may also be expressed as

$$\mathbf{F}_{q^m} \cong \mathbf{F}_q[X]/(X^m - 1)\mathbf{F}_q[X] \quad \text{as } \mathbf{F}_q[X]\text{-modules},$$

which is analogous to

$$\mathbf{F}_{q^m}^* \cong \mathbf{Z}/(q^m - 1)\mathbf{Z} \quad \text{as } \mathbf{Z}\text{-modules}.$$

The theorem stated in the introduction may now be reformulated as follows.

(1.10) THEOREM. *For every prime power* $q > 1$ *and every positive integer* m *there exists an element* $\alpha \in \mathbf{F}_{q^m}^*$ *with* $\mathrm{Ord}(\alpha) = X^m - 1$ *and* $\mathrm{ord}(\alpha) = q^m - 1$.

In the proof of this theorem, which occupies the rest of this paper, we use the following notation. For given q, m, let

$$A = \left\{\alpha \in \mathbf{F}_{q^m} : \mathrm{Ord}(\alpha) = X^m - 1\right\}, \qquad B = \left\{\alpha \in \mathbf{F}_{q^m}^* : \mathrm{ord}(\alpha) = q^m - 1\right\}.$$

We have $\#A = \Phi(X^m - 1)$, $\#B = \varphi(q^m - 1)$, and the theorem is equivalent to the statement that $A \cap B \neq \varnothing$.

We define the subgroup $C \subset \mathbf{F}_{q^m}^*$ by

$$C = \left\{\gamma \in \mathbf{F}_{q^m}^* : \gamma^{q-1} \in \mathbf{F}_q\right\} = \left\{\gamma \in \mathbf{F}_{q^m}^* : \gamma^{(q-1)^2} = 1\right\}.$$

One easily proves that $\#C = (q-1) \cdot \gcd(m, q-1)$. We denote the index of C in $\mathbf{F}_{q^m}^*$ by P,

$$P = \#\mathbf{F}_{q^m}^*/C = \frac{q^m - 1}{(q-1) \cdot \gcd(m, q-1)}. \tag{1.11}$$

Alternatively, we can define C by $C = \{\gamma \in \mathbf{F}_{q^m} : \deg(\mathrm{Ord}(\gamma)) = 1\}$.

Let M be an $\mathbf{F}_q[X]$-submodule of $\mathbf{F}_{q^m}$, and let $\gamma \in C$. Then the $\mathbf{F}_q$-vector space $\gamma M = \{\gamma\mu : \mu \in M\}$ is in fact an $\mathbf{F}_q[X]$-module. To see this, note that $X \circ \gamma\mu = (\gamma\mu)^q = \gamma \cdot \gamma^{q-1} \cdot (X \circ \mu) \in \gamma M$ for any $\mu \in M$, since $\gamma^{q-1} \in \mathbf{F}_q^*$. It follows that the submodules of $\mathbf{F}_{q^m}$ are permuted by C. Since A consists exactly of those elements of $\mathbf{F}_{q^m}$ that do not belong to any proper submodule, we conclude that

$$CA = A, \tag{1.12}$$

where $CA = \{\gamma\alpha : \gamma \in C, \alpha \in A\}$.

If $\alpha \in A$, $\beta \in B$, $\gamma \in C$ are such that $\alpha = \beta\gamma \in A \cap (BC)$, then $\beta = \gamma^{-1}\alpha \in (CA) \cap B = A \cap B$. Hence $A \cap B$ is nonempty if and only if $A \cap (BC)$ is nonempty, and

(1.13) Theorem (1.10) is equivalent to the assertion that $A \cap (BC) \neq \varnothing$.

Concerning the set BC we note that

$$BC = \left\{\beta \in \mathbf{F}_{q^m}^* : \beta C \text{ generates the group } \mathbf{F}_{q^m}^*/C\right\}. \tag{1.14}$$

This is a direct consequence of the fact that any surjective group homomorphism of finite cyclic groups, such as $\mathbf{F}_{q^m}^* \to \mathbf{F}_{q^m}^*/C$, induces a *surjective* map on the sets of generators. Since the cyclic group $\mathbf{F}_{q^m}^*/C$ of order P has exactly $\varphi(P)$ generators, we find that

$$\#BC = \varphi(P) \cdot \#C = \varphi(P) \cdot \gcd(m, q-1) \cdot (q-1).$$

Without proof we remark that C is the largest subset of $\mathbf{F}_{q^m}^*$ satisfying (1.12). More generally, one can prove the following result.

(1.15) *Let $K \subset L$ be a finite Galois extension of fields, with Galois group G. Let $A = \{\alpha \in L\colon (\tau(\alpha))_{\tau \in G}$ is a basis of L over $K\}$, and denote by w the number of $\#G$th roots of unity in K^*. Then for $\gamma \in L^*$ the following four assertions are equivalent*: (i) $\gamma A \subset A$; (ii) $\gamma A = A$; (iii) $\tau(\gamma)/\gamma \in K^*$ *for all* $\tau \in G$; (iv) $\gamma^w \in K^*$. *The set C of all $\gamma \in L^*$ satisfying these conditions is a subgroup of L^* containing K^*, and C/K^* is isomorphic to the group of all group homomorphisms $G \to K^*$.*

2. The Method of Carlitz and Davenport. Let G be a finite Abelian group. By a *character* of G we mean a group homomorphism $G \to \mathbf{C}^*$, where $\mathbf{C}$ denotes the field of complex numbers. The characters form an Abelian group $G^\wedge$, the *dual* of G. We denote the neutral element of $G^\wedge$ by 1. For the basic properties of characters see [8].

Suppose that G is cyclic of order n. Then the same is true for $G^\wedge$. For $\alpha \in G$ we define

$$\omega(\alpha) = \sum_{d|n} \frac{\mu(d)}{\varphi(d)} \sum_{\chi \in G^\wedge,\, \mathrm{ord}(\chi) = d} \chi(\alpha),$$

where $\mathrm{ord}(\chi)$ denotes the order of χ and μ the Moebius function. We have

(2.1) $\qquad \omega(\alpha) = 0 \quad$ if α does not generate G.

