CONSECUTIVE PRIMITIVE ROOTS IN A FINITE FIELD

STEPHEN D. COHEN

ABSTRACT. Every finite field of order $q(> 3)$ such that $q \not\equiv 7 \pmod{12}$ and $q \not\equiv 1 \pmod{60}$ contains a pair of consecutive primitive roots.

1. Introduction. For any prime power q , let F_q denote the finite field of order q . F_q contains $\phi(q-1)$ primitive roots, where ϕ denotes Euler's function. (By definition, a primitive root generates the cyclic multiplicative group of F_q .) Put another way, the proportion of primitive roots among the nonzero members of F_q is $\theta(q-1)$, where, for any n , $\theta(n)$ is defined to be $\phi(n)/n$.

We denote by C the set of prime powers q for which F_q contains a primitive root γ whose successor $\gamma + 1$ is also a primitive root. It is easily seen that 2, 3 and 7 are not in C . In this paper we go a considerable way towards proving that every other prime power is in C . More generally, we shall denote by C^* the subset of C comprising prime powers q for which, given any α in F_q , there exists a primitive root γ for which $\gamma + \alpha$ is also a primitive root.

By elementary means, E. Vegh [5, 6] has proved the following when $q = p$, an odd prime.

THEOREM A. *Suppose $p \equiv 1 \pmod{4}$. If also $\theta(p-1) > \frac{1}{4}$, then p belongs to C .*

THEOREM B. *Suppose $p \equiv 11 \pmod{12}$. If also $\theta(p-1) > \frac{1}{3}$, then p belongs to C .*

(Actually, Vegh's statement of Theorem B postulates only $p \equiv 3 \pmod{4}$ and $p > 3$. However, the condition $\theta(p-1) > \frac{1}{3}$ renders it vacuous when $p \equiv 7 \pmod{12}$.)

Theorems A and B re-emerge below for general q . More significantly, we show that, except when $q \equiv 1 \pmod{60}$ (in Theorem A), Theorems A and B apply *irrespective of the value of $\theta(q-1)$* . In fact, we prove the following result which, in particular, is valid whenever $q(> 3)$ is a power of 2, 3 or 5.

THEOREM 1.1. *Let $q(> 3)$ be a prime power such that $q \not\equiv 7 \pmod{12}$ and $q \not\equiv 1 \pmod{60}$. Then q is in C .*

Indeed, for even values of q , it is virtually no more difficult to establish a more general result.

Received by the editors November 29, 1983 and, in revised form, April 12, 1984.
 1980 *Mathematics Subject Classification*. Primary 10H35, 12C30.

THEOREM 1.2. *Suppose $q(> 4)$ is even. Then q is in C^* . (Alternatively, every member of F_q is the sum of two primitive roots.)*

It is, of course, evident (see [2]) that every sufficiently large q is in C (and even in C^*). Our method (using elementary estimates for Jacobi sums) demonstrates this in an explicit way. Even in the cases excluded in Theorem 1.1, it provides a test which is inconclusive only in a finite set of values of q which could be listed explicitly. From the evidence on display here and the computations mentioned in [6, §4] it seems reasonable to conjecture that C contains all prime powers except 2, 3 and 7.

2. Theoretical estimates. We suppose that α is a nonzero member of F_q ; from time to time we set $\alpha = 1$. Let e_1 and e_2 be divisors of $q - 1$. We denote by $N(e_1, e_2)$ the number of elements $\xi (\neq 0, -\alpha)$ in F_q for which the greatest common divisor $(s(\xi), e_1) = 1$ and $(s(\xi + \alpha), e_2) = 1$. Here $s(\xi)$ is the divisor of $q - 1$ for which $(q - 1)/s(\xi)$ is the order (index) of ξ in the cyclic group F_q^* . Since our desire is to show that $N(q - 1, q - 1)$ is positive, we abbreviate this number to N_q . However, as we now indicate, it is valuable to consider $N(e_1, e_2)$ in general.

PROPOSITION 2.1. $N_q \geq N(e_1, q - 1) + N(q - 1, e_2) - N(e_1, e_2)$.

