Primes modulo which almost all Fermat numbers are primitive roots

Amin Witno
Department of Basic Sciences, Philadelphia University, Jordan 19392
avitno@gmail.com

Received: 23.11.2009; accepted: 20.1.2010.

Abstract. A prime $p$ is called elite, or anti-elite, when all but finitely many Fermat numbers are quadratic nonresidues or residues, respectively, modulo $p$. It is known that if the multiplicative order of $2$ modulo $p$ is of the form $2^s \times 5$, where $s \geq 2$, then the prime $p$ is either elite or anti-elite. Modulo elite primes of this kind, we describe some criteria by which all sufficiently large Fermat numbers be primitive roots, or all nonprimitive roots.

Keywords: elite primes, Fermat numbers.

MSC 2000 classification: primary 11A07, secondary 11A41.

Introduction

The primality of the Fermat number $F_n = 2^{2^n} + 1$ can be checked using the so-called Pepin’s test: $F_n$ is prime if and only if $3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}$. The choice of $p = 3$ in this test is not unique; it may be replaced by another prime number as long as $F_n$ is a quadratic nonresidue modulo $p$ for each $n$, or at least for all sufficiently large values of $n$ [2, Remark 5.10]. Aigner [1] called such a prime number $p$ an elite prime.

To clarify, an integer $a$ which is not a multiple of the prime $p$ is a quadratic residue modulo $p$ if the congruence $x^2 \equiv a \pmod{p}$ has a solution; otherwise $a$ is a quadratic nonresidue. The integer $a$ is a primitive root modulo $p$ if $|a|_p = p - 1$, where $|a|_p$ denotes the multiplicative order of $a$ modulo $p$. That a primitive root is necessarily a quadratic nonresidue is a known elementary fact.

It is moreover known that modulo $p > 2$, there are precisely $\frac{p - 1}{2}$ quadratic nonresidues, $\phi(p - 1)$ of which are primitive roots. Now a prime Fermat number, $p = 2^{2^n} + 1$, has the peculiar property where $\phi(p - 1) = \frac{p - 1}{2}$, thus every quadratic nonresidue is also a primitive root modulo $p$. This fact is interesting at least theoretically, for no one has seen a prime Fermat number beyond $F_4$.

This paper is a brief investigation into a subfamily of elite primes, wherein we consider primes modulo which all Fermat numbers $F_n$, beyond a certain value of $n$, are primitive roots. The first eight primes with this property are

$3, 5, 7, 23041, 3208642561, 912680550401, 1825696645121, 3580135407617$,

the last of which is the 29th elite prime.

http://siba-ese.unisalento.it/ © 2010 Università del Salento
Furthermore, it seems natural that in studying such primes we will eventually cross path with their counterpart, namely the elite primes modulo which all large enough \(F_n\) are non-primitive roots (while they are quadratic nonresidues). Our initial results on these two classes of elite primes, which we name ultra-elite primes, are limited to the specific case where \(|2|^p\) is 5 times a power of 2. Under this assumption, we are able to test for ultra-eliteness involving only modular exponentiations to the power \(\frac{p-1}{5}\).

1 Elite and Anti-Elite Primes

Let \(p\) denote an odd prime number of the form \(p = 2^r \times h + 1\), for some odd number \(h\). Aigner [1] and Müller [5, 6] have established the following results.

The Fermat numbers \(F_n\), for all \(n \geq 0\), satisfy the recurrence relation

\[
F_{n+1} = (F_n - 1)^2 + 1.
\]

Therefore, the sequence \(F_n \mod p\) is eventually periodic. The length of this periodicity is given by \(L = |2|^t\), where \(t\) is the divisor of \(h\) which appears in the relation \(|2|^p = 2^s \times t\), for some integer \(s \leq r\).

The \(L\) distinct terms of \(F_n \mod p\), forming one complete cycle, are called the Fermat remainders of the prime \(p\), or modulo \(p\). We call the prime \(p\) elite (anti-elite) when all of these \(L\) Fermat remainders are quadratic nonresidues (residues) modulo \(p\).

We also know that the repeated terms in the sequence \(F_n \mod p\) begin at \(n = s\). As \(r \geq s\), the \(L\) Fermat remainders may always be represented by the numbers

\[
F_r, F_{r+1}, F_{r+2}, \ldots, F_{r+L-1} \mod p.
\]

Moreover, a necessary condition for the prime \(p\) to be elite is that \(L\) be an even number in the range \(4 \leq L < \frac{p-1}{5}\), with the following exceptions.

