On consecutive primitive elements in a finite field

Stephen D. Cohen, Tomás Oliveira e Silva and Tim Trudgian

Abstract

For \( q \) an odd prime power with \( q > 169 \), we prove that there are always three consecutive primitive elements in the finite field \( \mathbb{F}_q \). Indeed, there are precisely eleven values of \( q \leq 169 \) for which this is false. For \( 4 \leq n \leq 8 \), we present conjectures on the size of \( q_0(n) \) such that \( q > q_0(n) \) guarantees the existence of \( n \) consecutive primitive elements in \( \mathbb{F}_q \), provided that \( \mathbb{F}_q \) has characteristic at least \( n \). Finally, we improve the upper bound on \( q_0(n) \) for all \( n \geq 3 \).

1. Introduction

Let \( q \) be a prime power and consider primitive elements in \( \mathbb{F}_q \), the finite field of order \( q \). Cohen [2–4] proved that \( \mathbb{F}_q \) contains two consecutive distinct primitive elements whenever \( q > 7 \). For \( n \geq 2 \), we wish to determine \( q_0(n) \) such that \( \mathbb{F}_q \), assumed to have characteristic larger than or equal to \( n \), contains \( n \) consecutive distinct primitive elements for all \( q > q_0(n) \).

Carlitz [1] showed that \( q_0(n) \) exists for all \( n \). Tanti and Thangadurai [9, Theorem 1.3] showed that

\[
q_0(n) \leq \exp(2^{5.54n}), \quad (n \geq 2).
\]

(1.1)

When \( n = 3 \) this gives the enormous bound \( 10^{4343} \). The main point of this article is to apply techniques from [5] to prove the following result.

Theorem 1. The finite field \( \mathbb{F}_q \) contains three consecutive primitive elements for all odd \( q > 169 \). Indeed, the only fields \( \mathbb{F}_q \) (with \( q \) odd) that do not contain three consecutive primitive elements are those for which \( q = 3, 5, 7, 9, 13, 25, 29, 61, 81, 121 \), or 169.

When \( n \geq 4 \) we improve the estimate for \( q_0(n) \) in the following theorem.

Theorem 2. The field \( \mathbb{F}_q \), assumed to have characteristic at least \( n \), contains \( n \) consecutive primitive elements provided that \( q > q_0(n) \), where values of \( q_0(n) \) are given in the third column of Table 1 for \( 4 \leq n \leq 10 \) and \( q_0(n) = \exp(2^{2.77n}) \) for \( n \geq 11 \).

We prove Theorem 2 and discuss the construction of Table 1 in Section 4.

We remark that the outer exponent in the bound in Theorem 2 is half of that given in (1.1) owing entirely to the superior sieving inequality used in Theorem 3. The double exponent still gives an enormous bound on \( q_0(n) \). Were one interested in bounds for specific values of \( n \geq 11 \), one should extend Table 1 as per Section 4.

In Section 5, we present an algorithm that, along with Theorem 2, proves Theorem 1.

Whereas we are not able to resolve completely the values of \( q_0(n) \) for \( n \geq 4 \), we present, in Section 6, some conjectures as to the size of \( q_0(n) \) for \( 4 \leq n \leq 8 \).

Received 22 October 2014; revised 7 January 2015; published online 31 March 2015.

2010 Mathematics Subject Classification 11T30 (primary), 11N69 (secondary).

The third author is supported by Australian Research Council DECRA Grant DE120100173.
2. Character sum expressions and estimates

Let $\omega(m)$ denote the number of distinct prime factors of $m$ so that $W(m) = 2^{\omega(m)}$ is the number of square-free divisors of $m$. Also, let $\theta(m) = \prod_{p \mid m} (1 - p^{-1})$. For any integer $m$ define its radical $\text{Rad}(m)$ as the product of all distinct prime factors of $m$.

Let $e$ be a divisor of $q - 1$. Call $g \in \mathbb{F}_q$ $e$-free if $g \neq 0$ and $g = h^d$, where $h \in \mathbb{F}_q$ and $d \mid e$ implies $d = 1$. The notion of $e$-free depends (among divisors of $q - 1$) only on $\text{Rad}(e)$. Moreover, in this terminology a primitive element of $\mathbb{F}_q$ is a $(q - 1)$-free element.

