9

AN IMPLEMENTATION OF THE ELLIPTIC CURVE INTEGER FACTORIZATION METHOD

Wieb Bosma* and Arjen K. Lenstra**

* *School of Mathematics and Statistics*
University of Sydney
Sydney NSW 2006
Australia
wieb@maths.su.oz.au

** *Room MRE–2Q334*
Bellcore
445 South Street
Morristown, NJ 07960
U. S. A.
lenstra@bellcore.com

ABSTRACT

This paper describes the second author's implementation of the elliptic curve method for the factorization of integers as it is currently available in the computational algebra package Magma, which is under development at the University of Sydney.

1991 Mathematics Subject Classification: 11Y05, 11A51, 11G05, 11–04.

1 INTRODUCTION

The *elliptic curve method* (ECM) is an integer factorization method that was proposed by H. W. Lenstra, Jr., in 1985 [9]. Several authors (cf. [1, 11]) have proposed practical improvements on the original method. The resulting implementations of ECM currently provide the fastest means of finding factors of up to approximately 30 decimal digits. The purpose of this paper is to document the Magma implementation of ECM, which is based on a combination of ideas from [1, 3, 11, 16].

In Section 2 we recapitulate some basic facts about elliptic curves. In Section 3 we will describe the very simple and elegant ideas behind the original algorithm, and we will give an overview of the practical variant that we will describe in detail in

W. Bosma and A. van der Poorten (eds.), Computational Algebra and Number Theory, 119–136.

later sections. Section 4 is devoted to two different models of elliptic curves and the explicit addition algorithms on them. In Sections 5 and 6 the two main steps of ECM are described. Finally, in Section 7 we present some examples.

2 ELLIPTIC CURVES

To define elliptic curves modulo some integer n, we first summarize well-known results for the special case that n is prime. Although these results are readily generalized to arbitrary finite fields, or to fields in general, we restrict our attention to prime order fields and refer the reader to [15].

2.1 Elliptic curves over $\mathbf{F}_p$. Let $p > 3$ be a prime number. An *elliptic curve* $E = E_{a,b}$ *over a finite field* $\mathbf{F}_p$ of order p consists of a pair $a, b \in \mathbf{F}_p$ for which $4a^3 + 27b^2 \neq 0$. This pair is to be thought of as coefficients for a Weierstraß model

$$Y^2 Z = X^3 + aXZ^2 + bZ^3 \tag{1}$$

of E. The *set of points* $E(\mathbf{F}_p)$ of E over $\mathbf{F}_p$ is the set of projective solutions $(x : y : z)$ over $\mathbf{F}_p$ to the Weierstraß equation (1); here a projective point $(x : y : z)$ over $\mathbf{F}_p$ is an equivalence class of triples $(0,0,0) \neq (x,y,z) \in (\mathbf{F}_p)^3$, under the equivalence

$$(x,y,z) \sim (x',y',z') \iff \exists \alpha \in \mathbf{F}_p^* : x' = \alpha x,\ y' = \alpha y,\ z' = \alpha z$$

where $\mathbf{F}_p^*$ denotes the multiplicative group of units of $\mathbf{F}_p$. Since z may be thought of as the denominator of the point $(x : y : z)$, we will call the elements of $E(\mathbf{F}_p)$ with $z \neq 0$ the *finite points* on E; the point $O = (0 : 1 : 0)$ is the only point on E *at infinity*.

The set $E(\mathbf{F}_p)$ forms an abelian group, usually written additively. The zero element is the point $O = (0 : 1 : 0)$.

The addition of points $P = (x_1 : y_1 : z_1)$ and $Q = (x_2 : y_2 : z_2)$ can be given explicitly and uniformly by simple polynomials in the coordinates of the points and the coefficient a as follows, using the rule that the sum of two points on the curve is the opposite of the third point of intersection of the curve with the line joining the two points (see [15] for more details). First of all $P + O = O + P = P$ for any P. Next assume that both P and Q are non-zero. If $x_1 = \alpha x_2, y_1 = -\alpha y_2$ and $z_1 = \alpha z_2$ for some $\alpha \in \mathbf{F}_p$, then $P + Q = O$; in other words, the opposite $-(x : y : z)$ of a point on E is given by $(x : -y : z)$. In all other cases the intersection of the curve and the line $y = \lambda x + \nu z$ joining P and Q is determined, where this line is taken to be the tangent to the curve if $P = Q$. Explicitly, with

