Journal of Integer Sequences, Vol. 10 (2007),
Article 07.9.4

On Anti-Elite Prime Numbers

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

Abstract

An odd prime number p is called anti-elite if only finitely many Fermat numbers are quadratic non-residues to p. This concept is the exact opposite to that of elite prime numbers. We study some fundamental properties of anti-elites and show that there are infinitely many of them. A computational search among all the numbers up to 100 billion yielded 84 anti-elite primes.

1 Introduction

Let $F_n := 2^{2^n} + 1$ be the sequence of Fermat numbers. In recent research some effort has been spent on so-called elite primes. A prime number p is called *elite* if there is an integer index m for which all F_n with $n > m$ are quadratic non-residues to p, i.e., there is no solution to the congruence $x^2 \equiv F_n \pmod{p}$ for $n > m$. Aigner [1], who first defined and studied elite primes, discovered 14 such numbers between 1 and 35 million. More computational effort yielded all 27 elites up to $2.5 \cdot 10^{12}$ together with some 60 much larger numbers [7, 3, 4]. Despite these results, the question whether there are infinitely many such numbers remains open.

The opposite concept of elite primes is the following. An odd prime number p is called *anti-elite* if only finitely many Fermat numbers are quadratic non-residues modulo p. Due to the well-known relation for Fermat numbers

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

it is obvious that for any prime number p the congruences $F_n \pmod{p}$ will become periodic at some point. Aigner showed that for any prime number written in the form $p = 2^r h + 1$

with $r \in \mathbb{N}$ and $h > 1$ 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 $F_{r+L} \equiv F_r \pmod{p}$. L can be computed in the following way. The multiplicative order of 2 modulo p is of the form $2^s k$ with $0 \leq s \leq r$ and k a divisor of h. Then L is the multiplicative order of 2 modulo k, i.e., $2^L \equiv 1 \pmod{k}$. [1]

The terms $F_{r+\nu} \pmod{p}$ with $\nu = 0, \ldots, L-1$ are called *Fermat remainders* of p. Therefore, a prime number p is anti-elite if and only if all L Fermat remainders are quadratic residues modulo p. Moreover, it is easy to see that against the concept of elites there is no necessary condition on the parity of L. That L has to be smaller than $\frac{p-1}{4}$ is still true (compare Aigner [1, pp. 89 et seq.]).

By partly adapting the proof given by Křížek, Luca and Somer [6] for elites we find that the number $N(x)$ of all anti-elite primes less than or equal to x is asymptotically bounded by

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

i.e., the series S of the reciprocals of all anti-elite primes is convergent. In the following section we will deal with some fundamental properties of anti-elite prime numbers. We show, inter alia, that there are infinitely many anti-elite primes. In addition to these theoretic results we computed all anti-elite primes up to 10^{11}.

2 Theoretical Results

Theorem 2.1. *Let $p > 5$ be a prime number. Then p is a divisor of a Fermat number F_n with $n \geq 2$ if and only if p is anti-elite with $L = 1$.*

Proof. Let p be a prime factor of F_n with $n \geq 2$. If $p = F_n$, then equation (1) implies

$$F_m \equiv 2 \pmod{F_n} \tag{3}$$

for all $m > n$ and we get $\left(\frac{F_m}{F_n}\right) = 1$ since $F_n \equiv 1 \pmod{8}$. If F_n is not prime, all of its prime divisors have the form $p = 2^{n+2}k + 1$ with a natural number $k > 1$. Here again, we get from (1) that

$$F_m \equiv 2 \pmod{p} \tag{4}$$

for all $m > n$. In both cases we find $L = 1$ and hence p is anti-elite.

Let now $p = 2^r h + 1$ with h odd be an anti-elite prime number with $L = 1$. This means that $F_{r+1} \equiv F_{r+2} \pmod{p}$, i.e., there exists a quadratic residue c modulo p such that