To see this, we write

$$\omega(\alpha) = \prod_{l|n,\, l \text{ prime}} \left(1 - \frac{1}{l-1} \cdot \sum_{\chi \in G^\wedge,\, \mathrm{ord}(\chi) = l} \chi(\alpha)\right)$$

$$= \prod_{l|n,\, l \text{ prime}} \left(\frac{l}{l-1} - \frac{1}{l-1} \cdot \sum_{\chi \in G^\wedge,\, \chi^l = 1} \chi(\alpha)\right).$$

If α does not generate G, then $\alpha = \beta^l$ for some $\beta \in G$ and some prime l dividing n. Then $\chi(\alpha) = \chi^l(\beta) = 1$ whenever $\chi^l = 1$, so $\sum_{\chi \in G^\wedge, \chi^l = 1} \chi(\alpha) = l$ and the lth factor in the above product vanishes, as required.

We apply this result to $G = \mathbf{F}_{q^m}^*/C$, $n = P$, using the notation of the previous section. In view of (1.14) we then find

(2.2) *Define* $\omega\colon \mathbf{F}_{q^m}^* \to \mathbf{C}$ *by*

$$\omega(\alpha) = \sum_{d|P} \frac{\mu(d)}{\varphi(d)} \sum_{\chi,\, \mathrm{ord}(\chi) = d} \chi(\alpha),$$

with χ ranging over $\mathbf{F}_{q^m}^{*\wedge}$. Then

$$\omega(\alpha) = 0 \quad \textit{for } \alpha \notin BC.$$

The additive analogue to (2.2) presents no difficulties. Let $\mathbf{F}_{q^m}^\wedge$ be the dual of the additive group of $\mathbf{F}_{q^m}$. We write $\mathbf{F}_{q^m}^\wedge$ multiplicatively, and we make it into an $\mathbf{F}_q[X]$-module by defining

$$(\lambda^f)(\alpha) = \lambda(f \circ \alpha) \quad \text{for } \lambda \in \mathbf{F}_{q^m}^\wedge,\ f \in \mathbf{F}_q[X],\ \alpha \in \mathbf{F}_{q^m}.$$

The Order $\operatorname{Ord}(\lambda)$ of a character λ is defined to be the monic polynomial generating the annihilator of λ in $\mathbf{F}_q[X]$; it clearly divides $X^m - 1$. Conversely, let f be a monic divisor of $X^m - 1$ in $\mathbf{F}_q[X]$. We claim that precisely $\Phi(f)$ characters $\lambda \in \mathbf{F}_{q^m}^{\wedge}$ have Order f. As in the proof of (1.8) it suffices, by (1.5), to show that

$$\sum_{g \mid f} \#\{\lambda \colon \operatorname{Ord}(\lambda) = g\} = N(f).$$

Here the left-hand side equals the order of the subgroup $\{\lambda\colon \lambda^f = 1\}$ of $\mathbf{F}_{q^m}^{\wedge}$. This subgroup may be identified with the dual of $\mathbf{F}_{q^m}/f \circ \mathbf{F}_{q^m}$, which indeed has order $N(f)$, as required.

Denote by M the analogue of the Moebius function for $\mathbf{F}_q[X]$; so for $f \in \mathbf{F}_q[X]$, f monic, we have $M(f) = (-1)^r$ if f is the product of r distinct monic irreducible factors, and $M(f) = 0$ if f is divisible by the square of an irreducible polynomial.

We now have the following analogue to (2.2). We omit the proof, which is completely analogous.

(2.3) *Define* $\Omega\colon \mathbf{F}_{q^m} \to \mathbf{C}$ *by*

$$\Omega(\alpha) = \sum_{g \mid X^m - 1} \frac{M(g)}{\Phi(g)} \sum_{\lambda, \operatorname{Ord}(\lambda) = g} \lambda(\alpha)$$

with λ *ranging over* $\mathbf{F}_{q^m}^{\wedge}$. *Then*

$$\Omega(\alpha) = 0 \quad \textit{for } \alpha \notin A.$$

From (2.2) and (2.3) we see that

$$\text{(2.4)} \qquad \omega(\alpha)\Omega(\alpha) = 0 \quad \text{for } \alpha \notin A \cap (BC).$$

We extend the characters of $\mathbf{F}_{q^m}^*$ to all of $\mathbf{F}_{q^m}$ by putting $\chi(0) = 0$ for $\chi \neq 1$, and $1(0) = 1$. Then $\omega(0)\Omega(0) = 0$.

(2.5) PROPOSITION. *Let s be the number of distinct prime factors of P (see* (1.11)) *and t the number of distinct monic irreducible factors of $X^m - 1$ in $\mathbf{F}_q[X]$. Suppose that*

$$(2^s - 1)(2^t - 1) < q^{m/2}.$$

Then there exists an element $\alpha \in \mathbf{F}_{q^m}^*$ with $\operatorname{Ord}(\alpha) = X^m - 1$ *and* $\operatorname{ord}(\alpha) = q^m - 1$.

Proof. Suppose not. Then $A \cap (BC) = \varnothing$, by (1.13), so (2.4) implies that $\omega(\alpha)\Omega(\alpha) = 0$ for all $\alpha \in \mathbf{F}_{q^m}$, and

$$\sum_{\alpha \in \mathbf{F}_{q^m}} \omega(\alpha)\Omega(\alpha) = 0.$$

We have

$$\sum_{\alpha \in \mathbf{F}_{q^m}} \omega(\alpha)\Omega(\alpha) = \sum_{d \mid P} \sum_{g \mid X^m - 1} \frac{\mu(d)M(g)}{\varphi(d)\Phi(g)} \sum_{\chi, \operatorname{ord}(\chi) = d} \sum_{\lambda, \operatorname{Ord}(\lambda) = g} \tau(\chi, \lambda),$$

where $\tau(\chi, \lambda)$ is the Gauss sum

$$\tau(\chi, \lambda) = \sum_{\alpha \in \mathbf{F}_{q^m}} \chi(\alpha)\lambda(\alpha).$$

It is easily checked that

$$\tau(1,1) = q^m,$$
$$\tau(1,\lambda) = 0 \quad \text{for } \lambda \neq 1,$$
$$\tau(\chi,1) = 0 \quad \text{for } \chi \neq 1,$$

and it is well known [2, pp. 375–376] that

$$|\tau(\chi,\lambda)| = q^{m/2} \quad \text{if } \chi \neq 1,\ \lambda \neq 1.$$

We find that

$$-q^m = \sum_{d\,|\,P,\, d\neq 1} \ \sum_{g\,|\,X^m-1,\, g\neq 1} \frac{\mu(d)M(g)}{\varphi(d)\Phi(g)} \sum_{\chi,\, \mathrm{ord}(\chi)=d} \ \sum_{\lambda,\, \mathrm{Ord}(\lambda)=g} \tau(\chi,\lambda).$$

There are exactly $\varphi(d)$ characters χ of order d, and exactly $\Phi(g)$ characters λ of Order g. Hence, taking absolute values, we obtain

$$q^m \leqslant \sum_{d\,|\,P,\, d\neq 1} \ \sum_{g\,|\,X^m-1,\, g\neq 1} |\mu(d)M(g)| \cdot q^{m/2} = (2^s-1)(2^t-1)q^{m/2},$$

contradicting our assumption. This proves Proposition (2.5). □

To apply (2.5) we need upper bounds for s and t. The upper bounds that we give below are refinements of those given by Davenport [4]. We begin with s.