The definition of any multiplicative character $\chi$ on $\mathbb{F}_q^*$ is extended to the whole of $\mathbb{F}_q$ by setting $\chi(0) = 0$. In fact, for any divisor $d$ of $\phi(q - 1)$, there are precisely $\phi(d)$ characters of order (precisely) $d$, a typical such character being denoted by $\chi_d$. In particular, $\chi_1$, the principal character, takes the value 1 at all non-zero elements of $\mathbb{F}_q$ (whereas $\chi_1(0) = 0$). A convenient shorthand notation to be employed for any divisor $e$ of $q - 1$ is

$$
\int_{d \mid e} = \sum_{d \mid e} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d}
$$

(2.1)

where the sum over $\chi_d$ is the sum over all $\phi(d)$ multiplicative characters $\chi_d$ of $\mathbb{F}_q$ of exact order $d$, and where $\mu(n)$ is the Möbius function. Its significance is that, for any $g \in \mathbb{F}_q$,

$$
\theta(e) \int_{d \mid e} \chi_d(g) = \begin{cases} 1 & \text{if } g \text{ is non-zero and } e\text{-free}, \\ 0 & \text{otherwise.} \end{cases}
$$

In this expression (and throughout) only characters $\chi_d$ with $d$ square-free contribute (even if $e$ is not square-free).

The present investigation concerns the question of the existence of $n \geq 2$ consecutive distinct primitive elements in $\mathbb{F}_q$, that is, whether there exists $g \in \mathbb{F}_q$ such that $\{g, g + 1, \ldots, g + n - 1\}$ is a set of $n$ distinct primitive elements of $\mathbb{F}_q$. Define $p$ to be the characteristic of $\mathbb{F}_q$, so that $q$ is a power of $p$. Then, necessarily, $n \leq p$ and, by [5, Theorem 1], we can suppose $n \geq 3$. Assume therefore throughout that $3 \leq n \leq p$. In particular, $q$ is odd.

Let $e_1, \ldots, e_n$ be divisors of $q - 1$. (In practice all divisors will be even.) Define $N(e_1, \ldots, e_n)$ to be the number of (non-zero) $g \in \mathbb{F}_q$ such that $g + k - 1$ is $e_k$-free for each $k = 1, \ldots, n$. The first step is the standard expression for this quantity in terms of the multiplicative characters of $\mathbb{F}_q^*$.

**Lemma 1.** Suppose $3 \leq n \leq p$ and $e_1, \ldots, e_n$ are divisors of $q - 1$. Then

$$
N(e_1, \ldots, e_n) = \theta(e_1) \cdots \theta(e_n) \int_{d_1 \mid e_1} \cdots \int_{d_n \mid e_n} S(\chi_{d_1}, \ldots, \chi_{d_n}),
$$

where $S$ is a constant depending on $p$ and $n$.
where
\[ S(\chi_{d_1}, \ldots, \chi_{d_n}) = \sum_{g \in \mathbb{F}_q} \chi_{d_1}(g) \cdots \chi_{d_n}(g + n - 1). \]

We now provide a bound on the size of \( S(\chi_{d_1}, \ldots, \chi_{d_n}) \).

**Lemma 2.** Suppose \( d_1, \ldots, d_n \) are square-free divisors of \( q - 1 \). Then
\[ S(\chi_{d_1}, \ldots, \chi_{d_n}) = q - n \text{ if } d_1 = \cdots = d_n = 1, \]
and otherwise
\[ |S(\chi_{d_1}, \ldots, \chi_{d_n})| \leq (n - 1)\sqrt{q}. \]

**Proof.** We can assume not all of \( d_1, \ldots, d_n \) have the value 1. Then \( d := \text{lcm}(d_1, \ldots, d_n) \) is also a square-free divisor of \( q - 1 \) and \( d > 1 \). Evidently, there are positive integers \( c_1, \ldots, c_n \) with \( \gcd(c_k, d_k) = 1 \) such that
\[ S(\chi_{d_1}, \ldots, \chi_{d_n}) = \sum_{g \in \mathbb{F}_q} \chi_d(f(g)), \]
where \( f(x) = x^{c_1}(x + 1)^{c_2} \cdots (x + n - 1)^{c_n} \). Since the radical of the polynomial \( f \) has degree \( n \) the result holds by Weil’s theorem (see [6, Theorem 5.41, p. 225] and also [7]). \( \square \)

When \( e_1 = e_2 = \cdots = e_n = e \), say, we shall abbreviate \( N(e, \ldots, e) \) to \( N_n(e) \). We obtain a lower bound for \( N_n(e) \) in the following lemma.