$$(c-1)^2 + 1 \equiv c \pmod{p}. \tag{5}$$

This is equivalent to

$$(c-1)(c-2) \equiv 0 \pmod{p}, \tag{6}$$

and so either $c \equiv 1$ or $c \equiv 2 \pmod{p}$. The first case leads us to $2^{2^{r+1}} \equiv 0 \pmod{p}$ which is impossible for all odd primes p. Hence, $c \equiv 2 \pmod{p}$, resp. $F_{r+1} \equiv 2 \pmod{p}$. Using relation (1), we see that either $F_r \equiv 0 \pmod{p}$, i.e. $p|F_r$, or $F_r \equiv 2 \pmod{p}$. In the latter case we obtain – again with formula (1) – either $F_{r-1} \equiv 0$ or $F_{r-1} \equiv 2 \pmod{p}$ and so on. As we have $p > 5$ there will hence be an index n such that $3 < F_n < p$. This implies that $F_n \equiv 2 \pmod{p}$ is impossible which leaves us with an index $n < m < r$ with $F_m \equiv 0 \pmod{p}$, i.e., $p|F_m$. This completes the proof. □

From this immediately follows

Corollary 2.2. *There are infinitely many anti-elite primes with $L = 1$.*

Proof. It is well-known that the Fermat numbers are pairwise coprime. As every F_n with $n \geq 2$ is divided at least by one prime factor, Theorem 2.1 guarantees that each F_n contributes an element to the set of all anti-elite primes with $L = 1$, which hence is infinite. □

Remark: It is of interest to note that all primes dividing Fermat numbers are either elite primes or anti-elite primes. Moreover, a prime p dividing a Fermat number is an elite prime if and only if p is equal to the Fermat prime 3 or p is equal to the Fermat prime 5. Furthermore, since the series S is convergent, this provides once more an affirmative answer to a famous problem of Golomb, who asked in 1955 whether the series of the reciprocals of all prime divisors of the Fermat numbers converges [5].

We shall now turn our attention to the period lengths $L > 1$.

Theorem 2.3. *Let $p = 2^r h + 1$ be an anti-elite prime number with a Fermat period of length $L > 1$. Then there exists a quadratic residue c modulo p such that $F_r \equiv c + 1 \,(\mathrm{mod}\, p)$ and which is a solution of the Diophantine equation*

$$\sum_{\nu=0}^{2^L-2} c^\nu \equiv 0 \pmod{p}. \tag{7}$$

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

$$c^{2^L} \equiv c \pmod{p}, \tag{8}$$

which is equivalent to

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

Notice that $c = 0$ gives $F_r \equiv 1 \pmod{p}$ which by (1) leads to $F_m \equiv 1 \pmod{p}$ for all $m > r$ contradicting $L > 1$. The solution $c = 1$ again only leads, as we have seen in the proof to Theorem 2.1, to $L = 1$. Hence, for $L > 1$,

$$\sum_{\nu=0}^{2^L-2} c^\nu \equiv 0 \pmod{p}. \tag{10}$$

This completes the proof. □

Let us now have a look at the special case $L = 2$.

Corollary 2.4. *Let $p = 2^r h + 1$ be a prime number. Then p is anti-elite with $L = 2$ if and only if p fulfills the congruential equation $p \equiv 1 \,(\mathrm{mod}\ 12)$ and is a divisor of the number $N_r := F_r(F_r - 1) + 1 = 2^{2^r}\left(2^{2^r} + 1\right) + 1$.*

Proof.

1) If p is anti-elite with $L = 2$ then there must exist a solution c to the Diophantine equation

$$c^2 + c + 1 = kp, \tag{11}$$

where k is an appropriate natural number. Notice that in Theorem 2.3 the residue c is defined to be congruent to $F_r - 1$. With (11), we hence get

$$0 \equiv c(c+1) + 1 \equiv F_r(F_r - 1) + 1 \pmod{p}, \tag{12}$$

i.e., p is a divisor of N_r. Equation (11) has the two solutions

$$c_1 = \frac{-1 + \sqrt{4kp - 3}}{2} \quad \text{and} \quad c_2 = \frac{-1 - \sqrt{4kp - 3}}{2}, \tag{13}$$