(2.6) Lemma. *Let P be a positive integer and s the number of distinct prime factors of P. Let further $l > 1$ be an integer, Λ a set of prime numbers $\leqslant l$ such that every prime factor $r < l$ of P belongs to Λ, and put $L = \prod_{r\in\Lambda} r$. Then*

$$s \leqslant \frac{\log P - \log L}{\log l} + \#\Lambda.$$

Proof. Let M be the set of prime divisors of P. Then $\#M = s$ and each $r \in M - \Lambda$ satisfies $r \geqslant l$. Therefore,

$$P \geqslant \prod_{r\in M} r = \Big(\prod_{r\in\Lambda} r\Big)\cdot\Big(\prod_{r\in M-\Lambda} r\Big)\Big/\Big(\prod_{r\in\Lambda-M} r\Big)$$
$$\geqslant \Big(\prod_{r\in\Lambda} r\Big)\cdot l^{\#(M-\Lambda)}/l^{\#(\Lambda-M)} = L\cdot l^{\#M-\#\Lambda} = L\cdot l^{s-\#\Lambda},$$

and the lemma follows. This proves (2.6). □

The following lemma gives a formula for t.

(2.7) Lemma. *Let q be a prime power > 1 and m a positive integer. Then the number t of monic irreducible factors of $X^m - 1$ in $\mathbf{F}_q[X]$ is given by*

$$t = \sum_{d\,|\,m,\, \gcd(d,q)=1} \frac{\varphi(d)}{k(d)},$$

where $k(d)$ denotes the order of $(q \bmod d)$ in $(\mathbf{Z}/d\mathbf{Z})^*$.

Proof. If p^n denotes the largest power of the characteristic p of $\mathbf{F}_q$ dividing m, then $X^m - 1 = (X^{m/p^n} - 1)^{p^n}$. Therefore we may assume that p does not divide m. Then $X^m - 1 = \prod_{d|m}\Phi_d$, where

$$\Phi_d = \prod_{\alpha\in\overline{\mathbf{F}}_q,\, \mathrm{ord}(\alpha)=d} (X-\alpha).$$

The degree of Φ_d equals $\varphi(d)$, and by (1.1) each irreducible factor of Φ_d has degree $k(d)$. Since $X^m - 1$ has no repeated factors, this implies (2.7). □

We note the following additive analogue of (2.7), which is proved in a completely analogous way. It generalizes a theorem of Zierler [6], [9].

(2.8) *Let $f \in \mathbf{F}_q[X]$ be monic, and f^* as defined in* (1.7). *Then the number of monic irreducible factors of f^* in $\mathbf{F}_q[X]$ equals*

$$\sum_{g \mid f,\, \gcd(g, X) = 1} \frac{\Phi(g)}{K(g)},$$

where $K(g)$ denotes the order of $(X \bmod g)$ in $(\mathbf{F}_q[X]/g\mathbf{F}_q[X])^*$. More precisely, we can write

$$f^* = \Bigg(\prod_{g \mid f,\, \gcd(g, X) = 1} \Psi_g \Bigg)^{q^n},$$

where n is the degree of the lowest-degree term of f, the polynomials Ψ_g are pairwise relatively prime, and each Ψ_g factors as a product of $\Phi(g)/K(g)$ distinct monic irreducible factors of degree $K(g)$.

We next derive upper bounds for t.

(2.9) LEMMA. *Let q, m, t be as in* (2.7), *and e a positive integer. Let further D be a set of positive divisors of m such that every $d \in D$ is relatively prime to q, and such that D contains all positive divisors of* $\gcd(m, q^{e'} - 1)$ *for all positive integers $e' < e$. Then we have*

$$t \leqslant \frac{m}{e} + \sum_{d \in D} \varphi(d) \left(\frac{1}{k(d)} - \frac{1}{e} \right),$$

with $k(d)$ as in (2.7).

Proof. We may clearly assume that $\gcd(m, q) = 1$. Then the hypothesis on D implies that $k(d) \geqslant e$ for all $d \mid m$ with $d \notin D$. Hence, by (2.7),

$$t = \sum_{d \mid m,\, d \notin D} \frac{\varphi(d)}{k(d)} + \sum_{d \in D} \frac{\varphi(d)}{k(d)} \leqslant \sum_{d \mid m,\, d \notin D} \frac{\varphi(d)}{e} + \sum_{d \in D} \frac{\varphi(d)}{k(d)}$$

$$= \sum_{d \mid m} \frac{\varphi(d)}{e} + \sum_{d \in D} \left(\frac{\varphi(d)}{k(d)} - \frac{\varphi(d)}{e} \right) = \frac{m}{e} + \sum_{d \in D} \varphi(d) \left(\frac{1}{k(d)} - \frac{1}{e} \right).$$

This proves (2.9). □

With $e = 1$, $D = \varnothing$, one obtains from (2.9) the trivial bound

$$t \leqslant m.$$

With $e = 2$, and D equal to the set of divisors of $\gcd(m, q - 1)$, one finds

(2.10) $$t \leqslant \tfrac{1}{2}(m + \gcd(m, q - 1)).$$

The following lemma gives better estimates for t for small values of q.

(2.11) LEMMA. *Let q, m, t be as in* (2.7).

