Journal of Integer Sequences, Vol. 12 (2009),
Article 09.4.7

Verifying Two Conjectures on Generalized Elite Primes

Xiaoqin Li [1]
Mathematics Department
Anhui Normal University
Wuhu 241000, Anhui
People's Republic of China
qinlxss@163.com
lxq623@mail.ahnu.edu.cn

Abstract

A prime number p is called b-*elite* if only finitely many generalized Fermat numbers $F_{b,n} = b^{2^n} + 1$ are quadratic residues modulo p. Let p be a prime. Write $p - 1 = 2^r h$ with $r \geq 0$ and h odd. Define the length of the b-*Fermat period of* p to be the minimal natural number L such that $F_{b,r+L} \equiv F_{b,r} \pmod{p}$. Recently Müller and Reinhart derived three conjectures on b-*elite* primes, two of them being the following. (1) For every natural number $b > 1$ there is a b-*elite* prime. (2) There are generalized elite primes with elite periods of arbitrarily large lengths. We extend Müller and Reinhart's observations and computational results to further support above two conjectures. We show that Conjecture 1 is true for $b \leq 10^{13}$ and that for every possible length $1 \leq L \leq 40$ there actually exists a generalized elite prime with elite period length L.

1 Introduction

The numbers of the form

$$F_{b,n} = b^{2^n} + 1$$

are called generalized Fermat numbers (GFNs) for natural numbers b and n. The definition generalizes the usual Fermat numbers $F_n = 2^{2^n} + 1$, which were named after Pierre Simon

[1] Research supported by NSF of China Grant 10726074.

de Fermat (1601-1665). A lot of research has been done on Fermat numbers and their generalization since then (see [2, 6, 7, 8]).

In 1986 Aigner [1] called a prime number p *elite* if only finitely many Fermat numbers F_n are quadratic residues modulo p, i.e., there is an integer index m for which all F_n with $n > m$ are quadratic non-residues modulo p. He discovered only 14 such prime numbers less than $3.5 \cdot 10^7$. More computational effort yielded all 27 elites up to $2.5 \cdot 10^{12}$ together with some 60 much larger numbers [3, 4, 9]. These prime numbers are summarized in sequence A102742 of Sloane's *On-Line Encyclopedia of Integer Sequences* [13].

Müller and Reinhart [10] generalized Aigner's concept of elite primes in analogy to that of Fermat numbers.

Definition 1.1. ([10, Definition 1.1]). Let p be a prime number and $b \geq 2$ be a natural number. Then p is called a *b-elite* prime if there exists a natural number m, such that for all $n \geq m$ the GFNs $F_{b,n}$ are quadratic non-residues modulo p.

By the recurrence relation

$$F_{b,n+1} = (F_{b,n} - 1)^2 + 1, \tag{1}$$

one sees that the congruences $F_{b,n} \pmod p$ eventually become periodic. Write $p - 1 = 2^r h$ with $r \geq 0$ and h odd. Then this period – Müller and Reinhart [10] called it *b-Fermat period of p* – begins at latest with the term $F_{b,r}$. So there has to be a minimal natural number L such that

$$F_{b,r+L} \equiv F_{b,r} \pmod p, \tag{2}$$

which they [10] call the *length of the b-Fermat period* of p. The terms $F_{b,n} \pmod p$ for $n = r, \ldots, r + L - 1$ are the *b-Fermat remainders* of p.

Therefore, a prime number p is *b-elite* if and only if all L *b-Fermat remainders* are quadratic non-residues modulo p. It is moreover known that for all p it is a necessary condition for eliteness with $L > 1$ that L is an even number smaller than $\frac{p+1}{4}$ (compare [10]).

Müller and Reinhart [10] gave fundamental observations on *b-elite* primes and presented selected computational results from which three conjectures are derived, two of them being the following.

Conjecture 1. *[10, Conjecture 4.1] For every natural number $b > 1$ there is a b-elite prime.*

Conjecture 2. *[10, Conjecture 4.2] There are generalized elite primes with elite periods of arbitrarily large lengths.*

Concerning Conjecture 1, Müller and Reinhart [10] observed that most of the bases b actually have the prime 3 or 5 as *b-elite* – only the bases $b \equiv 0 \pmod{15}$ do not belong to one of these two "trivial" families. Conjecture 2 seems to be supported by their computations. They [10] proved the following Lemma 1.1.

Lemma 1.1. *For every*

$$L \in \mathcal{L}_1 = \{1, 2, 4, 6, 8, 10, 12\}, \tag{3}$$

there is a generalized elite prime $p < 10^4$ with elite period length L.

