PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 94, Number 4, August 1985

CONSECUTIVE PRIMITIVE ROOTS IN A FINITE FIELD. II

STEPHEN D. COHEN

ABSTRACT. The proof of the theorem that every finite field of order q (> 3) such that $q \not\equiv 7 \pmod{12}$ contains a pair of consecutive primitive roots is completed by consideration of the case in which $q \equiv 1 \pmod{60}$.

1. Introduction. For any prime power q, let F_q denote the finite field of order q. As in [**3**], let C denote the class of prime powers q for which F_q contains a primitive root γ whose successor $\gamma + 1$ is also a primitive root. The object of this paper is to complete the proof of the following theorem.

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

For any n, let $\theta(n) = \phi(n)/n$, where ϕ is Euler's function. A conditional version of Theorem 1.1 was proved by Vegh [**5**, **6**] for *primes* $q \not\equiv 7 \pmod{12}$ satisfying $\theta(q-1) > \frac{1}{4}$ when $q \equiv 1 \pmod 4$ and $\theta(q-1) > \frac{1}{3}$ when $q \equiv 11 \pmod{12}$. More significantly, the theorem was proved unconditionally by the author in the first part [**3**] except when $q \equiv 1 \pmod{60}$. In this second part, although we begin with a brief treatment of general fields of odd *square* order, the main business is a discussion of this exceptional case. By a distinct development of the work of [**3**] including careful handling of the Jacobi sums involved, we deal theoretically with all prime powers q apart from 33 prime values, the largest of which is 2,762,761. Finally, using a computer, we have been able to exhibit explicitly a pair of consecutive primitive roots for each of these remaining values.

We should remark here that it was noted in Theorem 3.1 of [**3**] that, even if $q \equiv 7 \pmod{12}$, then q is in C provided $q > 1.16 \times 10^{18}$. Further work, probably requiring more extensive computation, is needed to consider all smaller values of q; this may be the subject of further study.

2. Fields of square order. From now on we suppose that q is an *odd* prime power. In this section we also suppose that $q = q_0^2$ is a square and establish the fact that such a q is always in C as a consequence of the work of [**2**] (which itself included some delicate calculation).

THEOREM 2.1. *Suppose $q = q_0^2$. Then every nonzero member of F_{q_0} is the sum of two primitive roots of F_q.*

Received by the editors July 2, 1984.
1980 *Mathematics Subject Classification*. Primary 10H35, 12C30.

PROOF. Let $a\ (\neq 0) \in F_{q_0}$. Select any nonsquare b in F_{q_0} and let $\sqrt{b}$ be a square root of b in F_q. Then, by Theorem 1.1 of [**2**], there exists c in F_{q_0} such that $\gamma = a/2 + c\sqrt{b}$ is a primitive root in F_q. Now, γ is conjugate over F_{q_0} to $\bar{\gamma} = \gamma^{q_0} = a/2 - c\sqrt{b}$, itself a primitive root of F_q. Since $\gamma + \bar{\gamma} = a$, the proof is complete.

COROLLARY 2.2. *Suppose $q = q_0^2$. Then q is in C.*

PROOF. By Theorem 2.1, there exist primitive roots γ_1, γ_2 in F_q such that $\gamma_1 + \gamma_2 = 1$. However, since $q \equiv 1 \pmod 4$, then $-\gamma_2$ is also a primitive root and so $\gamma_1 - 1$ and γ_1 are consecutive primitive roots.

3. General formulae and estimates. We suppose from now on that $q \equiv 1 \pmod 4$ (and even, when necessary, that $q \equiv 1 \pmod{60}$). This implies that if χ is any multiplicative character of F_q of *square-free* order, then $\chi(-1) = 1$. In particular, if η is also a character of F_q, then the Jacobi sum $J(\chi, \eta)$ is given by

$$J(\chi, \eta) = \sum_{\xi \in F_q} \chi(\xi)\eta(\xi + 1).$$

As in [**3**], for any divisors e_1 and e_2 of $q - 1$, we denote by $N(e_1, e_2)$ the number of elements $\xi\ (\neq 0, -1)$ in F_q for which $s(\xi)$ and e_1 are coprime and $s(\xi + 1)$ and e_2 are coprime, where $(q - 1)/s(\xi)$ is the order of ξ in F_q^*.

