Journal of Integer Sequences, Vol. 11 (2008),
Article 08.3.1

On Generalized Elite Primes

Tom Müller and Andreas Reinhart
Institut für Cusanus-Forschung an der
Universität und der Theologischen Fakultät Trier
Domfreihof 3
D-54290 Trier
Germany
muel4503@uni-trier.de
rein4503@uni-trier.de

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 to p. So far, only the case $b = 2$ was subjected to theoretical and experimental researches by several authors. Most of the results obtained for this special case can be generalized for all bases $b > 2$. Moreover, the generalization allows an insight to more general structures in which standard elite primes are embedded. We present selected computational results from which some conjectures are derived.

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. They were named after Pierre Simon de Fermat (1601–1665) who studied the special case $b = 2$ in the seventeenth century. A lot of research has been done on Fermat numbers and their generalization since then (compare [9]). One particular field of interest focusses on the primality and the divisors of GFNs. It is known that a divisor d of $F_{b,n}$ has the form $d = 2^n \cdot k + 1$, where k denotes a natural number. Other main theoretical and computational results on the factors of GFNs can be found in the works of Björn and Riesel [2], Dubner and Keller [7], resp. Dubner and Gallot [6].

In 1986 the Austrian mathematician Alexander Aigner studied prime numbers p to which the Fermat numbers $F_{2,n}$ are quadratic residues modulo p for at most finitely many natural numbers n. Because of their rareness – Aigner found only 14 such prime numbers less than 35 million – he called them "elite" primes [1]. There has been some research done on this family of prime numbers in the past few years. If we denote by $N(x)$ the number of elite primes being less than or equal to $x > 0$ then it is known by a theorem of Křížek, Luca and Somer that $N(x) = O\left(\frac{x}{\log^2 x}\right)$, i.e., the series of reciprocals of all elite primes is convergent [10]. This result can be generalized for all bases $b \geq 2$. Moreover, all elites up to $2.5 \cdot 10^{12}$ have been computed in [4, 5, 11]. These prime numbers are summerarized in sequence A102742 of Sloane's *On-Line Encyclopedia of Integer Sequences* [14].

Aigner's concept of elite primes can, in analogy to that of Fermat numbers, be generalized too.

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.*

Because of the recurrence relation

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

it is obvious that the congruences $F_{b,n} \pmod{p}$ eventually become periodic. We will see in the following section that if p is of the form $2^r \cdot h + 1$ with h odd, then this period – we shall call 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 $F_{b,r+L} \equiv F_{b,r} \pmod{p}$, which we 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.

2 Elite primes, bases and periods

2.1 Elementary results

We begin our investigation with some fundamental observations, which are of some importance for the computational part of this paper.

Observation 2.1. *Let $b \equiv 0 \pmod{p}$. Then p is not b-elite since $F_{b,n} \equiv 1 \pmod{p}$ for all natural numbers n.*

Observation 2.2. *Because of the congruence relation $F_{b+pk,n} \equiv F_{b,n} \pmod{p}$, we see that we only need to search for all bases $b \in \{1, 2, \ldots, p-1\}$ to which p is b-elite to know all possible bases. Notice that for the bases $b + pk$ the Fermat remainders and so the respective length of the Fermat period are the same.*

Observation 2.3. *The symmetry relation $F_{p-b,n} \equiv F_{b,n} \pmod{p}$ allows to reduce the search for suitable bases to $b \in \{1, 2, \ldots, \frac{p-1}{2}\}$ in order to know all possible bases to which p is elite. Again we obtain equal Fermat remainders and period lengths for the bases b and $p - b$.*

The following two results are immediate consequences of the law of Quadratic Reciprocity.

Theorem 2.4. *Let p be a prime GFN of base b with an index larger than or equal to 2. Then p is not a b-elite prime.*

Proof. It is clear that b is an even number, since odd bases only give even GFNs which hence are not prime. Let $n \geq 2$ be the index of $p = F_{b,n}$ written as a GFN, this means that $p \equiv 1 \pmod 8$. Because of relation (1) we get

$$F_{b,n+1} \equiv 2 \pmod p. \tag{2}$$

Using induction over the index $m \geq n+1$ we additionally obtain that

$$F_{b,m} \equiv 2 \pmod p \tag{3}$$

is fulfilled for every such m. Hence,

$$\left(\frac{F_{b,m}}{p}\right) = \left(\frac{2}{p}\right) = 1. \tag{4}$$

This means that all GFNs with indices larger than n are actually quadratic residues modulo p. $\square$

