Searching for Large Elite Primes

Tom Müller

CONTENTS

A prime number p is called elite if only finitely many Fermat numbers $2^{2^n}+1$ are quadratic residues modulo p. Previously, only fourteen elite primes were known explicitly, all of them smaller than 35 million. Using computers, we searched all primes less than 10^9 for other elite primes and discovered $p = 159\,318\,017$ and $p = 446\,960\,641$ as the fifteenth and sixteenth elite primes. Moreover, with another approach we found 26 other elite primes larger than a billion, the largest of which has 1172 decimal digits. Finally, we derive some conjectures about elite primes from the results of our computations.

1. INTRODUCTION

Fermat numbers are numbers of the form $F_n := 2^{2^n}+1$. They were named after the French mathematician Pierre de Fermat (1601–1665), who demonstrated that the five numbers $F_0, F_1, \ldots, F_4$ are prime and conjectured that these numbers might be prime for all F_n. This claim was disproved by Euler, when he found the divisor 641 to F_5. No Fermat prime has since been found, and it was conjectured by Hardy and Wright [Hardy and Wright 79] that their number is finite. For further open problems on Fermat numbers see Richard Guy's famous book [Guy 04]. We call a prime number p *elite* if there is an integer index m for which all F_n with $n > m$ are quadratic nonresidues modulo p, i.e., there is no solution to the congruence $x^2 \equiv F_n \bmod p$ for all $n > m$.

Elite primes were defined and first studied by Alexander Aigner [Aigner 86], who discovered 14 such numbers with values less than 35 million. No other elite prime was thereafter explicitly given, nor is it known whether there are infinitely many of them. An important result in this context is a theorem of Křížek, Luca, and Somer [Křížek et al. 02] that the (possibly infinite) sum of the reciprocals of all elite primes is finite. Their method is based on a study of the distribution of such numbers, showing that the set of all elite primes is not sufficiently "dense" to produce divergence.

The purpose of this paper is to present some new results about elite primes. In a computational search we

2000 AMS Subject Classification: 11A15, 11A41

Keywords: elite primes, Fermat numbers

1058-6458/2006 $0.50 per page
Experimental Mathematics **15**:2, page 183

were able to find 28 hitherto unknown elite primes. The algorithms are based on a necessary and sufficient arithmetic property proved in the following section. A final section deals with a number of open problems and conjectures concerning elite primes.

2. PRELIMINARIES

Due to the well-known relation

$$F_{n+1} = (F_n - 1)^2 + 1 \tag{2–1}$$

for Fermat numbers, it is obvious that for any prime number p, the congruences $F_n \bmod p$ will eventually become periodic. Aigner [Aigner 86] showed that for any prime number written in the form $p = 2^r h + 1$ with $r \in \mathbb{N}$ and $h \geq 1$ odd, this period begins at the latest with the term F_r. We call L the *length of the Fermat period* if L is the smallest natural number satisfying the congruence $F_{r+L} \equiv F_r \bmod p$. The terms $F_{r+\nu} \bmod p$ with $\nu = 0, \ldots, L-1$ are called *Fermat remainders* of p. Therefore, a prime number p is elite if and only if all L Fermat remainders are quadratic nonresidues modulo p. Moreover, it is known that for $p > 10$ it is a necessary condition for eliteness that L be an even number smaller than $\frac{p-1}{4}$ (see [Aigner 86]). The following result gives another characterization of elite primes, one very appropriate for practical use.

Theorem 2.1. *Let $p = 2^r h + 1$ be a prime number with h odd. Then p is elite if and only if the multiplicative order of every Fermat remainder is a multiple of 2^r modulo p.*

Proof: Let $p = 2^r h + 1$ be a prime number with h odd. Let f be a Fermat remainder of p that is a quadratic nonresidue modulo p. Since the multiplicative order modulo p of any natural number has to be a divisor of $\varphi(p) = p - 1 = 2^r h$, the multiplicative order of f is of the form $d = 2^q k$ with $q \leq r$ and $k \mid h$. Then by Euler's criterion, we obtain the congruence

$$f^{2^{r-1}h} \equiv \left(\frac{f}{p}\right) = -1 \bmod p,$$

where $\left(\frac{f}{p}\right)$ is the Legendre symbol. This implies that $q = r$. If, on the other hand, the multiplicative order is a multiple of 2^r, then f cannot be a quadratic residue modulo p, since we have $f^{\frac{p-1}{2}} \not\equiv 1 \bmod p$, which again with Euler is equivalent to $\left(\frac{f}{p}\right) \neq 1$. □