$$\lambda = \begin{cases} \dfrac{3x_1^2 + a z_1^2}{2 y_1 z_1} & \text{if } P = Q \\ \dfrac{y_1 z_2 - y_2 z_1}{x_1 z_2 - x_2 z_1} & \text{if } P \neq Q \end{cases} \tag{2}$$

we find $P+Q=(x_3:y_3:z_3)$ with

$$\begin{aligned}\frac{x_3}{z_3} &= \lambda^2-\frac{x_1}{z_1}-\frac{x_2}{z_2}\\ \frac{y_3}{z_3} &= \lambda\left(\frac{x_1}{z_1}-\frac{x_3}{z_3}\right)-\frac{y_1}{z_1}\,.\end{aligned} \tag{3}$$

Two elliptic curves $E=E_{a,b}$ and $E'=E_{a',b'}$ over $\mathbf{F}_p$ are *isomorphic* if there exists $u\in\mathbf{F}_p^*$ such that $a'=u^4a$ and $b'=u^6b$; the map sending $(x:y:z)$ to $(u^2x:u^3y:z)$ gives an isomorphism between the groups of points of E and E'.

2.2 Elliptic curves modulo n. We must generalize the above concept of elliptic curves slightly, to define curves modulo any integer n; from now on we will assume that n is not divisible by 2 or 3. An *elliptic curve $E=E_{a,b}$ over $\mathbf{Z}/n\mathbf{Z}$* consists of a pair $a,b\in\mathbf{Z}/n\mathbf{Z}$ for which $4a^3+27b^2\in(\mathbf{Z}/n\mathbf{Z})^*$. The *set of points $E(\mathbf{Z}/n\mathbf{Z})$ of E modulo n* is the set of projective solutions $(x:y:z)$ to (1) over $\mathbf{Z}/n\mathbf{Z}$; a projective point $(x:y:z)$ over $\mathbf{Z}/n\mathbf{Z}$ is an equivalence class of triples $(x,y,z)\in(\mathbf{Z}/n\mathbf{Z})^3$ for which $\gcd(x,y,z,n)=1$, under the equivalence

$$(x,y,z)\sim(x',y',z') \iff \exists\alpha\in(\mathbf{Z}/n\mathbf{Z})^* : x'=\alpha x,\ y'=\alpha y,\ z'=\alpha z\,.$$

Again it is true that $E(\mathbf{Z}/n\mathbf{Z})$ can be made into an abelian group [10], but we will not need this fact. Note that over $\mathbf{Z}/n\mathbf{Z}$ it is not necessarily true any more that $O=(0:1:0)$ is the only point on E with $z=0$.

We will call the elements of $E(\mathbf{Z}/n\mathbf{Z})$ with $z=1$ *everywhere finite*, for the following reason. Taking $\bar{a}=a \bmod p$ and $\bar{b}=b \bmod p$ modulo some prime p dividing n, the elliptic curve $E_{a,b}$ over $\mathbf{Z}/n\mathbf{Z}$ gives rise to an elliptic curve $E_{\bar{a},\bar{b}}$ over $\mathbf{F}_p$. Any point in $E(\mathbf{Z}/n\mathbf{Z})$ gives a point in $E(\mathbf{F}_p)$ when we take its coordinates modulo p (*reduction of E modulo p*). Only those elements of $E(\mathbf{Z}/n\mathbf{Z})$ that are everywhere finite yield a finite point on E over $\mathbf{F}_p$ for every p dividing n. Note that a triple (x,y,z) with $x,y,z\in\mathbf{Z}/n\mathbf{Z}$ satisfying (1) thus defines an everywhere finite point if and only if $\gcd(z,n)=1$.

Two curves $E=E_{a,b}$ and $E'=E_{a',b'}$ over $\mathbf{Z}/n\mathbf{Z}$ will be called *isomorphic* again if there exists $u\in(\mathbf{Z}/n\mathbf{Z})^*$ such that $a'=u^4a$ and $b'=u^6b$.