1. The primes 3 and 5 are elite with \(L = 1\).
2. The prime 7 is elite with \(L = 2\).

For the anti-elite case, \(L\) is allowed to be odd and, in particular, \(p\) is anti-elite with \(L = 1\) if and only if \(p\) is a divisor of some Fermat number larger than 5 [6, Theorem 2.1].

Müller [5, Conjecture 5.4] conjectured that the number of elite primes is infinite, with an estimate for their counting function, possibly, as little as \(O(\log x)\). Meanwhile, Křížek et al. [3] had earlier shown that the number of elite primes up to \(x\) is \(O(x/(\log x)^2)\). Additionally, Müller, who first introduced the concept of anti-elite primes, also proved [6, Consequence 2.5] that there are infinitely many anti-elite primes with \(L = 2\).

A more recent work [7] applies to the specific case where \(t = 5\): If \(|2|^p = 2^s \times 5\), with \(s \geq 2\), then \(p\) is either elite or anti-elite with \(L = 4\). In particular, if \(\Phi_m(X)\) is the \(m\)th cyclotomic polynomial, then the sequence \(\Phi_{2^n \times 5}(2)\), for \(n > 2\), contains only products of elite and anti-elite primes of this type.

2 Ultra-Elite Primes

The first 29 elite primes are listed in Sloane’s Online Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/b102742.txt. For each prime \(p = 2^r \times h + 1\), we provide in Table 1 below the factorization of \(h\) and the period length \(L\), as well as \(M\), which is the number of primitive roots among the Fermat remainders modulo \(p\).
To determine whether or not a Fermat remainder \( x \) is a primitive root, we compute the modular exponentiation \( x^{\frac{p-1}{q}} \mod p \), for each prime \( q \) that divides \( h \). If none of these residues is equal to one, then and only then \( x \) is a primitive root.

<table>
<thead>
<tr>
<th>( p )</th>
<th>( r )</th>
<th>( h )</th>
<th>( L )</th>
<th>( M )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>41</td>
<td>3</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>15361</td>
<td>10</td>
<td>3 \times 5</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>23041</td>
<td>9</td>
<td>3^2 \times 5</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>26881</td>
<td>8</td>
<td>3 \times 5 \times 7</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>61441</td>
<td>12</td>
<td>3 \times 5</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>87041</td>
<td>10</td>
<td>5 \times 17</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>163841</td>
<td>15</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>11</td>
<td>544001</td>
<td>8</td>
<td>5^3 \times 17</td>
<td>8</td>
</tr>
<tr>
<td>12</td>
<td>604801</td>
<td>7</td>
<td>3^3 \times 5^2 \times 7</td>
<td>6</td>
</tr>
<tr>
<td>13</td>
<td>6684673</td>
<td>17</td>
<td>3 \times 17</td>
<td>8</td>
</tr>
<tr>
<td>14</td>
<td>14172161</td>
<td>14</td>
<td>5 \times 173</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>159318017</td>
<td>16</td>
<td>11 \times 13 \times 17</td>
<td>8</td>
</tr>
<tr>
<td>16</td>
<td>446960641</td>
<td>10</td>
<td>3 \times 5 \times 7 \times 4157</td>
<td>4</td>
</tr>
<tr>
<td>17</td>
<td>1151139841</td>
<td>16</td>
<td>3 \times 5 \times 1171</td>
<td>4</td>
</tr>
<tr>
<td>18</td>
<td>3208642561</td>
<td>22</td>
<td>3^2 \times 5 \times 17</td>
<td>4</td>
</tr>
<tr>
<td>19</td>
<td>38126223361</td>
<td>23</td>
<td>3^2 \times 5 \times 101</td>
<td>4</td>
</tr>
<tr>
<td>20</td>
<td>108905103361</td>
<td>22</td>
<td>3^2 \times 5 \times 577</td>
<td>4</td>
</tr>
<tr>
<td>21</td>
<td>171727482881</td>
<td>12</td>
<td>5 \times 17 \times 493243</td>
<td>8</td>
</tr>
<tr>
<td>22</td>
<td>318093312001</td>
<td>14</td>
<td>3 \times 5^3 \times 23 \times 2251</td>
<td>4</td>
</tr>
<tr>
<td>23</td>
<td>443069456129</td>
<td>8</td>
<td>13 \times 17 \times 7831403</td>
<td>8</td>
</tr>
<tr>
<td>24</td>
<td>912680550401</td>
<td>31</td>
<td>5^2 \times 17</td>
<td>4</td>
</tr>
<tr>
<td>25</td>
<td>1295536619521</td>
<td>26</td>
<td>3^3 \times 5 \times 11 \times 13</td>
<td>4</td>
</tr>
<tr>
<td>26</td>
<td>1825696645121</td>
<td>26</td>
<td>5 \times 5441</td>
<td>4</td>
</tr>
<tr>
<td>27</td>
<td>2061584302081</td>
<td>37</td>
<td>3 \times 5</td>
<td>4</td>
</tr>
<tr>
<td>28</td>
<td>2769999339521</td>
<td>13</td>
<td>5 \times 7 \times 47 \times 205553</td>
<td>4</td>
</tr>
<tr>
<td>29</td>
<td>3580135407617</td>
<td>16</td>
<td>17 \times 53 \times 60631</td>
<td>8</td>
</tr>
</tbody>
</table>