In practice, the Fermat periods of elite primes are of particularly small lengths L. Indeed, for all examples known to date, we have $L \leq 12$, with a striking trend of $L = 4$. For nonelite primes, on the other hand, in most cases there exists among the very first Fermat remainders one that fails Theorem 2.1. Therefore, it is quite simple using computers to check any given prime number p for eliteness.

3. THE METHOD

The algorithm for checking a given prime number $p = 2^r h + 1$ for eliteness is based on Theorem 2.1. We have seen that the Fermat period modulo p begins with the term F_r; so, using relation (2–1) modulo p, the first Fermat remainder $F_r \bmod p$ can be easily computed. The pseudocode of our eliteness test appears as Algorithm 3.1

Algorithm 3.1.

```
01 f[0] := (F_r mod p)
02 f := f[0]
03 bvar := false

04 WHILE bvar = false DO
05   k := (f^h mod p)
06   IF k = 1 THEN bvar := true AND STOP FI
07     FOR var = 0 to r − 2 DO
08       k := (k^2 mod p)
09       IF k = 1 THEN bvar := true AND STOP FI
10     OD
11   f := ((f − 1)^2 + 1 mod p)
12   IF f = f[0] THEN bvar := true FI
13 OD
```

The algorithm generates the Fermat remainders f of p: the first one in line `02`, the following ones in line `11`. For every given f the algorithm checks whether its multiplicative order modulo p is a multiple of 2^r (lines `06` to `10`). Thus the program has two ways in which it can end: First, the `WHILE` loop terminates when the condition `f = f[0]` in line `12` is satisfied, i.e., an entire Fermat period (of length L) has been successfully checked. So, if the algorithm ends with the results `bvar = true` and `f = f[0]`, then p is elite. The second possibility for termination occurs at line `06` or in the `FOR` loop after line `09`. In such cases we have found a Fermat remainder that fails the condition of Theorem 2.1, and hence p is not elite. Both possibilities need a worst-case number of arbitrary precision multiplications of $O(L \cdot r)$. However, during our computations nonelite primes p generally produced Fermat remainders, leading very quickly to the end of the computation in line `06` or `09`.

The question still remaining is how to find the prime numbers p. Our first goal was to search for all elite primes in the range up to one billion. For this, with the help of a variation of the well-known sieve method of Eratosthenes, we produced a list of all primes in the interval $[2, 10^9]$, followed by some preliminary checks based on a congruence criterion already proved by Aigner in his above-mentioned paper. These checks disqualified a large number of primes. The remaining prime numbers were tested one by one using Algorithm 3.1. A second approach made use of the fact that all of the larger elite primes found previously have the form $p = 2^r h + 1$ with $r \geq 3$ and h odd. Especially when r is large enough for 2^r to be larger than h, the numbers p can very easily be checked for primality with the following well-known criterion.

Theorem 3.2. *Let $r \geq 2$, $2^r > h$ odd, and $p = 2^r \cdot h + 1$ a quadratic nonresidue modulo q for some odd prime q. Then a necessary and sufficient condition for p to be a prime is that*

$$q^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

This result is Theorem 102 of [Hardy and Wright 79], where a proof is given. Considering this, we searched all prime numbers of the form $2^r h+1$ with $2^r > h$, $r \leq 1000$ for $h \leq 5001$, and $r \leq 500$ for $5003 \leq h \leq 15001$ odd. These again were checked one by one for eliteness.

4. THE RESULTS

Our first approach, i.e., searching all elite primes in the interval $[2, 10^9]$, ended up with two previously unknown elite primes. Thus there are altogether 16 elite primes less than one billion. These are as follows:

3, 5, 7, 41, 15 361, 23 041, 26 881, 61 441, 87 041,
163 841, 544 001, 604 801, 6 684 673, 14 172 161,
159 318 017, 446 960 641.