PROOF. Suppose ξ is such that either $(s(\xi), e_1) = (s(\xi + \alpha), q - 1) = 1$ or $(s(\xi), q - 1) = (s(\xi + \alpha), e_2) = 1$. Then certainly $(s(\xi), e_1) = (s(\xi + \alpha), e_2) = 1$. Thus $N(e_1, q - 1) + N(q - 1, e_2) - N_q \leq N(e_1, e_2)$ and the result follows.

It is easy to give the value of $N(e_1, e_2)$ when either e_1 or $e_2 = 1$. To do so, we introduce the notation

$$\delta_\alpha(e) = \begin{cases} 1, & \text{if } (s(\alpha), e) = 1, \\ 0, & \text{otherwise.} \end{cases}$$

PROPOSITION 2.2. *Suppose $e|q - 1$. Then*

$$(2.1) \quad N(1, e) = \theta(e)(q - 1) - \delta_\alpha(e), \quad N(e, 1) = \theta(e)(q - 1) - \delta_{-\alpha}(e).$$

In particular, if $\alpha = 1$ and $e > 1$, then

(2.2)

$$N(1, e) = \theta(e)(q - 1), \quad N(e, 1) = \begin{cases} \frac{1}{2}(q - 3), & \text{if } q \equiv 3 \pmod{4} \text{ and } e = 2, \\ \theta(e)(q - 1), & \text{otherwise.} \end{cases}$$

PROOF. Clearly, the number of ξ in F_q for which $(s(\xi), e) = 1$ is just the number of integers i ($0 \leq i < q - 1$) for which $(i, e) = 1$; namely $\theta(e)(q - 1)$. (2.1) and (2.2) are clear from this and the fact that, writing N_α for N , we have

$$(2.3) \quad N_\alpha(e_1, e_2) = N_{-\alpha}(e_2, e_1).$$

For odd values of q , the next result (dealing with e_1 or $e_2 = 2$) has the important consequence that, for smaller values of q , it is significantly easier to handle the value $\alpha = 1$ than a general value of α .

PROPOSITION 2.3. *Suppose q is odd, $\alpha = 1$ and e is an even divisor of $q - 1$. Then*

$$(2.4) \quad N(e, 2) = \begin{cases} \frac{1}{4}(q - 3), & \text{if } q \equiv 3 \pmod{4} \text{ and } e = 2, \\ \frac{1}{2}\theta(e)(q - 1), & \text{otherwise.} \end{cases}$$

Suppose further that $q \equiv 1 \pmod{4}$. Then

$$(2.5) \quad N(2, e) = \frac{1}{2}\theta(e)(q-1).$$

PROOF. Let χ denote the quadratic character in F_q and $\sum_{\xi}$ a sum over ξ in F_q . Then

$$N(e, 2) = \frac{1}{2} \sum_{\substack{\xi \neq 0, -1 \\ (s(\xi), e)=1}} (1 - \chi(\xi + 1)) = \frac{1}{2}(\theta(e)(q-1) - \delta_{-1}(e)) - \frac{1}{2}S,$$

where

$$S = \sum_{\substack{\xi (\neq 0) \\ (s(\xi), e)=1}} \chi(\xi + 1).$$

Now, for any nonzero ξ , $(s(\xi), e) = (s(1/\xi), e)$. Also, $\chi(\xi) = -1$ whenever $(s(\xi), e) = 1$ because e is even. Thus

$$S = \sum_{(s(\xi), e)=1} \chi(\xi)\chi(1 + \xi^{-1}) = - \sum_{(s(1/\xi), e)=1} \chi(1 + \xi^{-1}) = -S.$$

Accordingly, $S = 0$. Since $\delta_{-1}(e) = 1$ if and only if $q \equiv 3 \pmod{4}$ and $e = 2$, then (2.4) holds.

Similarly, since $\delta_1(e) = 0$,

$$N(2, e) = \frac{1}{2} \sum_{\substack{\xi \neq 0, -1 \\ (s(\xi+1), e)=1}} (1 - \chi(\xi)) = \frac{1}{2}\theta(e)(q-1) - \frac{1}{2}T,$$

where $T = \sum_{(s(\xi), e)=1} \chi(\xi - 1)$. However, if $q \equiv 1 \pmod{4}$, then $\chi(-\xi) = -1$ and we get $T = -\sum_{(s(\xi), e)=1} \chi(1 - \xi^{-1}) = -T$ yielding $T = 0$. Thus (2.5) holds.