Table 1. The first 29 elite primes \( p = 2^r \times h + 1 \), modulo each of which \( M \) stands for the number of primitive roots among the \( L \) Fermat remainders.
two classes of elite primes we wish to consider, and we give them the name ultra-elite primes, for convenience as well as for their seeming rarity as a subfamily of elite primes.

Definition 1. An elite prime $p$ is called ultra-elite if all its Fermat remainders are either primitive roots, or all nonprimitive roots, modulo $p$. When distinction between the two classes is needed, we shall call $p$ a primitive ultra-elite prime, or nonprimitive ultra-elite prime, respectively.

Note that when a prime $p$ is known to be ultra-elite, it is left to find the order modulo $p$ of any one Fermat remainder $x$. If $x$ is a primitive root, then $p$ is primitive ultra-elite, else nonprimitive ultra-elite.

Of the first few elite primes arising from the sequence $\Phi_{2^n \times 5}(2)$, we also find two nonprimitive ultra-elite primes, one of which also appears in Table 1, i.e.,

$446960641$ and $777164631747163593256655841281$,

as well as two primitive ultra-elite primes, i.e.,

$46454107161999112389551048616961$ and $3587745015951361$.

These four ultra-elite primes are divisors of $\Phi_{2^n \times 5}(2)$ with $n = 7, 8, 9, 10$, respectively, and they belong to a special subclass of elite primes to which we shall now limit our main discussion, i.e., the elite primes $p$ for which $|2|_p = 2^s \times 5$.

To avoid repetition, some notation will henceforth be fixed, unless otherwise stated.

Definition 2. Let the prime $p = 2^r \times h + 1$, where $h$ is odd, be an elite prime for which $|2|_p = 2^s \times 5$. Hence, it is necessary that $s \leq r$ and $h$ be a multiple of 5. Moreover, the sequence $F_n$ modulo $p$ will have period length $L = |2|_p = 4$. Let $\omega = 2^{2^k}$ for any chosen value of $k \geq s$, e.g., $k = r$, so that by Eqn. (1), we may denote the four Fermat remainders modulo $p$ by $a, b, c, d \mod p$, where

$$a = 1 + \omega, \quad b = 1 + \omega^2, \quad c = 1 + \omega^4, \quad d = 1 + \omega^8.$$ 

Part of the following lemma was established in our recent work [7, Proof of Theorem 3.1], but we reproduce the results here for their subsequent usefulness.

Lemma 1. The numbers $a, b, c, d,$ and $\omega$ are ruled by the following congruences modulo $p$:

\begin{align*}
ab &\equiv -\omega^4 \pmod{p}, \\
bc &\equiv -\omega^3 \pmod{p}, \\
bd &\equiv -\omega \pmod{p}, \\
d\omega &\equiv -\omega^2 \pmod{p}.
\end{align*}

Proof. It is clear that $\omega^5 \equiv 1 \pmod{p}$, and hence $\omega^8 \equiv \omega^3 \pmod{p}$. Moreover,

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 \equiv 0 \pmod{p},$$

because this sum is $\frac{\omega^5 - 1}{\omega - 1}$ and $p$ does not divide $\omega - 1$. The four congruences that we claim follow directly from this one. \(\Box\)

Definition 3. Refering to Definition 2 for our notation, we now assign four integers $A, B, C, \text{ and } D$, to be the least positive residues modulo $p$, as follows.

$$A = a^{\frac{p-1}{3}} \mod p, \quad B = b^{\frac{p-1}{3}} \mod p, \quad C = c^{\frac{p-1}{3}} \mod p, \quad D = d^{\frac{p-1}{3}} \mod p.$$
Theorem 1. If none of the four numbers \( A, B, C, D \) is equal to one, then the elite prime \( p \) is ultra-elite.

