Journal of Integer Sequences, Vol. 9 (2006),
Article 06.3.8

All Elite Primes Up to 250 Billion

Alain Chaumont
Laboratoire de Modélisation et Simulations Moléculaires “MSM”
Université Louis Pasteur
4, rue B. Pascal
67000 Strasbourg
France
chaumont@chimie.u-strasbg.fr

Tom Müller
Institut für Cusanus-Forschung
Universität Trier
Domfreihof 3
54290 Trier
Germany
muel4503@uni-trier.de

Abstract

A prime number p is called *elite* if only finitely many Fermat numbers $2^{2^n}+1$ are quadratic residues of p. Previously only the interval up to 10^9 was systematically searched for elite primes and 16 such primes were found. We extended this research up to $2.5 \cdot 10^{11}$ and found five further elites, among which 1 151 139 841 is the smallest and 171 727 482 881 the largest.

1 Introduction

Let $\{F_n\}$ with $F_n := 2^{2^n}+1$ denote the sequence of Fermat numbers. Further details on these numbers, some of their properties and open problems can be found, e.g., in the work of Hardy and Wright [3], in section A3 of Guy's problem book [2] or in the *17 lectures* on this topic by Křížek, Luca and Somer [4].

We call a prime number p *elite*, if there is an integer index m for which all F_n with $n > m$ are quadratic non-residues of p, i.e., there is no solution to the congruence $x^2 \equiv F_n \pmod{p}$

for $n > m$. Alexander Aigner [1], who first defined and studied elite primes, discovered 14 such numbers with values less than 35 million. Two further primes less than 10^9 were found by the second author [6]. All these primes are summarized in Table 1.

elite primes	discovered
3, 5, 7, 41, 15361, 23041, 26881, 61441, 87041, 163841, 544001, 604801, 6684673, 14172161	Aigner (1986)
159318017, 446960641	Müller (2005)

Table 1: All elite primes $< 10^9$

A further important result was given by Křížek, Luca and Somer [5] with a theorem assuring that the series S of the reciprocals of all elite primes is convergent. They proved their claim by showing that the number $N(x)$ of elite primes less than or equal to x is asymptotically bounded by the same functions as prime twins are, i.e.,

$$N(x) = O\left(\frac{x}{(\log x)^2}\right). \tag{1}$$

Further computations of larger elite primes [6] suggested moreover that the asymptotic (1) is rather rough and could perhaps be lowered to

$$N(x) = O\left((\log x)^c\right), \tag{2}$$

with an option for $c = 1$. This would mean that all larger interval of the form $[10^n, 10^{n+1}]$ should contain a more or less constant number of elite primes.

The purpose of the project presented in this paper was to find all elite primes up to $2.5 \cdot 10^{11}$. These results seem to confirm conjecture (2).

2 Preliminaries

From the well-known relation for Fermat numbers

$$F_{n+1} = (F_n - 1)^2 + 1 \tag{3}$$

it is obvious that for any prime number p, the residues $F_n \bmod p$ are ultimately periodic. Aigner [1] 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 fulfilling the congruence $F_{r+L} \equiv F_r \pmod p$. 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 non-residues modulo p. It is moreover known that for all $p > 10$ it is a necessary condition for eliteness that L is an even number smaller than $\frac{p-1}{4}$ (compare [1]).

But it seems that the Fermat periods of elite primes are very often of particularly small length L. Actually, for all examples known to date [6], we have $L \leq 12$ with a vast majority of cases where $L = 4$.

3 The method

First, we constructed all prime numbers in the range up to 250 billion with the help of a variant of the well-known sieve method of Erathostenes. It is proved in [1] that prime numbers of the form $p = 120k + a$ with $k \in \mathbb{N}$ and $a \in \{11, 13, 19, 23, 31, 47, 59, 61, 71, 79, 91, 109, 119\}$ cannot be elite, so that a simple preliminary congruential test combined with some elementary results on quadratic residues already allowed one to eliminate a large number of candidates. All the remaining prime numbers were tested one by one using an algorithm based on the following necessary and sufficient condition:

Theorem 3.1. *Let $p = 2^r h + 1$ be a prime number with h odd. Then p is elite if and only if every Fermat remainder has a multiplicative order modulo p being a multiple of 2^r.*

So, if f denotes a given Fermat remainder of a prime $p = 2^r h + 1$, the algorithm checked whether the congruence

$$f^{2^k h} \equiv 1 \pmod{p} \tag{4}$$

is solvable only for $k = r$. If this is fulfilled, equation (4) is solved for the next Fermat remainder of p and so on, until either an entire Fermat period is successfully checked and hence p is elite, or a Fermat remainder f is found with $k < r$ in (4) leading to a negative answer regarding the eliteness of p (compare [6]).

As in all known cases elite primes have Fermat periods of rather small length and moreover almost all non-elite primes in our research presented rather quickly a Fermat remainder contradicting the sufficient condition of theorem 3.1, the computational effort needed for testing a given p turned out to be on average equivalent to five Fermat-tests.

4 The results

In the interval $[10^9, 2.5 \cdot 10^{11}]$ we found five elite primes. Two primes were found between 10^9 and 10^{10}, while the set of elite primes contained in the interval $[10^{10}, 3 \cdot 10^{10}]$ is empty. Only one further elite was discovered smaller than 100 billion. Two supplementary primes turned up between 10^{11} and $2 \cdot 10^{11}$. The final subinterval again turned out to be "elite-free". These elite primes are listed in Table 2 together with the respective length L of their Fermat period.

So, there are 21 elite prime numbers less than 250 billion and in total 45 such primes known to date.

p	L
1 151 139 841	4
3 208 642 561	4
38 126 223 361	4
108 905 103 361	4
171 727 482 881	8

Table 2: All elite primes between 10^9 and 250 billion

The results of this section as well as the known numbers presented in the introduction are summarized in Sloane's OEIS A102742.

The several computations were run on a AMD Sempron 2600 XP+ and a Pentium-III-processed PC. A total CPU-time of about 1680 hours was needed to complete this project.

5 Interpretations and conjectures

It was conjectured that there are infinitely many elite primes. If this is so, it is certainly interesting to know more about their distribution among natural numbers. Table 3 gives a comparison of $N(x)$ and $\log x$ for some x in the interval $[10, 2.5 \cdot 10^{11}]$ suggesting that the growth of both functions is perhaps asymptotically the same.

x	$N(x)$	$\log x$
10	3	2.3
10^2	4	4.6
10^5	9	11.5
10^6	12	13.8
10^9	16	20.7
$2.5 \cdot 10^{11}$	21	26.2

Table 3: Comparison of $N(x)$ and $\log x$

Moreover, with the bound of $N(x)$ proved by Křížek and al. [5] we can now give the following value of the sum S of the series of reciprocals of all elite primes:

$$0.70 \leq S \leq 0.74, \tag{5}$$

i.e., the first digit after the decimal point is settled. Our conjectured bound would lead to seven more digits:

$$S = 0.700764011 \pm 0.12 \cdot 10^{-8}. \tag{6}$$

References

[1] A. Aigner, Über Primzahlen, nach denen (fast) alle Fermatzahlen quadratische Nichtreste sind, *Monatsh. Math.* **101** (1987), 85–93.

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

[3] G. H. Hardy, E. L. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1979.

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

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

[6] T. Müller, Searching for large elite primes, *Experiment. Math.* **15**:2 (2006), 183–186.

[7] 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, Fermat Numbers.

(Concerned with sequence A102742.)

Received January 18 2006; revised version received August 21 2006. Published in *Journal of Integer Sequences*, August 21 2006.

Return to Journal of Integer Sequences home page.