**Lemma 3.** Suppose \( 3 \leq n \leq p \) and \( e \) is a divisor of \( q - 1 \). Then
\[ N_n(e) \geq \theta(e)^n(q - (n - 1)W(e)^n\sqrt{q}). \]

**Proof.** The presence of the Möbius function in the integral notation in (2.1) means that we need only concern ourselves with the square-free divisors \((d_1, \ldots, d_n)\) of \( e \). The contribution of each \( n \)-tuple is given by Lemma 2. Hence, \( N_n(e) \geq \theta(e)^n(q - n - (n - 1)W(e)^{n - 1}\sqrt{q}) \). The result will follow provided that \( \sqrt{q}(n - 1) - n \) is positive. This is easy to see, since \( n \geq 3 \) and \( q \geq 3 \). \( \square \)

Applying Lemma 3 with \( e = q - 1 \) gives the basic criterion that guarantees \( n \) consecutive primitive elements for sufficiently large \( q \).

**Theorem 3.** Suppose \( 3 \leq n \leq p \). Suppose
\[ q \geq (n - 1)^2 W(q - 1)^{2n} = (n - 1)^2 2^{2n\omega(q - 1)}. \]
Then there exists a set of \( n \) consecutive primitive elements in \( \mathbb{F}_q \).

As an application of Theorem 3, consider the case \( n = 3 \). Let \( P_m \) be the product of the first \( m \) primes. A quick numerical computation reveals that for \( m \geq 50 \) one has \( P_m + 1 \geq 2^{2 + 6m} \). Hence, it follows that \( \mathbb{F}_q \) has three consecutive primitive elements when \( \omega(q - 1) \geq 50 \) or when \( q \geq 2^{2 + 6 \times 50} \). We shall soon improve this markedly.

We now briefly present an improvement in the above discussion when \( q \equiv 3 \) (mod 4). The improvement in this case, in which \(-1\) is a non-square in \( \mathbb{F}_q \), is related to a device used in [4]. Note that, in Lemma 1, in the definition of \( S(\chi_{d_1}, \ldots, \chi_{d_n}) \) we may replace \( g \) by \(-g - (n - 1)\)
and obtain
\[
S(\chi d_1, \ldots, \chi d_n) = \sum_{g \in \mathbb{F}_q} \prod_{i=1}^n \chi d_i (-g - n + 1 + i - 1) = \sum_{g \in \mathbb{F}_q} \prod_{i=1}^n \chi d_i (g + n - i)
\]
\[
= (\chi d_1 \chi d_2 \cdots \chi d_n)(-1)S(\chi d_n, \ldots, \chi d_1).
\]
In particular, if an odd number of the integers \(d_1, \ldots, d_n\) are even, then \(S(\chi d_n, \ldots, \chi d_1) = -S(\chi d_1, \ldots, \chi d_n)\). As a consequence, in Lemma 1, if \(e_1 = \cdots = e_n = e\) is even, then, on the right-hand side of the expression for \(N_n(e)\), the terms corresponding to divisors \((d_1, \ldots, d_n)\) with an odd number of even divisors cancel out exactly and only those with an even number of even divisors contribute. This accounts for precisely half the \(n\)-tuples \((d_1, \ldots, d_n)\). Accordingly, we obtain the following improvement of Lemma 3 and Theorem 3 in this situation.

**Theorem 4.** Suppose \(3 \leq n \leq p\) and \(e\) is an even divisor of \(q - 1\), where \(q \equiv 3 \pmod{4}\) and \(q \geq 7\). Then
\[
N_n(e) \geq \theta(e)^n \left( q - \frac{n - 1}{2} W(e)^n \sqrt{q} \right).
\]
Moreover, if
\[
q \geq \frac{(n - 1)^2}{4} W(q - 1)^2n = (n - 1)^2 2^{2(n\omega(q - 1) - 1)},
\]
then there exists a set of \(n\) consecutive primitive elements in \(\mathbb{F}_q\).