COROLLARY 2.4. Suppose $q \equiv 1 \pmod{4}$. If $\alpha = 1$, then

$$N_q \geq (\theta(q-1) - \frac{1}{4})(q-1).$$

In particular, if $\theta(q-1) > \frac{1}{4}$, then $q \in C$.

PROOF. Put $e_1 = e_2 = 2$ in Proposition 2.1 and use Proposition 2.3.

COROLLARY 2.5. Suppose $q \equiv 3 \pmod{4}$ and $q > 3$. If $\alpha = 1$, then

$$N_q \geq \frac{1}{2}(3\theta(q-1) - 1)(q-1).$$

In particular, if $\theta(q-1) > \frac{1}{3}$, then $q \in C$.

PROOF. Put $e_1 = 1$ and $e_2 = 2$ in Proposition 2.1 and use (2.2) and (2.4).

We now attempt to estimate $N(e_1, e_2)$ for any α . For any divisor d of $q-1$, let $\sum_{\chi \pmod{d}}$ denote a sum over all $\phi(d)$ multiplicative characters χ of F_q of order d . Then, as in [1, 3], if $e|q-1$, $\xi \in F_q$ and μ denotes the Möbius function,

$$\delta_{\xi}(e) = \theta(e) \sum_{d|e} \frac{\mu(d)}{\phi(d)} \sum_{\chi \pmod{d}} \chi(\xi).$$

Defining $K(\chi_1, \chi_2)$ to be $\sum_{\xi} \chi_1(\xi)\chi_2(\xi + \alpha)$, where χ_1 and χ_2 are characters of order dividing e_1 and e_2 respectively, we immediately obtain the following expression for $N(e_1, e_2)$.

PROPOSITION 2.6.

$$N(e_1, e_2) = \theta(e_1)\theta(e_2) \sum_{d_1|e_1} \sum_{d_2|e_2} \frac{\mu(d_1)\mu(d_2)}{\phi(d_1)\phi(d_2)} \sum_{\chi_1 \pmod{d_1}} \sum_{\chi_2 \pmod{d_2}} K(\chi_1, \chi_2).$$

Let χ_0 be the principal character on F_q . We clearly have $K(\chi_0, \chi_0) = q - 2$. Further, if $\chi \neq \chi_0$, it is straightforward to verify that

$$(2.6) \quad K(\chi_0, \chi) = -\chi(\alpha), \quad K(\chi, \chi_0) = -\chi(-\alpha), \quad K(\chi, \chi^{-1}) = -1.$$

Moreover, $K(\chi_1, \chi_2) = \chi_1(-\alpha)\chi_2(\alpha)J(\chi_1, \chi_2)$, where $J(\chi_1, \chi_2)$ is the Jacobi sum $\sum_{\xi} \chi_1(\xi)\chi_2(1 - \xi)$. By an elementary property of such sums [4, pp. 94, 147], if none of χ_1, χ_2 and $\chi_1\chi_2$ is principal, we have

$$(2.7) \quad |K(\chi_1, \chi_2)| = \sqrt{q}, \quad \chi_1, \chi_2, \chi_1\chi_2 \neq \chi_0.$$

We now give our general estimates for $N(e_1, e_2)$. These involve the function $W(n)$ defined to be the number of square-free divisors of n ; thus $W(n) = 2^{\omega(n)}$, where $\omega(n)$ is the number of distinct primes dividing n .

THEOREM 2.7. Let $e = (e_1, e_2)$. Then

$$(2.8) \quad N(e_1, e_2) = \theta(e_1)\theta(e_2)(q - 1 + E),$$

where

$$(2.9) \quad |E| \leq \left((W(e_1) - 1)(W(e_2) - 1) - \frac{1}{\theta(e)} + 1 \right) \sqrt{q} + \frac{1}{\theta(e)} \\ \leq (W(e_1) - 1)(W(e_2) - 1)\sqrt{q} + 1.$$