Theorem 2.5. *Let p be a prime factor of $F_{b,n}$ for any natural index $n \geq 3$. Then p is not a b-elite prime.*

Proof. It is known that a prime factor p of $F_{b,n}$ is of the form $2^n \cdot k + 1$, i.e., $p \equiv 1 \pmod 8$. In analogy to the proof of the previous theorem, we here again get the congruence $F_{b,m} \equiv 2 \pmod p$ for all $m > n$ and hence we will find no quadratic non-residue among all these GFNs. $\square$

2.2 The Fermat periods of b-elite primes

We have seen, that as a consequence of equation (1) we get the periodicity of the system of equations $F_{b,n} \pmod p$ for all n that are large enough. We will now give a more precise characterization of the first term of the Fermat period and its length L.

Theorem 2.6. *Let $b > 1$ be a natural number and let $p = 2^r \cdot h + 1$ be a prime number with $r \geq 0$ and h odd. The multiplicative order of $b \pmod p$ is of the form $2^s \cdot t$, with $0 \leq s \leq r$ and t a divisor of h. Then the Fermat period of p begins with the term $F_{b,s}$ and its length L is the multiplicative order of 2 modulo t.*

Proof. Let $k > l$ be natural numbers such that

$$F_{b,k} \equiv F_{b,l} \pmod p. \tag{5}$$

This implies that

$$b^{2^l(2^{k-l}-1)} \equiv 1 \pmod p, \tag{6}$$

and hence $2^l(2^{k-l} - 1)$ has to be a multiple of the multiplicative order of $b \pmod p$. The odd part of this exponent $2^{k-l} - 1$ is a multiple of t, i.e., $2^{k-l} \equiv 1 \pmod t$, and we obtain the fact that the difference $k - l$ is a multiple of the multiplicative order of $2 \pmod t$. $\square$

Remark: Theorem 2.6 states that the Fermat period begins at least with the term $F_{b,r}$ modulo $p = 2^r \cdot h + 1$. Hence, p is b-elite if and only if the L GFNs $F_{b,n}$ $(n = r, r+1, \ldots, r+L-1)$ are quadratic non-residues modulo p.

Moreover, two results of Aigner concerning the period length L can easily be generalized for b-elites.

Theorem 2.7. *Let p be a b-elite prime with $L > 1$. Then L is an even number.*

Proof. Let $p = 2^r h + 1$ be a b-elite prime with period length $L > 1$. Then there is a quadratic residue $c > 1$ modulo p such that $F_{b,r} \equiv c + 1 \pmod{p}$. Consider the product of all GFNs of one entire period

$$Q := \prod_{\nu=0}^{L-1} F_{b,r+\nu}. \tag{7}$$

From this it follows immediately that

$$Q \equiv \prod_{\nu=0}^{L-1} (c^{2^\nu} + 1) \pmod{p}, \tag{8}$$

and since evaluating this latter product leads us to a geometric sum of all c powers up to the exponent $2^L - 1$, we obtain

$$Q \equiv \sum_{\nu=0}^{2^L-1} c^\nu = \frac{c^{2^L} - 1}{c - 1} \pmod{p}. \tag{9}$$

Now, as L is the length of the b-Fermat period of p we have $c^{2^L} \equiv c \pmod{p}$ and hence

$$Q \equiv \frac{c - 1}{c - 1} = 1 \pmod{p}. \tag{10}$$

This means that $\left(\frac{Q}{p}\right) = 1$. Using the fact that the Legendre symbol is multiplicative, the definition of Q gives

$$1 = \left(\frac{Q}{p}\right) = \prod_{\nu=0}^{L-1} \left(\frac{F_{b,r+\nu}}{p}\right) = (-1)^L \tag{11}$$

since p is b-elite. From this it follows that $L > 1$ is an even number. ∎

Theorem 2.8. *Let p be a b-elite prime with a b-Fermat period of length L. Then $L \le \frac{p+1}{4}$.*

Proof. It is known from elementary number theory that if p is an odd prime number there are exactly $\frac{p-1}{2}$ different quadratic residues modulo p among the numbers $1, 2, \ldots, p-1$. The other half of these numbers actually are quadratic non-residues modulo p. Another result (probably due to Gauss; see, e.g., Bundschuh [3, p. 148]) states, that among the

