Journal of Integer Sequences, Vol. 14 (2011),
Article 11.1.2

On the Complexity of Testing Elite Primes

Michal Křížek
Institute of Mathematics
Academy of Sciences
Žitná 25
CZ – 115 67, Praha 1
Czech Republic
krizek@math.cas.cz

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán
México
fluca@matmor.unam.mx

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109
Australia
igor@ics.mq.edu.au

Lawrence Somer
Department of Mathematics
Catholic University of America
Washington, DC 20064
USA
somer@cua.edu

Abstract

Aigner has defined elite primes as primes p such that all but finitely many of Fermat numbers $F(n) = 2^{2^n} + 1$, $n = 0, 1, 2, \ldots$, are quadratic nonresidues modulo p. Since the sequence of Fermat numbers is eventually periodic modulo any p with at most p distinct elements in the image, both the period length t_p and the number of arithmetic operations modulo p to test p for being elite are also bounded by p. We show that $t_p = O(p^{3/4})$, in particular improving the estimate $t_p \leq (p+1)/4$ of Müller and Reinhart in 2008. The same bound $O(p^{3/4})$ also holds for testing anti-elite primes.

1 Introduction

Motivated by a generalization of the Pepin primality test for Fermat numbers $F(n) = 2^{2^n} + 1$, $n = 0, 1, 2, \ldots$, Aigner [1] introduced the notion of *elite primes* which are the primes p such that F_n is a quadratic nonresidue modulo p for all but finitely many n. For example, 3, 5, 7, and 41 are elite primes. See [3, 5] and the references therein for various results about elite primes and their generalizations.

One such generalization appears in the work of Müller and Reinhart [5], where *b-elite primes* have been defined for an integer $b \geqslant 2$ as those primes p for which all but finitely many elements of the sequence $F_b(n) = b^{2^n} + 1$ are quadratic nonresidues modulo p. One can easily see that the estimate $O(x/(\log x)^2)$ on the number of elite primes up to $x \geqslant 2$, proved in [3], immediately extends to b-elite primes. It has also been noted in [5] that for any p, the sequence $\{F_b(n)\}_{n \geqslant 0}$ is eventually periodic modulo p with some period length t_p. That is, for some period length t_p and preperiod length $s_p \geqslant 0$ we have

$$F_b(n + t_p) \equiv F_b(n) \pmod p, \quad n = s_p, s_p + 1, \ldots. \tag{1}$$

It is also obvious that the smallest values of s_p and t_p satisfy the inequality $s_p + t_p \leqslant p$.

Müller and Reinhart [5, Theorem 2.8] have shown that for b-elite primes p the period t_p satisfies the inequality

$$t_p \leqslant \frac{p+1}{4}.$$

It follows immediately from [5, Theorem 2.6] that the preperiod s_p is less than or equal to the exponent of the prime 2 in the factorization of $p - 1$, and thus satisfies

$$s_p \leqslant \frac{\log(p-1)}{\log 2}. \tag{2}$$

We now improve these results as follows.

Theorem 1. *For a b-elite prime p, we have*

$$t_p \leqslant 3p^{3/4}.$$

Clearly, p is b-elite if and only if all numbers $F_b(n)$ for $n \geqslant s_p$ are quadratic nonresidues. We also recall that quadratic residuosity on an integer a can be tested in $O(\log p)$ arithmetic operations modulo p (for example, computing $a^{(p-1)/2}$ via repeated squaring). Thus any prime p can be tested for being b-elite in $O((s_p + t_p)\log p)$ arithmetic operations modulo p (see [5, Section 3] for a description of such an algorithm). This complexity can be trivially estimated as $O(p \log p)$.

Using Theorem 1 together with (2) and the fact that the inequality

$$s_p \leqslant \frac{\log(p-1)}{\log 2} < p^{3/4} \qquad \text{for all} \quad p \geqslant 5,$$

we now improve this trivial bound as follows:

Corollary 2. *A prime p can be tested for being a b-elite prime in at most $O(p^{3/4}\log p)$ arithmetic operations modulo p.*

2 Proof of Theorem 1

In what follows, we let (z/p) denote, as usual, the Legendre symbol of the integer z modulo the odd prime p.