We summarise some immediate consequences of Propositions 2.1, 2.3 and 2.6 of [**3**] taking into account the fact that here $q \equiv 1 \pmod 4$.

PROPOSITION 3.1. *Suppose that e_1 and e_2 are divisors of $q - 1$. Then*
(i) $N(e_1, e_2) = N(e_2, e_1)$;
(ii) $N_q \geq N(e_1, q - 1) + N(q - 1, e_2) - N(e_1, e_2)$;

(iii) $$N(e_1, e_2) = \theta(e_1)\theta(e_2) \sum_{d_1 | e_1} \sum_{d_2 | e_2} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\chi \pmod{d_1}} \sum_{\eta \pmod{d_2}} J(\chi, \eta)$$

where $\sum_{\chi(\mathrm{mod}\ d)}$ denotes a sum over all $\phi(d)$ characters of order d;
(iv) $N(2, e_2) = \frac{1}{2}\theta(e_2)(q - 1)$.

COROLLARY 3.2. *Suppose $2|e|q - 1$. Then*

$$N_q \geq \left(2\frac{\theta(q-1)}{\theta(e)} - 1\right)N(e, e) + 2\theta(e)\theta(q - 1) \sum_{\substack{d|e \\ d>2}} M_e(d), \tag{3.1}$$

where

$$M_e(d) = \frac{\mu(d)}{\phi(d)} \sum_{\substack{d'|q-1 \\ d' \nmid e}} \frac{\mu(d')}{\phi(d')} \sum_{\chi \pmod d} \sum_{\eta \pmod{d'}} J(\chi, \eta). \tag{3.2}$$

PROOF. By Proposition 3.1, the right-hand side of (3.1) equals

$$N(e, q - 1) + N(q - 1, e) - N(e, e) - 2\{\theta(e)N(2, q - 1) - \theta(q - 1)N(2, e)\},$$

the quantity in braces, in fact, having the value 0.

LEMMA 3.3. *Suppose $d\,(>2)$ and e are divisors of $q-1$ with e even and $d|e$. Then*

$$|M_e(d)| \le \lambda_d(W(q-1)-W(e))\sqrt{q}, \tag{3.3}$$

where $W(n)=2^{\omega(n)}$, the number of square-free divisors of n, and

$$\lambda_d = \sum_{i=1}^{d} |\varepsilon_d(i)+\varepsilon_d(d+1-i)|/2\phi(d)W(d) \le 1, \tag{3.4}$$

where $\varepsilon_d(i)=\mu((d,i))\phi((d,i))$. In particular, if $q\equiv 1 \pmod{60}$, $\lambda_3=\frac{1}{2}$, $\lambda_5=\frac{3}{4}$, $\lambda_6=\frac{3}{4}$, $\lambda_{10}=\frac{5}{8}$, $\lambda_{15}=\frac{3}{4}$, $\lambda_{30}=\frac{23}{32}$.

PROOF. We can suppose that d is square-free. The absolute value of each Jacobi sum in (3.2) equals $\sqrt{q}$ which quickly yields (3.3) with $\lambda_d \le 1$ (cf. Theorem 2.7 of [**3**]). The key to the distinct improvement (3.4) is the identity (see pp. 92, 93 and 147 of [**4**])

$$J(\chi,\eta)=J(\chi,\chi^{-1}\eta^{-1}) \tag{3.5}$$

(again recalling that here $\chi(-1)=1$).

Write the product of the distinct primes in $q-1$ as Qd and the product of the distinct primes in e as Ed. Then a divisor d' of $q-1$ (in (3.2)) can be expressed as d_1d_2, where $d_1|Q$, $d_2|d$ with $d'\nmid e$ if and only if $d_1\nmid E$. Hence,

$$M_e(d)=\frac{\mu(d)}{\phi(d)}\sum_{\substack{d_1|Q\\ d_1\nmid E}}\frac{\mu(d_1)}{\phi(d_1)}\sum_{\chi \,(\mathrm{mod}\, d)}\ \sum_{\eta\,(\mathrm{mod}\, d_1)} L(\chi,\eta), \tag{3.6}$$