(a) *Let $q = 5$. Then*

$$t \leqslant \frac{m}{3} + 6;$$

$$t \leqslant \frac{m}{3} + \frac{10}{3} \quad \textit{if } m \not\equiv 0 \bmod 3;$$

$$t \leqslant \frac{m}{3} + \frac{4}{3} \quad \textit{if } m \not\equiv 0 \bmod 4,\ m \neq 6.$$

(b) *Let $q = 4$. Then*

$$t \leqslant \frac{m}{3} + 2 \quad \textit{if } m \neq 15;$$

$$t \leqslant \frac{m}{3} + \frac{2}{3} \quad \textit{if } m \not\equiv 0 \bmod 3,\ m \neq 5;$$

$$t \leqslant \frac{m}{4} + \frac{3}{2} \quad \textit{if } m \textit{ is even}.$$

(c) *Let $q = 3$. Then*

$$t \leqslant \frac{m}{3} + \frac{4}{3} \quad \textit{if } m \neq 4, 8, 16;$$

$$t \leqslant \frac{m}{6} + 1 \quad \textit{if } m \equiv 0 \bmod 3.$$

(d) *Let $q = 2$. Then*

$$t \leqslant \frac{m}{4} + \frac{5}{4};$$

$$t \leqslant \frac{m}{5} + \frac{4}{5} \quad \textit{if } m \textit{ is odd},\ m \neq 3, 5, 7, 9, 15, 21;$$

$$t \leqslant \frac{m}{8} + \frac{5}{4} \quad \textit{if } m \equiv 0 \bmod 2;$$

$$t \leqslant \frac{m}{8} + \frac{1}{2} \quad \textit{if } m \equiv 0 \bmod 4.$$

Proof. Since the proofs are all similar, we only do (a) as an example. Let $q = 5$. We apply (2.9) with $e = 3$ and D equal to the set of divisors of $\gcd(m, 24)$. This yields

$$t \leqslant \frac{m}{3} + \frac{1}{6}\gcd(m, 24) + \frac{1}{2}\gcd(m, 4) \leqslant \frac{m}{3} + 6,$$

as required. If $m \not\equiv 0 \bmod 3$ we have $\gcd(m, 24) \leqslant 8$, and the same estimate now gives $t \leqslant \frac{m}{3} + \frac{10}{3}$. Suppose finally that $m \not\equiv 0 \bmod 4$. If m is odd, then $t \leqslant \frac{m}{3} + \frac{1}{6} \cdot 3 + \frac{1}{2} \cdot 1 = \frac{m}{3} + 1$. If $m \equiv 2 \bmod 4$, $m \not\equiv 0 \bmod 3$, then $t \leqslant \frac{m}{3} + \frac{1}{6} \cdot 2 + \frac{1}{2} \cdot 2 = \frac{m}{3} + \frac{4}{3}$. We are left with the case $m \equiv 6 \bmod 12$. If also $31 \mid m$ we apply (2.9) with $e = 4$ and $D = \{d\colon d \mid 2 \cdot 3 \cdot 31\}$ to obtain $t \leqslant \frac{m}{4} - \frac{5}{2}$. If 31 does not divide m we take $e = 4$ and $D = \{1, 2, 3, 6\}$ in (2.9) and find $t \leqslant \frac{m}{4} + \frac{5}{2}$ which is $\leqslant \frac{m}{3} + \frac{4}{3}$ for $m \equiv 6 \bmod 12$, $m \neq 6$. This concludes the proof of (a). □

Combining our inequalities we obtain the following result.

(2.12) Lemma. *Let $q > 1$ be a prime power, m a positive integer, P as in* (1.11), *s and t as in* (2.5), *and l, Λ, L as in* (2.6). *Suppose that*

$$(2^s - 1)(2^t - 1) \geqslant q^{m/2}.$$

Let further δ be an integer with $1 \leqslant \delta \leqslant \gcd(q - 1, m)$. Then we have

$$\text{(2.13)} \qquad \frac{1}{\log 2}\log\left(\frac{q^{m/2}}{2^t - 1} + 1\right) \leqslant \frac{1}{\log l}\left(\log\left(\frac{q^m - 1}{q - 1}\right) - \log(\delta L)\right) + \#\Lambda.$$

If moreover $\alpha, \beta \in \mathbf{R}$ are such that $t \leqslant \alpha m + \beta$, then

$$\text{(2.14)} \qquad m\left(\frac{\log q}{\log 4} - \frac{\log q}{\log l} - \alpha\right) \leqslant \beta + \#\Lambda - \frac{\log(\delta L(q - 1))}{\log l}.$$

Proof. The first inequality is obtained by writing $(2^s - 1)(2^t - 1) \geqslant q^{m/2}$ as a lower estimate for s and applying (2.6). For the second one, note that $4^{s+t} \geqslant ((2^s - 1)(2^t - 1))^2 \geqslant q^m$, so $m(\log q/\log 4) \leqslant s + t$, and next apply the upper bound from (2.6) for s, the upper bound $P \leqslant q^m/(\delta(q - 1))$ for P, and $t \leqslant \alpha m + \beta$. This proves (2.12). □

3. Determination of the Exceptional Cases. In this section we determine all pairs q, m to which (2.5) does not apply.

(3.1) PROPOSITION. *Let $q > 1$ be a prime power, m a positive integer, and P, s, t as in* (1.11) *and* (2.5). *Then we have*

$$(2^s - 1)(2^t - 1) \geqslant q^{m/2}$$

if and only if (q, m) is one of the nine pairs

$$(2,3), (2,6), (2,15), (3,2), (3,4), (3,8), (5,4), (5,8), (7,6).$$

Proof. Table (3.2) contains, for 31 pairs (q, m), the value of t, the prime factorization of P, and the values of $(2^s - 1)(2^t - 1)$. For these pairs the proposition is readily checked; the nine cases in which $(2^s - 1)(2^t - 1) \geqslant q^{m/2}$ are indicated by stars in the last column.