Indeed, suppose q is odd, $\alpha = 1$ and e_1 and e_2 are even. Then

$$(2.10) \quad \left| E + \frac{1}{\theta(e)} - 2 + 2\delta \right| \leq \left\{ (W(e_1) - t)(W(e_2) - 2) - \frac{1}{\theta(e)} + 2 \right\} \sqrt{q},$$

where $t = (2, \frac{1}{2}(q - 1))$ and $\delta = \delta_{-1}(e_1)$ ($= 0$, unless $q \equiv 3 \pmod{4}$ and $e_1 = 2$). In particular

$$(2.11) \quad |E + 2\delta| \leq (W(e_1) - t)(W(e_2) - 2)\sqrt{q}.$$

PROOF. Suppose $q \equiv 1 \pmod{4}$, $\alpha = 1$ and e_1 and e_2 are even. Here set

$$M(e_1, e_2) = N(e_1, e_2) - 2\theta(e_1)N(2, e_2) - 2\theta(e_2)N(e_1, 2) + 4\theta(e_1)\theta(e_2)N(2, 2).$$

By (2.4) and (2.5),

$$M(e_1, e_2) = N(e_1, e_2) - \theta(e_1)\theta(e_2)(q - 1) = \theta(e_1)\theta(e_2)E.$$

On the other hand, by Proposition 2.6

$$(2.12) \quad M(e_1, e_2) = \theta(e_1)\theta(e_2) \sum_{\substack{d_1|e_1 \\ d_1 > 2}} \sum_{\substack{d_2|e_2 \\ d_2 > 2}} \frac{\mu(d_1)\mu(d_2)}{\phi(d_1)\phi(d_2)} \sum_{\chi_1 \pmod{d_1}} \sum_{\chi_2 \pmod{d_2}} K(\chi_1, \chi_2).$$

To estimate the contribution to (2.12) of terms for which $\chi_1\chi_2 = \chi_0$, observe that

$$\sum_{\substack{d|e \\ d > 2}} \frac{\mu^2(d)}{\phi^2(d)} \sum_{\chi \pmod{d}} 1 = \frac{1}{\theta(e)} - 2.$$

Hence, by (2.6) and (2.7)

$$\left| E + \frac{1}{\theta(e)} - 2 \right| \leq \left\{ (W(e_1) - 2)(W(e_2) - 2) - \frac{1}{\theta(e)} + 2 \right\} \sqrt{q},$$

which is (2.10) in this case.

For the remaining case of (2.10), we apply Propositions 2.3 and 2.6 in a similar way to the expression

$$N(e_1, e_2) - \theta(e_1)N(1, e_2) - 2\theta(e_2)N(e_1, 2) + 2\theta(e_1)\theta(e_2)N(1, 2).$$

More generally, for (2.9) we consider

$$N(e_1, e_2) - \theta(e_1)N(1, e_2) - \theta(e_2)N(e_1, 1) + \theta(e_1)\theta(e_2)N(1, 1)$$

and employ Propositions 2.2 and 2.6. This completes the proof.

COROLLARY 2.8. *Suppose $q \geq W^4(q-1)$. Then $q \in C^*$.*

PROOF. By (2.8) and (2.9),

$$(2.13) \quad \begin{aligned} N_q &\geq \theta^2(q-1)(q-2-(W(q-1)-1)^2\sqrt{q}) \\ &> \theta^2(q-1)\sqrt{q}(\sqrt{q}-W^2(q-1)). \end{aligned}$$

3. Calculations—odd q . With Theorem 1.1 in mind we introduce notation for various subsets of $\mathcal{P}$, the set of odd positive integers. Set $\mathcal{Q} = \{n \in \mathcal{P}; n \not\equiv 1 \pmod{3}\}$ and $\mathcal{R} = \{n \in \mathcal{P}; n \equiv 1 \pmod{12}, n \not\equiv 1 \pmod{60}\}$. Further, for any positive integer r , let $\mathcal{P}_r, \mathcal{Q}_r, \mathcal{R}_r$ be those subsets of $\mathcal{P}, \mathcal{Q}, \mathcal{R}$, respectively, comprising integers for which $\omega(n-1) = r$. Finally, we let P_r, Q_r, R_r be the least integers in $\mathcal{P}_r, \mathcal{Q}_r, \mathcal{R}_r$, respectively. Thus $P_1 = 2+1=3, P_2 = 2 \cdot 3+1=7, P_3 = 2 \cdot 3 \cdot 5+1=31, \dots; Q_2 = 2 \cdot 5+1=11, Q_3 = 2 \cdot 5 \cdot 7+1=71, \dots; R_2 = 4 \cdot 3+1=13, R_3 = 4 \cdot 3 \cdot 7+1=85, R_4 = 4 \cdot 3 \cdot 7 \cdot 11+1=925, \dots$. Clearly, the odd values of q covered by Theorem 1 are prime powers (> 3) in $\mathcal{Q} \cup \mathcal{R}$.