Proof. The Fermat remainder \( a \) is a primitive root if and only if \( a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p} \) for every odd prime \( q \) which is a factor of \( p-1 \). (The case \( q = 2 \) is already included in the condition for being elite.) We assume that this incongruence holds with \( q = 5 \), and similarly for \( b, c, \) and \( d \) as well. Now for any odd prime \( q \neq 5 \) which divides \( p-1 \), we may write following (2),

\[
\frac{p-1}{q} \equiv \left(-\omega^3\right)^{\frac{p-1}{q}} \equiv 1 \pmod{p},
\]

because \( \frac{p-1}{q} \) is an even multiple of 5. It follows that \( a^{\frac{p-1}{q}} \equiv 1 \pmod{p} \) if and only if \( b^{\frac{p-1}{q}} \equiv 1 \pmod{p} \). Therefore, \( a \) is a primitive root modulo \( p \) if and only if \( b \) is. Quite similarly, by (3) and (4), we establish the equivalence relation between \( b \) and \( c \), and that between \( c \) and \( d \), respectively. This proves that \( p \) is ultra-elite.

QED

Note 1. In particular, in the above proof we see that if there is an odd prime factor \( q \neq 5 \) for which \( a^{\frac{p-1}{q}} \equiv 1 \pmod{p} \), or similarly with \( b, c, \) or \( d \), then \( p \) is a nonprimitive ultra-elite prime.

Note also that (6) is still valid for \( q = 5 \), provided that \( \frac{p-1}{5} \) is a multiple of 5. In this special case, either \( A, B, C, D \) are all equal to one—which of course, would make \( p \) nonprimitive ultra-elite—or none is. Both possibilities anyhow lead to an ultra-elite prime. This is a corollary which we state in a more elegant fashion, as follows.

Theorem 2. Let \( p \) be a prime number such that \( |2|^s \equiv 2^s \cdot 5 \), with \( s \geq 2 \). If \( p-1 \) is divisible by \( 25 \), then \( p \) is either anti-elite or ultra-elite.

Proof. Such a prime \( p \) is always elite or anti-elite [7, Theorem 3.1]. And when elite, \( p \) is necessarily ultra-elite, since \( \frac{p-1}{5} \) is divisible by 5.

QED

Next, we wish to slightly improve our ultra-eliteness criteria, eventually showing that only three, sometimes less, of the numbers \( A, B, C, D \) are really needed.

Lemma 2. Any one of the following three relations implies the other two.

(1) \( A = C \).
(2) \( B = D \).
(3) \( p \equiv 1 \pmod{25} \).

Proof. By their definitions, we easily see that \( a\omega^4 \equiv c \pmod{p} \) and \( b\omega^3 \equiv d \pmod{p} \). If \( A = C \), then \( (\omega^4)^{\frac{p-1}{5}} \equiv 1 \pmod{p} \). Since \( |\omega|_p = 5 \), this last congruence is possible only when \( \frac{p-1}{5} \) is divisible by 5. This same conclusion also holds when \( B = D \). Conversely, if \( p \equiv 1 \pmod{25} \), then \( \omega^{\frac{p-1}{5}} \equiv 1 \pmod{p} \), which implies both \( A = C \) and \( B = D \).

QED

Theorem 3. The elite prime \( p \) is ultra-elite if \( A = C \) or \( B = D \).

Proof. By Lemma 2, each one of the two conditions is equivalent to having \( p \equiv 1 \pmod{25} \). The claim is then a consequence of Theorem 2.

QED

Lemma 3. We have the following four equivalence relations.

(1) \( A = 1 \) if and only if \( B = C \),
(2) \( B = 1 \) if and only if \( C = D \),
(3) \( C = 1 \) if and only if \( D = A \),
(4) \( D = 1 \) if and only if \( A = B \).