TABLE (3.2)

q	m	t	P	$(2^s - 1)(2^t - 1)$	$q^{m/2}$	
2	3	2	7	3	2.83	*
2	4	1	$3 \cdot 5$	3	4	
2	6	2	$3^2 \cdot 7$	9	8	*
2	9	3	$7 \cdot 73$	21	22.6	
2	10	2	$3 \cdot 11 \cdot 31$	21	32	
2	12	2	$3^2 \cdot 5 \cdot 7 \cdot 13$	45	64	
2	14	3	$3 \cdot 43 \cdot 127$	49	128	
2	15	5	$7 \cdot 31 \cdot 151$	217	181.0	*
2	21	6	$7^2 \cdot 127 \cdot 337$	441	1448.2	
3	2	2	2	3	3	*
3	4	3	$2^2 \cdot 5$	21	9	*
3	6	2	$2 \cdot 7 \cdot 13$	21	27	
3	8	5	$2^3 \cdot 5 \cdot 41$	217	81	*
3	10	4	$2 \cdot 11^2 \cdot 61$	105	243	
3	16	7	$2^4 \cdot 5 \cdot 17 \cdot 41 \cdot 193$	3937	6561	
4	5	3	$11 \cdot 31$	21	32	
4	6	3	$5 \cdot 7 \cdot 13$	49	64	
4	9	5	$3 \cdot 7 \cdot 19 \cdot 73$	465	512	
4	15	9	$7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$	15841	32768	
5	4	4	$3 \cdot 13$	45	25	*
5	6	4	$3^2 \cdot 7 \cdot 31$	105	125	
5	8	6	$2 \cdot 3 \cdot 13 \cdot 313$	945	625	*
5	12	8	$3^2 \cdot 7 \cdot 13 \cdot 31 \cdot 601$	7905	15625	
7	4	3	$2^3 \cdot 5^2$	21	49	
7	6	6	$2^2 \cdot 19 \cdot 43$	441	343	*
7	12	9	$2^3 \cdot 5^2 \cdot 13 \cdot 19 \cdot 43 \cdot 181$	32193	117649	
9	4	4	$5 \cdot 41$	45	81	
9	8	8	$5 \cdot 17 \cdot 41 \cdot 193$	3825	6561	
11	4	3	$2^2 \cdot 3 \cdot 61$	49	121	
11	10	10	$2 \cdot 3 \cdot 3221 \cdot 13421$	15345	161051	
13	4	4	$5 \cdot 7 \cdot 17$	105	169	

In the rest of this proof we assume that (q, m) is a pair *not* occurring in the table for which $(2^s - 1)(2^t - 1) \geqslant q^{m/2}$. We shall derive a contradiction from this.

Clearly, our inequality implies $s > 0$, so $P \neq 1$ and $m \neq 1$. If $m = 2$ and q is even then $t = 1$, and since $P = q + 1$ is odd, we have $q = P - 1 \geqslant 3^s - 1 > (2^s - 1) = (2^s - 1)(2^t - 1)$. If $m = 2$ and q is odd, we have $2^t - 1 = 3$, and applying (2.13) with $l = 3$, $\Lambda = \{2\}$, $\delta = 2$ we find that

$$\frac{\log(\frac{1}{3}q + 1)}{\log 2} - \frac{\log(q + 1)}{\log 3} \leqslant 1 - \frac{\log 4}{\log 3},$$

so $q \leqslant 3$; but the pair $(3, 2)$ is in the table. We have proved

$$(3.3) \qquad m \geqslant 3.$$

Next we prove that

(3.4) m is not a power of the characteristic p of $\mathbf{F}_q$.

Suppose not. Then $t = 1$. If p is odd then each prime r dividing P is 1 mod $2p$, so $\geqslant 7$, hence $P \geqslant 7^s$, and $(2^s - 1)(2^t - 1) < 7^{s/2} \leqslant P^{1/2} < q^{m/2}$. If $p = 2$ then (2.13) with $\delta = 1$ yields

$$\log(q^m)\left(\frac{1}{\log 4} - \frac{1}{\log l}\right) \leqslant \#\Lambda - \frac{\log L}{\log l}.$$

With $l = 5$, $\Lambda = \{3\}$ this implies $q^m \leqslant 24$, so by (3.3) we have $(q, m) = (2, 4)$, which is in the table. This proves (3.4).

(3.5) P is not a prime power.

If not, then $s = 1$ and $4^t > (2^t - 1)^2 \geqslant q^m$, so $t > m(\log q/\log 4)$, which by $t \leqslant m$ implies that $q = 2$ or 3. If $q = 3$ then by (3.3) and (3.4) we have $m \geqslant 4$, so (2.10) leads to the contradiction $t \leqslant \frac{1}{2}m + 1 < m(\log q/\log 4)$. If $q = 2$ then $m \geqslant 5$ by (3.4) (since $(2, 3)$ is in the table), so (2.11)(d) gives $t \leqslant \frac{m}{4} + \frac{5}{4} \leqslant m(\log q/\log 4)$, also a contradiction. This proves (3.5).

Suppose now that m is *prime*. Then m is odd, by (3.3), and this easily implies that each prime divisor of P is 1 modulo $2m$. Hence, we can take $l = 4m + 1$ and $\Lambda = \{r\colon\ r \text{ prime},\ r \equiv 1 \bmod 2m,\ r < 4m + 1\}$ in (2.6); clearly either $\#\Lambda = 0$, $L = 1$ or $\#\Lambda = 1$, $L = 2m + 1$. Inequality (2.14) yields

$$\left(\frac{1}{\log 4} - \frac{1}{\log(4m + 1)}\right)\log q$$
$$\leqslant \alpha + \frac{1}{m}\left(\beta + 1 - \frac{\log(\delta(2m + 1)(q - 1))}{\log(4m + 1)}\right).$$

If $q \equiv 1 \bmod m$, then with $\alpha = 1$, $\beta = 0$, $\delta = m$, $q - 1 \geqslant m$, this yields $q \leqslant 7$ for $m \geqslant 7$; and $q \leqslant 8$ for $m = 5$; and $q \leqslant 11$ for $m = 3$. For $q \equiv 1 \bmod m$ this leaves only the pairs $(4, 3)$ and $(7, 3)$, which both contradict (3.5). If $q \equiv -1 \bmod m$ we can take $\alpha = \beta = \frac{1}{2}$, by (2.10), and with $\delta = 1$, $q - 1 \geqslant m - 2$ the above inequality yields $q \leqslant 4$ for $m \geqslant 5$ and $q \leqslant 9$ for $m = 3$; this leaves only the cases $(4, 5)$, $(2, 3)$,