2.3 Partial addition and scalar multiplication. For an elliptic curve modulo n a *partial addition* algorithm is an algorithm that does the following. Given two points $P,Q\in E(\mathbf{Z}/n\mathbf{Z})$ that are each either O or everywhere finite, the algorithm determines either a non-trivial divisor of n, or a point $R\in E(\mathbf{Z}/n\mathbf{Z})$ that again is O or everywhere finite, but in any case has the property that for every prime divisor p of n the reductions P_p,Q_p,R_p of P,Q,R modulo p satisfy $R_p=P_p+Q_p$, in the abelian group $E(\mathbf{F}_p)$.

We will describe partial addition algorithms explicitly in Section 4.

By repeated application of the partial addition algorithm, one gets a *partial scalar multiplication* algorithm which, for given $k \in \mathbf{Z}_{\geq 1}$ and everywhere finite point $P \in E(\mathbf{Z}/n\mathbf{Z})$, determines either a non-trivial divisor of n, or a point $R \in E(\mathbf{Z}/n\mathbf{Z})$ that may be $(0:1:0)$ or everywhere finite, with the property that the reduction modulo any prime p dividing n satisfies $R_p = kP_p$ in $E(\mathbf{F}_p)$.

3 THE ELLIPTIC CURVE METHOD

Lenstra's original elliptic curve method can be briefly described as follows.

3.1 Elliptic curve method. Let $n \in \mathbf{Z}_{>1}$ be an integer coprime to 6, and not of the form $n = m^e$ with $m, e \in \mathbf{Z}_{>1}$. To find a non-trivial factor of n, repeat the following two steps until such factor has been found.

(i) Select a random pair (E, P), consisting of an elliptic curve E modulo n and an everywhere finite point P on E.

(ii) Select a suitable positive integer k and apply the partial multiplication algorithm to compute $Q = kP$.

3.2 Remarks. The obvious way to choose a pair (E, P) of an elliptic curve and a point, is to put $z = 1$, choose $x, y, a \in \mathbf{Z}/n\mathbf{Z}$ at random, and let b be determined by the equation $y^2z = x^3 + axz^2 + bz^3$. (We will show in Section 5 what we do in practice.) It may be that $\gcd(n, abxy)$ is non-trivial, in which case the algorithm terminates in Step (i). Usually however, a factor of n will be found in Step (ii), during the execution of the partial multiplication algorithm. We explain next how this can happen, and how to choose k to improve the chances.

3.3 The choice of k. Suppose that p and q are different prime factors of n. If k is a multiple of the order of P_p in $E(\mathbf{F}_p)$ but not a multiple of the order of P_q in $E(\mathbf{F}_q)$, then the partial multiplication algorithm on k and P must yield a non-trivial divisor of n. For suppose that it succeeded in finding the point $Q = kP$ on $E(\mathbf{Z}/n\mathbf{Z})$; then Q_p must equal $kP_p = O$, the zero element in $E(\mathbf{F}_p)$, so Q cannot be everywhere finite and hence it equals $(0:1:0) \in E(\mathbf{Z}/n\mathbf{Z})$. But in that case also $kP_q = Q_q = O$ in $E(\mathbf{F}_q)$, which contradicts the assumption that k is not a multiple of the order of P_q in $E(\mathbf{F}_q)$.

If one chooses k as the product of "small" prime powers, it may happen that after some trials in (3.1) one will hit a pair (E, P) for which the order of P is a divisor of k on E modulo the smallest prime divisor p of n, but not so for the other primes dividing n. Let

$$B_1 = e^{(1+o(1))\sqrt{(\log p \log\log p)/2}} \quad \text{with} \quad p \to \infty .$$

Under a mild (but unproved) hypothesis on the smoothness of random integers in intervals, it has been shown in [9] that using ECM one may expect to find the smallest prime p dividing n in B_1 trials with

$$k = \prod_{r \leq B_1} r^{t_r} \tag{4}$$

where $t_r \in \mathbf{Z}_{\geq 0}$ is maximal such that $r^{t_r} \leq p + 2\sqrt{p} + 1$. Because each trial takes time $O((\log n)^2 B_1)$ this leads to a total expected time $O((\log n)^2 B_1^2)$. The value for k depends on p, thus is not known beforehand. Typically, for each new trial one selects a k that is slightly bigger than the previous one. In this way both the run-time and the probability of success per trial increase slowly. See Section 7 for examples.

