Easy numbers for the Elliptic Curve Primality Proving Algorithm

F. Morain [*†‡]
morain@inria.inria.fr

May 6, 1992

Abstract

We present some new classes of numbers that are easier to test for primality with the Elliptic Curve Primality Proving algorithm than average numbers. It is shown that this is the case for about half the numbers of the Cunningham project. Computational examples are given.

1 Introduction

The so-called Elliptic Curve Primality Proving algorithm (ECPP) is one of the most powerful algorithms for proving the primality of large numbers with up to 1500 decimal digits (see [2, 13, 16]). This algorithm generalizes the old Fermat-like primality proving tests based on the factorization of $N-1$ when N is the number to be proven prime.

There exist easy numbers for the $N-1$ test, namely those N for which the factorization of $N-1$ is trivial, such as Fermat numbers ($N = 2^{2^k}+1$) or special numbers: $N = 1+k!$, $N = 1+k\times a^n$, etc. (see [18] for all this).

The purpose of this paper is to exhibit some numbers that are easy to test with ECPP. It appears that many numbers of the form b^n+1 are of this kind. Section 2 recalls a part of the theory of ECPP. In Section 3, we describe very easy numbers – numbers analogous to Fermat numbers – and easy numbers – numbers that can be dealt with more quickly than average numbers of the same size. Numerical computations are described that exemplify our results.

2 A brief presentation of ECPP

2.1 Fermat's test

Let us begin with the converse of Fermat's little Theorem.

Theorem 2.1 *If there exists an a prime to N such that*

$$a^{N-1} \equiv 1 \bmod N$$

but

$$a^{(N-1)/q} \not\equiv 1 \bmod N$$

for every prime divisor q of $N-1$, then N is prime.

*LIX, Laboratoire d'Informatique de l'Ecole Polytechnique Ecole Polytechnique, 91128 Palaiseau Cedex, France

†Institut National de Recherche en Informatique et en Automatique (INRIA), Domaine de Voluceau, B. P. 105 78153 LE CHESNAY CEDEX (France).

‡On leave from the French Department of Defense, Délégation Générale pour l'Armement.

If we cannot factor $N-1$ completely, it can happen that the cofactor of $N-1$, call it N_1, is a probable prime. Then, we can try to factor N_1-1 and so on. This idea forms the DOWNRUN process of [19]: Build a decreasing sequence of probable primes $N_0 = N > N_1 > \cdots > N_k$ such that the primality of N_{i+1} implies that of N_i (see [11, pp. 376–377]). As an example, consider a proof that $N = 10^5 + 3$ is prime. We find

$$\begin{aligned} N_0 &= 100003, \quad N_0 - 1 = 2 \times 3 \times 7 \times N_1, \\ N_1 &= 2381, \quad N_1 - 1 = 2^2 \times 5 \times 7 \times 17 \end{aligned}$$

if we assume that we can decide the primality of numbers less than 20 very quickly. Then, we can take $a = 3$ for proving that N_1 is prime and $a = 2$ for N_0, now that we know that N_1 is prime.

More sensitive tests are described in [5]. A different type of primality proving algorithm is described in [1, 9, 8].

2.2 Elliptic curves

The material of this section is taken from [3]. In order to overcome the difficulty of having just one number to factor, we use elliptic curves. Informally, an elliptic curve over a finite field $\mathbf{Z}/p\mathbf{Z}$ is the set (of classes) of points in the projective plane of $\mathbf{Z}/p\mathbf{Z}$

$$E(\mathbf{Z}/p\mathbf{Z}) = \{(x : y : z) \in \mathbf{P}^2(\mathbf{Z}/p\mathbf{Z}),$$

$$y^2 z \equiv x^3 + axz^2 + bz^3 \bmod p\}.$$

We can define a group law on this set, known as the tangent–and–chord method, ordinarily denoted by $+$. If m is the cardinality of $E(\mathbf{Z}/p\mathbf{Z})$, then Hasse's theorem tells us that $|m-(p+1)| \leq 2\sqrt{p}$. More precisely, there exists an algebraic integer π in a quadratic field $K = \mathbf{Q}(\sqrt{-D})$, D a positive integer, such that $p = N_K(\pi)$ and $m = N_K(\pi - 1)$, where $N_K(\theta)$ is the norm of the algebraic number θ in K.