Proof. By squaring both sides of each one of the congruences given in (2) to (5), followed by a substitution, we obtain another four:

\[
\begin{align*}
a^2b &\equiv -c \pmod{p}, \\
b^2c &\equiv -d \pmod{p}, \\
c^2d &\equiv -a \pmod{p}, \\
d^2a &\equiv -b \pmod{p}.
\end{align*}
\]

The relation (7) gives \( A^2B \equiv C \pmod{p} \). If \( A = 1 \), then \( B = C \) since both \( B \) and \( C \) are least positive residues. Conversely, if \( B = C \) (and not a multiple of \( p \), lest \( p \) divides a Fermat remainder) then \( A^2 \equiv 1 \pmod{p} \). We cannot have \( A \equiv -1 \pmod{p} \) since we know that \( A^5 \equiv 1 \pmod{p} \). Hence, \( A = 1 \). This proves the first equivalence, while the remaining three follow in quite a symmetrical manner.

**Theorem 4.** The elite prime \( p \) is ultra-elite if any three of the four numbers \( A, B, C, D \) are distinct and not equal one.

Proof. By Lemma 3, if one number equals one, two others are identical. Hence, the stated condition forces all four not equal one, where \( p \) is ultra-elite by Theorem 1.

Another consequence of Lemma 3 is that if any two of the numbers \( A, B, C, D \) are equal to one, then all four of them are. More precisely,

**Theorem 5.** Let \( M \) denote the number of primitive roots among the four Fermat remainders modulo the elite prime \( p \). If \( p \) is not ultra-elite, then \( M = 3 \). In particular, if at least two of the numbers \( A, B, C, D \) are equal to one, then \( p \) is nonprimitive ultra-elite.

Proof. Assume that \( p \) is not ultra-elite. Then at least one of \( A, B, C, D \) is equal to one, while \( M \) counts how many of them are not. Suppose first that \( A = 1 \), as the other three cases will follow by symmetry. Using entirely Lemma 3, we observe that if \( B = 1 \), or \( C = 1 \), or \( D = 1 \), then all \( A, B, C, D \) would equal one, and \( M = 0 \), which is not true. Therefore, \( M = 3 \).

### 3 Numerical Examples

We list a few numerical results which serve to illustrate the applicability of the theorems given in the preceding section. In what follows, the notation \( p_n \) refers to the \( n \)th elite prime given in Table 1.

(1) Of the 29 elite primes in Table 1, ten of them have the property that \( |2|_{p_n} = 2^* \times 5 \). Of these ten, only three are primitive ultra-elite, i.e., \( n = 18, 24, 26 \), in which cases none of \( A, B, C, D \) is one. And of these three, only \( p_{24} \equiv 1 \pmod{25} \), in which case \( A = C \) and \( B = D \).

(2) Although all \( A, B, C, D \) are distinct and none equals one, \( p_{16} \) is nonprimitive ultra-elite. In this case, \( x^{p_{16} - 1} \equiv 1 \pmod{p_{16}} \) for each Fermat remainder \( x = a, b, c, d \).

(3) Six elite primes have \( M = 3 \), hence exactly one of \( A, B, C, D \) equals one. These correspond to \( n = 4 \) and \( n = 10 \) (\( D = 1 \)), \( n = 8 \) (\( C = 1 \)), \( n = 14 \) (\( B = 1 \)), \( n = 27 \) and \( n = 28 \) (\( A = 1 \)).
(4) Even though exactly one of $A$, $B$, $C$, $D$ equals one, the prime $p = 2^{352} \times 165 + 1$, found by Müller [5], is nonprimitive ultra-elite, i.e., $M = 0$.

(5) Another elite prime found by Müller [5], $p = 2^{145} \times 9575 + 1$ is nonprimitive ultra-elite with $A = B = C = D = 1$, hence $p \equiv 1 \pmod{25}$.

We conclude this section by providing a pseudo-code for a suggested algorithm which can be used to test for ultra-eliteness, if factoring $p - 1$ is not desired.

**Theorem 6.** Let $p$ be an elite prime such that $2|p = 2' \times 5$, together with the quantities $A$, $B$, $C$, $D$, and $M$ as before. The following pseudo-code returns three possible outcomes, represented by $X$, enumerated below.