$\frac{p-1}{2}$ quadratic residues there are exactly $\frac{1}{4}\left(p-4+(-1)^{\frac{p+1}{2}}\right)$ pairs of successive quadratic residues. So we find that at most

$$\frac{p-1}{2}-\frac{1}{4}\left(p-4+(-1)^{\frac{p+1}{2}}\right)=\frac{p+2-(-1)^{\frac{p+1}{2}}}{4} \tag{12}$$

quadratic residues can be succeeded by a quadratic non-residue less than p. This is of interest to us because for b-elite p the Fermat remainders of the form $c^{2^n}+1$ always are quadratic non-residues modulo p succeeding the quadratic residues c^{2^n} $(n=0,\dots,L-1)$.
If $p \equiv -1 \pmod 4$ this gives $L \leq \frac{p+1}{4}$ as desired. For $p \equiv 1 \pmod 4$ we first get $L \leq \frac{p+3}{4}$. But, notice that for this congruential class we have $\left(\frac{-1}{p}\right)=1$, such that $p-1$ is a quadratic residue, which actually cannot have any successor less than p. Hence, $L \leq \frac{p+3}{4}-1=\frac{p-1}{4}$. □

2.3 Characterization of b-elite primes

We now turn our attention to different period lengths L, beginning with a characterization of the bases leading to an elite period with $L=1$ for a given prime number p.

Theorem 2.9. *Let b be a natural number and let p be a prime number. Then p is b-elite with $L=1$ if and only if either $p \equiv 3 \,(\mathrm{mod}\, 8)$ and $b \equiv \pm 1 \,(\mathrm{mod}\, p)$ or $p \equiv -3 \,(\mathrm{mod}\, 8)$ and $b^4 \equiv 1 \,(\mathrm{mod}\, p)$.*

Proof. Let $p=2^r h+1$ with h odd be b-elite with $L=1$. Then there is a quadratic non-residue a modulo p with

$$F_{b,r} \equiv a \pmod{p}, \tag{13}$$

and hence, $a \equiv F_{b,r+1} \equiv (a-1)^2+1 \pmod p$ by using relation (1). This finally leads to

$$(a-1)(a-2) \equiv 0 \pmod p, \tag{14}$$

i.e., $a \equiv 1$ or $a \equiv 2 \pmod p$. Since $a \equiv 1$ is a quadratic residue, we get $a \equiv 2 \pmod p$ as the only possible solution. Notice that the law of Quadratic Reciprocity states that $\left(\frac{2}{p}\right)=-1$ if and only if $p \equiv \pm 3 \pmod 8$. The case $p=8k+3=2(4k+1)+1$ then gives the condition $b^2 \equiv 1$ (mod p), i.e., $b \equiv \pm 1$ (mod p), while $p=8k-3=4(2k-1)+1$ leads to $b^4 \equiv 1$ (mod p) in relation (13). The converse is trivial. □

From this we immediately obtain

Consequence 2.10. *1) The prime 3 is b-elite if and only if the base b is not a multiple of 3.*

2) The prime 5 is b-elite if and only if the base b is not a multiple of 5.

3) If $p \in \{3,5\}$ is b-elite then it has a b-Fermat period of length $L=1$.

Proof. Fermat's little theorem states that for every prime number p and every natural number b relatively prime to p we have $b^{p-1} \equiv 1 \pmod p$. So for $p=3 \equiv 3 \pmod 8$ we get $b^2 \equiv 1 \pmod 3$ for every b not a multiple of 3. For $p=5 \equiv -3 \pmod 8$ every non-multiple b fulfills $b^4 \equiv 1 \pmod 5$. These facts together with Theorem 2.9 imply the claims. □

We see, that for any given prime p we can decide whether there are bases b such that p is b-elite with $L = 1$ and in the affirmative case we are even able to construct all these bases. Now, we will have a look at the general case $L > 1$.

