BUILDING CYCLIC ELLIPTIC CURVES MODULO LARGE PRIMES

François Morain *
INRIA, B. P. 105
78153 LE CHESNAY CEDEX (France)
morain@inria.inria.fr

Abstract

Elliptic curves play an important rôle in many areas of modern cryptology such as integer factorization and primality proving. Moreover, they can be used in cryptosystems based on discrete logarithms for building one-way permutations. For the latter purpose, it is required to have cyclic elliptic curves over finite fields. The aim of this note is to explain how to construct such curves over a finite field of large prime cardinality, using the ECPP primality proving test of Atkin and Morain.

1 Introduction

Elliptic curves prove to be a powerful tool in modern cryptology. Following the original work of H. W. Lenstra, Jr. [18] concerning integer factorization, many researchers have used this new idea to work out primality proving algorithms [8, 14, 2, 4, 22] as well as cryptosystems [21, 16] generalizing those of [12, 1, 9]. Recent work on these topics can be found in [20, 19].

More recently, Kaliski [15] has used elliptic curves in the design of one-way permutations. For this, the author needs elliptic curves which are cyclic and the easiest solution is to build elliptic curves with squarefree order. The aim of this paper is to show how to construct such elliptic curves using some byproducts of the Elliptic Curve Primality Proving (ECPP) algorithm of Atkin and Morain [4].

The problem of building elliptic curves of given order in finite fields of small characteristic is dealt with in [5] and our work can be seen as solving the same problem in large characteristic.

The paper is organized as follows. Section 2 contains a brief summary of the properties of elliptic curves modulo some prime p. Section 3 gives the heart of ECPP. Section 4 describes a theoretical means of building curves of given order and it is shown that the running time of this procedure would be exponential in $\log p$. Section 5 explains how ECPP can be used to find cyclic curves in a faster way, the running time of the process being that of ECPP that is conjectured to be polynomial with complexity $O((\log p)^{5+\epsilon})$.

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

2 Elliptic curves modulo p

2.1 Group law

We briefly describe some properties of elliptic curves. For more information, see [25].

An elliptic curve E over a field $\mathbf{Z}/\mathrm{p}\mathbf{Z}$ with p a prime greater than 3 can be described as a pair (a, b) of elements of $\mathbf{Z}/\mathrm{p}\mathbf{Z}$ such that $\Delta(E) = -16(4a^3 + 27b^2)$ is invertible in $\mathbf{Z}/\mathrm{p}\mathbf{Z}$. This quantity is called the *discriminant* of E. The set of points of E, noted $E(\mathbf{Z}/p\mathbf{Z})$ is the set of triples $(x : y : z)$ of elements of $\mathbf{Z}/\mathrm{p}\mathbf{Z}$ that are solution of

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

These triples can be interpreted as the coordinates of points in the projective plane of $\mathbf{Z}/\mathrm{p}\mathbf{Z}$. There is a well known law on $E(\mathbf{Z}/p\mathbf{Z})$. This is called the *tangent-and-chord* method and the law is noted additively. The neutral element is just the point at infinity: $O_E = (0 : 1 : 0)$.

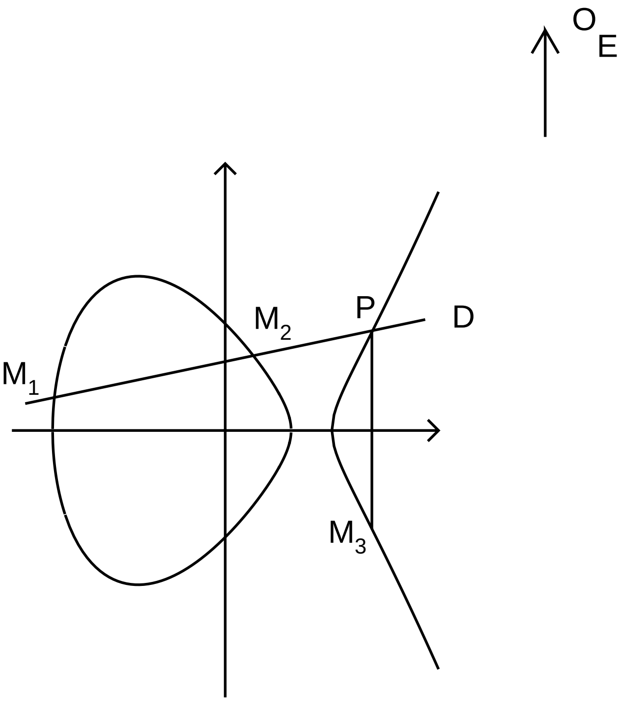

Figure 1: An elliptic curve over $\mathbf{R}$.