where (replacing χ by χ^{-1} for convenience) we have

$$\begin{aligned}
L(\chi,\eta) &= \sum_{d_2|d}\frac{\mu(d_2)}{\phi(d_2)}\sum_{\eta^*\,(\mathrm{mod}\, d_2)} J(\chi^{-1},\eta^*\eta) \\
&= \sum_{d_2|d}\frac{\mu(d_2)}{\phi(d_2)}\sum_{\substack{j=1\\ (j,d_2)=1}}^{d_2} J(\chi^{-1},\chi^{jd/d_2}\eta) \\
&= \frac{\mu(d)}{\phi(d)}\sum_{i=1}^{d}\varepsilon(i)J(\chi^{-1},\chi^i\eta) \\
&= \frac{\mu(d)}{2\phi(d)}\sum_{i=1}^{d}\varepsilon(i)\big(J(\chi^{-1},\chi^i\eta)+J(\chi^{-1},\chi^{d+1-i}\eta^{-1})\big), \quad \text{by (3.5)}, \\
&= \frac{\mu(d)}{2\phi(d)}\sum_{i=1}^{d}\big(\varepsilon(i)J(\chi^{-1},\chi^i\eta)+\varepsilon(d+1-i)J(\chi^{-1},\chi^i\eta^{-1})\big).
\end{aligned} \tag{3.7}$$

Now, because e is even, whenever E is odd then d is even and Q is odd. Thus, if $d_1|Q$ but $d_1\nmid E$, then $d_1>2$ and so $\eta\ne\eta^{-1}$ in (3.6). By (3.7), we have

$$\begin{aligned}
&L(\chi,\eta)+L(\chi,\eta^{-1}) \\
&\quad= \frac{\mu(d)}{2\phi(d)}\sum_{i=1}^{d}(\varepsilon(i)+\varepsilon(d+1-i))\big(J(\chi^{-1},\chi^i\eta)+J(\chi^{-1},\chi^i\eta^{-1})\big),
\end{aligned}$$

which has absolute value at most $\nu_d\sqrt{q}/\phi(d)$, where

$$\nu_d = \sum_{i=1}^{d} |\varepsilon(i) + \varepsilon(d+1-i)|.$$

Hence, from (3.6),

$$\begin{aligned}|M_e(d)| &\le (\nu_d\sqrt{q}/\phi(d)) \cdot \tfrac{1}{2}\phi(d_1) \cdot \phi(d) \cdot (\phi(d_1))^{-1} \cdot (W(Q) - W(E)) \cdot (\phi(d))^{-1} \\ &= \lambda_d(W(q-1) - W(e))\sqrt{q},\end{aligned}$$

since $W(Q) - W(E) = (W(q-1) - W(e))/W(d)$.

Finally, short calculations yield the displayed explicit values of λ_d.

By Lemma 3.3, in order to apply Corollary 3.2 it remains to estimate $N(e, e)$. In fact, as in Theorem 2.7 of [**3**], we have

$$N(e,e) = \theta^2(e)\{q + 1 - 1/\theta(e) + E(e)\},$$

where

$$E(e) = \sum_{\substack{d_1 \mid e \\ d_1 > 2}} \sum_{\substack{d_2 \mid e \\ d_2 > 2}} \frac{\mu(d_1)}{\phi(d_1)} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\substack{\chi (\mathrm{mod}\, d_1)\, \eta (\mathrm{mod}\, d_2) \\ \chi \ne \eta^{-1}}} \sum J(\chi, \eta), \tag{3.8}$$

so that

$$|E(e)| \le \left\{(W(e) - 2)^2 - (\theta(e))^{-1} + 2\right\}\sqrt{q};$$

in particular,

$$|E(6)| \le 3\sqrt{q}, \qquad |E(30)| \le (137/4)\sqrt{q} \quad (q \equiv 1 \pmod{60}). \tag{3.9}$$

We outline some improvements of (3.9) based on the use of (3.5) in (3.8).

