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 \( q \equiv 7 \pmod{12} \) 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 \( \gamma \) 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 \( q \equiv 7 \pmod{12} \). Then \( q \) is in \( C \).

For any \( n \), let \( \theta(n) = \phi(n)/n \), where \( \phi \) is Euler's function. A conditional version of Theorem 1.1 was proved by Vegh [5, 6] for primes \( q \equiv 7 \pmod{12} \) 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 \( F_q \).
Proof. Let \( a (\neq 0) \in F_{q_0} \). Select any nonsquare \( b \) in \( F_{q_0} \) and let \( \gamma b \) 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
\[
\gamma = a/2 + c\gamma b
\]
is a primitive root in \( F_q \). Now, \( \gamma \) is conjugate over \( F_{q_0} \) to \( \gamma = \gamma q_0 = a/2 - c\gamma b \), itself a primitive root of \( F_q \). Since \( \gamma + \gamma = a \), 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 \( \gamma_1, \gamma_2 \) 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 \( \gamma_1 \) 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 \( \chi \) is any multiplicative character of \( F_q \) of square-free order, then \( \chi(-1) = 1 \). In particular, if \( \eta \) 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 \( \xi \) 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
\[
\begin{align*}
(i) & \quad N(e_1, e_2) = N(e_2, e_1); \\
(ii) & \quad N_q \geq N(e_1, q - 1) + N(q - 1, e_2) - N(e_1, e_2); \\
(iii) & \quad N(e_1, e_2) = \theta(e_1)\theta(e_2) \sum_{d_1|e_1} \mu(d_1) \sum_{d_2|e_2} \mu(d_2) \sum_{\chi \pmod{d_1}} \sum_{\eta \pmod{d_2}} J(\chi, \eta)
\end{align*}
\]
where \( \sum_{\chi \pmod{d}} \) denotes a sum over all \( \phi(d) \) characters of order \( d \);
\[
(iv) \quad N(2, e_2) = \frac{1}{2}\theta(e_2)(q - 1).
\]

Corollary 3.2. Suppose \( 2|e|q - 1 \). Then
\[
N_q \geq \left(2 - \frac{\theta(q - 1)}{\theta(e)} - 1\right)N(e, e) + 2\theta(e)\theta(q - 1) \sum_{d|e} M_e(d),
\]

where
\[
M_e(d) = \frac{\mu(d)}{\phi(d)} \sum_{d'|q - 1} \mu(d') \frac{\phi(d')}{\phi(d)} \sum_{\chi \pmod{d}} \sum_{\eta \pmod{d'}} J(\chi, \eta).
\]

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

\[
|M_e(d)| \leq \lambda_d(W(q - 1) - W(e))q,
\]

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

\[
\lambda_d = \sum_{i=1}^{d} |e_d(i) + e_d(d + 1 - i)|/2\phi(d)W(d) \leq 1,
\]

where \( e_d(i) = \mu((d, i))\phi((d, i)). \) In particular, if \( q \equiv 1 \pmod{60} \), \( \lambda_3 = \frac{1}{2}, \lambda_5 = \frac{3}{4}, \lambda_6 = \frac{3}{4}, \lambda_{10} = \frac{5}{8}, \lambda_{15} = \frac{1}{2}, \lambda_{30} = \frac{21}{32} \).

Proof. We can suppose that \( d \) is square-free. The absolute value of each Jacobi sum in (3.2) equals \( jq \) which quickly yields (3.3) with \( \lambda_d \leq 1 \) (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])

\[
J(\chi, \eta) = J(\chi, \chi^{-1}\eta^{-1})
\]

(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 \( d_1|Q, d_2|e \) if and only if \( d_1 \nmid E \). Hence,

\[
M_e(d) = \frac{\mu(d)}{\phi(d)} \sum_{d_1|Q} \frac{\mu(d_1)}{\phi(d_1)} \sum_{d_2|d, d_1|Q} \sum_{\chi \equiv \eta \pmod{d_1}} L(\chi, \eta),
\]

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

\[
L(\chi, \eta) = \sum_{d_2|d} \frac{\mu(d_2)}{\phi(d_2)} \sum_{\eta \equiv \eta \pmod{d_2}} J(\chi^{-1}, \eta^*\eta) = \sum_{d_2|d} \frac{\mu(d_2)}{\phi(d_2)} \sum_{j=1}^{d_2} J(\chi^{-1}, \chi^{jd/d_2}\eta) = \frac{\mu(d)}{\phi(d)} \sum_{i=1}^{d} e(i)J(\chi^{-1}, \chi^i\eta) = \frac{\mu(d)}{2\phi(d)} \sum_{i=1}^{d} e(i)(J(\chi^{-1}, \chi^i\eta) + J(\chi^{-1}, \chi^{d+1-i}\eta^{-1})), \quad \text{by (3.5)},
\]

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 \( \eta \neq \eta^{-1} \) in (3.6). By (3.7), we have

\[
L(\chi, \eta) + L(\chi, \eta^{-1}) = \frac{\mu(d)}{2\phi(d)} \sum_{i=1}^{d} (e(i) + e(d + 1 - i))(J(\chi^{-1}, \chi^i\eta) + J(\chi^{-1}, \chi^{d+1-i}\eta^{-1})),
\]
which has absolute value at most \( v_d \sqrt{q/\phi(d)} \), where
\[
v_d = \sum_{i=1}^{d} |e(i) + e(d + 1 - i)|.
\]

Hence, from (3.6),
\[
|M_\epsilon(d)| \leq (v_d \sqrt{q/\phi(d)}) \cdot \frac{1}{2} \phi(d_1) \cdot \phi(d) \cdot (\phi(d_1))^{-1} \cdot (W(Q) - W(E)) \cdot (\phi(d))^{-1}
\]
\[
= \lambda_d (W(q - 1) - W(e)) q,
\]
since \( W(Q) - W(E) = (W(q - 1) - W(e))/W(d) \).