In order to add two points $M_1 = (x_1 : y_1 : 1)$ and $M_2 = (x_2 : y_2 : 1)$ on E, resulting in $M_3 = (x_3 : y_3 : z_3)$, 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

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

We define also the *invariant* of the curve E, noted $j(E)$:

$$j(E) = -\frac{12^3 a^3}{\Delta(E)}.$$

We then have the following easy result.

Proposition 1 *All elements of* $\mathbf{Z}/p\mathbf{Z}$ *are invariant of an elliptic curve.*

Proof: Let j_0 be an element of $\mathbf{Z}/\mathrm{p}\mathbf{Z}$. We look for an elliptic curve $E = (a, b)$ such that $j(E) = j_0$. If $j_0 = 0$, take $a = 0$, and any nonzero b. If $j_0 = 1728$, take any nonzero a and $b = 0$. In the general case, let $k = j_0/(1728 - j_0)$ and choose $a = 3k, b = 2k$.

Among the interesting and deep properties of these objects, we note the following. (We use the notation $\#\mathcal{A}$ to designate the cardinality of a set $\mathcal{A}$.)

Theorem 1 (Hasse) *Let m be the cardinality of an elliptic curve* $E(\mathbf{Z}/p\mathbf{Z})$*, then*

$$(\sqrt{p} - 1)^2 \leq m \leq (\sqrt{p} + 1)^2. \tag{1}$$

We use the notations of [18] for what follows and we refer the reader to it for more information.

Theorem 2 (Deuring [11]) *Let t be any integer such that $|t| \leq 2\sqrt{p}$. Letting $K(d)$ denote the Kronecker class number of d, there exists $K(t^2 - 4p)$ elliptic curves over* $\mathbf{Z}/p\mathbf{Z}$ *with number of points $m = p + 1 - t$, up to isomorphisms.*

Concerning the group structure of $E(\mathbf{Z}/p\mathbf{Z})$, we have:

Theorem 3 (Cassels [7]) *The group* $E(\mathbf{Z}/p\mathbf{Z})$ *is either cyclic or the product of two cyclic groups or order m_1 and m_2 that satisfy*

$$m_1 | m_2, \quad m_1 | \gcd(m, p - 1), \tag{2}$$

where $m = \#E(\mathbf{Z}/p\mathbf{Z})$.

Note that if m is squarefree, then surely $E(\mathbf{Z}/p\mathbf{Z})$ is cyclic.

2.2 Twists

We define the *twisted* curve E' of E as the curve

$$E' : y^2 z = x^3 + ac^2 xz^2 + bc^3 z^3,$$

where c is any non-quadratic residue modulo p. The main point in this is that if the cardinality of E is $m = p + 1 - t$, then $\#E'(\mathbf{Z}/p\mathbf{Z}) = p + 1 + t$. Note that E and its twist have the same invariant j_0.

2.3 Computing $\#E(\mathbf{Z}/p\mathbf{Z})$

From a theoretical point of view, there exists an algorithm of Schoof's that solves the problem in time polynomial in $\log p$, see [23]. However, it appears difficult to implement, even after some improvements of Atkin [3] and Elkies [13]. In practice, it is not feasible as soon as p has more than 65 decimal digits.

3 Overview of ECPP

The following results are at the heart of the Elliptic Curve Primality Proving algorithm in [4]. The first one can be found as [10, Prop. (5.29)] and the second one is a summary of the theory involved in [4].

Theorem 4 *Let p be a prime number and D any positive integer. Then $4p = x^2 + Dy^2$ has a solution in integers (x, y) if and only if $-D$ is a quadratic residue modulo p and the polynomial $H_D(X)$ has a root modulo p, where $H_D(X)$ is a monic polynomial with integer coefficients depending on D only.*

Theorem 5 *Let p be a prime that can be written as $4p = x^2 + Dy^2$ for a given D. Then there exists an elliptic curve E defined over $\mathbf{Z}/p\mathbf{Z}$ such that $4\#(E(\mathbf{Z}/p\mathbf{Z})) = (x-2)^2 + Dy^2$. Moreover, this curve can be computed explicitly using any root of the polynomial $H_D(X)$ modulo p.*

The algorithm then proceeds as in the classical DOWNRUN process of the well known primality proving algorithms based on the converse of Fermat's Theorem [6, 22].

