Astérisque

FRANÇOIS MORAIN

Elliptic curves, primality proving and some Titanic primes

Astérisque, tome 198-199-200 (1991), p. 245-251

<http://www.numdam.org/item?id=AST_1991__198-199-200__245_0>

ELLIPTIC CURVES, PRIMALITY PROVING AND SOME TITANIC PRIMES

Abstract

We describe how to generate large primes using the primality proving algorithm of Atkin.

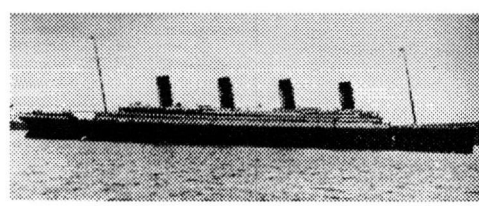

Figure 1: The Titanic*.

1. Introduction. During the last ten years, primality testing evolved at great speed. Motivated by the RSA cryptosystem [3], the first deterministic primality proving algorithm was designed by Adleman, Pomerance and Rumely [2] and made practical by Cohen, H. W. Lenstra and A. K. Lenstra (see [9, 10] and more recently [5]). It was then proved that the time needed to test an arbitrary integer N for primality is $O((\log N)^{c \log\log\log N})$ for some positive constant $c > 0$. When implemented on a huge computer, the algorithm was able to test 200 digit numbers in about 10 minutes of CPU time.

A few years ago, Goldwasser and Kilian [11], used the theory of elliptic curves over finite fields to give the first primality proving algorithm whose running time is polynomial in $\log N$ (assuming a plausible conjecture in number theory). Atkin [4] used the theory of complex multiplication to give a practical version of this algorithm.

*Taken from *Titanic, Destination disaster, The Legends and the Reality* by J. P. Eaton and C. A. Haas, W. W. Norton and Company, New York 1987.

The aim of this paper is to present some results the author has obtained using his own implementation of this algorithm in the search for large primes.

2. Elliptic curves. Let $\mathbf{K}$ be a field of characteristic prime to 6. An elliptic curve E over $\mathbf{K}$ is a non singular algebraic projective curve of genus 1. It can be shown [7, 23] that E is isomorphic to a curve with equation:

$$y^2z = x^3 + axz^2 + bz^3, \tag{1}$$

where a and b are in $\mathbf{K}$. The *discriminant* of E is $\Delta = -16(4a^3 + 27b^2)$ and the *invariant* is

$$j = 2^8 3^3 \frac{a^3}{4a^3 + 27b^2}.$$

We write $E(\mathbf{K})$ for the set of points with coordinates $(x : y : z)$ which satisfy (1) with $z = 1$, together with the point at infinity: $O_E = (0 : 1 : 0)$. We will use the well-known *tangent-and-chord* addition law on a cubic [13] over $\mathbf{Z}/N\mathbf{Z}$ (see [17] for a justification).

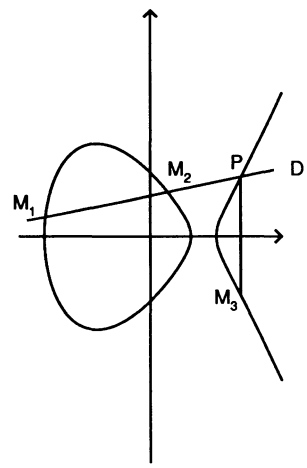

Figure 2: An elliptic curve over $\mathbf{R}$.

In order to add two points $M_1 = (x_1, y_1)$ and $M_2 = (x_2, y_2)$ on E resulting in $M_3 = (x_3, y_3)$, the equations are

$$\begin{cases} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{cases}$$

where

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{if } x_2 \neq x_1 \\ \\ (3x_1^2 + a)(2y_1)^{-1} & \text{otherwise.} \end{cases}$$

3. Primality testing. Let us recall one of the converses of Fermat's theorem (see for example [6]).

Theorem 1 *Let a be such that $\gcd(a, N) = 1$, q a prime divisor of $N - 1$. If*

$$a^{N-1} \equiv 1 \bmod N \text{ and } \gcd(a^{(N-1)/q} - 1, N) = 1$$

then each prime divisor p of N satisfies: $p \equiv 1 \bmod q$.