From [10], we have a primality theorem analogous to Theorem 2.1:

Theorem 2.2 *Let N be an integer prime to 6, E an elliptic curve over $\mathbf{Z}/N\mathbf{Z}$, together with a point P on E and m and s two integers with $s \mid m$. For each prime divisor q of s, we put $(m/q)P = (x_q : y_q : z_q)$. We assume that $mP = O_E$ and $\gcd(z_q, N) = 1$ for all q. Then, if p is a prime divisor of N, one has $\#E(\mathbf{Z}/p\mathbf{Z}) \equiv 0 \bmod s$.*

We have also:

Corollary 2.1 *With the same conditions, if $s > (\sqrt[4]{N} + 1)^2$, then N is prime.*

It should be noted that in order for the preceding condition on s to be fulfilled, m must not be a perfect square. It was shown in [3] that this can only happen if $D = 3$ (resp. $D = 4$) for $N = x^2 + x + 1$ (resp. $N = x^2 + 1$).

We can now give a brief description of the algorithm.

function ECPP(N)

1. find a quadratic field $K = \mathbf{Q}(\sqrt{-D})$ in which N is the norm of an algebraic integer π and for which $m = N_K(\pi - 1)$ is completely factored or has a probable prime cofactor M;

2. put $s = m$ and use Theorem 2.2 to prove the primality of N;

3. recursively prove the primality of M.

This algorithm combines a Fermat-like theorem and the DOWNRUN approach. For the actual implementation of this test, we refer to the article [3] as well as [13]. We insist on the following points. That N is a norm in an imaginary quadratic field is equivalent to the fact that

$$4N = A^2 + DB^2 = (A + B\sqrt{-D})(A - B\sqrt{-D})$$

with A and B two rational integers. In turn, this implies that

$$4m = (A-2)^2 + DB^2.$$

A number N will be easy to test if the largest prime factor of m is easy to find, for instance if it is small. For average numbers, the cofactor we get is smaller than N, say the ratio m/M is about 10^{10} at best. The following section will deal with extraordinary numbers with respect to this problem.

Throughout the paper, we keep the preceding notations.

3 Easy numbers

3.1 Building easy numbers

It follows from the preceding section that there exist numbers for which ECPP is very easy. This is indeed the case when $N = N_K(\pi)$ and where $N_K(\pi - 1)$ is easy to factor. An example of such numbers is $\pi = \alpha_0\alpha_1^k + 1$ where α_i is an algebraic integer of small norm of K and k a positive integer. These numbers, called *Elliptic Mersenne primes* were introduced in [7] and some large ones were given in [15] (see also [4]).

Let us assume for simplicity that $D \equiv 0 \bmod 4$. Then, starting from

$$1 + D/4 = U$$

we can multiply both sides by k^2 and have

$$k^2 + k^2D/4 = Uk^2 = m.$$

To m, we can now associate $N(k) = (k+1)^2 + k^2D/4$ and sometimes we get a prime. If k is easy to factor, we have built a prime N for which the ratio N/N_1 is quite large. For example, taking $D = 8$ and $k = 10^{100} + 15034 = 2 \times 6397 \times 2967583 \times k_1$ yields a corresponding number $N(k)$ which is a 201-digit prime and we can prove that N is prime by proving that $N_1 = k_1$ is prime. The ratio N/N_1 is about 10^{112}.

3.2 Finding easy numbers

Another kind of relatively easy number was discovered during the actual implementation of ECPP. Suppose we are given a probable prime N that can be written as

$$\begin{aligned} N &= (c^2 + Da^2)/(c^2 + Db^2) \\ &= N_K((c + a\sqrt{-D})/(c + b\sqrt{-D})) \\ &= N_K(\pi) \end{aligned}$$

where D is a suitable squarefree positive integer and $2a$, $2b$ and $2c$ are integer. Then a potential number of points on an elliptic curve modulo N is

$$m = N_K(\pi - 1) = \frac{D(a-b)^2}{c^2 + Db^2}.$$

We must select the signs of a and b such that this is an integer in $\mathbf{Z}$. If we have luck, then $a - b$ is easy to factor and we can get a probable prime cofactor N_1 of m with size about half that of N.

3.2.1 Examples

Many numbers taken from the Cunningham project [6] are indeed easy numbers. The first and third examples are taken from a list of probable primes that S. S. Wagstaff sent to the author recently.