4 Building curves of given order

Let p be a given prime number greater than 3. Suppose we want to build an elliptic curve of order m, where m satisfies (1). We will use the theory of ECPP to achieve this. The algorithm runs as follows:
procedure `BuildCurveGivenM`(p)

1. compute $t = p + 1 - m$ and $D = 4p - t^2$;
2. compute $H_D(X)$, the minimal polynomial of $j(\sqrt{D})$ where
$$j(z) = \frac{\left(1 + 240 \sum_{k\geq 1} \frac{k^3 q^k}{1-q^k}\right)^3}{q \prod_{k\geq 1}(1-q^k)^{24}}$$
with $q = \exp(2i\pi z)$ (see [4]);
3. find a root j_0 of $H_D(X) \equiv 0 \bmod p$;
4. build the curve E of invariant j_0 and cardinality m.

5. **end.**

The validity of this method is easily seen once we remark that $4p = t^2 + D$ and that the Theorems 4 and 5 of the preceding section apply.

Note also that there are a lot of technical details involved in such computations and the interested reader should consult [4, 22].

Example. Suppose that $p = 101$. By Hasse's theorem, a good m satisfies: $82 \leq m \leq 122$. Let us try to build a curve of cardinality $m = 85$. We get $t = 17$ and $D = 5 \times 23$. Using the algorithms described in [4], we compute

$$H_{115}(X) = X^2 + 427864611225600X + 130231327260672000.$$

This polynomial has two roots modulo 101, namely $\{67, 96\}$. We choose $j_0 = 67$ and get

$$k = 98, a = 3k = 92, b = 2k = 95.$$

Next, we select the point $(1 : 17 : 1)$ on the curve

$$E : y^2z = x^3 + axz^2 + bz^3 \bmod p.$$

But we find that

$$85P = (24 : 88 : 1)$$

and thus the cardinality of $E(\mathbb{Z}/101\mathbb{Z})$ is not m. We then consider the twisted curve E' obtained by replacing a (resp. b) by ac^2 (resp. bc^3) with $c = 2$. On

$$E' : y^2z = x^3 + 65xz^2 + 53z^3$$

we take $P' = (7 : 12 : 1)$ and find that

$$85P' = O_{E'}.$$

It is now easy to verify that P' is a point of maximal order on E'.

A rough analysis. We can now state the following result.

Proposition 4.1 *The running time of* `BuildCurveGivenM` *is exponential in* $\log p$*.*

Proof: By Siegel's Theorem [24], we know that $h(-D)$ is $O(D^{1/2+\epsilon})$. Hence, we may want to find D small. If we brutally apply the preceding algorithm, we require that m be as close of $(\sqrt{p} \pm 1)^2$ as possible. This implies that D is $O(\sqrt{p})$, yielding $h(-D) = O(p^{1/4+\epsilon})$.

5 Finding cyclic curves

Let p be as usual a given (large) prime. Suppose now that we do not insist on having a curve with given number of points, but simply that the curve be cyclic. This is the case in [15]. The easiest way to do this is to find a curve with squarefree order. It then follows from Theorem 3 that the resulting curve is cyclic. Note that we can relax this condition by imposing that any prime factor dividing m with a multiplicity greater than 1 does not divide $p - 1$:

$$q^2 \mid m \Rightarrow q \nmid p - 1.$$

5.1 Brute force

Let us first consider the following brute force algorithm.

procedure `BruteForce`(p)

repeat

choose E (i.e. a and b) at random and compute $m = \#E(\mathbf{Z}/p\mathbf{Z})$ using Schoof's algorithm

until m is squarefree.

From a theoretical point of view, this is quite nice, since the proportion of squarefree numbers is $6/\pi^2 \approx 0.608$ and that Schoof's algorithm runs in polynomial time. However, this is not a practical algorithm.

Let us turn to a more subtle way. We simply use ECPP and just modify it in such a way that we select a squarefree number of points in the process. The idea is that we will find a good squarefree m by looking at a list of D with small class numbers for which $4p = x^2 + Dy^2$. Once we find a good m, we can build the curve by using a process similar to that of `BuildCurveGivenM`, but this time, the degree of H_D is small. The algorithm is then

procedure `ModifiedECPP`(p)

1. **repeat**

    1. find D such that $4p = x^2 + Dy^2$; compute $m = ((x-2)^2 + Dy^2)/4$

    until m is squarefree and m is completely factored, maybe with a large prime cofactor.