First, if χ is a character of order 6, we have

$$E(6) = -\tfrac{1}{2}\mathrm{Re}\{J(\chi,\chi) + 2J(\chi,\chi^2) - J(\chi^2,\chi^2)\}$$

so that

$$|E(6)| \le 2\sqrt{q}. \tag{3.10}$$

Indeed, while the fact is not used in the sequel, it is interesting to note that if q is a prime, then $E(6)$ can be evaluated explicitly in terms of a specific quadratic partition of q (see [**1**, §3.1]). Thus, $E(6) = -a - \frac{3}{2}zb$ and

$$N(6,6) = \tfrac{1}{9}(q - 2 - a - \tfrac{3}{2}zb),$$

where $a^2 + 3b^2 = q$, $a \equiv -1 \pmod 3$ and $z \in \{0, 1, -1\}$ with $z = 0$ if and only if 2 is a cubic residue in F_q. It follows that, when q is prime,

$$|E(6)| < \begin{cases} \sqrt{q} & \text{if 2 is a cubic residue in } F_q, \\ \tfrac{1}{2}\sqrt{(7q)} & \text{otherwise,} \end{cases}$$

an improvement on (3.10).

Resuming the discussion with a general prime power $q \equiv 1 \pmod{60}$ and similarly working carefully with (3.5) in (3.8) with $e = 30$, we obtain

$$N(30,30) = \frac{16}{225}\left(q - \frac{11}{4} + E(30)\right), \qquad |E(30)| \le \frac{35}{2}\sqrt{q}, \tag{3.11}$$

although, for our purposes, (3.9) would suffice almost as well.

Now select, in turn, $e = 6$, 30 in Corollary 3.2 and use the estimates of Lemma 3.3, (3.10) and (3.11) observing, in particular, that $\lambda_3 + \lambda_6 = \frac{5}{4}$ and $\lambda_3 + \lambda_5 + \lambda_6 + \lambda_{10} + \lambda_{15} + \lambda_{30} = \frac{131}{32}$.

PROPOSITION 3.4. *Suppose* $q \equiv 1 \pmod{12}$ *and* $\theta(q-1) > \frac{1}{6}$. *Then*

$$N_q \geq \tfrac{1}{9}(6\theta(q-1)-1)\sqrt{q}R_q(\theta(q-1)),$$

where

$$R_q(\theta) = \sqrt{q} - \left\{\frac{5(W(q-1)-4)}{4(1-(1/6\theta))} + 2 + \frac{2}{\sqrt{q}}\right\}.$$

PROPOSITION 3.5. *Suppose* $q \equiv 1 \pmod{60}$ *and* $\theta(q-1) > \frac{2}{15}$. *Then*

$$N_q \geq \tfrac{8}{225}(15\theta(q-1)-2)\sqrt{q}S_q(\theta(q-1)),$$

where

$$S_q(\theta) = \sqrt{q} - \left\{\frac{131(W(q-1)-8)}{32(1-(2/15\theta))} + \frac{35}{2} + \frac{11}{4\sqrt{q}}\right\}.$$

Finally in this section, we refine the bound (3.1) of [**3**] when $e = 6$. By Proposition 3.1 we have

$$\begin{aligned} N_q &\geq N(6, q-1) + N(q-1, 2) - N(6, 2) \\ &= 3\theta(q-1)N(6,6) + \tfrac{1}{3}\theta(q-1)(M_6(3) + M_6(6)) \\ &\quad + (\tfrac{1}{2}\theta(q-1) - \tfrac{1}{6})(q-1) \end{aligned}$$

and an application of Lemma 3.3 yields the following result:

PROPOSITION 3.6. *Suppose* $q \equiv 1 \pmod{12}$ *and* $\theta(q-1) > \frac{1}{5}$. *Then*

$$N_q \geq \frac{1}{6}(5\theta(q-1)-1)\sqrt{q}\left\{\frac{q-1}{\sqrt{q}} - \frac{5W(q-1)-12}{2(5-(1/\theta(q-1)))}\right\} - \frac{\theta(q-1)}{3}.$$

4. Calculations. Let $\mathscr{T}$ be the set of positive integers n for which $n \equiv 1 \pmod{60}$ and, for $r \geq 3$, $\mathscr{T}_r$ the subset comprising those n with $\omega(n-1) = r$. Also let $T_r = 4 \cdot 3 \cdot 5 \cdots p_r + 1$ (where p_r is the rth prime) be the least member of $\mathscr{T}_r$.