First, let us consider the 208-digit probable prime

$$N = (12^{193} + 1)/13$$

and write it as

$$\begin{aligned} N &= (1^2 + 3(2X)^2)/(1^2 + 3 \times 2^2) \\ &= N_K(\alpha)/N_K(\beta) = N_K(\alpha/\beta) = N_K(\pi) \end{aligned}$$

with $X = 12^{96}$, $\alpha = 1 + 2X\sqrt{-3}$ and $\beta = 1 + 2\sqrt{-3}$. A potential number of points is

$$m = N_K(\pi - 1) = \frac{3}{13}(2X - 2)^2.$$

With this, $X - 1 = 13X_0$ and

$$m = 3 \times 13 \times (2X_0)^2.$$

Therefore, we are done if $X - 1 = 12^{96} - 1$ is easy to factor, which it is:

$$z^{96} - 1 = \prod_{d|96} \Phi_d(z),$$

d	$\Phi_d(z)$	factors of $\Phi_d(12)$
1	$z-1$	11
2	$z+1$	13
3	z^2+z+1	157
4	z^2+1	5×29
6	z^2-z+1	7×19
8	z^4+1	89×233
12	z^4-z^2+1	20593
16	z^8+1	$17 \times 97 \times 260753$
24	z^8-z^4+1	193×2227777
32	$z^{16}+1$	$1200913648289 \times 153953$
48	$z^{16}-z^8+1$	$592734049 \times 40609 \times 7681$
96	$z^{32}-z^{16}+1$	$7489 \times 3122881 \times 1461573322938242802306049$

where $\Phi_d(z)$ stands for the d-th cyclotomic polynomial ($\Phi_d(z) = \prod_{(a,d)=1}(z - \exp(2i\pi a/d))$). We list in the following table the algebraic factors of $12^{96}-1$. (It should be noted that one can find the factors of such a number quite rapidly without resorting to cyclotomic factorization by using Pollard's $p-1$ method [17].) In the DOWNRUN process, we may take $N_1 = 1461573322938242802306049$, the largest probable prime factor of $12^{96}-1$. The ratio m/N_1 is approximatively 10^{183}.

Another very interesting example is the following. Take

$$N = \frac{2^{3539}+1}{3}$$

which was first proved prime by Morain [14]. We have

$$N = \frac{1^2+2X^2}{1^2+2(1)^2}$$

with $X = 2^{1769}$. Write this as

$$N = N_K(\alpha/\beta) = N_K((1+X\sqrt{-2})/(1-\sqrt{-2})).$$

With $\pi = \alpha/\beta$, one gets

$$m = N_K(\pi - 1) = \frac{2}{3}(X+1)^2.$$

And hopefully, we have that

$$X^{1769}+1 = -((-X)^{1769}-1) = -\prod_{d|1769}\Phi_d(-X)$$

yielding

$$2^{1769}+1 = 3 \times 59 \times 3033169 \times p_{18} \times C_{506}$$

(with $C_{506} = \Phi_{1769}(-2)$ a strong pseudoprime to base 2) so that the primality of N can be deduced from the factorization of a 506-digit number instead of a 1065 number as in [14].

A less trivial example is given by the cofactor of $10^{327}+1$. We first write

$$X^{327}+1 = -\Phi_1(-X)\Phi_3(-X)\Phi_{109}(-X)\Phi_{327}(-X).$$

The number we are interested in is $N = \Phi_{327}(-10)$. We rewrite this as

$$\Phi_3(-10)N = 91N = \frac{1+10^{327}}{1+10^{109}} = 1 - Y + Y^2$$

where $Y = 10^{109}$. Now comes the trick: Multiply this relation by 4 in order to get

$$4 \times 91 \times N = 4 - 4Y + 4Y^2 = 3 + (2Y-1)^2.$$

We multiply each side by 3 and finally get

$$N = \frac{3^2+3(2Y-1)^2}{12 \times 91} = \frac{3^2+3(2Y-1)^2}{3^2+3 \times 19^2}.$$

Choosing $\pi = (3+(2Y-1)\sqrt{-3})/(3+19\sqrt{-3})$, this implies that a potential number of points is

$$\begin{aligned} m &= N_K(\pi-1) \\ &= (2Y-20)^2/364 = (Y-10)^2/91. \end{aligned}$$

3.2.2 Comments

We can hope that this situation occurs whenever we try to prove the primality of (a factor of) a number of the form $b^n + 1$ with $b \in \{2, 3, 5, 6, 7, 10, 11, 12\}$ and particularly numbers of the form $(b^{2k+1} + 1)/(b + 1)$. If $b \in \{2, 3, 7, 11, 12\}$, the field $\mathbf{Q}(\sqrt{-b})$ has unique factorization and the preceding tricks might work. For other values, we can have some luck as demonstrated by our last numerical example.