Theorem 2.11. *Let b be a natural number and let $p = 2^r h + 1$ be a b-elite prime number with a Fermat period of length $L > 1$. Then there exists a quadratic residue c modulo p such that $F_{b,r} \equiv c + 1 \pmod{p}$ and which is a solution of the Diophantine equation*

$$\sum_{\nu=0}^{2^L-2} c^\nu = \frac{c^{2^L-1} - 1}{c - 1} \equiv 0 \pmod{p}. \tag{15}$$

Proof. Let $p = 2^r h + 1$ be a b-elite prime. Write $F_{b,r} \equiv c + 1 \pmod{p}$ where c is a quadratic residue modulo p. Then $F_{b,r+L} \equiv c^{2^L} + 1 \pmod{p}$ and since L is the length of the Fermat period of p, we obtain

$$c^{2^L} \equiv c \pmod{p}, \tag{16}$$

which is equivalent to

$$c(c-1) \sum_{\nu=0}^{2^L-2} c^\nu \equiv 0 \pmod{p}. \tag{17}$$

Notice that $c \equiv 0$ gives $F_{b,r} \equiv 1 \pmod{p}$ contradicting the eliteness of p. The solution $c \equiv 1$ only leads, as we have seen in the proof to Theorem 2.9, to $L = 1$. Hence, for $L > 1$,

$$\sum_{\nu=0}^{2^L-2} c^\nu \equiv 0 \pmod{p}. \tag{18}$$

The well-known fact that the left side geometric sum sums up to the fraction $\frac{c^{2^L-1}-1}{c-1}$ completes the proof. □

For the special case $L = 2$ we therefore get the following necessary condition.

Corollary 2.12. *Let b be a natural number and let p be a b-elite prime number with $L = 2$. Then $p \equiv 1 \pmod{3}$.*

Proof. If p is b-elite with $L = 2$ then there must exist a solution c to the Diophantine equation

$$c^2 + c + 1 = kp, \tag{19}$$

where k is an appropriate natural number. This equation has the two solutions

$$c_1 = \frac{-1 + \sqrt{4kp - 3}}{2} \quad \text{and} \quad c_2 = \frac{-1 - \sqrt{4kp - 3}}{2},$$

which are natural numbers only if $\sqrt{4kp-3}$ is a natural number, i.e., 4kp-3 is a perfect square. Therefore there exists a solution to the quadratic congruential equation $x^2 \equiv -3$ (mod 4p) and hence $\left(\frac{-3}{4p}\right) = 1$. Now we have

$$\left(\frac{-3}{4p}\right) = \left(\frac{-3}{4}\right)\left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

A simple computation shows that $\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1 \pmod 3$. □

This latter Corollary is used for the proof of a necessary and sufficient characterization of elites with $L = 2$.

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 $\left(\frac{b}{p}\right) = 1$.*

Proof. 1) Let p be b-elite with $L = 2$. By Corollary 2.12 we know that the even number $p - 1$ is a multiple of 3. Hence $\frac{p-1}{6}$ is a natural number. From group theory we get the fact that our two Fermat remainders can be considered to be members of a cyclic subgroup G of order 6 and index $\omega := \frac{p-1}{6}$. This means that there is a primitive root a modulo p, such that the numbers $a^{\omega n}$ with $n = 0, 1, \ldots, 5$ represent the elements of G. As a^{2l} is a quadratic residue modulo p for all natural number l, we see that ω is odd, i.e., $p \equiv 7 \pmod{12}$. This implies that there is a natural number k such that $p = 12k + 7 = 2(6k + 3) + 1$, i.e., $r = 1$ and $h = 6k + 3$. Hence $b^8 \equiv b^2 \pmod p$ which is equivalent to

$$b^6 - 1 = (b-1)(b+1)(b^2+b+1)(b^2-b+1) \equiv 0 \pmod p. \tag{20}$$

As $b \equiv \pm 1 \pmod p$ leads to $L = 1$, either $b^2 + 1 \equiv b$ or $b^2 + 1 \equiv -b \pmod p$ has to be fulfilled. Notice that $b^2 + 1$ is a quadratic non-residue modulo p.

2) We now turn to showing the reverse implication. Let $p \equiv 7 \pmod{12}$.

i) If $b^2 + 1 \equiv b \pmod p$ with $\left(\frac{b}{p}\right) = -1$ then we obtain

$$-1 = \left(\frac{b}{p}\right) = \left(\frac{b^2+1}{p}\right), \tag{21}$$

i.e., $F_{b,r}$ is a quadratic non-residue modulo p. Moreover, we get

$$b^4 + 1 \;=\; \left((b^2+1) - 1\right)^2 + 1 \equiv -(b-1) \pmod p, \tag{22}$$

where $\left(\frac{-(b-1)}{p}\right) = -1$ because $p \equiv -1 \pmod 4$. Finally,

$$b^8 + 1 = \left((b^4+1) - 1\right)^2 + 1 \equiv b^2 + 1 \pmod p. \tag{23}$$

So $F_{b,r+2} \equiv F_{b,r} \pmod p$ and therefore, p is b-elite with $L = 2$.