By Corollary 2.4 and Theorem 3.1(i) of [**3**], Theorem 1.1 holds for prime powers q in $\mathscr{T} \setminus \bigcup_{r=4}^{15} \mathscr{T}_r$. Our principal tool for considering q in $\bigcup_{r=7}^{15} \mathscr{T}_r$ is Proposition 3.5 (wherein we set $S_q = S_q(\theta(q-1))$); for q in $\mathscr{T}_5 \cup \mathscr{T}_6$ we similarly rely mainly on Proposition 3.4 (with $R_q = R_q(\theta(q-1))$) while Proposition 3.6 is used for q in $\mathscr{T}_4$.

First, suppose $q \in \bigcup_{r=10}^{15} \mathscr{T}_r$. Then $\theta(q-1) \geq \theta(T_{15}-1) > .1417$ and, easily,

$$\frac{S_q}{W(q-1)} \geq \frac{S_{T_{15}}(.1417)}{W(q-1)} > \frac{\sqrt{T_{10}}}{1024} - \frac{131}{32(1-(2/15(.1417)))} > 40.$$

Hence, N_q is positive. Similarly, if $q \in \mathscr{T}_9$, then $\theta(q-1) \geq \theta(T_9 - 1) > .1613$ and $S_q \geq S_{T_9}(.1613) > 9200$. Next, if $q \in \mathscr{T}_8$, then $\theta(q-1) > .171$ and $S_q > S_q(.171)$ which is positive certainly if $q > 21{,}410{,}000$. Moreover, T_8 ($= 19{,}399{,}381 = 47 \cdot 289543$), the only member of $\mathscr{T}_8$ less than this bound, is not a prime power. More

precision is required for q in $\mathscr{T}_7$, in which case $\theta(q-1) > .1805$. As above, we can dispose of all such $q > 3{,}600{,}300$ for then $S_q(.1805)$ is positive. A few smaller values of q in $\mathscr{T}_7$ are, however, also covered by Propositions 3.4 or 3.5. For example, temporarily setting $n = 4 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ we find that R_q is positive when $q = nm + 1$, where $m = 13 \cdot 37$, $17 \cdot 23$, $2 \cdot 13 \cdot 29$ or $2 \cdot 17 \cdot 19$. In fact, just 12 members of $\mathscr{T}_7$ (not all prime powers) remain unaccounted for; these (along with their prime factorisations if composite) are

$$\begin{aligned}
1{,}021{,}021\ (= T_7) &= 181 \cdot 5641; & 1{,}141{,}141 &= n \cdot 13 \cdot 19 + 1 \\
& & &= 31 \cdot 131 \cdot 281; \\
1{,}381{,}381 &= n \cdot 13 \cdot 23 + 1; & 1{,}492{,}261 &= n \cdot 17 \cdot 19 + 1; \\
1{,}741{,}741 &= n \cdot 13 \cdot 29 + 1; & 1{,}806{,}421 &= n \cdot 17 \cdot 23 + 1; \\
1{,}861{,}861 &= n \cdot 13 \cdot 31 + 1; & 2{,}042{,}041 &= 2T_7 - 1 = 1429^2; \\
2{,}282{,}281 &= n \cdot 2 \cdot 13 \cdot 19 + 1; & 2{,}762{,}761 &= n \cdot 2 \cdot 13 \cdot 23 + 1; \\
3{,}063{,}061 &= 3T_7 - 2 & 3{,}423{,}421 &= n \cdot 2 \cdot 3 \cdot 13 \cdot 19 + 1 \\
&= 1451 \cdot 2111; & &= 29 \cdot 97 \cdot 121.
\end{aligned}$$

Fortunately, $1429^2 \in C$ by Corollary 2.2. It therefore remains to check the seven primes which occur in the above list; for this we refer to the Table at the end.

We summarise rather briefly a similar program applied to $\mathscr{T}_5 \cup \mathscr{T}_6$ but based on Proposition 3.4.