THEOREM 3.1. *Suppose q is odd. Then $q \in C^*$ provided one of (i)–(iii) is valid, where*

- (i) $\omega(q-1) \geq 16$ or $q > 1.16 \times 10^{18}$,
- (ii) $q \in \mathcal{Q}$ and $(\omega(q-1) \geq 14$ or $q > 4.51 \times 10^{15})$,
- (iii) $q \in \mathcal{R}$ and $(\omega(q-1) \geq 13$ or $q > 2.82 \times 10^{14})$.

PROOF. Suppose $\omega(q-1) \geq 16$. Then clearly $q/W^4(q-1) \geq P_{16}/2^{64} > 1.76$ (because $P_{16} = 2 \cdot 3 \cdot 5 \cdots 53 + 1 > 3.25 \times 10^{19}$). Thus $q \in C^*$ by Corollary 2.8. Further, by (2.13), if $\omega(q-1) \leq 15$ and $q \notin C^*$, then $q \leq 2^{60} < 1.153 \times 10^{18}$. This proves the theorem under condition (i); the argument is similar for (ii) and (iii) using the inequalities $Q_{14}/2^{56} > 2.84$ and $R_{13}/2^{52} > 1.16$.

From now on in this section we suppose $\alpha = 1$. For an even divisor e of $q-1$, we have, by Propositions 2.1 and 2.3 together with (2.8) and (2.11)

$$(3.1) \quad \begin{aligned} N_q &\geq N(e, q-1) + N(q-1, 2) - N(e, 2) \\ &\geq \{\theta(e)\theta(q-1) + \tfrac{1}{2}\theta(q-1) - \tfrac{1}{2}\theta(e)\}(q-1) \\ &\quad - \theta(e)\theta(q-1)(W(e)-1)(W(q-1)-2)\sqrt{q}, \end{aligned}$$

where

$$t = \begin{cases} 2, & \text{if } q \equiv 1 \pmod{4}, \\ 1, & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

For $W(e) > t$ we now define a quantity $T = T_q(e)$ by $T = UV$, where

$$(3.2) \quad U = U_q(e) = \frac{1 + 1/2\theta(e) - 1/2\theta(q-1)}{W(e) - t},$$

$$V = V_q = \frac{q-1}{(W(q-1) - 2)\sqrt{q}}.$$

It is evident from (3.1) that $q \in C$ provided $T_q(e) > 1$ for some even divisor e of $q-1$. For that follows we observe some useful principles regarding lower bounds for T . First, for fixed $\omega(q-1)$, V is an increasing function. Moreover, V_{Q_r} and V_{R_r} are increasing functions of r ($r \geq 3$). With regard to U , we note that

$$0 \geq \frac{1}{\theta(e)} - \frac{1}{\theta(q-1)} = \frac{1}{\theta(e)} \left(1 - \frac{1}{\theta(e')} \right),$$

where e' is the product of the primes in $q-1$ not in e . It follows from (3.2) that, if the integer n (not necessarily a prime power) is obtained from q by replacing some of the primes in $q-1$ by smaller primes to yield a number $n-1$ with $\omega(n-1) = \omega(q-1)$ and if e is replaced by e^* , the product of the smallest $\omega(e)$ primes in $n-1$, then $U_q(e) \geq U_n(e^*)$. For example, if $q \in \mathcal{Q}_r$ and $\omega(e) = m$, then $U_q(e) \geq U_{Q_r}(Q_m - 1)$.

We now complete the proof of Theorem 1.1 for odd q . First suppose $q \in \mathcal{Q}_r$, so that $t = 1$ in (3.1) and (3.2). If $r \leq 3$, then $\theta(q-1) \geq \theta(Q_3 - 1) = \frac{12}{35} > \frac{1}{3}$ and $q \in C$ by Corollary 2.5. By Theorem 3.1 we may therefore suppose that $4 \leq r \leq 13$. We also suppose $q \geq n$, where $n \in \mathcal{Q}_r$. For $4 \leq r \leq 6$ we take $e = 2$ and use the fact that

$$(3.3) \quad T_q(2) \geq U_{Q_r}(2)V_n = \left(2 - \frac{1}{2\theta(Q_r - 1)} \right) V_n.$$

Then (3.3) yields lower bounds for $T_q(2)$ ($q \geq n$) as in the following table.

r	$\theta(Q_r - 1)$	n	$T_q(2)$
4	.3116	1331	1.02
5	.2877	14631	1.05
6	.2707	Q_6	1.01

The only relevant prime power in $\mathcal{Q}$ not covered by this table is 911 (for example, 10011 and 13091 in $\mathcal{Q}_5$ are not prime powers). However, it can be verified directly that -5 and -6 are both primitive roots in F_{911} .