3.4 Practical improvements. So far, we have only described ECM in theory. In practice the performance of ECM is greatly enhanced by adding a *second phase* to each trial. One possible extension is to compute qQ for a number of primes q that do not occur in k. If n has a prime divisor p such that the order of P_p divides k times one of the qs, then p will most likely be detected. This computation can be carried out quite efficiently, as shown in [11], and considerably increases the probability of success per trial. Another extension is to apply the idea from Pollard's ρ-method by simulating a random walk in the group generated by Q and wait for a collision to occur, cf. [1]. This is the approach that we have chosen in our implementation for reasons described in Section 7; it will be described in detail in Section 6.

Other improvements that have been incorporated in our implementation are concerned with the choice of the initial curve and point, and the parameterization of the curve. They will be described in sections 4 and 5.

As a result, our ECM implementation can be outlined as follows.

3.5 Algorithm. Let $n \in \mathbf{Z}_{>1}$ be an integer coprime to 6, and not of the form $n = m^e$ with $m, e \in \mathbf{Z}_{>1}$. Repeat the following steps until a non-trivial factor of n has been found.

(i) *Curve setup*: select a random pair (E, P) consisting of an elliptic curve E modulo n and an everywhere finite point P on $E(\mathbf{Z}/n\mathbf{Z})$, such that the order of $E(\mathbf{F}_p)$ for any prime p dividing n is divisible by 12, cf. Section 5.

(ii) *First phase*: select a suitable positive integer k and apply the partial multiplication algorithm to determine $Q = kP$, cf. Section 5.

(iii) *Second phase*: simulate a random walk $Q_1 = (x_1 : y_1 : 1)$, $Q_2 = (x_2 : y_2 : 1)$, ... in $<Q>$; compute $\gcd(n, \prod(x_i - x_j))$, for i, j as described in Section 6.

4 CURVE PARAMETERIZATIONS

In the first phase of Algorithm (3.5) it is advantageous to use another parametrization of the elliptic curve than the usual Weierstraß form; we follow the approach suggested by Chudnovsky, Montgomery, and Suyama (cf. [3]; [11]; [16]). For the second phase it is more efficient to transform back to the Weierstraß form (1).

In this section we describe partial addition and multiplication algorithms for both parameterizations of the elliptic curve.

4.1 Partial scalar multiplication in the Weierstraß model. We first describe a partial addition algorithm for two points $P, Q \in E(\mathbf{Z}/n\mathbf{Z})$, with E as in (1) (i.e., in the Weierstraß model), satisfying the description in (2.3). Next we discuss how this can be used to formulate a partial scalar multiplication algorithm. Because we will only encounter points $(x : y : z)$ that are either equal to the zero point $O = (0 : 1 : 0)$ or everywhere finite (i.e. $z = 1$), we will only keep track of the affine coordinates (x, y) of the non-zero points.

It should be understood that if any of the algorithms described here fails, a non-trivial factor of n has been detected. Because we only intend to apply them in algorithms that attempt to factor n, failure implies that the factoring attempt was successful.

4.1.1 ***Partial addition.*** Let $P, Q \in E(\mathbf{Z}/n\mathbf{Z})$, both either O or everywhere finite. We describe a method that either finds a non-trivial factor of n, or computes an element $R \in E(\mathbf{Z}/n\mathbf{Z})$ that can be interpreted as the sum $P + Q$ of P and Q, as in (2.3). First, for any P we have again that $P + O = O + P = P$. Now assume that P and Q are everywhere finite; we can work affinely: $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. If $x_1 = x_2$ and $y_1 = -y_2$, put $R = O$. Otherwise, attempt to compute (cf. (2))

$$\lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1} & \text{if } x_1 = x_2 \\ \dfrac{y_1 - y_2}{x_1 - x_2} & \text{if } x_1 \neq x_2 \end{cases}$$

in $\mathbf{Z}/n\mathbf{Z}$. If λ could be computed put $x = \lambda^2 - x_1 - x_2$ and $R = (x, \lambda(x_1 - x) - y_1)$ (cf. (3)); otherwise a non-trivial factor of n has been detected. It follows that a point can be doubled in eight additions, two squarings, two multiplications, and one inversion modulo n (where the multiplication by 3 accounts for two additions); addition of two distinct points can be done in six additions, one squaring, two multiplications and one inversion modulo n.