The main purpose of this paper is to extend Müller and Reinhart's observations and computational results to give further support to the two conjectures above. We state our main results as the following two Theorems.

Theorem 1. *Conjecture 1 is true for* $1 < b \leq 10^{13}$. *More precisely, for every natural number* $1 < b \leq 10^{13}$, *there is a b-elite prime* $p \leq 472166881$.

Theorem 2. *For every*

$$L \in \{1, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40\},$$

there is a generalized elite prime $p \leq 100663393$ *with elite period length* L.

In Section 2 we give an algorithm to test the b-eliteness of p for given $b \geq 2$ and prime p. The main tool of our algorithm is the Legendre symbol. Comparison of effectiveness with Müller's method for testing the 2-eliteness of p is given, see Remark 2.2.

In Section 3 we prove Theorem 1. We first propose a sufficient and necessary condition on base $b \geq 2$ to which there is a b-*elite* prime $p \in \{3, 5, 7, 11, 13, 19, 41, 641\}$. Using the condition and the Chinese Remainder Theorem, it is easy to compute a set $\mathcal{R}$ with cardinality $|\mathcal{R}| = 3667599$ such that Conjecture 1 is already true for those bases b such that $b \pmod{m} \notin \mathcal{R}$, where $m = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 41 \cdot 641 = 7497575085$. Thus we only need to consider the bases b with $b\,(\bmod\, m) \in \mathcal{R}$. We then give an algorithm to find the smallest b-*elite* prime P_b for each base $b = um + b_i \leq 10^{13}$ with $b_i \in \mathcal{R}$. At last we tabulate $\overline{P}(B)$ and the smallest b with $P_b = \overline{P}(B)$ for $B = 10^{10}, 10^{11}, 10^{12}, 10^{13}$, where $\overline{P}(B)$ is defined by (15) in section 3. In particular, we have $\overline{P}(10^{13}) = 472166881 = P_{9703200080805}$. Theorem 1 follows.

In Section 4 we prove Theorem 2. At first we compute all the elite periods of every generalized elite prime $p < 10^7$ based on the method described by Müller and Reinhart [10]. As a result we find some elite period lengths

$$L \in \mathcal{L}_2 = \{14, 16, 18, 20, 22, 24, 26, 28, 30, 36\}. \tag{4}$$

For every $L \in \mathcal{L}_2$, we tabulate $P(L)$ and the smallest b to which $P(L)$ is elite with length L, where $P(L)$ is defined by (17) in section 4. In particular we have $P(36) = 742073$(the smallest base $b = 5369$). We also give a new method to find some elite primes with elite period lengths 32,34,38 and 40, where $L = 40$ is realized by the elite prime $p = 100663393$ (the smallest base $b = 54712$). Thus Theorem 2 follows.

2 A b-eliteness testing algorithm

Let $b > 1$ be an integer, and let $p = 2^r \cdot h + 1$ be a prime number with $r \geq 1$ and h odd. In this section, we will give an algorithm to test the b-eliteness of p. Let $\left(\frac{*}{*}\right)$ denote the Legendre symbol. Our algorithm is based on the following criterion.

$$F_{b,n} \text{ is a quadratic non-residue modulo } p \text{ if and only if } \left(\frac{F_{b,n}}{p}\right) = -1. \tag{5}$$

Given $b \geq 2$ and prime $p = 2^r \cdot h + 1$ with h odd, we check whether

$$\left(\frac{F_{b,n}}{p}\right) = -1 \tag{6}$$

holds for $n = r, r+1, r+2, \ldots$ consecutively, where $F_{b,n} \pmod{p}$ are computed recursively by (1). If (6) does not hold for some $n \geq r$, then p is not b-*elite*. If (6) holds for $r \leq n \leq r+L-1$, then p is b-*elite*, where L is the *length of the* b-*Fermat period* of p, namely the least positive integer such that (2) holds.

Now we describe our Algorithm 2.1 in the following pseudocode.