The first 14 of these numbers were discovered by Aigner in 1986. The two new items have Fermat periods of lengths 8 and 4. These results are summarized in sequence A102742 of Neil Sloane's *On-Line Encyclopedia of Integer Sequences* [Sloane 05]. In our second computational project we found 23 further elite primes greater than one billion. Their parameters are listed in Table 1.

A glance at this table shows that the parameter $h = 15$ appears to be quite favorable to the production of elite primes. That is why we extended the search to numbers of the form $p = 2^r \cdot 15 + 1$ with $r < 5000$. And indeed, three further elite prime numbers were found with $2^{1518} \cdot 15 + 1$, $2^{2875} \cdot 15 + 1$, and $2^{3888} \cdot 15 + 1$. These three elite primes all have Fermat period of length $L = 4$ and respectively 459, 867, and 1172 decimal digits. The computations were carried out on a PC with a Pentium-I processor and on two Pentium-III computers. The search among all the numbers up to 10^9 took an average CPU time of 910 seconds (just over 15 minutes) per interval of one million numbers, so that for this part of the project some 253 hours of CPU time were needed. The computations that yielded the large elite primes consumed about 60 CPU hours.

h	r	L	digits	h	r	L	digits
5	55	4	18	855	478	4	147
15	37	4	13	949	142	12	46
15	900	4	273	969	273	8	86
17	471	8	144	1875	172	4	56
165	352	4	109	3717	351	6	110
255	71	4	24	3865	82	4	29
395	839	4	256	3985	52	4	20
425	31	4	12	4365	35	4	15
645	113	4	37	4545	23	4	11
745	138	4	45	7701	156	8	51
765	22	4	10	9575	145	4	48
				10425	135	4	45

TABLE 1. Large elite primes of the form $2^r h + 1$.

5. CONJECTURES

Considering the results of our computations, we would like to formulate some conjectures on some unsolved problems related to elite primes.

Conjecture 5.1. *The number of elite primes is infinite.*

Conjecture 5.2. *The number of elite primes of the form $2^r \cdot 15 + 1$ is infinite.*

These two conjectures seem anything but easy to settle. But if they are true (or at least the first one), it makes sense to make an additional conjecture:

Conjecture 5.3. *The lengths of the Fermat periods of elite primes are unbounded. That is, there are elite primes with arbitrarily large L.*

In 2002, Křížek, Luca, and Somer [Křížek et al. 02] proved that the number $N(x)$ of elite primes less than or

equal to x has the asymptotic bound

$$N(x) = O\left(\frac{x}{(\log x)^2}\right)$$

as $x \to \infty$. It seems that this upper bound is probably too coarse. The trend given by our computations indicates a much lower bound.

Conjecture 5.4. *There exists a constant $c \geq 1$ such that $N(x) = O(\log^c x)$ as $x \to \infty$.*

Perhaps we can choose $c = 1$.

ACKNOWLEDGMENTS

The author wishes to thank Alain Chaumont for a copy of Křížek's paper. Thanks are due to Beppo for computational resources and to Andreas Reinhart for his help in finalizing the algorithmic section.

REFERENCES

[Aigner 86] A. Aigner. "Über Primzahlen, nach denen (fast) alle Fermatzahlen quadratische Nichtreste sind." *Monatshefte Mathematik* 101 (1986), 85–93.

[Guy 04] R. K. Guy. *Unsolved Problems in Number Theory*. Third edition. New York: Springer, 2004.

[Hardy and Wright 79] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Fifth edition. Oxford: Academic Press, 1979.

[Křížek et al. 02] M. Křížek, F. Luca, and L. Somer. "On the convergence of series of reciprocals of primes related to the Fermat numbers." *Journal of Number Theory* 97 (2002), 95–112.

[Sloane 05] N. Sloane. "Online Encyclopedia of Integer Sequences (OEIS)." Available online at (http://www.research.att.com/~njas/sequences/).

Tom Müller, Institut für Cusanus-Forschung an der Universität und der Theologischen Fakultät Trier, 54290 Trier, Germany, (muel4503@uni-trier.de)

Received June 12, 2005; accepted September 20, 2005.