### 3. Sieving inequalities and estimates

As before, assume \(3 \leq n \leq p\) and let \(e\) be a divisor of \(q - 1\). Given positive integers \(m, j, k\) with \(1 \leq j, k \leq n\) define \(m_{jk} = m\) if \(j = k\) and otherwise \(m_{jk} = 1\).

**Lemma 4.** Suppose \(3 \leq n \leq p\) and \(e\) is a divisor of \(q - 1\). Let \(l\) be a prime divisor of \(q - 1\) not dividing \(e\). Then, for each \(j \in \{1, \ldots, n\},\)
\[
|N(l_{j_1}e, \ldots, l_{j_n}e) - \theta(l)N_n(e)| \leq (1 - 1/l) \theta(e)^n (n - 1)W(e)^n \sqrt{q}.
\]

**Proof.** Observe that \(\theta(le) = (1 - 1/l) \theta(e)\) and that, by Lemma 1, all the character sums in \(\theta(l)N_n(e)\) appear identically in \(N(l_{j_1}e, \ldots, l_{j_n}e)\). Hence, by Lemma 2,
\[
|N(l_{j_1}e, \ldots, l_{j_n}e) - \theta(l)N_n(e)| \leq (1 - 1/l) \theta(e)^n (n - 1)W(e)^n - (W(le) - W(e))\sqrt{q}
\]
and the result follows since \(W(le) = 2W(e)\).

This leads to the main sieving result. Let \(e\) be a divisor of \(q - 1\). In what follows, if \(\text{Rad}(e) = \text{Rad}(q - 1)\) set \(s = 0\) and \(\delta = 1\). Otherwise, let \(p_1, \ldots, p_s, s \geq 1\), be the primes dividing \(q - 1\) but not \(e\), and set \(\delta = 1 - n \sum_{i=1}^s p_i^{-1}\). It is essential to choose \(e\) so that \(\delta > 0\).

**Lemma 5.** Suppose \(3 \leq n \leq p\) and \(e\) is a divisor of \(q - 1\). Then, with the above notation,
\[
N_n(q - 1) \geq \left( \sum_{j=1}^n \sum_{i=1}^s N(p_{ij_1}e, \ldots, p_{ij_n}e) \right) - (ns - 1)N_n(e), \tag{3.1}
\]
where \(p_{ijk}\) means \((p_i)_{jk}\). Hence
\[
N_n(q - 1) \geq \delta N_n(e) + \sum_{i=1}^s \left( \sum_{j=1}^n N(p_{ij_1}e, \ldots, p_{ij_n}e) - \theta(p_i)N_n(e) \right). \tag{3.2}
\]
Proof. It suffices to suppose \( s \geq 1 \). The various \( N \) terms on the right-hand side of (3.1) can be regarded as counting functions on the set of \( g \in \mathbb{F}_q \) for which \( g + j - 1 \) is \( e \)-free for each \( j = 1, \ldots, n \). In particular, \( N_n(e) \) counts all such elements, whereas, for each \( i = 1, \ldots, s \), and \( 1 \leq j \leq n \), \( N(p_{ij1}e, \ldots, p_{ijn}e) \) counts only those for which additionally \( g + j - 1 \) is \( p_i \)-free. Note that \( N_n(q-1) \) is the number of elements \( g \) such that not only are \( g + j - 1 \) \( e \)-free for each \( j = 1, \ldots, n \) but additionally \( g + j - 1 \) is \( p_i \)-free for each \( 1 \leq i \leq s \), \( 1 \leq j \leq n \). Hence we see that, for a given \( g \in \mathbb{F}_q \), the right-hand side of (3.1) clocks up 1 if \( g + k - 1 \) is primitive for every \( 1 \leq k \leq n \), and otherwise contributes a non-positive (integral) quantity. This establishes (3.1).

We are now able to provide a condition that, if satisfied, is sufficient to prove the existence of \( n \) consecutive primitive elements.