Algorithm 2.1. Testing the b-eliteness of prime p;
{Input $b \geq 2$ and prime p}
{Determine whether p is b-*elite* or not; if p is b-*elite* then output the length L}
Begin Finding r and h such that $p = 2^r h + 1$ with h odd;
  $f_b \leftarrow F_{b,r} \pmod{p}$; $f \leftarrow f_b$; $L \leftarrow 0$; $elite \leftarrow\ True$;
  Repeat Computing $\left(\frac{f_b}{p}\right)$ by [5, Algorithm 2.3.5] (cf. also [12, §11.3]);
    If $\left(\frac{f_b}{p}\right) \neq -1$ **Then** $elite \leftarrow False$ **Else**
      begin $f_b \leftarrow (f_b - 1)^2 + 1 \pmod{p}$; $L \leftarrow L + 1$ **end**;
  Until (**not** $elite$) **or** ($f_b = f$);
  If $elite$ **Then** output L **Else** output "p is not b-elite"
End.

Remark 2.1. The prime 2 is not b-*elite* to any $b \geq 2$ since there is no quadratic non-residue modulo 2. So here and for the rest of this paper, we only need to consider odd primes p.

Remark 2.2. Let q be a prime and c be a positive integer with $q \nmid c$. Denote by $\mathrm{ord}_q(c)$ the multiplicative order of $c \pmod{p}$. Müller [9] gave an eliteness testing algorithm [9, Algorithm 3.1] for the base $b = 2$ based on the following criterion [9, Theorem 2.1].

$$F_{2,n} \text{ is a quadratic non-residue modulo } p \text{ if and only if } 2^r \mid \mathrm{ord}_p(F_{2,n}). \tag{7}$$

To check whether 2^r divides $\mathrm{ord}_p(F_{2,n})$ for $n = r, r+1, r+2, \ldots$, the algorithm computes $F_{2,n}^{2^k h} \pmod{p}$ for $k = 0, 1, \ldots, k_0$, where $k_0 = \min\{0 \leq k \leq r : F_{2,n}^{2^k h} \equiv 1 \pmod{p}\}$. It is well-known [5, §2.1.2] (see also [12, Theorem 4.9]) that it takes

$$O(\ln s \cdot \ln^2 p)$$

bit operations to compute the modular exponentiation $F_{2,n}^s \pmod{p}$. With our method, we compute the Legendre symbol $\left(\frac{F_{2,n}}{p}\right)$, which requires only

$$O(\ln^2 p)$$

bit operations [5, §2.3] (see also [12, Corollary 11.12.1 and Exerice 11.3.16]). So, for testing the b-eliteness of p, using criterion (5) is faster than using criterion (7).

3 Proof of Theorem 1

Throughout this section, let $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ be the set of all natural numbers. Let $\mathcal{B} \subset \mathcal{A}$ be two sets. We denote by $|\mathcal{A}|$ the number of elements in $\mathcal{A}$, and

$$\mathcal{A} - \mathcal{B} = \{c : c \in \mathcal{A}, c \notin \mathcal{B}\}.$$

Let p be an odd prime. Define the sets

$$\mathcal{A}_p = \{0, 1, 2, \ldots, p-1\};$$

$$\mathcal{B}_p = \begin{cases} \{b(\geq 2) \in \mathcal{A}_p : p \text{ is } b\text{-}elite\} \cup \{1\}, & \text{if } p \ \text{ is } (p-1)\text{-}elite; \\ \{b(\geq 2) \in \mathcal{A}_p : p \text{ is } b\text{-}elite\}, & \text{if } p \ \text{ is not } (p-1)\text{-}elite; \end{cases}$$

and

$$\mathcal{R}_p = \mathcal{A}_p - \mathcal{B}_p.$$

To prove Theorem 1, we need nine Lemmata.

Lemma 3.1. *[10, Observation 2.2,2.3] Let p be an odd prime number, b be a natural number. If p is b-elite, then*

(1) p is $(b + pk)$-elite for $k \in \{a, a+1, a+2, \ldots\}$, where $a = \lceil \frac{-b}{p} \rceil$;

(2) p is $(p - b)$-elite if $2 \leq b < p$.

Moreover, the Fermat remainders and the respective length of the Fermat period for the bases $b + pk$ and $p - b$ are the same.

By Lemma 3.1 we have

Lemma 3.2. *Let p be an odd prime and $b\,(> 1) \in \mathbb{N}$. Then*

$$p \text{ is } b\text{-elite if and only if } b \pmod p \in \mathcal{B}_p.$$

Lemma 3.3. *[10, Consequence 2.10] We have $\mathcal{R}_3 = \mathcal{R}_5 = \{0\}$.*

Lemma 3.4. *[10, Theorem 2.13] Let b be a natural number and p be an odd prime number. Then p is b-elite with $L = 2$ if and only if $p \equiv 7 \pmod{12}$ and either $b^2 + 1 \equiv b \pmod p$ with $\left(\frac{b}{p}\right) = -1$ or $b^2 + 1 \equiv -b \pmod p$ with $\left(\frac{b}{p}\right) = 1$.*