To compute $P - Q$, apply the above to P and $-Q = (x_2, -y_2)$.

4.1.2 ***Partial scalar multiplication.*** Let $P \in E(\mathbf{Z}/n\mathbf{Z})$ and let m be some positive integer. There are many ways to compute $mP \in E(\mathbf{Z}/n\mathbf{Z})$ (or a factor

of n) using (4.1.1). The ordinary "double and add"-strategy, for instance, works as follows. Let $m = \sum_{i=0}^{r} m_i 2^i$ with $m_i \in \{0,1\}$ and $m_r \neq 0$, and let $Q = P$. For $i = r-1, r-2, \ldots, 0$ in succession, first replace Q by $Q+Q$ and next if $m_i = 1$ replace Q by $Q+P$ (cf. (4.1.1)). As a result we have $Q = mP$ unless one of the steps failed, in which case a factor of n has been detected. For a randomly chosen m approximately half of the m_i will be equal to 1, so that mP can be computed in about 11 $\log_2 m$ additions, 2.5 $\log_2 m$ squarings, 3 $\log_2 m$ multiplications, and 1.5 $\log_2 m$ inversions modulo n.

Other strategies might use different addition chains and, for instance, minimize the number of doublings (which are more expensive than additions) and/or introduce subtractions (which are as hard as additions). In [4] the ordinary approach is used, but the ms are constructed such that there are only a few m_i equal to 1 per m; this led to a speed up of 18%. In Magma we use the 4-ary approach: write $m = \sum_{i=0}^{r} m_i 4^i$ with $m_i \in \{0,1,2,3\}$ and $m_r \neq 0$, pre-compute $3P$ if at least one of the m_i equals 3, and build mP in the obvious way using two doublings and at most one addition per i.

4.2 The Montgomery model. In this subsection we describe the model for elliptic curves proposed in [11].

Suppose that $(x : y : z)$ is a point on an elliptic curve given by the Weierstraß equation (1). Suppose moreover that the coefficients a, b of the curve are of the form

$$a = \left(1 - \tfrac{1}{3}\tilde{a}^2\right)\tilde{b}^{-2} \qquad \text{and} \qquad b = \left(\tfrac{2}{27}\tilde{a}^3 - \tfrac{1}{3}\tilde{a}\right)\tilde{b}^{-3} \tag{5}$$

for certain $\tilde{a}, \tilde{b}$ in the field of definition of the curve. A straightforward calculation then shows that the projective point $(\tilde{x} : \tilde{y} : \tilde{z}) = \left((\tilde{b}x - \frac{1}{3}\tilde{a}z) : \tilde{b}y : z\right)$ satisfies the equation:

$$\tilde{E}_{\tilde{a},\tilde{b}} \; : \quad \tilde{b}Y^2Z = X^3 + \tilde{a}X^2Z + XZ^2 \,. \tag{6}$$

Thus, a linear transformation converts the Weierstraß form (1) into the *Montgomery* form (6), if it exists for this particular curve. Conversely, the inverse of the above transformation clearly converts any curve in Montgomery form to a curve in Weierstraß form, and this represents an elliptic curve provided $4a^3 + 27b^2 \neq 0$; that is, $\tilde{b} \neq 0$ and $\tilde{a}^2 \neq 4$.

Below we will point out why partial multiplication is more efficient on a curve in Montgomery form. Since the elliptic curve method allows us a free choice of elliptic curve, we simply start out with a point on some curve in Montgomery form (see Section 5 on how this is done), and transform back to Weierstraß form for the second phase (cf. Remark (6.5)).

Let $\tilde{E} = \tilde{E}_{\tilde{a},\tilde{b}}$ be an elliptic curve over $\mathbf{Z}/n\mathbf{Z}$ in Montgomery form, where we assume that $\gcd\bigl(n, \tilde{b}(\tilde{a}+2)(\tilde{a}-2)\bigr) = 1$. The curve parameterization in (6) allows