Finally, short calculations yield the displayed explicit values of \( \lambda_d \).

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
\[
(3.8) \quad E(e) = \sum_{d_1 | e} \sum_{d_2 | e} \mu(d_1) \mu(d_2) \sum_{\chi \equiv \eta^{-1}} \sum_{\chi \equiv \eta^{-1}} J(\chi, \eta),
\]
so that
\[
|E(e)| \leq \left\{(W(e) - 2)^2 - (\theta(e))^{-1} + 2\right\} q;
\]
in particular,
\[
(3.9) \quad |E(6)| \leq 3/4 q, \quad |E(30)| \leq (137/4) q \quad (q \equiv 1 (\text{mod } 60)).
\]
We outline some improvements of (3.9) based on the use of (3.5) in (3.8).

First, if \( \chi \) is a character of order 6, we have
\[
E(6) = -\frac{1}{2} \Re \left\{ J(\chi, \chi) + 2J(\chi, \chi^2) - J(\chi^2, \chi^2) \right\}
\]
so that
\[
(3.10) \quad |E(6)| \leq 2q.
\]
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, \( E(6) = -a - \frac{3}{2} b \) and
\[
N(6, 6) = \frac{1}{6} (q - 2 - a - \frac{3}{2} b),
\]
where \( a^2 + 3b^2 = q \), \( a \equiv -1 (\text{mod } 3) \) 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,
\[
|E(6)| < \left\{ \begin{array}{ll}
q & \text{if } 2 \text{ is a cubic residue in } F_q, \\
\frac{1}{2} \sqrt{7q} & \text{otherwise},
\end{array} \right.
\]
an improvement on (3.10).

Resuming the discussion with a general prime power \( q \equiv 1 (\text{mod } 60) \) and similarly working carefully with (3.5) in (3.8) with \( e = 30 \), we obtain
\[
(3.11) \quad N(30, 30) = \frac{16}{225} \left( q - \frac{11}{4} + E(30) \right), \quad |E(30)| \leq \frac{35}{2} \sqrt{q},
\]
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 $\lambda_3 + \lambda_5 + \lambda_6 + \lambda_{10} + \lambda_{15} + \lambda_{30} = \frac{131}{31}$.

**Proposition 3.4.** Suppose $q \equiv 1 \pmod{12}$ and $\theta(q - 1) > \frac{1}{5}$. Then

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

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 $\theta(q - 1) > \frac{1}{15}$. Then

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

where

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

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

$$N_q \geq N(6, q - 1) + N(q - 1, 2) - N(6, 2)$$

$$= 3\theta(q - 1)N(6, 6) + \frac{1}{2}\theta(q - 1)(M_6(3) + M_6(6))$$

$$+ (\frac{1}{2}\theta(q - 1) - \frac{1}{6})(q - 1)$$

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

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

4. Calculations. Let $\mathcal{F}$ be the set of positive integers $n$ for which $n \equiv 1 \pmod{60}$ and, for $r \geq 3$, $\mathcal{F}_r$ 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 $r$th prime) be the least member of $\mathcal{F}_r$.

By Corollary 2.4 and Theorem 3.1(i) of [3], Theorem 1.1 holds for prime powers $q$ in $\mathcal{F} \cup \bigcup_{r=4}^{15} \mathcal{F}_r$. Our principal tool for considering $q$ in $\bigcup_{r=7}^{15} \mathcal{F}_r$ is Proposition 3.5 (wherewith we set $S_q = S_q(\theta(q - 1))$); for $q$ in $\mathcal{F}_5 \cup \mathcal{F}_6$ 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 $\mathcal{F}_4$.

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

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

Hence, $N_q$ is positive. Similarly, if $q \in \mathcal{F}_9$, then $\theta(q - 1) \geq \theta(T_9 - 1) > .1613$ and $S_q \geq S_{T_9}(.1613) > 9200$. Next, if $q \in \mathcal{F}_8$, then $\theta(q - 1) > .171$ and $S_q > S_{T_8}(.171)$ which is positive certainly if $q > 21,410,000$. Moreover, $T_8 = 19,399,381 = 47 \cdot 289543$, the only member of $\mathcal{F}_8$ less than this bound, is not a prime power. More
precision is required for \( q \) in \( \mathcal{T}_7 \), 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 \( \mathcal{T}_7 \) 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 \( \mathcal{T}_7 \) (not all prime powers) remain unaccounted for; these (along with their prime factorisations if composite) are

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

Fortunately, \( 1429^2 \notin C \) 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 \( \mathcal{T}_5 \cup \mathcal{T}_6 \) but based on Proposition 3.4.

If \( q \in \mathcal{T}_6 \), 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 \( \mathcal{T}_6 \) 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 \( 212,521 = 8 \cdot 3 \cdot 5 \cdot 7 \cdot 23 + 1 = 461^2 \) to which Corollary 2.2 applies.

If \( q \geq 4621 \in \mathcal{T}_5 \), then \( R_q \) (greater than \( R_q(.20779) \)) 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 \( \mathcal{T}_5 \) (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 \( \mathcal{T}_5 \)) are not prime powers.

For \( q \in \mathcal{T}_4 \) (so that \( q \geq 421 \) and \( \theta(q - 1) \geq \frac{3}{5} \)) note that \( \theta(q - 1) \leq \frac{1}{2} \) 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 \( \mathcal{T} \) 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 \( \gamma_q \); note that the largest value of \( \gamma_q \) 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

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

References


Department of Mathematics, University of Glasgow, Glasgow G12 8QW, Scotland