Lemma 3.5. *We have $\mathcal{R}_7 = \{0, 1, 6\}$.*

Proof. Let $k \in \{0, 1, 2, 3, 4, 5, 6\}$. Then

$$k^2 + 1 \pmod 7 = \begin{cases} k, & if \quad k = 3, 5; \\ 7 - k, & if \quad k = 2, 4; \\ 1, & if \quad k = 0; \\ 2, & if \quad k = 1, 6; \end{cases}$$

and

$$\left(\frac{k}{7}\right) = \begin{cases} 1, & if \quad k = 1, 2, 4; \\ 0, & if \quad k = 0; \\ -1, & if \quad k = 3, 5, 6; \end{cases}$$

Based on Lemma 3.4, we have $\mathcal{B}_7 = \{2, 3, 4, 5\}$. Thus the Lemma follows. $\square$

Using Algorithm 2.1, we can easily get the following Lemma 3.6 and Lemma 3.7.

Lemma 3.6. *We have*

$$\mathcal{R}_{11} = \{0, 2, 3, 4, 5, 6, 7, 8, 9\}; \mathcal{R}_{13} = \{0, 2, 3, 4, 6, 7, 9, 10, 11\};$$

$$\mathcal{R}_{19} = \{0, 2, 3, 4, 5, 6, 9, 10, 13, 14, 15, 16, 17\};$$

$$\mathcal{R}_{17} = \mathcal{A}_{17} \text{ and } \mathcal{R}_{23} = \mathcal{A}_{23}.$$

Lemma 3.7. *Let $p < 1000$ be an odd prime. Then*

$$|\mathcal{R}_p| < \frac{1}{2}|\mathcal{A}_p| \text{ if and only if } p \in \{3, 5, 7, 41, 641\},$$

where

$$\mathcal{R}_{41} = \{0, 1, 3, 9, 14, 27, 32, 38, 40\}$$

and

$$\begin{aligned}\mathcal{R}_{641} = \{&0, 1, 2, 4, 5, 8, 10, 16, 20, 21, 25, 29, 31, 32, 40, 42, 50, 58, 61, 62, 64, 67, 77,\\ &80, 84, 100, 105, 116, 122, 124, 125, 128, 129, 134, 141, 145, 153, 154, 155,\\ &159, 160, 168, 177, 199, 200, 210, 221, 232, 241, 243, 244, 248, 250, 256, 258,\\ &268, 282, 287, 290, 305, 306, 308, 310, 318, 320, 321, 323, 331, 333, 335, 336,\\ &351, 354, 359, 373, 383, 385, 391, 393, 397, 398, 400, 409, 420, 431, 441, 442,\\ &464, 473, 481, 482, 486, 487, 488, 496, 500, 507, 512, 513, 516, 517, 519, 525,\\ &536, 541, 557, 561, 564, 574, 577, 579, 580, 583, 591, 599, 601, 609, 610, 612,\\ &616, 620, 621, 625, 631, 633, 636, 637, 639, 640\}.\end{aligned}$$

Remark 3.1. In fact, the two results "$\mathcal{R}_{17} = \mathcal{A}_{17}$" and "$\mathcal{R}_{23} = \mathcal{A}_{23}$" were already given by Müller and Reinhart [10] where they are immediate consequences of Theorem 2.15 and Theorem 2.16. By Lemma 3.6 and Lemma 3.1, the primes 17 and 23 are not b-*elite* to any natural number $b \geq 2$.

Let

$$m = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 41 \cdot 641 = 7497575085. \tag{8}$$

Applying the Chinese Remainder Theorem, it is easy to compute the set

$$\mathcal{R} = \{0 \leq b < m : b \,(\mathrm{mod} p) \in \mathcal{R}_p \text{ for } p = 3, 5, 7, 11, 13, 19, 41, 641\} \tag{9}$$

which has cardinality

$$R = |\mathcal{R}| = 1 \cdot 1 \cdot 3 \cdot 9 \cdot 9 \cdot 13 \cdot 9 \cdot 129 = 3667599. \tag{10}$$

Using the Heap Sort Algorithm [11, §8.3], we sort the elements of $\mathcal{R}$ in an increasing order

$$\mathcal{R} = \{b_1 < b_2 < \cdots < b_R\}, \tag{11}$$

where

$$b_1 = 0, b_2 = 1590, b_3 = 2955, b_4 = 5685, b_5 = 6405, b_6 = 7020, \ldots, b_R = 7497573495.$$

By Lemma 3.2 and the Chinese Remainder Theorem we have the following Lemma 3.8.