ii) The case $b^2 + 1 \equiv -b \pmod p$ with $\left(\frac{b}{p}\right) = 1$ works in total analogy to the subpoint i). □

Remarks: 1) Theorem 2.13 implies that for any given b there are only finitely many b-elite primes p with $L = 2$. Notice that for all primes p larger than $b^2 + b + 1$ the congruence $b^2 + 1 \equiv \pm b \pmod{p}$ cannot be fulfilled any more. Hence, for the special case $b = 2$ the only elite prime with $L = 2$ is $p = 7$.

2) It is easy to see that $b^2 + 1 \equiv b \pmod{p}$ if and only if $(b-1)^2 + 1 \equiv -(b-1) \pmod{p}$, such that we always find pairs $(b, b-1)$ of bases to which p is b-elite, resp. $(b-1)$-elite with $L = 2$.

3) Since the cases $L = 1$ and $L = 2$ are fully characterized by Theorems 2.9 and 2.13, we will call "elite periods" of these two lengths *trivial* periods.

Finally, there is a necessary and sufficient condition for a prime p to be b-elite.

Theorem 2.14. *Let $p = 2^r \cdot h + 1$ be a prime number where $r \geq 1$ and h is odd. Then p is b-elite if and only if the multiplicative order of $F_{b,n} \pmod{p}$ is a multiple of 2^r for all $n = r, \ldots, r + L - 1$.*

Proof. This theorem is an immediate consequence of Euler's criterion, which guarantees that the congruence $F_{b,n}^{\frac{p-1}{2}} \equiv \left(\frac{F_{b,n}}{p}\right) \pmod{p}$ holds for every prime number p, and hence $\left(\frac{F_{b,n}}{p}\right) = -1$ if and only if 2^r divides the multiplicative order of $F_{b,n}$ modulo p. □

2.4 Non-elite primes

To every given prime number p is there always a base b such that p is b-elite? The answer to this is no.

Theorem 2.15. *Let $p = 2^{2^n} + 1$ be a prime Fermat number with $n \geq 2$. Then p is not b-elite for all natural numbers b.*

Proof. If $n \geq 2$ then $p = 2^{2^n} + 1 \equiv 1 \pmod{8}$, so that we get $\left(\frac{2}{p}\right) = 1$. Additionally, Fermat's little theorem guarantees that

$$F_{b,2^n+m} = \left(b^{2^m}\right)^{2^{2^n}} + 1 \equiv 2 \pmod{p} \tag{24}$$

for any given base $b \not\equiv 0 \pmod{p}$ and for all natural numbers m. So there are infinitely many different GFNs $F_{b,k}$ with $\left(\frac{F_{b,k}}{p}\right) = 1$. The fact that for $b \equiv 0 \pmod{p}$ the prime number p is not b-elite was already established in Observation 2.1. □

This latter theorem concerns the primes $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$ which are b-elite for no base b. Furthermore, one may ask whether there are other prime numbers which are never b-elite for all natural numbers b. Especially the numbers of the form $p = 24k - 1$ seem most likely in this respect. And indeed, we can use Theorem 2.6 to characterize a special family of Sophie Germain primes that always are such *non-elite* primes!

Theorem 2.16. *Let l be a natural number such that $q_1 := 2l + 1$, $q := 4l + 3$ and $p := 8l + 7$ are primes. Then p is non-elite.*

Proof. Suppose that there is a natural number b such that p is b-elite. We see that $p \equiv -1 \pmod 8$ and $p = 2(4l+3)+1$, i.e., $r = 1$ and $h = 4l+3 = q$ in the notation of Theorem 2.6. We know that the multiplicative order of a natural number b modulo p has the form $2^s t$, where $s \leq r$ and t is a divisor of h. Hence, this multiplicative order of b equals $1, 2, q$ or $2q$. The first two cases are given by $t = 1$ which implies $L = 1$, in order that p cannot be b-elite by Theorem 2.9.