If $q \in \mathscr{T}_6$, then $q \geq T_6 = 60{,}061$ and $R_q > R_q(.1918) > 0$ provided $q > 330{,}000$. More delicately, R_q is positive when $q = nm + 1$, where now $n = 2 \cdot 3 \cdot 5 \cdot 7$ and $m = 11 \cdot 41$, $13 \cdot 37$, $17 \cdot 23$, $2 \cdot 13 \cdot 19$ or $3 \cdot 11 \cdot 19$. Excluding non-prime-power members of $\mathscr{T}_6$ we are left with twelve primes along with $175{,}561 = 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 + 1 = 419^2$ and $212{,}521 = 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 + 1 = 461^2$ to which Corollary 2.2 applies.

If $q\ (\geq 4621) \in \mathscr{T}_5$, then $R_q\ (> R_q(.20779))$ is positive whenever $q > 32{,}000$ and also when $q = 19{,}741 = 4 \cdot 3 \cdot 5 \cdot 7 \cdot 47 + 1$. Additionally, by Proposition 3.6, N_q is positive when $q = 15{,}181 = 4 \cdot 3 \cdot 5 \cdot 11 \cdot 23 + 1$. Just ten primes in $\mathscr{T}_5$ (lying between 4,621 and 21,841) remain along with $17{,}161 = 8 \cdot 3 \cdot 5 \cdot 11 \cdot 13 + 1 = 131^2$ and $19{,}321 = 8 \cdot 3 \cdot 5 \cdot 7 \cdot 23 + 1 = 139^2$; for example 23,101, 23,941, 27,301 and 27,721 (all larger members of $\mathscr{T}_5$) are not prime powers.

For q in $\mathscr{T}_4$ (so that $q \geq 421$ and $\theta(q-1) \geq \frac{8}{35}$) note that $\theta(q-1) \leq \frac{1}{4}$ only if 7, 11 or 13 divides $q - 1$. Here Proposition 3.6 immediately eliminates all $q > 2{,}970$ and, after further application, all prime powers except the primes 421, 661, 1,321 and 2,521 along with $841 = 29^2$.

Finally, each of the remaining 33 primes q in $\mathscr{T}$ have been shown to be in C by means of a computer program which calculated the smallest positive pair $(\gamma_q, \gamma_q + 1)$ of consecutive primitive roots in F_q. Our Table lists these values of q together with the corresponding prime decomposition of $q - 1$ and value of γ_q; note that the largest value of γ_q which occurs is 233.

The computer program was prepared by David Hare and the results checked independently by Mohan Nair and Richard Pinch at Glasgow. I am very grateful to all of them for their assistance and also to my friend Peter Clark for his help.

TABLE

q	$q-1$	γ_q	q	$q-1$	γ_q
421	$2^2 \cdot 3 \cdot 5 \cdot 7$	22	120,121	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	58
661	$2^2 \cdot 3 \cdot 5 \cdot 11$	34	133,981	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 29$	101
1,321	$2^3 \cdot 3 \cdot 5 \cdot 11$	56	135,661	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 19$	13
2,521	$2^3 \cdot 3^2 \cdot 5 \cdot 7$	22	157,081	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17$	233
4,621	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	23	158,341	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 29$	50
8,581	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13$	6	180,181	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	22
9,241	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	61	185,641	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$	93
9,661	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 23$	39	235,621	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17$	30
12,541	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 19$	72	300,301	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	40
14,281	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 17$	38	1,381,381	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23$	103
15,541	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 37$	17	1,492,261	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19$	72
16,381	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$	17	1,741,741	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29$	72
18,481	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	57	1,806,421	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23$	29
21,841	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	22	1,861,861	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31$	71
78,541	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17$	13	2,282,281	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19$	68
92,821	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$	53	2,762,761	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23$	203
106,261	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	18			

REFERENCES

1. B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi and Jacobsthal*, J. Number Theory **11** (1979), 349–398.

2. S. D. Cohen, *Primitive roots in the quadratic extension of a finite field*, J. London Math. Soc. (2) **27** (1983), 221–228.

3. _____, *Consecutive primitive roots in a finite field*, Proc. Amer. Math. Soc. **93** (1985), 189–197.

4. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, Heidelberg, Berlin, 1982.

5. E. Vegh, *Pairs of consecutive primitive roots modulo a prime*, Proc. Amer. Math. Soc. **19** (1968), 1169–70.

6. _____, *A note on the distribution of the primitive roots of a prime*, J. Number Theory **3** (1971), 13–18.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF GLASGOW, GLASGOW G12 8QW, SCOTLAND