$(5,3)$, $(8,3)$, of which the first is in the table and the other three contradict (3.5). If $q \not\equiv \pm 1 \bmod m$, then $m \geqslant 5$ by (3.4), and using $e = 3$, $D = \{1\}$ in (2.9), we see that we can take $\alpha = \frac{1}{3}$, $\beta = \frac{2}{3}$ in the above inequality; for $q \neq 2$ this yields $q \leqslant 2$ for $m \geqslant 7$ and $q \leqslant 3$ for $m = 5$, leaving only the pair $(3,5)$, which contradicts (3.5) because $P = 11^2$. Finally, let $q = 2$. Then $m \geqslant 11$ by (3.5), and we can take $\alpha = \frac{1}{5}$, $\beta = \frac{4}{5}$ in the inequality (choose $e = 5$, $D = \{1\}$ in (2.9)), which leads to the contradiction $m \leqslant 9$. We have proved

$$(3.6) \qquad m \text{ is not prime.}$$

If $m = 4$, $q \equiv -1 \bmod 4$ we have $t = 3$, and applying (2.13) with $\delta = 2$, $l = 7$, $\Lambda = \{2,3,5\}$ one finds that $q \leqslant 15$, so $q = 3$, 7 or 11, which are all in the table. If $m = 4$, $q \equiv 1 \bmod 4$ we have $t = 4$, and applying (2.13) with $\delta = 4$, $l = 7$, $\Lambda = \{3,5\}$ (P is odd) one finds that $q \leqslant 16$, so $q = 5$, 9 or 13, which are also in the table. In view of (3.4) we conclude that $m \neq 4$, and with (3.3) and (3.6) this implies

$$(3.7) \qquad m \geqslant 6.$$

Next suppose that $q \equiv 1 \bmod m$. We apply (2.14) with $\alpha = 1$, $\beta = 0$, $\delta = m$. In order to make the coefficient $\log q/\log 4 - \log q/\log l - 1$ in (2.14) positive we have to take l fairly large. For $q \geqslant 23$ we choose $\Lambda = \{2,3,5,7,11,13,17\}$, $l = 19$; this leads to a contradiction with (3.7). For smaller q we observe that P is relatively prime to $\frac{1}{2}q(q-1)$, because m divides $q - 1$, and change Λ, l accordingly. With

$$\begin{array}{lll}
\Lambda = \{2,5,7,11\}, & l = 13 & \text{for } q = 19, \\
\Lambda = \{3,5,7,11,13\}, & l = 19 & \text{for } q = 17, \\
\Lambda = \{7,11\}, & l = 13 & \text{for } q = 16, \\
\Lambda = \{5,7,11,17,19\}, & l = 23 & \text{for } q = 13
\end{array}$$

we find in all cases the contradiction $m \leqslant 3$. For $q \leqslant 11$, the condition $q \equiv 1 \bmod m$ forces by (3.6) and (3.7) that (q, m) is one of $(7,6)$, $(9,8)$, and $(11,10)$, which are all in the table. The conclusion is that

$$(3.8) \qquad q \not\equiv 1 \bmod m.$$

The proof of (3.1) is now concluded by another series of applications of (2.14), as indicated by Table (3.9). Every line of the table corresponds to one application of (2.14). The first two columns, headed "q" and "m", indicate for which values of q and m the inequality (2.14) is applied. The next two columns give values for α and β for which $t \leqslant \alpha m + \beta$. These are either derived from (2.10) (note that $\gcd(q-1, m) \leqslant \frac{1}{2}m$, by (3.8)), or from (2.11) (the exceptions to (2.11) are dealt with in the last column). The fifth column gives a lower bound δ for $\gcd(q-1, m)$. Next one finds Λ and l. To check that these satisfy the conditions of (2.6), it may be necessary to use the information on m in the second column; e.g., if $q = 7$, $3 \nmid m$, then $7^m \not\equiv 1 \bmod 9$, so 3 does not divide P. In the final column one first finds the upper bound for m that is obtained by applying (2.14); next a complete list of all $m \geqslant 6$ (see (3.7)) that satisfy this upper bound (or are exceptions in (2.11)) and also meet the condition in the second column; and finally how to deal with these remaining values.

This concludes the proof of (3.1). □

Table (3.9)

q	m	α	β	δ	Λ	l	m
$\geqslant 16$	all m	$\frac{3}{4}$	0	1	2, 3, 5, 7, 11, 13	17	$\leqslant 5$; –
13	all m	$\frac{3}{4}$	0	1	2, 3, 5, 7, 11, 13	17	$\leqslant 7$; 6, 7; (3.8), (3.6)
11	$2 \nmid m, 5 \nmid m$	$\frac{1}{2}$	$\frac{1}{2}$	1	2, 3, 5, 7	13	$\leqslant 5$; –
11	$2 \mid m, 5 \nmid m$	$\frac{1}{2}$	1	2	2, 3, 5, 7	13	$\leqslant 5$; –
11	$2 \nmid m, 5 \mid m$	$\frac{1}{2}$	$\frac{5}{2}$	5	2, 3, 5, 7	13	$\leqslant 9$; –
11	$2 \mid m, 5 \mid m$	$\frac{1}{2}$	5	10	2, 3, 5, 7	13	$\leqslant 17$; 10; (3.8)
9	$2 \nmid m$	$\frac{1}{2}$	$\frac{1}{2}$	1	2, 5, 7, 11, 13	17	$\leqslant 4$; –
9	$2 \mid m, 4 \nmid m$	$\frac{1}{2}$	1	2	2, 5, 7, 11, 13	17	$\leqslant 5$; –
9	$4 \mid m, 8 \nmid m$	$\frac{1}{2}$	2	4	2,5,7,11,13	17	$\leqslant 8$; –
9	$8 \mid m$	$\frac{1}{2}$	4	8	2, 5, 7, 11, 13	17	$\leqslant 13$; 8; (3.8)
8	$7 \nmid m$	$\frac{1}{2}$	$\frac{1}{2}$	1	3, 5, 7, 11, 13, 17	19	$\leqslant 5$; –
8	$7 \mid m$	$\frac{1}{2}$	$\frac{7}{2}$	7	3, 5, 7, 11, 13, 17	19	$\leqslant 13$; 7; (3.6)
7	$3 \nmid m$	$\frac{1}{2}$	1	1	2, 5, 11	17	$\leqslant 7$; 7; (3.6)
7	$2 \nmid m, 3 \mid m$	$\frac{1}{2}$	$\frac{3}{2}$	3	3	19	$\leqslant 4$; –
7	$2 \mid m, 3 \mid m$	$\frac{1}{2}$	3	6	2, 3, 5, 11, 13	17	$\leqslant 17$; 6, 12; (3.2)
5	$4 \nmid m$	$\frac{1}{3}$	$\frac{4}{3}$	1	3, 7, 11	19	$\leqslant 7$; 6, 7; (3.2), (3.6)
5	$3 \nmid m, 4 \mid m$	$\frac{1}{3}$	$\frac{10}{3}$	4	2, 3, 11, 13	17	$\leqslant 15$; 8; (3.2)
5	$3 \mid m, 4 \mid m$	$\frac{1}{3}$	6	4	2, 3, 7, 11, 13, 17, 19	23	$\leqslant 23$; 12; (3.2)
4	$3 \nmid m$	$\frac{1}{3}$	$\frac{2}{3}$	1	5	11	$\leqslant 6$; –
4	$2 \nmid m, 3 \mid m$	$\frac{1}{3}$	2	3	3, 7	11	$\leqslant 20$; 9, 15; (3.2)
4	$2 \mid m, 3 \mid m$	$\frac{1}{4}$	$\frac{3}{2}$	3	3, 5, 7	11	$\leqslant 9$; 6; (3.2)
3	$3 \mid m$	$\frac{1}{6}$	1	1	2,5,7	11	$\leqslant 11$; 6, 9; (3.2), (3.4)
3	$2 \nmid m, 3 \nmid m$	$\frac{1}{3}$	$\frac{4}{3}$	1	11	23	$\leqslant 12$; 7, 11; (3.6)
3	$2 \mid m, 4 \nmid m, 3 \nmid m$	$\frac{1}{3}$	$\frac{4}{3}$	2	2, 11, 23	47	$\leqslant 13$; 10; (3.2)
3	$4 \mid m, 3 \nmid m$	$\frac{1}{3}$	$\frac{4}{3}$	2	2, 5, 11, 17, 23, 29	41	$\leqslant 19$; 8, 16; (3.2)
2	$2 \nmid m$	$\frac{1}{5}$	$\frac{4}{5}$	1	7	23	$\leqslant 14$; 7, 9, 11, 13, 15, 21; (3.6), (3.2)
2	$2 \mid m, 4 \nmid m$	$\frac{1}{8}$	$\frac{5}{4}$	1	3, 7, 11	19	$\leqslant 17$; 6, 10, 14; (3.2)
2	$4 \mid m$	$\frac{1}{8}$	$\frac{1}{2}$	1	3, 5, 7	11	$\leqslant 18$; 8, 12, 16; (3.4), (3.2)