which are integer 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

$$\left(\frac{-3}{4p}\right) = \left(\frac{p}{3}\right) \tag{14}$$

using the fundamental properties of the Jacobi symbol and the Law of Quadratic Reciprocity. A simple computation shows that $\left(\frac{p}{3}\right) = 1$ if and only if $p \equiv 1$ (mod 3). Hence, the even number $p - 1$ is a multiple of 3. This means that $\omega := \frac{p-1}{6}$ is a natural number and that there exists a cyclic subgroup G modulo p of order 6 and index ω such that the two Fermat remainders of the period of p are elements of G. So, there is a primitive root a modulo p such that the elements of G have the form $a^{\omega\nu}$ with $\nu = 0, 1, \ldots, 5$. Suppose that ω is odd, then $a^{\omega\nu}$ is a quadratic residue modulo p only if ν is even. For $\nu = 0$, we have $a^{\omega\nu} = 1$ which cannot lead to $L = 2$. So, the two Fermat remainders must be of the form $a^{2\omega}$, resp. $a^{4\omega}$. Furthermore, the relation

$$\left(a^{2\omega} - 1\right)^2 + 1 \equiv a^{4\omega} \pmod{p} \tag{15}$$

has to be fulfilled. But a simple transformation of this gives

$$a^{2\omega} \equiv 1 \pmod{p}, \tag{16}$$

i.e., we again obtain a contradiction to the fact that $L = 2$. Therefore, the index ω has to be an even number. This finally leads to $p \equiv 1$ (mod 12).

2) Let p be a prime with $p \equiv 1 \pmod{12}$ and p a divisor of N_r. There exists a quadratic residue c modulo p such that $F_r \equiv c+1 \pmod{p}$. Hence, $N_r \equiv c^2+c+1 \equiv 0 \pmod{p}$. This implies that $F_r \equiv -c^2 \pmod{p}$ and so, we get $\left(\frac{F_r}{p}\right) = \left(\frac{-1}{p}\right) = 1$. Moreover, we obtain $F_{r+1} \equiv c^2+1 \equiv -c \pmod{p}$, where $-c$ again is a quadratic residue modulo p. Finally, there is $F_{r+2} \equiv c^4+1 \equiv (-c-1)^2+1 \equiv c+1 \pmod{p}$, i.e., $F_{r+2} \equiv F_r \pmod{p}$ and hence p is anti-elite with $L=2$. This completes the proof. □

Consequence 2.5. *There are infinitely many anti-elite primes with $L = 2$.*

Proof. With relation (1) we get

$$\begin{aligned} N_{r+1} &= F_{r+1}^2 - F_{r+1} + 1 \\ &= \left((F_r-1)^2+1\right)^2 - (F_r-1)^2 \\ &= (F_r^2 - 3F_r + 3)(F_r^2 - F_r + 1) \\ &= N_r(N_r - 2(F_r-1)). \end{aligned}$$

Hence, for all natural numbers $m \leq M$ the number N_m is a divisor of N_M. Especially, $N_1 = 21$ is a divisor of all N_r. It is an easy computation to check that

$$N_r \equiv 9 \pmod{12} \tag{17}$$

and with this that

$$\frac{N_r}{21} \equiv 1 \pmod{12}, \tag{18}$$

resp.,

$$\frac{N_{r+1}}{N_r} \equiv 1 \pmod{12}, \tag{19}$$

hold for all natural numbers r. Notice that the two odd numbers N_r and $\frac{N_{r+1}}{N_r}$ are relatively prime. Since any of their common divisors d divides their difference, i.e., $d | 2^{2^r}+1$, we see that d is of the form 2^s. This is possible only if $s = 0$, i.e., $d = 1$.

As we have shown in the proof to the previous Corollary, every prime factor $p > 3$ of N_r has a Fermat period of length $L = 2$. Write $p = 2^s h + 1$ with h odd. By the above mentioned Theorem of Aigner [1], we know that if $2^j k$ with $0 \leq j \leq s$ and k a divisor of h is the multiplicative order of 2 modulo p, then $2^L = 4 \equiv 1 \pmod{k}$. This implies that $k = 3$. Because $2^j \cdot 3$ is a divisor of $\phi(p) = p-1$ we get $p \equiv 1 \pmod{3}$.

Suppose that $j \leq 1$. Then we get either $2^3 = 8 \equiv 1 \pmod{p}$, i.e., $p = 7$ or $2^6 = 64 \equiv 1 \pmod{p}$, i.e., $p = 3$ or $p = 7$. But we already know that $(21, \frac{N_r}{21}) = 1$ and hence every prime factor $p > 7$ of N_r fulfills $p \equiv 1 \pmod{4}$.