**Theorem 5.** Suppose \( 3 \leq n \leq p \) and \( e \) is a divisor of \( q - 1 \). If \( \text{Rad}(e) = \text{Rad}(q-1) \), then set \( s = 0 \) and \( \delta = 1 \). Otherwise, let \( p_1, \ldots, p_s, s \geq 1 \), be the primes dividing \( q - 1 \) but not \( e \) and set \( \delta = 1 - n \sum_{i=1}^{s} p_i^{-1} \). Assume \( \delta > 0 \). If also

\[
q > \left( n-1 \right) \left( \frac{ns-1}{\delta} + 2 \right) W(e)^n, \tag{3.3}
\]

then there exist \( n \) consecutive primitive elements in \( \mathbb{F}_q \).

Proof. Assume \( \delta > 0 \). From (3.2) and Lemmas 3 and 4 (noting that for each \( j = 1, \ldots, n \) the contribution to (3.2) is the same),

\[
N_n(q-1) \geq \theta(e)^n \left( \delta(q - (n - 1)W(e)^n\sqrt{q}) - n \sum_{i=1}^{s} \left( 1 - \frac{1}{p_i} \right) (n-1)W(e)^n\sqrt{q} \right)
= \delta \theta(e)^n \sqrt{q} \left( \sqrt{q} - (n - 1)W(e)^n - (n-1) \left( \frac{ns-1}{\delta} + 1 \right) W(e)^n \right).
\]

The conclusion follows.

We conclude this section with the slight improvement when \( q \equiv 3 \pmod{4} \). Now, when \( e \) is even, the character sum expressions for the terms \( \sum_{j=1}^{n} N(p_{ij1}e, \ldots, p_{ijn}e) - \theta(p_i)N_n(e) \) in (3.2) cancel unless an even number of divisors \( d_1, \ldots, d_n \) are even. This reduces the bound in Lemma 4 by a factor of two, and gives the following improvement to Theorem 5.

**Theorem 6.** Suppose \( q \equiv 3 \pmod{4} \), \( q \geq 7 \), \( 3 \leq n \leq p \) and \( e \) is an even divisor of \( q - 1 \). If \( \text{Rad}(e) = \text{Rad}(q-1) \) set \( s = 0 \) and \( \delta = 1 \). Otherwise, let \( p_1, \ldots, p_s, s \geq 1 \), be the primes dividing \( q - 1 \) but not \( e \) and set \( \delta = 1 - n \sum_{i=1}^{s} p_i^{-1} \). Assume \( \delta > 0 \). If also

\[
q > \left( n-1 \right) \left( \frac{ns-1}{2\delta} + 2 \right) W(e)^n, \tag{3.4}
\]

then there exist \( n \) consecutive primitive elements in \( \mathbb{F}_q \).

**Remark 1.** In Theorems 5 and 6, for a given \( s \) the best (largest) value of \( \delta \) is obtained when the largest \( s \) prime factors of \( q - 1 \) are used to compute \( \delta \).
4. Application of Theorems 3 and 5 for generic \( n \); proof of Theorem 2

As an application of Theorem 5, consider the case \( n = 3 \). We showed after Theorem 3 that \( \mathbb{F}_q \) contains three consecutive primitive elements for all \( q \) satisfying \( \omega(q-1) \geq 50 \). For \( 14 \leq \omega(q-1) \leq 49 \), we verify easily that (3.3) holds with \( s = 8 \). As an example, consider \( \omega(q-1) = 14 \) and \( s = 8 \), whence \( \delta \geq 1 - 3\left( \frac{13}{17} + \frac{1}{17} \right) + \frac{1}{17} + \frac{1}{17} + \frac{1}{17} + \frac{1}{17} + \frac{1}{17} + \frac{1}{17} + \frac{1}{17} + \frac{1}{17} + \frac{1}{17} \) \( \geq 0.1109 \). It follows that the right-hand side of (3.3) is slightly larger than \( 1203974811470119 \), which is smaller than \( P_{14} \). It follows that \( \mathbb{F}_q \) has three consecutive primitive elements when \( \omega(q-1) = 14 \).

We are unable to proceed directly when \( \omega(q-1) \leq 13 \). For example, when \( \omega(q-1) = 13 \) there is no value of \( s \) with \( 1 \leq s \leq 13 \) that resolves (3.3). If we choose \( s = 8 \), then we minimize the right-hand side of (3.3) whence it follows that we need only consider \( \omega(q-1) \leq 13 \) and \( q \leq 3.49 \times 10^{15} \).