4. Completion of the Proof. In this section we prove Theorem (1.10) for the nine pairs (q, m) listed in Proposition (3.1). Davenport [4] handles these cases by explicitly giving an element of $\mathbf{F}_{q^m}^*$ of Order $X^m - 1$ and order $q^m - 1$. Alternatively, one can consult the tables of Beard and West [1]. We employ two methods. The first depends on a refinement of Proposition (2.5), the second is a counting argument.

We denote by q a prime power, $q > 1$, and by m an integer, $m > 1$. As before, we write $P = (q^m - 1)/((q - 1)\gcd(q - 1, m))$ and we let s be the number of distinct prime divisors of P. By t we denote the number of distinct irreducible factors of $X^m - 1$ in $\mathbf{F}_q[X]$.

(4.1) Proposition. *Suppose that m is a power of l, where l is a prime dividing $q - 1$. Let $Q = (q^m - 1)/(l(q^{m/l} - 1))$. Suppose that Q is a prime number and that*

$$(2^{s-1} - 1)(2^t - 1) < q^{m/2}.$$

Then $\mathbf{F}_{q^m}$ has a primitive normal basis over $\mathbf{F}_q$.

Proof. One readily checks that Q divides P and is larger than P/Q, so that the prime Q divides P exactly once. Let C' be the subgroup of $\mathbf{F}_{q^m}^*$ of order $l(q^{m/l}-1)$ and index Q. Then C' contains C, and the cyclic group $\mathbf{F}_{q^m}^*/C$ of order P is the direct product of the cyclic group C'/C of order P/Q and a group of prime order Q. Hence, for any $\alpha \in \mathbf{F}_{q^m}^*$, the coset αC can in a unique way be written as $\alpha_1\alpha_2$ with $\alpha_1 \in C'/C$ and $\alpha_2^Q = 1$. Moreover, we have $\alpha \in BC$ if and only if αC generates $\mathbf{F}_{q^m}^*/C$, and if and only if both α_1 generates C'/C and $\alpha_2 \neq 1$; here we use (1.14) and the fact that Q is prime.

For $\alpha \in \mathbf{F}_{q^m}$ we define

$$\omega'(\alpha) = \sum_{d \mid P/Q} \frac{\mu(d)}{\varphi(d)} \sum_{\chi,\, \operatorname{ord}(\chi)=d} \chi(\alpha)$$

with χ ranging over $\mathbf{F}_{q^m}^{*\wedge}$. Applying (2.1) to the cyclic group $G = C'/C$ of order $n = P/Q$ we find that $\omega'(\alpha) = 0$ if $\alpha \in \mathbf{F}_{q^m}^*$ is such that α_1 does not generate C'/C. We now claim that

$$(4.2) \qquad \omega'(\alpha)\Omega(\alpha) = 0 \quad \text{for } \alpha \notin A \cap (BC)$$

with Ω as in (2.3). To prove this, suppose that $\omega'(\alpha)\Omega(\alpha) \neq 0$. Then $\alpha \in A$ and α_1 generates C'/C. Hence to prove that $\alpha \in A \cap (BC)$ it suffices, by the above, to show that $\alpha_2 \neq 1$. Suppose that $\alpha_2 = 1$. Then $\alpha \in C'$, so the $l(q^{m/l}-1)$th power of α equals 1, and therefore

$$\alpha^{q^{m/l}-1} = \zeta$$

for some lth root of unity $\zeta \in \mathbf{F}_q^*$. This implies that $(X^{m/l} - \zeta) \circ \alpha = 0$, contradicting that $\alpha \in A$. This proves (4.2).

To complete the proof of (4.1) one now copies the proof of Proposition (2.5), with ω replaced by ω' and (2.4) by (4.2). The role of P is then played by P/Q, which has one prime divisor less, so that s is replaced by $s - 1$. This proves (4.1). □

It follows that $\mathbf{F}_{q^m}$ has a primitive normal basis over $\mathbf{F}_q$ if (q, m) is one of the pairs $(3,2)$, $(3,4)$, $(5,4)$, $(5,8)$. In these cases, Proposition (4.1) applies with $l = 2$ and $Q = 2, 5, 13, 313$, respectively.