Note also that if $N = (b^{2k+1} + 1)/(b + 1)$, one has

$$N - 1 = \frac{b(b^k - 1)(b^k + 1)}{b + 1}$$

and a potential m is:

$$m = \frac{(b^k \pm 1)^2 b}{b + 1}.$$

ECPP does not give a faster primality proof than the use of one of the refined version of the $N - 1$ test, which needs the factorisation of $N - 1$ up to $\sqrt{N}$ (see [5]). Similar remarks can be made concerning the $N + 1$ test.

These numbers illustrate the need for a robust factorization routine for ECPP. As a matter of fact, the program must take into account the miraculous phenomena described above.

4 Conclusion

We have seen that there are potentially many easy numbers for ECPP. In particular, many Cunningham numbers are easy. This strengthens the idea that these numbers are not random numbers with respect to primality proving. Primality proving algorithms should be run on more random numbers, such as partition numbers [12] or numbers built up from the decimal representation of π (see [2]).

Acknowledgments. We wish to thank S. S. Wagstaff for providing us with the list of probable primes cited above; V. Ménissier, P. Dumas and M. Golin for reading earlier versions of the manuscript.

References

[1] L. M. Adleman, C. Pomerance, and R. S. Rumely. On distinguishing prime numbers from composite numbers. *Annals of Math. 117* (1983), 173–206.

[2] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. Research Report 1256, INRIA, Juin 1990. Submitted to *Math. Comp.*

[3] A. O. L. Atkin and F. Morain. Finding suitable curves for the elliptic curve method of factorization. To appear in *Mathematics of Computation*. Also available as INRIA Research Report no 1547, March 1991.

[4] W. Bosma. Primality testing using elliptic curves. Tech. Rep. 85-12, Math. Instituut, Universiteit van Amsterdam, 1985.

[5] J. Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Math. Comp. 29*, 130 (1975), 620–647.

[6] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers*, 2 ed. No. 22 in Contemporary Mathematics. AMS, 1988.

[7] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Advances in Applied Mathematics 7* (1986), 385–434.

[8] H. Cohen and A. K. Lenstra. Implementation of a new primality test. *Math. Comp. 48*, 177 (1987), 103–121.

[9] H. Cohen and H. W. Lenstra, Jr. Primality testing and Jacobi sums. *Math. Comp. 42*, 165 (1984), 297–330.

[10] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. In *Proc. 18th STOC* (Berkeley, May 28–30 1986), pp. 316–329.

[11] D. E. Knuth. *The Art of Computer Programming: Seminumerical Algorithms.* Addison-Wesley, 1981.

[12] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard. The factorization of the ninth Fermat number. To appear, 1991.

[13] F. Morain. *Courbes elliptiques et tests de primalité.* PhD thesis, Université Claude Bernard–Lyon I, Septembre 1990.

[14] F. Morain. Distributed primality proving and the primality of $(2^{3539} + 1)/3$. In *Advances in Cryptology – EUROCRYPT '90* (1991), I. B. Damgård, Ed., vol. 473 of *Lect. Notes in Computer Science*, Springer–Verlag, pp. 110–123. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Aarhus, Denmark, May 21–24, 1990.

[15] F. Morain. Elliptic curves, primality proving and some Titanic primes. In *Journées Arithmétiques 1989* (1992), vol. 198–199-200 of *Astérisque*, SMF, pp. 245–251.

[16] F. Morain. Prime values of partition numbers and some new large primes. In preparation, Apr. 1992.

[17] J. M. Pollard. Theorems on factorization and primality testing. *Proc. Cambr. Philos. Soc. 76* (1974), 521–528.

[18] P. Ribenboim. *The book of prime number records*, 2nd ed. Springer, 1989.

[19] M. C. Wunderlich. A performance analysis of a simple prime-testing algorithm. *Math. Comp. 40*, 162 (1983), 709–714.