Lemma 3.8. *Let $b\,(>1) \in \mathbb{N}$, and let m be given as in (8). Then*
there is a b-elite prime $p \in \{3,5,7,11,13,19,41,641\}$
if and only if $b \pmod p \in \mathcal{B}_p$ for some $p \in \{3,5,7,11,13,19,41,641\}$
if and only if $b \pmod m \notin \mathcal{R}$.

From Lemma 3.8, we see that Conjecture 1 is already true for those bases b such that $b \pmod m \notin \mathcal{R}$. Thus we only need to consider the bases b with $b \pmod m \in \mathcal{R}$.

Lemma 3.9. *For every base $1 < b \le 10^{13}$ with $b \pmod m \in \mathcal{R}$, there is a prime $p \le 472166881$ such that p is b-elite.*

Proof. Given $b \ge 2$ with $b \pmod m \in \mathcal{R}$, let

$$\mathcal{P}_b = \{\text{prime } p : p \text{ is } b\text{-elite}\}, \tag{12}$$

and let

$$P_b = \begin{cases} \infty, & \text{if } \mathcal{P}_b = \emptyset, \\ \min\{p : p \in \mathcal{P}_b\}, & \text{otherwise.} \end{cases} \tag{13}$$

Let $1 \le B_1 < B_2$ be two natural numbers such that

$$\mathcal{R} \cap \{b \pmod m : B_1 < b \le B_2\} \ne \emptyset.$$

Define the functions

$$\overline{P}(B_1, B_2) = \max\{P_b : B_1 < b \le B_2, b \pmod m \in \mathcal{R}\}, \tag{14}$$

and

$$\overline{P}(B_2) = \overline{P}(1, B_2) = \max\{\overline{P}(1, B_1), \overline{P}(B_1, B_2)\}, \tag{15}$$

With the above preparation, we describe our algorithm for verifying Lemma 3.9 for those bases b with $B_1 < b \le B_2$ and $b \pmod m \in \mathcal{R}$.

Algorithm 3.1. Verifying Lemma 3.9 for $B_1 < b \le B_2$ with $b \pmod m \in \mathcal{R}$;
$\{$Input B_1, B_2 and $maxp$ with $1 \le B_1 < B_2$, say $B_1 = 10^{10}$, $B_2 = 10^{11}$, and $maxp = 10^9\}$
$\{$Output either $\overline{P} = \overline{P}(B_1, B_2) < maxp$ and the smallest $b \in (B_1, B_2]$ such that $\overline{P} = P_b\}$
$\{$or the smallest $b \in (B_1, B_2]$ with $b \pmod m \in \mathcal{R}$ such that Lemma 3.9 fails$\}$
Begin $\overline{P} \leftarrow 3$; $u \leftarrow \lfloor \frac{B_1}{m} \rfloor \cdot m$; $b' \leftarrow u$; $j \leftarrow 1$; $First \leftarrow True$;
  While $b' \le B_1$ **Do begin** $j \leftarrow j+1$; $b' \leftarrow u + b_j$ **end**;
  Repeat If $First$ **Then begin** $i \leftarrow j$; $First \leftarrow False$ **end Else** $i \leftarrow 0$;
    repeat $p \leftarrow 29$; $Found \leftarrow False$;
      Repeat $b'' \leftarrow b' \pmod p$;
        Using Algorithm 2.1 to test the b''-eliteness of p;
        If p is b''-elite **Then**
          begin $Found \leftarrow True$; **If** $p > \overline{P}$ **Then Begin** $\overline{P} \leftarrow p$; $b \leftarrow b'$ **End**
          end   **Else**
        begin $p \leftarrow$ the next prime $> p$;
          If $(p = 41)$ or $(p = 641)$ **then** $p \leftarrow$ the next prime $> p$

end
Until *Found* **Or** $(p > maxp)$;
If not *Found* **Then**
begin output "the lemma fails at b', enlarge $maxp$ and try again"; exit
end;
$i \leftarrow i+1$; $b' \leftarrow u + b_i$;
until $(i > R)$ or $(b' > B_2)$;
$u \leftarrow u + m$;
Until $u > B_2$;
Output $\overline{P}$ and b;
End;