Finally, every prime factor of $\frac{N_{r+1}}{N_r}$ has the form $p \equiv 1 \pmod{12}$ and it is relatively prime to all prime factors of the numbers N_m with $m \leq r$. Corollary 2.4 actually implies that every such prime factor is an anti-elite prime with $L = 2$, such that there are infinitely many of these numbers. □

Remarks: 1) Consequence 2.5 implies that for every $R > 0$ there exists a natural number $r \geq R$ and an odd number $h > 1$ such that $p = 2^r h + 1$ is anti-elite. Suppose that r were bounded by R. Then all anti-elites p with $L = 2$ fulfill

$$2^{2^{\lfloor R \rfloor} \cdot 3} \equiv 1 \pmod{p}. \tag{20}$$

This is possible only if $2^{2^{\lfloor R \rfloor} \cdot 3} > p$, i.e., for only finitely many p's. The claim follows from this contradiction.

2) There is an alternate proof of Consequence 2.5 based on a well-known Theorem, first proved by A. S. Bang in 1886 [2]. It states that for any given integer $a > 1$ and every natural number $n > 6$ the number $a^n - 1$ has a prime factor p which does not divide $a^k - 1$ for $1 \leq k < n$. By Fermat's little Theorem, it follows that $p \equiv 1 \pmod{n}$ in this case. Now, we can write N_r with $r \geq 2$ as

$$N_r = \frac{2^{3(2^r)} - 1}{2^{2^r} - 1}. \tag{21}$$

Then by Bang's Theorem, the numerator of N_r has a prime factor p that does not divide any number of the form $2^k - 1$ with $1 \leq k < 3 \cdot 2^r$. Hence, p divides N_r but none of the numbers N_s with $1 \leq s < r$. Note that this prime number p fulfills $p \equiv 1 \pmod{3(2^r)}$, and as $r \geq 2$ this implies $p \equiv 1 \pmod{12}$ for all $r \geq 2$. With these two properties and Corollary 2.4 we again get the fact that there are infinitely many anti-elite primes with $L = 2$.

Using elementary congruential arguments we can derive some arithmetic progressions that cannot contain anti-elite primes.

Theorem 2.6. *There are no anti-elite primes of the forms* $240k + a$ *where*

$$a \in \{7, 23, 43, 47, 67, 83, 103, 107, 127, 143, 163, 167, 187, 203, 223, 227\}.$$

Proof. Suppose the prime number p to be of the form $240k + a$ with the restrictions $1 \leq a < 240$, $(240, a) = 1$ and $a \equiv 3 \pmod{4}$. Then p has the form $2(120k + 2l + 1) + 1$, i.e., in the notation $p = 2^r h + 1$ we have $r = 1$ and $h = (120k + 2l + 1)$. So, by Aigner's Theorem we know that $F_1 = 5$ is a Fermat remainder of p. As $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{a}{5}\right)$, we can exclude all residue classes a modulo 240 fulfilling $(240, a) = 1$, $a \equiv 3 \pmod{4}$ and $\left(\frac{a}{5}\right) = -1$. A simple computation shows that these are exactly the 16 remainders a given in the Theorem. □

Remark: Theorem 2.6 excludes 16 of the $\phi(240) = 64$ residue classes able to contain prime numbers. It is not difficult to get further residue classes excluded by similar congruential arguments. E.g., using $F_2 = 17$ we could exclude the classes $p \equiv a \pmod{204}$ with $a \in \{7, 31, 79, 91, 139, 163, 175, 199\}$, etc.

3 All anti-elite primes up to 100 billion

Using a variant of the well-known sieve method of Erathostenes, we constructed all prime numbers up to 100 billion. After the elimination of all the primes contained in one of the

residue classes excluded by Theorem 2.6 the remaining numbers were tested one by one for anti-eliteness. Our test is based on the following necessary and sufficient condition for the eliteness of a prime number:

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.*

A proof of this result can be found in [7]. Taking the exact logical negation of this claim gives us a necessary and sufficient test for anti-eliteness.

Theorem 3.2. *Let $p = 2^r h + 1$ be a prime number with h odd. Then p is anti-elite if and only if no 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 $p = 2^r h + 1$, our algorithm checked whether the congruence

$$f^{2^k h} \equiv 1 \bmod p \tag{22}$$

is solvable for any $k < r$. If this is fulfilled, equation (22) 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 anti-elite, or a Fermat remainder f is found with $k = r$ being the smallest solution in (22) leading to a negative answer regarding the anti-eliteness of p.