Next let $q \in \mathcal{Q}_r$, where $r = 7$ or 8 . We take $\omega(e) = 2$ so that $W(e) - 1 = 3$. Then

$$T_q(e) \geq U_{Q_8}(10)V_{Q_7} > 1.006,$$

because $\theta(10) = .4$, $Q_7 = 3233231$, $Q_8 = 2 \cdot 3 \cdot 5 \cdots 23 + 1$, $\theta(Q_8 - 1) > .2453$. Similarly, if $9 \leq r \leq 13$, we take $\omega(e) = 3$ so that $\theta(e) \geq \theta(70) = 12/35$ and

$$T_q(e) > U_{Q_{13}}(70)V_{Q_9} > 1.38.$$

Since $Q_9 = 2156564411$ and $\theta(Q_{13} - 1) > .2125$, this completes the proof for q in $\mathcal{Q}$.

We turn our attention now to prime powers q in $\mathcal{R}_r$ with the consequence (crucial for smaller values) that $t = 2$ in (3.2) (for $\omega(e) \geq 2$). If $r \leq 4$, then $\theta(q - 1) \geq \theta(462) = \frac{20}{77} > \frac{1}{4}$ so that, by Corollary 2.4 and Theorem 3.1, we may assume that $5 \leq r \leq 12$.

Suppose $5 \leq r \leq 8$ and $q \geq n \in \mathcal{R}_r$. Then $T_q(6) \geq U_{R_r}(6)V_n$, where

$$U_{R_r}(6) = \frac{1}{2} \left(2.5 - \frac{1}{2\theta(R_r - 1)} \right).$$

As before, we construct a table of lower bounds for $T_q(6)$ as follows.

r	$\theta(R_r - 1)$	n	$T_q(6)$
5	.2397	21253	1.006
6	.2256	R_6	1.03
7	.2137	R_7	1.25
8	.2044	R_8	1.0007

This table applies to all relevant prime powers in $\mathcal{R}$ except $20749 = 4 \cdot 3 \cdot 7 \cdot 13 \cdot 19 + 1$ (for example, 12013, 15709 and 17557 in $\mathcal{R}_5$ are not prime powers). However, $\theta(20748) > .2498$ so that $T_{20749}(6) > 1.19$.

Finally, we can deal with all q in $\mathcal{R}_r$, $9 \leq r \leq 12$, simultaneously by setting $\omega(e) = 4$ so that $\theta(e) \geq \theta(462) = \frac{20}{77}$ while $W(e) - 2 = 14$. We have

$$T_q(e) \geq U_{R_{12}}(462)V_{R_9} > 1.19,$$

since $\theta(R_{12} - 1) > .1813$ and $R_9 > 2.587 \times 10^9$. This completes the proof of Theorem 1.1 for odd q .

When q is an odd prime power not in $\mathcal{Q} \cup \mathcal{R}$, (3.1) can be used to test whether q is in C but fails for many smaller values (such as $43891 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 + 1$ and $(1429)^2 = 2042041 = 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1$). The author may make these the object of further study probably using computation. However, we conclude here with a simple example in which (2.10) is delicate enough to show that $q \in C$ when (2.11) fails. We have

$$(3.4) \quad \begin{aligned} N_{751} &\geq N(6, 750) + N(750, 2) - N(6, 2) \\ &\geq \frac{4}{45} (749 - 17\sqrt{751}) + 100 - 125 > .16. \end{aligned}$$

(If (2.11) had been used the bracketed term in (3.4) would have been $750 - 18\sqrt{751}$.)