The Delphi program ran about 105 hours on a PC AMD 3000+/2.0G to find

$$\overline{P}(1, 10^{10}),\ \overline{P}(10^{10}, 10^{11}),\ \overline{P}(10^{11}, 10^{12}),$$

and

$$\overline{P}(i \cdot 10^{12}, (i+1) \cdot 10^{12}),\ \text{for } i = 1, 2, \ldots, 9.$$

Then by (15) we get $\overline{P}(B)$ for $B = 10^{10}, 10^{11}, 10^{12}, 10^{13}$; see Table 1, where b is the first base with $P_b = \overline{P}(B)$. As a result we have

$$\overline{P}(10^{13}) = 472166881,$$

which means that for every base $1 < b \leq 10^{13}$ with $b \pmod m \in \mathcal{R}$, there is a prime $p \leq 472166881$ such that p is b-elite. The Lemma follows. □

Lemma 3.9 together with Lemma 3.8 implies Theorem 1.

Table 1: $\overline{P}(B)$ and b with $P_b = \overline{P}(B)$

B	10^{10}	10^{11}	10^{12}	10^{13}
$\overline{P}(B)$	5483521	24494081	167772161	472166881
b	4157043150	45329209185	224199632355	9703200080805
L	4	12	4	4

4 Proof of Theorem 2

Let $L \in \{1, 2, 4, 6, 8, \ldots\}$. Define

$$\mathcal{P}(L) = \{\text{prime } p : p \ \text{ is a generalized elite with period length } \ L\} \tag{16}$$

and let

$$P(L) = \begin{cases} \infty, & \text{if } \mathcal{P}(L) = \emptyset, \\ \min\{p : p \in \mathcal{P}(L)\}, & \text{otherwise.} \end{cases} \tag{17}$$

By Lemma 1.1, Müller and Reinhart [10] have found $P(L)$ for $L \in \mathcal{L}_1$($\mathcal{L}_1$ is given by (3)). We summarize their computations in the following Table 2, where b is the base to which $P(L)$ is elite with elite period length L.

Table 2: The function $P(L)$ for $L \in \mathcal{L}_1$

L	1	2	4	6	8	10	12
$P(L)$	3	7	41	199	409	331	3121
b	2	2	2	19	6	23	8

To prove Theorem 2, we need three Lemmata.

Lemma 4.1. *[10, Theorem 2.18] Let $p = 2^r h + 1$ with h odd. Let n be the number of all possible periods and denote by L_i the length of the period i. Then*

$$\sum_{i=1}^{n} L_i = h. \tag{18}$$

The number $N_{b,i}$ of all b's in the period i is

$$N_{b,i} = 2^r \cdot L_i. \tag{19}$$

Lemma 4.2. *For every $L \in \mathcal{L}_2$ ($\mathcal{L}_2$ is given by (4)), there is a generalized elite prime $p < 10^7$ with elite period length L.*

Proof. Based on Lemma 4.1, Müller and Reinhart [10] presented an algorithm to find the first elite period of prime p.

Given a prime $p = 2^r \cdot h + 1$ with h odd, let

$$\mathcal{S}_{2^r} = \{c \in \mathbb{Z}_p : \exists\, b \in \mathbb{Z}_p \text{ such that } b^{2^r} \equiv c \,(\mathrm{mod}\, p)\}. \tag{20}$$

Then we have $|\mathcal{S}_{2^r}| = h$ and

$$F_{b,n} - 1 \,(\mathrm{mod}\, p) \in \mathcal{S}_{2^r} \tag{21}$$

for $n = r, \ldots, r + L - 1$ and for all bases b. Moreover, elements of $\mathcal{S}_{2^r}$ belong to many different periods of various lengths.

Let g be a primitive root modulo p and let $c \in \mathcal{S}_{2^r}$. Then we have $c = g^{2^r k_0}$ with $k_0 \in \{0, 1, \ldots, h-1\}$. Let $g_0 = g^{k_0}$. We check whether

$$\left(\frac{g_0^{2^{r+i}} + 1}{p}\right) = -1 \tag{22}$$

holds for $i = 0, 1, 2, \ldots$ consecutively. If (22) does not hold for some i, then this Fermat period is not an elite period. If (22) holds for $0 \le i < l$, where l is the smallest natural number such that $g_0^{2^{r+l}} \equiv g_0^{2^r} \pmod p$, then the period $c+1, c^2+1, \ldots, c^{2^{l-1}}+1$ is an elite period with length $L = l$.

It is easy to modify Müller and Reinhart's computational method in order to find all elite periods of every generalized elite prime $p < Bound$, say $Bound = 10^7$. Now we describe the modified algorithm in the following pseudocode.