We found in total 84 anti-elite primes smaller than 10^{11}. These are listed in Table 1 together with the respective length L of their Fermat period. Notice that by Theorem 2.1 all prime factors of Fermat numbers are anti-elites with $L = 1$, such that the Table contains all possible prime factors p of Fermat numbers that fulfill $p < 10^{11}$.

The results of this section are summarized in sequence A128852 of Sloane [8].

The computations were run on an AMD Sempron 2600 XP+ and a Pentium-IV-processor PC. A total CPU-time of about 1200 hours was needed to complete this project.

p	L	p	L	p	L
13	2	1376257	6	394783681	4
17	1	1489153	3	597688321	2
97	2	1810433	8	618289153	12
193	2	2424833	1	663239809	6
241	2	3602561	4	825753601	1
257	1	6700417	1	902430721	4
641	1	6942721	4	1107296257	2
673	2	7340033	3	1214251009	1
769	2	11304961	4	2281701377	8
2689	3	12380161	4	3221225473	2
5953	5	13631489	1	4278255361	4
8929	5	15790321	3	4562284561	4
12289	2	17047297	6	5733744641	4
40961	4	22253377	2	6487031809	1
49921	4	26017793	1	6511656961	4
61681	4	39714817	2	7348420609	2
65537	1	45592577	1	11560943617	2
101377	6	63766529	1	15600713729	14
114689	1	67411969	12	23447531521	8
274177	1	89210881	6	29796335617	2
286721	4	93585409	6	30450647041	10
319489	1	113246209	6	46908728641	4
414721	4	119782433	10	48919385089	3
417793	8	152371201	2	70525124609	1
550801	8	167772161	1	74490839041	2
786433	2	171048961	6	77309411329	2
974849	1	185602561	12	83751862273	12
1130641	12	377487361	4	96645260801	4

Table 1: All anti-elite primes up to 100 billion

4 Interpretations and open problems

Corollary 2.2 and Consequence 2.5 tell us that the set $\mathcal{A}$ of all anti-elite primes is infinite. If we enumerate all anti-elites in order to get $\mathcal{A} = \{13 = p_1 < p_2 < p_3 < \ldots\}$ we can write the partial sums of S as follows.

$$S_n = \sum_{\nu=1}^{n} \frac{1}{p_\nu}. \tag{23}$$

As we know the first 84 anti-elite primes, we can compute

$$S_{84} \approx 0.16447547409738350032. \tag{24}$$

Here again, our computational results suggest that $N(x)$ might be asymptotically bounded by $N(x) = O(\log(x))$. If this is so, it is furthermore probable that $S = S_\infty$ is an irrational number.

Moreover, it would be interesting to know whether there is an anti-elite prime p with $L = n$ for every natural number n. The smallest L not appearing in Table 1 is $L = 7$. Notice, that the only number k fulfilling the congruential equation $2^7 \equiv 1 \pmod{k}$ is $k = 127$. Hence, all prime numbers with a period length $L = 7$ have to be of the form $p = 127 \cdot 2^r \cdot h + 1$ with $r \geq 1$ and h odd. In fact, there are primes of that form known (e.g., $127 \cdot 2^{12} + 1$, $127 \cdot 2^{18} + 1$ or $127 \cdot 2^{558} + 1$; this latter number is a divisor of F_{556}), but we were unable to find an anti-elite with $L = 7$ among all these primes with $r \leq 3000$ and $h < 10^9$.

Are there other $L > 2$ such that the number of anti-elites with period length L is infinite?

Acknowledgement

The author wishes to thank the friendly referee for his help to improve this paper and for pointing out an alternate proof of the main result.

References

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

[2] A. S. Bang, Taltheoretiske undersogelser, *Tidsskrift Math.* **5** (1886), 70–80, 730–137.

[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, submitted.

[5] S. W. Golomb, Sets of primes with intermediate density, *Math. Scand.* **3** (1955), 264–274.

[6] 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.

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

[8] N. J. A. Sloane, The 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: anti-elite primes, elite primes, Fermat numbers.

(Concerned with sequence A128852.)

Received June 28 2007; revised version received September 18 2007. Published in *Journal of Integer Sequences*, September 20 2007.