So we have $t = q$. Theorem 2.6 now states, that L equals the multiplicative order of 2 modulo q. This order has to be a divisor of $\phi(q) = 2q_1$, i.e., 1, 2, q_1 or $2q_1$. Here again, the case $L = 1$ is forbidden. Since $l \equiv -1 \pmod 3$, we have $p \equiv -1 \pmod 3$ as well, and so $L = 2$ is also contradicting the possible eliteness of p. In fact, $l \equiv 0 \pmod 3$ would lead to a composite q, while $l \equiv 1 \pmod 3$ implies that q_1 is not a prime.

Moreover, the case $L = q_1$ is impossible because $L > 1$ has to be an even number (Theorem 2.7). Finally, only $L = 2q_1$ seems compatible to the eliteness of p. But, by Theorem 2.8 we obtain the contradiction $L = 2q_1 > q_1 + 1 = \frac{p+1}{4} \geq L$. This means that p is non-elite. □

Remark: The first ten primes p with the properties of Theorem 2.16 are 23, 47, 167, 359, 719, 1439, 2039, 2879, 4079 and 4127. In this context, so called Cunningham chains, i.e., sequences of primes "with each member one more than twice the previous one", are of interest. Compare in this respect section A7 of Guy's problems book [8] or the chapter on Sophie Germain primes in the book of Ribenboim [13, p. 233ff].

It seems that there are many different kinds of non-elite primes. A lot of them actually have the form $24k-1$. But notice that not all primes of this shape are non-elite! A first counterexample is $p = 1871$ which is b-elite for

$$b \in \{33, 217, 293, 314, 323, 388, 447, 567, 782, 864\},$$

where $b \leq \frac{p-1}{2}$ and the Fermat period has length $L = 10$. Another interesting fact is that there are also non-elites of the form $8k+1$ which are not Fermat primes.

Theorem 2.17. *Let h be an odd prime number such that the multiplicative order of 2 modulo h is equal to an odd number. Then all primes of the form $2^r \cdot h + 1$ with $r \geq 3$ are non-elite.*

Proof. Let b be a natural number with multiplicative order $2^s t$ modulo $p = 2^r h + 1$. Then we have either $t = 1$ or $t = h$. The first case has to be excluded since for all $r \geq 3$ there is $p \equiv 1 \pmod 8$ and therefore $L \neq 1$ by Theorem 2.9. Now $t = h$ gives an odd multiplicative order to 2, such that L is odd and hence p is not b-elite by Theorem 2.7. □

Remark: The first prime number fulfilling the condition of the latter theorem is $h = 7$, such that all primes of the form $p = 2^r \cdot 7 + 1$ with $r \geq 3$ are non-elite, i.e., the primes $p \in \{113, 449, 114689, 7340033, 469762049, \ldots\}$.

Further examples are $h \in \{23, 31, 47, 71, 73, 79, 89, 103, 127, 151, 167, \ldots\}$. Notice that all non-elite primes provided by Theorem 2.16 can actually be used as h in Theorem 2.17! More generally, every odd prime of the form $h = 8k-1 = 2(4k-1)+1$ is suitable. To see this, use Euler's criterion. We obtain

$$2^{4k-1} = 2^{\frac{h-1}{2}} \equiv \left(\frac{2}{h}\right) = 1 \pmod{h}, \tag{25}$$

because $h \equiv -1 \pmod 8$. This implies that the multiplicative order of 2 modulo h is a divisor of the odd number $4k-1$. Therefore the length L of the Fermat period of $2^r \cdot h + 1$ is odd, which makes impossible any eliteness for $r \geq 3$.

Moreover, we found other types of $8k+1$ non-elite primes not characterized by the latter result. E.g., the primes $73 = 2^3 \cdot 9 + 1$, $89 = 2^3 \cdot 11 + 1$ or $97 = 2^5 \cdot 3 + 1$ are non-elites.

To conclude this section, we can summarize that the two incongruent residue classes modulo 8 which do not produce trivial eliteness with $L = 1$, actually have both elite and non-elite prime members. See section 4 for elite primes of the form $8k+1$.

2.5 Algebraic structures of bases modulo several classes of primes

Let us now have a group theoretical view on the periodicity of the Fermat remainders. Here again we consider primes of the form $p = 2^r h + 1$ where h denotes an odd number. All bases and Fermat remainders $\pmod p$ are elements of the set $\mathbb{N}_p$ of prime residue classes $\pmod p$ which forms a group with the multiplication $\pmod p$.

We already saw above that if a prime p is b-elite then every Fermat remainder $F_{b,\nu}$ in the period has to be a quadratic non-residue. Consequently, every $Q_{b,\nu} := F_{b,\nu} - 1 = b^{2^\nu}$ has to be a quadratic residue $\pmod p$ for $\nu \neq 0$.