4. Even prime powers. Let $q = 2^m$. Corollary 2.8 yields a simple sufficient condition for q to be in C^* .

PROPOSITION 4.1. *Suppose $m \geq 4\omega(q - 1)$. Then q is in C^* .*

COROLLARY 4.2. *Suppose $m > 12$. Then q is in C^* .*

PROOF. Suppose $r = \omega(q-1) \geq 13$. Then $q > 3 \cdot 5 \cdot 7 \cdot 11 \cdots 43 \times 16^{r-13} > (6.543 \times 10^{15}) \times 16^{r-13}$. Thus $m > 52.5 + 4(r-13) > 4r$. Hence $q \in C^*$ by Proposition 4.1. Again by Proposition 4.1, if $\omega(q-1) \leq 12$ and $m \geq 48$, then $q \in C^*$. Finally, whenever $13 \leq m \leq 47$, $m \geq 4\omega(q-1)$, as can quickly be verified directly. For example, writing ω_m for $\omega(2^m-1)$, we find that the most delicate cases are as follows:

$$\omega_{16} = \omega_{18} = 4, \quad \omega_{20} = 5, \quad \omega_{24} = \omega_{28} = \omega_{30} = 6, \quad \omega_{36} = 8.$$

(For instance, $2^{24} - 1 = 9 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$.) This completes the proof.

Next, the simple application of Proposition 2.1 (with $e_1 = e_2 = 1$) which follows proves that $q \in C^*$ when $m = 3, 5, 6, 7, 9, 10, 11$. We write $\varepsilon_\alpha = 2\delta_\alpha(q-1) - 1$ (so that $\varepsilon_\alpha = 1$, if α is a primitive root, and -1 , otherwise) and observe that here, by (2.3), $N(e_1, e_2) = N(e_2, e_1)$.

PROPOSITION 4.3. $N_q \geq 2(q-1)\{\theta(q-1) - (\frac{1}{2} + \frac{1}{2}\varepsilon_\alpha/(q-1))\}$. In particular, if $\theta(q-1) > \frac{1}{2} + 1/2(q-1)$, then $q \in C^*$.

Proposition 4.3 yields a little more. For, if $m = 2, 4$ or 8 , then actually $\theta(q-1) = \frac{1}{2} + 1/2(q-1)$, so that, since $\varepsilon_1 = -1$, then in these cases $q \in C$, at least. In summary, Theorem 1.1 is proven except when $q = 2^{12} = 4096$ while Theorem 1.2 remains unproved additionally when $q = 16$ or 256 . For their completion, we devise an improvement of Theorem 4.3 stated for convenience when m is a multiple of 4. For any divisors e_1 and e_2 of $q-1$, we now write $M(e_1, e_2)$ for the number of ξ in F_q for which ξ is an e_1 th power and $\xi + \alpha$ an e_2 th power (possibly 0) in F_q and note that $M(e_1, e_2) = M(e_2, e_1)$.

PROPOSITION 4.4. Suppose 4 divides m (so that 15 divides $q-1$). Then

$$(4.1) \quad N_q \geq 2\theta(q-1)(q-1) - q + M(3, 3) + 2M(3, 5) - 2M(3, 15)$$

$$(4.2) \quad \geq 2\theta(q-1)(q-1) - q + M(3, 3).$$

PROOF. The association $\xi \leftrightarrow \xi + \alpha$ partitions F_q into a set of $\frac{1}{2}q$ pairs. Regarding the pair $(\xi, \xi + \alpha)$ as distinct from $(\xi + \alpha, \xi)$ we obtain q ordered, associate pairs. Let $\mathcal{M}(e_1, e_2)$ denote the set of such pairs for which ξ is an e_1 th power and $\xi + \alpha$ an e_2 th power. Let $\mathcal{N}_i$ ($i = 1, 2$) be the set of such pairs containing precisely i primitive roots. Then $\mathcal{N}_1, \mathcal{N}_2$ and $\mathcal{M} := \mathcal{M}(3, 3) \cup \mathcal{M}(3, 5) \cup \mathcal{M}(5, 3)$ are pairwise disjoint sets. Hence

$$(4.3) \quad |\mathcal{N}_1| + |\mathcal{N}_2| + |\mathcal{M}| \leq q.$$

Now, $|\mathcal{N}_2| = N_q$ and $|\mathcal{N}_1| = 2(\theta(q-1)(q-1) - N_q)$. Also, for example, $\mathcal{M}(3, 3) \cap \mathcal{M}(3, 5) = \mathcal{M}(3, 15)$ so that, expressed as a union of disjoint sets, we have

$$\mathcal{M} = \mathcal{M}(3, 3) \cup (\mathcal{M}(3, 5) \setminus \mathcal{M}(3, 15)) \cup (\mathcal{M}(5, 3) \setminus \mathcal{M}(15, 3)).$$

It follows that $|\mathcal{M}| = M(3, 3) + 2M(3, 5) - 2M(3, 15)$. (4.1) and, consequently, (4.2) now flow from (4.3).