Our main tool is a special case of the *Weil bound* for multiplicative character sums in the following form that is convenient for our application (see [2, Theorem 11.23]):

Lemma 3. *For any polynomial $f(X) \in \mathbb{Z}[X]$ of degree m which is not a perfect square modulo p, we have*

$$\left| \sum_{u=0}^{p-1} \left(\frac{f(u)}{p} \right) \right| \leqslant mp^{1/2}.$$

Proof of Theorem 1. Let us consider the polynomials $f_k(X) = X^{2^k} + 1$. We assume that $p > 2$. We take some integer $K \geqslant 1$ to be fixed in a way depending on p later on, and count how often the values

$$f_k(u), \qquad k = 0, \ldots, K-1,$$

are simultaneously quadratic nonresidues modulo p for $u = 0, \ldots, p-1$. Call this number $T_p(K)$. We have

$$T_p(K) = \frac{1}{2^K} \sum_{u=0}^{p-1} \prod_{k=0}^{K-1} \left(1 - \left(\frac{f_k(u)}{p} \right) \right). \tag{3}$$

Expanding the product in (3), we obtain $2^K - 1$ character sums of the shape

$$\sum_{u=0}^{p-1} \left(\frac{F_{k_1,\ldots,k_\nu}(u)}{p} \right), \qquad 0 \leqslant k_1 < \cdots < k_\nu \leqslant K-1, \tag{4}$$

where

$$F_{k_1,\ldots,k_\nu}(X) = (-1)^\nu \prod_{j=1}^{\nu} f_{k_j}(X) \tag{5}$$

with $\nu \geqslant 1$, and one trivial sum that equals p (corresponding to taking all the terms equal to 1 in the product in (3)). Then $f_{k_\nu}(X)$ modulo p is square-free because its derivative is $2^{k_\nu} X^{2^{k_\nu}-1} \pmod p$ and its only zero is $X = 0$, which is not a zero of $f_{k_\nu}(X)$ modulo p. Since

$$\deg f_{k_\nu} = 2^\nu > 2^\nu - 1 = \sum_{j=0}^{k_\nu - 1} \deg f_j,$$

it follows that the polynomial $F_{k_1,\dots,k_\nu}$ is not a perfect square modulo p. Hence, Lemma 3 applies to every sum (4) and implies that each sum of the type (4) is at most $2^K p^{1/2}$ by absolute value. Thus,

$$\left| T_p(K) - \frac{p}{2^K} \right| < 2^K p^{1/2}. \tag{6}$$

The bound (6) holds for a general p. When p is a b-elite prime there are at least t_p solutions u for which $f_k(u)$ is a quadratic nonresidue for $k = 0, 1, \dots, K-1$, namely all u of the form

$$u = b^{2^{n+s_p}}, \qquad n = 0, \dots, t_p - 1.$$

Choosing K to satisfy

$$2^K \leqslant p^{1/4} < 2^{K+1}, \tag{7}$$

we easily get from (6) that

$$t_p \leqslant T_p(K) \leqslant 3p^{3/4},$$

which is the desired result. □

Remark 4. By replacing the inequalities (7) with $2^K \leqslant \sqrt{2} p^{1/4} < 2^{K+1}$, we can improve the constant 3 in Theorem 1 to $2\sqrt{2}$. It is easy to see that this can be further improved by a slightly more precise estimation of the degrees of the polynomials (5) and thus of the sums (4).

3 Anti-Elite Primes

In contrast with the elite primes, Müller in [4] defines an anti-elite prime as a prime p for which $F(n)$ is a quadratic residue modulo p for all but finitely many n. For example, 13 and 97 are anti-elite primes and so are all Fermat primes greater than 5. As with b-elite primes, we can define a b-anti-elite prime p, where $b \geqslant 2$, as a prime for which all but finitely many elements of the sequence $F_b(n)$ are quadratic residues modulo p. Thus, the period of $\{F_b(n)\}_{n \geqslant 0}$ modulo p consists only of quadratic residues when p is an anti-elite prime. We can prove the following analogue of Theorem 1 for b-anti-elite primes.

Theorem 5. *For a b-anti-elite prime p, we have*

$$t_p \leqslant 3p^{3/4},$$

where t_p is the period length of the eventually periodic sequence $\{F_b(n)\}_{n \geqslant 0}$ modulo p.

The proof of Theorem 5 is similar to the proof of Theorem 1. In the proof of Theorem 1, we only need to replace each occurrence of "quadratic nonresidue" by "quadratic residue", replace the minus sign in the equation (3) by a plus sign, and delete the factor $(-1)^\nu$ in (5).

References

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

[2] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., 2004.

[3] 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.

[4] T. Müller, On anti-elite prime numbers, *J. Integer Sequences* **10** (2007), Article 07.9.4.

[5] T. Müller and A. Reinhart, On generalized elite primes, *J. Integer Sequences* **11** (2008), Article 08.3.1.

2010 *Mathematics Subject Classification*: Primary 11A07; Secondary 11L40.
Keywords: elite prime testing, character sum.

(Concerned with sequences A102742 and A128852.)

Received October 12 2010; revised version received December 20 2010. Published in *Journal of Integer Sequences*, January 4 2011.