Algorithm 4.1. Finding all elite periods L of each prime $p < Bound$ if they exist.

{Input $Bound$, say $Bound = 10^7$; Output $p < Bound$ with $L > 12$.}

```
Begin p ← 3;
  Repeat Finding r and h such that p = 2^r h + 1 with h odd; g ← primitive root mod p;
      For i ← 0 To h Do tested_i ← False; periodstart ← 0;
      repeat index ← periodstart; elite ← True; L ← 0;
        Repeat tested_index ← True; If elite Then
          begin  f ← g^(2^r * index) + 1 (mod p);
            Computing (f/p) by [5, Algorithm 2.3.5] (cf. also [12, §11.3]);
            If (f/p) ≠ −1 Then elite ← False;
          end;
          index ← index * 2 (mod h); L ← L + 1 ;
        Until (index = periodstart);
        If elite and (L > 12) Then output p and L;
        While tested_periodstart Do periodstart ← periodstart + 1;
      until (periodstart = h);
      p ← the next prime > p ;
  Until p > Bound
End.
```

The Dephi program ran about 53 hours to compute all elite periods of every elite prime $p < 10^7$, and find some elite period lengths $L \in \mathcal{L}_2$. For every $L \in \mathcal{L}_2$, we summarize $P(L)$ and the smallest b to which $P(L)$ is elite with length L in Table 3. The Lemma follows. $\square$

Table 3: The function $P(L)$ for $L \in \mathcal{L}_2$

L	14	16	18	20	22	24	26	28	30	36
$P(L)$	32251	30841	17443	36901	50543	688297	180247	117973	796387	742073
b	247	75	726	298	182	2935	6143	432	27867	5369

Remark 4.1. The smallest base b in Table 3 can be easily obtained by using Algorithm 2.1 to test the b-eliteness of $P(L)$ for $b = 2, 3, \ldots, \frac{P(L)-1}{2}$ consecutively until the length of the elite period is found to be L.

Remark 4.2. There are no generalized elite primes $p < 10^7$ with $L = 32$ or 34 or $L > 36$.

In the following Table 4, we list the factorization of $2^{\frac{L}{2}}+1$ and the factorization of $P(L)-1$ for $L \in \mathcal{L}_3 = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 36\}$

Table 4: The factorizations of $2^{\frac{L}{2}}+1$ and of $P(L)-1$ for $L \in \mathcal{L}_3$

L	$P(L)$	The factorization of $2^{\frac{L}{2}}+1$	The factorization of $P(L)-1$
2	7	3	$2 \cdot 3$
4	41	5	$2^3 \cdot 5$
6	199	3^2	$2 \cdot 3 \cdot 11$
8	409	17	$2^3 \cdot 3 \cdot 17$
10	331	$3 \cdot 11$	$2 \cdot 3 \cdot 5 \cdot 11$
12	3121	$5 \cdot 13$	$2^4 \cdot 3 \cdot 5 \cdot 13$
14	32251	$3 \cdot 43$	$2 \cdot 3 \cdot 5^3 \cdot 43$
16	30841	257	$2^3 \cdot 3 \cdot 5 \cdot 257$
18	17443	$3^3 \cdot 19$	$2 \cdot 3^3 \cdot 17 \cdot 19$
20	36901	$5^2 \cdot 41$	$2^2 \cdot 3^2 \cdot 5^2 \cdot 41$
22	50543	$3 \cdot 683$	$2 \cdot 37 \cdot 683$
24	688297	$17 \cdot 241$	$2^3 \cdot 3 \cdot 7 \cdot 17 \cdot 241$
26	180247	$3 \cdot 2731$	$2 \cdot 3 \cdot 11 \cdot 2731$
28	117973	$5 \cdot 29 \cdot 113$	$2^2 \cdot 3^2 \cdot 29 \cdot 113$
30	796387	$3^2 \cdot 11 \cdot 331$	$2 \cdot 3 \cdot 331 \cdot 401$
36	742073	$5 \cdot 13 \cdot 37 \cdot 109$	$2^3 \cdot 23 \cdot 37 \cdot 109$

Let L be even. Define

$$q_L = \max\{\text{prime}\, q : q \mid 2^{\frac{L}{2}}+1\}.$$

Then for every $L \in \mathcal{L}_3$, we find that,

$$q_L \mid (P(L)-1). \tag{23}$$

Based on (23), we try to find some generalized elite primes p with elite period lengths 32,34,38 and 40. The method is as follows (taking $L = 32$ for example). Since $2^{\frac{L}{2}}+1 = 2^{16}+1 = 2^{2^4}+1 = 65537 = F_4$, we have $q_{32} = 65537$. In order to find the elite prime p with length 32, we consider primes $p\,(p > 10^7)$ which can be written in the form $p = 65537k+1$ with k an integer. Using Algorithm 4.1, we compute all the elite periods of these elite primes consecutively until the length of the elite period is L. As a result we find that prime 47710937 is b-*elite* with $L = 32$, where $b = 62792$ and $47710936 = 2^3 \cdot 7 \cdot 13 \cdot 65537$.