By Theorem 2.6 the period begins at least with $c := Q_{b,r}$ for all bases b. This gives us the relation

$$b^{2^r} \equiv c \qquad \pmod{p}. \tag{26}$$

It is well-known that this equation has 2^r solutions in b for a fixed c being a 2^r-residue (compare, e.g., [12, Theorem 2.27, p. 49]). Depending on the choice of b all c's in the period can be interpreted in this way. Therefore all elements in a period are 2^r-residues. The subset R_{2^r} of all 2^r-residues in $\mathbb{N}_p$ is a subgroup of order h. Elements of R_{2^r} may belong to many different periods of various lengths and only some of them may give rise to the eliteness property. With $c \in R_{2^r}$ and a primitive root ρ modulo p it is obvious that

$$\operatorname{ind}_\rho c = k \cdot 2^r \qquad \pmod{\phi(p)} \tag{27}$$

is solved by a $k \in \mathbb{N}$. Because of $\phi(p) = h \cdot 2^r$ we can "divide" this latter equation by 2^r and we get

$$2^{-r} \cdot \operatorname{ind}_\rho c = k \qquad \pmod{h}. \tag{28}$$

It is clear that k admits all values in the range $[0, h-1] \cap \mathbb{N}_0$. Therefore, we get a one to one correspondence between a given k and c by fixing the parameter ρ and for the given r. Notice that once again we get the important consequence that the length of a period is not depending on r. Moreover, a repeated squaring of c modulo p is equivalent to a repeated multiplication of k by 2 modulo h. All this implies the following result.

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*

$$\sum_{i=1}^{n} L_i = h. \tag{29}$$

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

$$N_{b,i} = 2^r \cdot L_i. \tag{30}$$

Remark: Applying this argument to our Diophantine equation (15), we see that this expression has at most h solutions, all of them being elements of the set R_{2^r}.

3 Computational methods

Now there are two ways to compute elite primes: one method consists in searching for primes which are elite to a given base $b \in \mathbb{N}$ while the other approach searches for all bases to which a given prime number is elite.

All the previous papers used algorithms of the first case for the base $b = 2$. Here one has to determine all Fermat remainders in the period and to test each one of them as to whether it is a quadratic residue or not. Based on Theorem 2.14 we can formulate an algorithm which uses the multiplicative order to check b-eliteness of a given prime number p. A second possibility was given by evaluating the Legendre symbols $\left(\frac{F_{r+n,2}}{p}\right)$ for every prime candidate p and $n = 0, \ldots, L-1$. To get a test for any given base b one could easily modify these types of algorithms.

For the second case one could adapt the following procedure: Generate all possible values for b and test it by using one of the above algorithms. But, as we saw in the theoretical section dealing with the algebraic structures of bases, there can be many such b's especially for large r's.

So a better approach would be to use only the 2^r-residues described in the previous section and check them one by one if they are quadratic non-residues modulo p or not. A pseudocode for this procedure could read:

```
01 p := h * 2^r + 1
02 g := primitive root MOD p
03 tested := boolean vector initialized false
04 period_start := 0
05 WHILE period_start < h DO
06   index := period_start
07   flag_elite := true
08   DO
09     tested[index] = true
10     IF g^(index*2^r) residue MOD p THEN flag_elite := false
11     index := 2*index MOD h
12   OD WHILE index <> period_start
13   IF flag_elite = true THEN
14     PRINT 'Tested prime is elite'
15     STOP
16   FI
17   WHILE tested[period_start] DO
18     period_start := period_start + 1
19   OD
20 OD
```

For a given prime number `p` line `02` generates a primitive root `g` modulo `p`. In line `03` a boolean vector is initialized by setting all components of the vector to `false`. During the test every 2^r-residue `g^(index*2^r)` that has been tested is marked by putting the component `tested[index]` to `true` (line `09`).

With line `05` a loop is started which searches for a new period when the previous one has been finished; the loop of the lines `17` to `19` increments `period_start` until the beginning of a new period is found.

The `do-while` loop in the lines `08` to `12` implements the test for every part of the actual period. If a residue fails the test then `flag_elite` is set to `false` in order to allow the continuation of the test. The `if` condition in line `13` causes the program to stop when `flag_elite` is still `true`. In that case, the tested period is elite and so the prime `p` has been found to be a generalized elite. If all periods are tested without an eliteness result, then `p` has been identified as a non-elite prime.