us to compute the $\tilde{x}$ and $\tilde{z}$ coordinate of the sum of two points in $\tilde{E}(\mathbf{Z}/n\mathbf{Z})$, if the $\tilde{x}$ and $\tilde{z}$ coordinates of the two points and of their difference is known: in (4.3) we describe how this can be done (cf. [11]) and how it can be used in a partial scalar multiplication algorithm that, given the $\tilde{x}$ and $\tilde{z}$ coordinates of an initial point in $\tilde{E}(\mathbf{Z}/n\mathbf{Z})$, computes the $\tilde{x}$ and $\tilde{z}$ coordinate of any scalar multiple (or finds a factor of n). Since only the $\tilde{x}$ and $\tilde{z}$ coordinates are involved, it suffices to obtain an initial point $(\tilde{x} : \tilde{y} : \tilde{z}) \in \tilde{E}_{\tilde{a},\tilde{b}}(\mathbf{Z}/n\mathbf{Z})$ for which we can show the existence of $\tilde{y}$ without the need to actually construct it. More precisely, we will show in (5.1) how $\tilde{x}$, $\tilde{a}$ and $\tilde{b}$ can be chosen such that $\tilde{b}^{-1}(\tilde{x}^3 + \tilde{a}\tilde{x}^2 + \tilde{x})$ is the square of an integer $\tilde{y}$.

To indicate that the $\tilde{y}$-coordinate does not enter into any of the formulas, it will often be replaced by an underline ('_').

Let $(\tilde{x} : \_ : 1) \in \tilde{E}(\mathbf{Z}/n\mathbf{Z})$, with $\tilde{E} = \tilde{E}_{\tilde{a},\tilde{b}}$ as in (6), so $\tilde{b}\tilde{y}^2 = \tilde{x}^3 + \tilde{a}\tilde{x}^2 + \tilde{x}$ for some unspecified $\tilde{y}$ in $\mathbf{Z}/n\mathbf{Z}$. To transform any such point $(\tilde{x} : \_ : 1)$ to a point on a curve in the Weierstraß model (1), put

$$\begin{aligned} t &= \tilde{x}^3 + \tilde{a}\,\tilde{x}^2 + \tilde{x} \\ a' &= \left(1 - \tfrac{1}{3}\,\tilde{a}^2\right) t^{-2} \\ b' &= \tfrac{1}{3}\left(\tfrac{2}{9}\,\tilde{a}^3 - \tilde{a}\right) t^{-3} \end{aligned} \tag{7}$$

then

$$(x, y) = \left(\left(\tilde{x} + \tfrac{1}{3}\,\tilde{a}\right) t^{-1} : t^{-1} : 1\right) \in E_{a',b'}(\mathbf{Z}/n\mathbf{Z}) \tag{8}$$

provided that $t \in (\mathbf{Z}/n\mathbf{Z})^*$. Since $t = \tilde{b}\tilde{y}^2$, we see that $a = \tilde{y}^4 a'$ and $b = \tilde{y}^6 b'$, with a, b as in (5), and therefore $E_{a,b}$ and $E_{a',b'}$ are isomorphic (cf. (2.2)). Hence it is possible to transform to the Weierstraß form of the curve without explicitly specifying $\tilde{y}$. Since $\tilde{b}$ is also not needed here, and since it will not appear in the partial addition and multiplication below either, there will be no need to compute it.

Note that is not necessary to actually compute b or b' either, because it is not needed for the scalar multiplication in the Weierstraß model (cf. (4.1)).

4.3 The group law in the Montgomery model. We will use the transformation

$$(x, y, z) = \left(\frac{\tilde{x}}{\tilde{b}} + \frac{\tilde{a}\,\tilde{z}}{3\tilde{b}}\,,\ \frac{\tilde{y}}{\tilde{b}}\,,\ \tilde{z}\right) \tag{9}$$

to transform a point $(\tilde{x} : \tilde{y} : \tilde{z})$ on an elliptic curve in Montgomery model (6) to a point $(x : y : z)$ on the curve in Weierstraß form (1), with a, b as in (5). Combining this with the explicit group law from (2.1) (cf. (2) and (3)), we will derive the explicit group law on an elliptic curve over a finite field in Montgomery form. As in (4.1), this is used to define partial addition on such a curve over $\mathbf{Z}/n\mathbf{Z}$, by interpreting divisions as taking inverses modulo n (if possible).