We continue this procedure for larger values of \( n \). We use Theorem 3 to obtain an initial bound on \( \omega(q-1) \), then use Theorem 5, with suitable values of \( s \), to reduce this bound as far as possible. We therefore reduce the problem of finding \( n \) consecutive primitive elements in \( \mathbb{F}_q \) to the finite computation in which we need only check those \( q \) in a certain range: this range is given in Table 1.

We now use Theorem 3 to obtain a bound on \( q_0(n) \) for a generic value of \( n \). To bound \( \omega(q-1) \) we use Robin’s result [8, Theorem 11] that \( \omega(n) \leq 1.38402 \log n / (\log \log n) \) for all \( n \geq 3 \). Since the function \( \log x / (\log \log x) \) is increasing for \( x \geq e^e \) we have

\[ \omega(q-1) \leq \frac{1.38402 \log q}{\log \log q}, \quad (4.1) \]

for all \( q \geq 17 \). It is easy to check that (4.1) holds also for all \( 3 \leq q \leq 17 \). We use (4.1) to rearrange the condition in (2.2), showing that

\[ \log q \left( 1 - \frac{2.76804n \log 2}{\log \log q} \right) \geq 2 \log(n-1). \quad (4.2) \]

We solve (4.2) by first insisting that the term in braces be bounded below by \( d \), where \( d \in (0, 1) \), and then insisting that \( d \log q \geq 2 \log(n-1) \). This shows that (2.2) is certainly true provided that

\[ q \geq \max\{ (n-1)^{2/d}, \exp(2.76804n/(1-d)) \}. \quad (4.3) \]

We choose \( d = 0.0001 \), so that we require \( q \geq \exp(2.77n) \) for all \( n \geq 6 \). This proves Theorem 2.

We remark that were one to use [8, Theorem 12] one could replace the bound in (4.1) by \( \log q / (\log \log q + 1.458 \log q / (\log \log q)^2 \). This would show, when \( n \) is sufficiently large, that the exponent in Theorem 2 could be reduced from 2.77 to 2 + \( \epsilon \) for any positive \( \epsilon \); we have not pursued this.

5. Three consecutive primitive elements

To prove Theorem 1, we verified numerically the existence of three consecutive primitive elements for all values of \( q \) that remained after the application of Theorem 5. As explained in Section 4, for \( n = 3 \) it is only necessary to consider the cases where \( \omega(q-1) \leq 13 \). For each possible value of \( \omega(q-1) \) Theorem 5 was used to compute a bound on the values of \( q \) below which the existence of three consecutive primitive elements was not ensured; these upper bounds are presented in the second column of Table 2. Algorithm 1 was then used to generate the values of \( q \) that required testing.

Lines 10–12 of Algorithm 1 ensure that \( \gcd(m_{d-1}, u_{d}) = 1 \) whenever line 13 is reached, and ensure that \( \omega(m_{d}) = \omega(m_{d-1}) + 1 \) (that is, that \( \omega(m_{d}) = d \)) every time line 17 is reached. Testing \( m + 1 \), with either \( m = m_1 \) or \( m = m_d \), amounts to verifying that \( m + 1 \) is an odd prime power. If so, we see whether Theorem 5 can deal with it; if not, we verify that there
Table 2. Bounds and number of tests performed when \( n = 3 \).

| \( \omega(q-1) \) | \( q \) upper bound (\( M \)) | \( m + 1 \) tests | \( m + 1 \) survivors | \( p \) tests | \( q \) tests |
|-----------------|-------------------------------|------------------|------------------------|-------------|---------------|
| 1               | 256                           | 7                | 7                      | 3           | 1             |
| 2               | 16384                         | 2425             | 805                    | 164         | 8             |
| 3               | 802816                        | 172827           | 21350                  | 4785        | 26            |
| 4               | 31719424                      | 5459954          | 149265                 | 33357       | 106           |
| 5               | 368212715                     | 30738304         | 695172                 | 159618      | 236           |
| 6               | 9777432663                    | 278578984        | 168065                 | 380984      | 405           |
| 7               | 48913046416                   | 262182675        | 2131439                | 478146      | 353           |
| 8               | 327363505978                  | 218209768        | 2162062                | 476569      | 203           |
| 9               | 6245429709655                 | 479005331        | 897028                 | 194276      | 63            |
| 10              | 22053999260750                | 68795792          | 262534                 | 55943       | 9             |
| 11              | 117121857096884               | 9250747           | 93920                  | 19315       | 1             |
| 12              | 1307042588523590              | 2378985           | 6566                   | 1294        | 0             |
| 13              | 3489135957826319              | 11547            | 964                    | 187         | 0             |

Algorithm 1: Enumeration of all odd integers \( m + 1 \) that satisfy the conditions \( m < M \) and \( \omega(m) = w \).