The algorithm presented here stops when a first elite period is found. It is easy to modify the algorithm in order to find all elite periods and hence all bases b to which a given prime number p is b-elite.

4 Observations and conjectures

4.1 Observations

Denote by E_b the set of all b-elite primes and define

$$E := \bigcup_{b \in \mathbb{N}} E_b. \tag{31}$$

By Theorem 2.9 we know that E is infinite since all primes of the form $p = 8k \pm 3$ are $(p-1)$-elite. Moreover, this implies that for all $x > 0$ the number $N(x)$ of the elements of E not exceeding x is $N(x) \asymp x \cdot \ln^{-1}(x)$.

It seemed that there were no elite primes p of the form $p = 24k - 1$ ($k \in \mathbb{N}$). But one counterexample is given for $k = 78$ yielding the prime $p = 1871$ which is elite to the bases $b = 33, 217, 293, 314, 323, 388, 447, 567, 782, 864 \leq \frac{p-1}{2}$ with $L = 10$. Elite primes of this special form seem to be very rare. In fact there exists no other counterexample of this form less than 10^4.

The period length L for a given elite prime p is often $L = 4$. We found the first elite prime with $L = 6$ to be $p = 199$ (smallest base $b = 19$). The prime $p = 409$ is the smallest elite with $L = 8$ ($b = 6$), while the first elite with $L = 10$ is $p = 331$ ($b = 23$). A period length of $L = 12$ is first realized by the elite prime $p = 3121$ ($b = 8$). There are no elite primes $p < 10^4$ with $L > 12$.

Theorem 2.18 implies that for a given prime number p there can be different periods depending on the choice of the bases b. Now it is possible that more than one of these different periods fulfill the generalized eliteness property. Moreover, it is possible that these different elite periods have different lengths. The smallest elite prime with two different non-trivial elite periods is $p = 181$ (since $181 \equiv 5 \pmod 8$ it is 180-elite with $L = 1$). Both periods have the length $L = 4$, the first being produced by the smallest base $b = 5$ the second by $b = 6$. The prime number $p = 5101$ has three non-trivial elite periods. Two of them have $L = 4$ (with the smallest bases $b = 123$, resp. $b = 146$). The third period has length $L = 8$ and turns up, e.g., for $b = 366$. Similar properties are shared by $p = 6121$. The prime $p = 8581$ has exactly two non-trivial elite periods with different lengths. One elite period has $L = 4$ ($b = 314$), the other $L = 12$ ($b = 98$).

4.2 Conjectures

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

Most of the bases b actually have the primes 3 or 5 as b-elites. Only the bases $b \equiv 0 \pmod{15}$ do not belong to one of these two "trivial" families.

Conjecture 4.2. *There are generalized elite primes with elite periods of arbitrarily large lengths.*

This conjecture seems to be supported by our computations. We found a generalized elite prime $p < 10^4$ with $L = 12$. Moreover, there is a 2-elite prime known with $L = 20$ (compare [5]).

Conjecture 4.3. *There are infinitely many non-elite primes.*

It is well-known that there are infinitely many primes of the form $h = 8k - 1$. Perhaps there are also infinitely many such primes for which there is an $r \geq 3$ such that $p = 2^r \cdot h + 1$ is prime. If this were true, Theorem 2.17 would imply that there are infinitely many non-elite primes.

Acknowledgement

The authors thank the friendly referee for his help in improving this 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] P. Bundschuh, *Einführung in die Zahlentheorie*, Springer, 1998.

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

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

[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] R. K. Guy, *Unsolved Problem in Number Theory*, Springer, 2004.

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

[10] M. Křížek, F. Luca and L. Somer, On the convergence of series of reciprocals of primes related to the Fermat numbers. *J. Number Theory* **97** (2002), 95–112.

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

[12] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, Wiley & Sons, 1972.

[13] P. Ribenboim, *Die Welt der Primzahlen. Geheimnisse und Rekorde*, Springer, 2006.

[14] 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 11A15; Secondary 11A41.
Keywords: elite primes, generalized Fermat numbers.

(Concerned with sequence A102742.)

Received May 8 2008; revised version received July 8 2008. Published in *Journal of Integer Sequences*, July 25 2008.

Return to Journal of Integer Sequences home page.