From (4.2), to show that either 16 or $256 \in C^*$ it suffices to prove that $M(3, 3)$ is positive. In fact, we estimate $M(3, 3)$, $M(3, 5)$ and $M(15, 3)$ using the notation

$$\eta(e) = \begin{cases} 1, & \text{if } \alpha \text{ is an } e\text{th power,} \\ 0, & \text{otherwise.} \end{cases}$$

First, let χ be a cubic character on F_q . Then

$$\begin{aligned} M(3, 3) &= \frac{1}{9} \sum_{\xi} (1 + \chi(\xi) + \chi^2(\xi))(1 + \chi(\xi + \alpha) + \chi^2(\xi + \alpha)) + \frac{4}{3} \eta(3) \\ &= \frac{1}{9} (q + 2K(\chi, \chi^2) + K(\chi, \chi) + K(\chi^2, \chi^2)) + \frac{4}{3} \eta(3) \\ &\geq \frac{1}{9} (q - 2 - 2\sqrt{q}) + \frac{4}{3} \eta(3), \end{aligned}$$

using (2.6) and (2.7). This is positive for all $q \geq 8$. Similarly, if χ_1 and χ_2 are characters of orders 3 and 5 respectively, then

$$\begin{aligned} M(3, 5) &= \frac{1}{15} \sum_{\xi} (1 + \chi_1(\xi) + \chi_1^2(\xi)) \\ &\quad \cdot (1 + \chi_2(\xi + \alpha) + \chi_2^2(\xi + \alpha) + \chi_2^3(\xi + \alpha) + \chi_2^4(\xi + \alpha)) \\ &\quad + \frac{2}{3} \eta(5) + \frac{4}{5} \eta(3) \\ &\geq \frac{1}{15} (q - 8\sqrt{q}) + \frac{2}{3} \eta(5) + \frac{4}{5} \eta(3). \end{aligned}$$

Finally, if χ is now a character of order 15, then

$$\begin{aligned} M(3, 15) &= \frac{1}{45} \sum_{\xi} (1 + \chi^5(\xi) + \chi^{10}(\xi))(1 + \chi(\xi + \alpha) + \cdots + \chi^{14}(\xi + \alpha)) \\ &\quad + \frac{2}{3} \eta(15) + \frac{14}{15} \eta(3) \\ &\leq \frac{1}{45} (q - 2 + 26\sqrt{q}) + \frac{2}{3} \eta(15) + \frac{14}{15} \eta(3). \end{aligned}$$

We deduce from these inequalities and (4.1) that, if 4 divides m , then

$$N_q \geq 2(q-1) \left(\theta(q-1) - \frac{2}{5}q - \frac{11\sqrt{q}/9 + 7/15}{q-1} \right) = 2(q-1)L_q,$$

say. Now $4095 = 9 \cdot 5 \cdot 7 \cdot 13$ so that $\theta(4095) > .42197$ and so $L_{4096} > .42197 - .41922 > .002$. Thus $4096 \in C^*$.

BIBLIOGRAPHY

1. L. Carlitz, *Distribution of primitive roots in a finite field*, Quart. J. Math. (2) **4** (1953), 4–10.
2. ———, *Sets of primitive roots*, Compositio Math. **13** (1956), 65–70.
3. S. D. Cohen, *Primitive roots in the quadratic extension of a finite field*, J. London Math. Soc. (2) **27** (1983), 221–228.
4. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, Heidelberg and Berlin, 1982.
5. E. Vegh, *Pairs of consecutive primitive roots modulo a prime*, Proc. Amer. Math. Soc. **19** (1968), 1169–1170.
6. ———, *A note on the distribution of the primitive roots of a prime*, J. Number Theory **3** (1971), 13–18.