1. Set \( L \) to \( \lfloor (M - 1)/\prod_{i=1}^{w-1} p_i \rfloor \); here, \( p_i \) is the \( i \)-th prime (\( p_1 = 2 \), \( p_2 = 3 \), and so on).
2. Generate all tuples \((u_i, v_i)\) of the form \((p^k, p)\), with \( p \) an odd prime, \( k \) a positive integer, and \( p^k \leq L \), and sort them in increasing order of the value of \( u_i \), so that \((u_1, v_1) = (3, 3)\), \((u_2, v_2) = (5, 5)\), \((u_3, v_3) = (7, 7)\), \((u_4, v_4) = (9, 3)\), and so on.
3. Append the tuple \((\infty, 0)\) to the list of tuples.
4. For \( k = 1, 2, \ldots, \lfloor \log(M - 1)/\log 2 \rfloor \), do:
   a. Set \( m_1 \) to \( 2^k \), \( i_2 \) to 0, and \( d \) to 2.
   b. If \( w = 1 \), then test \( m_1 + 1 \).
   c. Else:
      i. While \( d > 1 \) do:
         1. Repeat until \( v_i_d \notin \{v_{i_2}, \ldots, v_{i_{d-1}}\} \)
         2. If \( m_{d-1} u_{i_{d-1}} > M \) then:
            a. Decrement \( d \).
         Else:
            a. Set \( m_d \) to \( m_{d-1} u_{i_d} \).
            b. If \( d = w \), then test \( m_d + 1 \).
            Else:
               a. Increment \( d \) and then set \( i_d \) to \( i_{d-1} \).

exist three consecutive primitive elements in the corresponding finite field. It turned out to be faster to rule out values of \( m + 1 \) using all possible values of \( s \) in Theorem 5 (treating \( m + 1 \) as if it were a prime power) before testing if it were a prime or a prime power.

Algorithm 1 was coded using the PARI/GP calculator programming language [10] (version 2.7.2 using a GMP 6.0.0 kernel) and was run for \( w = 1, 2, \ldots, 13 \) on one core of a 3.3 GHz Intel i3-2120 processor. Since \( w = \omega(q - 1) \) this covers all cases that must be tested. It took about 7 h to confirm that the following odd values of \( q \) are the only odd ones for which the finite field \( \mathbb{F}_q \) does not have three consecutive primitive elements: 3, 5, 7, 3\(^2\), 13, 5\(^2\), 29, 61, 3\(^4\), 11\(^2\), and...
For each value of $\omega(q-1)$, Table 2 presents the value of $M$ that was used (second column), the number of $m+1$ values that required testing (third column), the number of $m+1$ values that survived an application of Theorem 5 (fourth column), the number of these that were actually primes (fifth column, 1804641 in total), and the number of these that were actually prime powers (sixth column, 1411 in total).

6. Conjectures

Based on numerical experiments up to $10^8$, the following conjectures appear to be plausible.

**Conjecture 1.** The finite field $\mathbb{F}_q$ has four consecutive primitive elements except when $q$ is divisible by 2 or by 3, or when $q$ is one of the following: 5, 7, 11, 13, 17, 19, 23, 5^2, 29, 31, 41, 43, 61, 67, 71, 73, 79, 113, 11^2, 13^2, 181, 199, 337, 19^2, 397, 23^2, 571, 1093, 1381, 7^4 = 2401.

At present this conjecture is very difficult to settle by computation: there are simply too many cases to test. Consider, for example, $\omega(q-1) = 12$. Even though, according to Table 1 we need to go up only to $\omega(q-1) = 23$, the hard cases are the intermediate values of $\omega(q-1)$. It is necessary to test values of $q$ up to about $4 \times 10^{21}$ that can have a prime power factor up to about $2 \times 10^{10}$. Given the large sizes of these numbers, the small savings gained from just considering $q \equiv 3 \pmod{4}$ and Theorem 6 will not be sufficient.