In Table 5, for $L = 32, 34, 38$ and 40, we tabulate the prime p, the base b to which p is elite with length L.

Table 5: Elite primes p with length $L = 32, 34, 38$ and 40

L	p	b	The factorization of $2^{\frac{L}{2}} + 1$	The factorization of $p - 1$
32	47710937	62792	65537	$2^3 \cdot 7 \cdot 13 \cdot 65537$
34	51118471	106257	$3 \cdot 43691$	$2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 43691$
38	78643351	661362	$3 \cdot 174763$	$2 \cdot 3^2 \cdot 5^2 \cdot 174763$
40	100663393	54712	$17 \cdot 61681$	$2^5 \cdot 3 \cdot 17 \cdot 61681$

Remark 4.3. For every $L \in \{32, 34, 38, 40\}$, the prime p we find in Table 5 may be larger than $P(L)$.

From Table 5, we have the following Lemma 4.3.

Lemma 4.3. *For every*

$$L \in \{32, 34, 38, 40\},$$

there is a generalized elite prime $p \leq 100663393$ *with elite period length* L.

Theorem 2 follows from Lemma 1.1, Lemma 4.2 and Lemma 4.3.

We have known that for each even $L \leq 40$, there is a generalized elite prime p with elite period length L such that $q_L \mid (p-1)$. But it is still an open problem whether for every even L there is a generalized elite prime p with elite period length L such that $q_L \mid (p-1)$.

5 Acknowledgement

We thank the referee for kind and helpful comments that improve the presentation of the paper.

References

[1] A. Aigner, Über Primzahlen, nach denen (fast) alle Fermatzahlen quadratische Nichtreste sind. *Monatsh. Math.* **101** (1986), 85–93.

[2] A. Björn and H. Riesel, Factors of generalized Fermat numbers. *Math. Comp.* **67** (1998), 441–446.

[3] A. Chaumont and T. Müller, All elite primes up to 250 billion. *J. Integer Seq.* **9** (2006), Article 06.3.8.

[4] A. Chaumont, J. Leicht, T. Müller and A. Reinhart, The continuing search for large elite primes. *Int. J. Number Theory.* **5** (2009), 209–218.

[5] R. Crandall and C. Pomerance, *Prime Numbers, a Computational Perspective*, 2nd ed., Springer-Verlag, 2005.

[6] H. Dubner and Y. Gallot, Distribution of generalized Fermat prime numbers. *Math. Comp.* **71** (2001), 825–832.

[7] H. Dubner and W. Keller, Factors of generalized Fermat numbers. *Math. Comp.* **64** (1995), 397–405.

[8] M. Křížek, F. Luca and L. Somer, *17 Lectures on Fermat numbers. From Number Theory to Geometry*, Springer, 2001.

[9] T. Müller, Searching for large elite primes. *Experiment. Math.* **15.2** (2006), 183–186.

[10] T.Müller and Andreas Reinhart, On generalized elite primes. *J. Integer Seq.* **11** (2008), Article 08.7.25.

[11] H. Press, A. Teukolsky, T. Vetterling and P. Flannery, *Numerical Recipes in C++. The Art of Computer Programming*, Cambridge University Press, 2002.

[12] H. Kenneth Rosen, *Elementary Number Theory and its Applications*, Addison-Wesley, Fourth edition, 2000.

[13] N. J. A. Sloane, Online Encyclopedia of Integer Sequences (OEIS). Electronically published at: http://www.research.att.com/~njas/sequences/

2000 *Mathematics Subject Classification*: Primary 11Y16; Secondary 11A15, 11A41, 11Y55.
Keywords: generalized elite primes, generalized Fermat numbers, b-Fermat periods.

(Concerned with sequence A102742.)

Received January 5 2009; revised version received June 4 2009. Appeared in *Journal of Integer Sequences*, June 20 2009.

Return to Journal of Integer Sequences home page.