(4.3) PROPOSITION. *The field* $\mathbf{F}_{q^m}$ *has a primitive normal basis over* $\mathbf{F}_q$ *if*

$$\Phi(X^m - 1) + \varphi(q^m - 1) > \sum_{d \mid m} \mu(m/d) q^d.$$

Proof. The right-hand side is the cardinality of the set of elements of $\mathbf{F}_{q^m}$ that are not contained in any proper subfield. Since A and B are contained in this set, and have cardinalities $\Phi(X^m - 1)$ and $\varphi(q^m - 1)$, respectively, the inequality clearly implies that A and B have a nonempty intersection. This proves (4.3). □

Proposition (4.3) implies that $\mathbf{F}_{q^m}$ has a primitive normal basis over $\mathbf{F}_q$ if (q, m) is one of the pairs $(2,3)$, $(2,6)$, $(2,15)$. We leave the calculations to the reader.

The remaining two cases $(q, m) = (3,8)$ and $(q, m) = (7,6)$ we treat with a refinement of this method.

First let $q = 3$ and $m = 8$. Let $\zeta \in \mathbf{F}_9 \subset \mathbf{F}_{3^8}$ be a primitive 8th root of unity. The group C has order 4, so $D = C \cup \zeta C$ is a group of order 8, and $DA = A \cup \zeta A$. We claim that A and ζA have empty intersection. To prove this, we note that for any $\alpha \in A$ the trace $T(\alpha)$ of α to $\mathbf{F}_9$ has Order $X^2 - 1$; i.e., $T(\alpha)$ is a zero of $X^9 - X$ but not of $X^3 \pm X$, so $T(\alpha)^4 = -1$. If now also $\zeta\alpha \in A$, then $T(\zeta\alpha)^4 = -1$ as well. Since T is $\mathbf{F}_9$-linear, this leads to the contradiction $\zeta^4 = 1$. This proves our claim.

It follows that DA has cardinality $2 \cdot \#A = 4096$. Since B has cardinality $\varphi(3^8 - 1) = 2560$, and $4096 + 2560 > 6561 = 3^8$, the sets DA and B have an element in common. Also $BD = B$, because 16 divides $3^8 - 1$, so A and B have an element in common as well, as required.

Next, let $q = 7$ and $m = 6$. As before, we denote by $\zeta \in \mathbf{F}_{49} \subset \mathbf{F}_{7^6}$ a primitive 8th root of unity, and by D the group generated by ζ. Since $\zeta^2 \in C$ we again have $DA = A \cup \zeta A$. We calculate $\#(A \cap \zeta A)$.

For any cube root of unity $\eta \in \mathbf{F}_7$ let V_η be the set of elements of Order dividing $X^2 - \eta$, and define the "trace" T_η: $\mathbf{F}_{7^6} \to V_\eta$ by $T_\eta(\alpha) = (X^4 + \eta^2 X^2 + \eta) \circ \alpha$; this is an $\mathbf{F}_{49}$-linear map. From $X^6 - 1 = \prod_\eta (X^2 - \eta)$ it follows that the combined map $\mathbf{F}_{7^6} \to \prod_\eta V_\eta$ is an isomorphism of $\mathbf{F}_7[X]$-modules. Also, α belongs to A if and only if each $T_\eta(\alpha)$ has Order $X^2 - \eta$; i.e., $T_\eta(\alpha)$ is a zero of $X^{49} - \eta X$ but not of $X^7 \pm \eta^2 X$. Furthermore, we have $\zeta\alpha \in A$ if and only if each $T_\eta(\zeta\alpha) = \zeta T_\eta(\alpha)$ satisfies the same condition. From

$$X^{48} - \eta = -(X^6 - \eta^2)(X^6 + \eta^2)\left((\zeta X)^6 - \eta^2\right)\left((\zeta X)^6 + \eta^2\right)(X^{24} + \eta^2)$$

we now see that both α and $\zeta\alpha$ belong to A if and only if each $T_\eta(\alpha)$ is a zero of $X^{24} + \eta^2$. Consequently, $A \cap \zeta A$ has cardinality 24^3.

We conclude that $\#DA = 2 \cdot \#A - 24^3 = 2 \cdot 6^6 - 24^3 = 79488$. Also, $\#BC = \varphi(P) \cdot \#C = 54432$ and $79488 + 54432 > 117649 = 7^6$, so DA and BC have an element in common. From $CA = A$ and $BD = B$ it follows that A and B have an element in common as well, as required.

This completes the proof of the theorem.

Mathematisch Instituut
Roetersstraat 15
1018 WB Amsterdam
The Netherlands

Mathematical Sciences Research Institute
1000 Centennial Drive
Berkeley, California 94720

1. J. T. B. Beard, Jr. & K. J. West, "Some primitive polynomials of the third kind," *Math. Comp.*, v. 28, 1974, pp. 1166–1167, with microfiche supplement.

2. L. Carlitz, "Primitive roots in a finite field," *Trans. Amer. Math. Soc.*, v. 73, 1952, pp. 373–382.

→ L. Carlitz, "Some problems involving primitive roots in a finite field," *Proc. Nat. Acad. Sci. U.S.A.*, v. 38, 1952, pp. 314–318, 618.

4. H. Davenport, "Bases for finite fields," *J. London Math. Soc.*, v. 43, 1968, pp. 21–39; v. 44, 1969, p. 378.

5. G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford University Press, Oxford, 1968.

6. W. H. Mills, "The degrees of the factors of certain polynomials over finite fields," *Proc. Amer. Math. Soc.*, v. 25, 1970, pp. 860–863.

7. O. Ore, "Contributions to the theory of finite fields," *Trans. Amer. Math. Soc.*, v. 36, 1934, pp. 243–274.

8. J - P. Serre, *Cours d'Arithmétique*, Presses Universitaires de France, 1970.

9. N. Zierler, "On the theorem of Gleason and Marsh," *Proc. Amer. Math. Soc.*, v. 9, 1958, pp. 236–237.

10. N. Zierler, "On $x^n + x + 1$ over GF(2)," *Inform. and Control*, v. 16, 1970, pp. 502–505.