**Conjecture 2.** The finite field $\mathbb{F}_q$ has five consecutive primitive elements except when $q$ is divisible by 2 or by 3, or when $q$ is one of the following: 5, 7, 11, 13, 17, 19, 23, 5^2, 29, 31, 37, 41, 43, 47, 7^2, 61, 67, 71, 73, 79, 101, 109, 113, 11^2, 5^3, 127, 131, 139, 151, 157, 163, 13^2, 181, 193, 199, 211, 229, 241, 271, 277, 281, 17^2, 307, 313, 331, 337, 19^2, 379, 397, 433, 439, 461, 463, 23^2, 547, 571, 577, 601, 613, 5^4, 631, 691, 751, 757, 29^2, 31^2, 1009, 1021, 1033, 1051, 1093, 1201, 1297, 1321, 1381, 1453, 1471, 1489, 1531, 1597, 1621, 1723, 1741, 1831, 43^2, 1861, 1933, 2017, 2161, 2221, 2311, 2341, 7^4, 3061, 59^2, 3541, 3571, 61^2, 4201, 4561, 4789, 4831, 71^2, 5281, 5881, 89^2, 8821, 9091, 9241, 113^2, 5^6 = 15625.

We also examined fields that do not have six, seven and eight consecutive primitive elements. Since there are many of these we do not list them as in Conjectures 1 and 2 but merely indicate the last one we found.

**Conjecture 3.** The finite field $\mathbb{F}_q$ has six consecutive primitive elements when $q$ is not divisible by 2, by 3, or by 5, and when $q > 65521$.

**Conjecture 4.** The finite field $\mathbb{F}_q$ has seven consecutive primitive elements when $q$ is not divisible by 2, by 3, or by 5, and when $q > 1037401$.

**Conjecture 5.** The finite field $\mathbb{F}_q$ has eight consecutive primitive elements when $q$ is not divisible by 2, by 3, by 5, or by 7, and when $q > 4476781$.

References

1. L. Carlitz, ‘Sets of primitive roots’, Compos. Math. 13 (1956) 65–70.
2. S. D. Cohen, ‘Consecutive primitive roots in a finite field’, Proc. Amer. Math. Soc. 93 (1985) 189–197.
3. S. D. Cohen, ‘Consecutive primitive roots in a finite field. II’, Proc. Amer. Math. Soc. 94 (1985) 605–611.
4. S. D. Cohen, ‘Pairs of primitive roots’, Mathematika 32 (1985) 276–285.
5. S. D. Cohen, T. Oliveira e Silva and T. S. Trudgian, ‘A proof of the conjecture of Cohen and Mullen on sums of primitive roots’, Math. Comp. (2014), accepted for publication. See also arXiv:1402.2724 [math.NT].
6. R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications 20 (Cambridge University Press, Cambridge, 1997).

7. C. Peng, Y. Shen, Y. Zhu and C. Liu, ‘A note on Weil’s multiplicative character sum’, *Finite Fields Appl.* 35 (2014) 132–133.

8. G. Robin, ‘Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction ω(n) nombre de diviseurs premiers de n’, *Acta Arith.* 42 (1983) 367–389.

9. J. Tanti and R. Thangadurai, ‘Distribution of residues and primitive roots’, *Proc. Indian Acad. Sci. (Math. Sci.)* 123 (2013) 203–211.

10. The PARI Group, Bordeaux, ‘PARI/GP version 2.7.2’, 2014, [http://pari.math.u-bordeaux.fr/](http://pari.math.u-bordeaux.fr/).

---

Stephen D. Cohen
School of Mathematics and Statistics
University of Glasgow
Glasgow G12 8QW
United Kingdom
Stephen.Cohen@glasgow.ac.uk

Tomás Oliveira e Silva
Departamento de Electrónica, Telecomunicações e Informática/IETEA
University of Aveiro
3810-193 Aveiro
Portugal
tos@ua.pt

Tim Trudgian
Mathematical Sciences Institute
The Australian National University
Canberra, ACT 0200
Australia
timothy.trudgian@anu.edu.au