Corollary 1 *Under the conditions of Theorem 1, if $q > \sqrt{N}$ then N is prime.*

A similar theorem can be stated for elliptic curves.

Theorem 2 ([11, 16]) *Let N be an integer greater than 1 and prime to 6. Let E be an elliptic curve over $\mathbf{Z}/N\mathbf{Z}$, m and s two integers such that $s \mid m$. Suppose we have found a point P on E that satisfies $m\,P = O_E$, and that for each prime factor q of s, we have verified that $\frac{m}{q}P \neq O_E$. Then if p is a prime divisor of N, $\#E(Z/pZ) \equiv 0 \bmod s$.*

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

4. Atkin's algorithm. In order to use the preceding theorem, we need to compute the number of points m. This process is far from trivial in general (see [22]). From a practical point of view, it is desirable to use deep properties of elliptic curves over finite fields. This involves the theory of complex multiplication and class fields and requires a lot of theory [18]. We can summarize the principal properties:

Theorem 3 *Let p be a rational prime number that splits as the product of two principal ideals in K (i.e. (p) splits completely in the ring class field of K): $p = \pi\pi'$ with π an integer of K. Then there exists an elliptic curve E defined over $\mathbf{Z}/p\mathbf{Z}$ having complex multiplication by the ring of integers of K, whose cardinality is $m = N_K(\pi - 1) = (\pi - 1)(\pi' - 1) = p + 1 - t$ with $|t| \leq 2\sqrt{p}$ (Hasse's Theorem) and whose invariant is a root of a fixed polynomial $H_D(X)$ (depending only upon D) modulo p.*

The computation of the polynomials H_D is dealt with in [18, 19] (see also [14, 15]).

We now explain how the preceding theorems are used in a *factor and conquer* algorithm similar to the DOWNRUN process of [24]. The first phase of the algorithm consists in finding a sequence $N_0 = N > N_1 > \cdots > N_k$ of probable primes such that: N_{i+1} prime $\Longrightarrow N_i$ prime. The second then proves that each number is prime, starting from N_k.

Procedure SearchN

1. $i := 0$; $N_0 := N$;
2. find a fundamental discriminant $-D$ such that (N_i) splits as the product of two principal ideals in $\mathbf{Q}(\sqrt{-D})$;
3. for each solution of $(N_i) = (\pi)(\pi')$, find all factors of $m_\pi = (\pi - 1)(\pi' - 1)$ less than a given bound B and let N_π be the corresponding cofactor;
4. **if** one of the N_π is a probable prime **then** set $N_{i+1} := N_\pi$, store $\{N_i, D, \pi, m\}$, $i := i + 1$, and go to step 2 **else** go to step 3.
5. **end.**

The second phase consists in proving that the numbers N_i are indeed primes: For each i, find a curve E whose invariant is a root of $H_{D_i}(X)$ modulo p and check the condition of theorem (2). For technical details, we refer to [18].

5. Implementation and some timings. I have implemented Atkin's algorithm on a SUN 3/60 (12 Mo) using the BigNum package described in [12]. For a comparison of my arithmetic with the one used by Cohen and Lenstra, see [20].

We list in Table 1 the time needed to test a number of d words of 32 bits with my program, for $d = 2(2)20$. Time are in seconds.

d	min	max	mean	st. dev.	d	min	max	mean	st. dev.
2	4.7	15.7	8.8	2.6	12	485.7	1278.7	746.4	227.3
4	14.6	40.5	25.5	7.1	14	700.5	1413.0	1037.3	153.2
6	46.8	126.6	85.9	22.2	16	1106.6	3577.1	1909.6	668.0
8	102.4	266.7	159.1	43.8	18	1578.7	5164.7	2858.4	802.4
10	191.2	609.7	357.5	97.0	20	3233.8	9025.3	5252.6	1483.0

Table 1: Time for testing a d word number for primality.

6. Titanic primes. Following Yates [25], a prime number with more than 1000 digits is called a *Titanic prime* (see also [21]). Let us explain how the author found some Titanic primes with Atkin's algorithm.