2. Build E as in `BuildCurveGivenM`. It is cyclic.

3. **end.**

To examplify this idea, take the smallest 100-digit prime number, namely

$$p = 10^{99} + 289.$$

Using ECPP, we find that

$$4p = A^2 + 1435B^2$$

with

$$A = 2122739902357851560845466093533544718303747803698 9,$$

$$B = 1572719859536665825156799896734976642256008720081.$$

We get

$$m = p + 1 - A = 7 \times 73 \times p_1$$

where p_1 is a probable prime. In order to prove the primality of p, we have to find a curve E of cardinality m. The degree of $H_{1435}(X)$ is equal to 4 and it is easy to compute this polynomial. We find that the right curve is $E : y^2z = x^3 + axz^2 + bz^3$ with

$$a = 8933258078031557797124312958905486309863421738766075186445504421131578950552451598544925757586521766,$$

$$b = 1861390451603215221795633533417382360591608356926510998535476050695658425870339737628160737564984 61$$

and E is cyclic with generator $P = (x : y : 1)$ where

$$x = 9087363263509253244229640436496602308174289454146419496648433254196350092836374662816982112684223 60,$$

$$y = 8098643551017452328053732456978618677062926871100236805706128274503981408728607257049016556102808 10.$$

We end this by the following results.

Conjecture 5.1 *Procedure* `ModifiedECPP` *has running time* $O((\log p)^{5+\epsilon})$.

Proof: It is easy to see that the complexity of `ModifiedECPP` is at most that of ECPP, which can be heuristically estimated to $O((\log p)^{5+\epsilon})$ (see [17]).

Acknowledgments. The author wants to thank A. Miyaji for some valuable remarks on the preliminary version of this paper.

References

[1] L. M. Adleman, R. L. Rivest, and A. Shamir. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM 21*, 2 (1978), 120–126.

[2] A. O. L. Atkin. Manuscript. Lecture Notes of a conference Boulder (Colorado), Aug. 1986.

[3] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime. Draft, 1988.

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

[5] T. Beth and F. Schaefer. Non supersingular elliptic curves for public key cryptosystems. In *Advances in Cryptology – EUROCRYPT '91* (1992), D. Davies, Ed., Springer–Verlag. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Brighton, United Kingdom, April 8–11, 1991.

[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] J. W. S. Cassels. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc. 41* (1966), 193–291.

[8] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. Research report RC 11262, IBM, Yorktown Heights, 1985.

[9] D. Coppersmith, A. M. Odlyzko, and R. Schroeppel. Discrete logarithms in GF(p). *Algorithmica 1* (1986), 1–15.

[10] D. A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley & Sons, 1989.

[11] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg 14* (1941), 197–272.

[12] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. on Information Theory IT-22-6* (Nov. 1976).

[13] N. Elkies. Computing the number of points on an elliptic curve modulo p. Email to Morain, 1990.

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

[15] B. S. Kaliski, Jr. One-way permutations on elliptic curves. *J. of Cryptology 3*, 3 (1991), 187–199.

[16] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp. 48*, 177 (Jan. 1987), 203–209.

[17] A. K. Lenstra and H. W. Lenstra, Jr. Algorithms in number theory. In *Handbook of Theoretical Computer Science*, J. van Leeuwen, Ed., vol. A: Algorithms and Complexity. North Holland, 1990, ch. 12, pp. 674–715.

[18] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2) 126* (1987), 649–673.

[19] A. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curves logarithms to logarithms in a finite field. Tech. rep., University of Waterloo, 1990. Preliminary version.

[20] A. Menezes and S. A. Vanstone. The implementation of elliptic curve cryptosystems. In *Advances in Cryptology – AUSCRYPT'90* (1990), J. Seberry and J. Pieprzyk, Eds., no. 453 in Lecture Notes in Comput. Sci., Springer–Verlag, pp. 2–13. Proceedings, Sysdney (Australia), January 1990.

[21] V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology – CRYPTO'86* (1987), A. M. Odlyzko, Ed., vol. 263 of *Lecture Notes in Comput. Sci.*, Springer-Verlag, pp. 417–426. Proceedings, Santa Barbara (USA), August11–15, 1986.

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

[23] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp. 44* (1985), 483–494.

[24] C. L. Siegel. Über die Classenzahl quadratischer Zahlkörper. *Acta Arith. 1* (1935), 83–86.

[25] J. H. Silverman. *The arithmetic of elliptic curves*, vol. 106 of *Graduate Texts in Mathematics*. Springer, 1986.