(1) If $X = 0$, then $p$ is nonprimitive ultra-elite, i.e., $M = 0$.

(2) If $X = 1$, then $p$ is not primitive ultra-elite, i.e., $M = 0$ or $3$.

(3) If $X = 2$, then $p$ is ultra-elite, i.e., $M = 0$ or $4$.

01. Set $X:=1$;
02. Compute $A$;
03. If $A=1$ then
   04. If $p\%25=1$ then $X:=0$;
   05. EXIT;
06. Else compute $B$;
07. If $B=1$ or $B=A$ then EXIT;
08. Else compute $C$;
09. If $C>1$ then $X:=2$;
10. EXIT;

**Proof.** By default (line 01), $M = 0$ or $3$. This remains valid if $A = 1$ (lines 03 through 05), but if also $p \equiv 1 \pmod{25}$ (line 04), then $A = C$ by Lemma 2 and $M = 0$ by Theorem 5.

Starting from line 06, we have $A \neq 1$. If $B = 1$, or if $D = 1$ (the check $B = A$ of line 07), the default is unchanged. At line 08, $A \neq B \neq 1$. Suppose that $C \neq 1$ (line 09), for otherwise the default will remain. Since $C \neq B$ by Lemma 3, either $C = A$ or $C \neq A$, so $p$ is ultra-elite by Theorem 3 or by Theorem 4, respectively.

The algorithm given in Theorem 6 is a nondeterministic test for ultra-eliteness, particularly when $X = 1$ or $X = 2$, since it does not tell whether $p$ is primitive or nonprimitive, or simply not ultra-elite. In those cases, we are forced to find the complete factorization of $p - 1$, in order to compute the order modulo $p$ of one of the four Fermat remainders.

### 4 Open Discussion

We close with some remarks concerning ultra-elite primes in general. But first, the following theorem is of some theoretical worth as a criterion for an arbitrary odd integer to be a primitive ultra-elite prime.

**Theorem 7.** Let $N$ be an odd positive integer. Then $N$ is a primitive ultra-elite prime if and only if every Fermat remainder $x$ modulo $N$ satisfies the following two conditions.

(1) $x^{N-1} \equiv -1 \pmod{N}$ and

(2) $x^{N-1} \not\equiv 1 \pmod{N}$, for every odd prime $q$ that divides $N - 1$. 


Proof. If $N$ is an elite prime, $x$ must meet the Euler’s criterion (the first condition) for being a quadratic nonresidue. The second condition is furthermore required for it to be a primitive root modulo $N$. Conversely, the two conditions imply, respectively, that $|x|_N$ divides $N - 1$ but not $\frac{N-1}{q}$ for every prime $q$ which divides $N - 1$. Hence $|x|_N = N - 1$, which is possible only when $N$ is a prime, and $x$ a primitive root.

**Note 2.** Theorem 7 is essentially the familiar primality-proving partial converse of Fermat’s little theorem, due to Lehmer [4]—it differs only in the added condition that the base number $x$ be applied to all Fermat remainders, in order to ensure primitive ultra-eliteness.

Assuming that the list of elite primes is indeed infinite, it seems plausible to expect that infinitely many elite primes will be ultra-elite. It would be interesting as well to know the distribution of ultra-elite primes among the elite primes.

Is there a known bound on the number of consecutive primitive roots, or nonprimitive roots, modulo a given prime $p$? Would this knowledge have a significant effect on the bound of the period length $L$ for ultra-elite primes?

We predict that the occurrence of an ultra-elite prime, given that $p$ is elite, is largely influenced by the prime divisors of $p - 1$, but not so much by the period length $L$. Generally speaking, the larger the number of distinct prime divisors $p - 1$ has, the smaller the number of primitive roots—thus the less primitive ultra-elite primes and the more nonprimitive ones.

As we have stated, modulo a prime Fermat number $p$, quadratic nonresidues and primitive roots are one and the same. For such, $p$ is elite if and only if primitive ultra-elite. Unfortunately though, other than 3 and 5, every prime divisor of a Fermat number is anti-elite!

If we now consider a Sophie Germain prime $q$, then the prime $p = 2q + 1$ has only one less primitive roots than it does quadratic nonresidues. In that case we have a good probability of $1 - L/q$ that a given elite prime $p$ is also primitive ultra-elite. But again, no one has seen an elite prime of this kind.

### References