Let $P = (\tilde{x}_1 : \tilde{y}_1 : \tilde{z}_1)$ and $Q = (\tilde{x}_2 : \tilde{y}_2 : \tilde{z}_2)$ be points on

$$\tilde{E}_{\tilde{a},\tilde{b}} \ : \ \tilde{b}\,Y^2 Z = X^3 + \tilde{a}\,X^2 Z + X\,Z^2\,.$$

If either point equals $(0 : 1 : 0)$ or if the points are opposites (i.e. $(\tilde{x}_1 : \tilde{y}_1 : \tilde{z}_1) = (\tilde{x}_2 : -\tilde{y}_2 : \tilde{z}_2)$), the sum $P+Q = (\tilde{x}_3 : \tilde{y}_3 : \tilde{z}_3)$ is found as usual. So suppose that this is not the case.

If $P \neq Q$ it follows from (2) and (9) that

$$\lambda = \frac{y_1 z_2 - y_2 z_1}{x_1 z_2 - x_2 z_1} = \frac{\tilde{y}_1 \tilde{z}_2 - \tilde{y}_2 \tilde{z}_1}{\tilde{x}_1 \tilde{z}_2 - \tilde{x}_2 \tilde{z}_1};$$

therefore (3), (6) and (9) imply

$$\begin{aligned}
\frac{\tilde{x}_3}{\tilde{z}_3} &= \tilde{b}\Big(\frac{\tilde{y}_1 \tilde{z}_2 - \tilde{y}_2 \tilde{z}_1}{\tilde{x}_1 \tilde{z}_2 - \tilde{x}_2 \tilde{z}_1}\Big)^2 - \Big(\frac{\tilde{x}_1}{\tilde{z}_1} + \frac{\tilde{x}_2}{\tilde{z}_2}\Big) - \tilde{a} \\
&= \frac{(\tilde{b}\,\tilde{y}_1^2 \tilde{z}_1 - \tilde{x}_1^3 - \tilde{a}\,\tilde{x}_1^2 \tilde{z}_1)\,\tilde{z}_2^3 + (\tilde{b}\,\tilde{y}_2^2 \tilde{z}_2 - \tilde{x}_2^3 - \tilde{a}\,\tilde{x}_2^2 \tilde{z}_2)\,\tilde{z}_1^3}{(\tilde{x}_1 \tilde{z}_2 - \tilde{x}_2 \tilde{z}_1)^2\,\tilde{z}_1 \tilde{z}_2} \\
&\quad + \frac{-2\tilde{b}\,\tilde{y}_1 \tilde{y}_2\,\tilde{z}_1^2 \tilde{z}_2^2 + \tilde{x}_1 \tilde{x}_2\,\tilde{z}_1 \tilde{z}_2\,(\tilde{x}_1 \tilde{z}_2 + \tilde{x}_2 \tilde{z}_1 + 2\tilde{a}\,\tilde{z}_1 \tilde{z}_2)}{(\tilde{x}_1 \tilde{z}_2 - \tilde{x}_2 \tilde{z}_1)^2\,\tilde{z}_1 \tilde{z}_2} \\
&= \frac{-2\tilde{b}\,\tilde{y}_1 \tilde{y}_2\,\tilde{z}_1 \tilde{z}_2 + \tilde{x}_1 \tilde{x}_2\,(\tilde{x}_1 \tilde{z}_2 + \tilde{x}_2 \tilde{z}_1 + 2\tilde{a}\,\tilde{z}_1 \tilde{z}_2) + (\tilde{x}_1 \tilde{z}_2 + \tilde{x}_2 \tilde{z}_1)\,\tilde{z}_1 \tilde{z}_2}{(\tilde{x}_1 \tilde{z}_2 - \tilde{x}_2 \tilde{z}_1)^2} \\
&= \frac{\tilde{b}\,(\tilde{x}_2 \tilde{y}_1 - \tilde{x}_1 \tilde{y}_2)^2\,\tilde{z}_1 \tilde{z}_2}{\tilde{x}_1 \tilde{x}_2\,(\tilde{x}_1 \tilde{z}_2 - \tilde{x}_2 \tilde{z}_1)^2}.
\end{aligned}$$

The difference $(\tilde{x}_4 : \tilde{y}_4 : \tilde{z}_4) = P - Q$ will then be given by

$$\frac{\tilde{x}_4}{\tilde{z}_4} = \frac{\tilde{b}\,(\tilde{x}_2 \tilde{y}_1 + \tilde{x}_1 \tilde{y}_2)^2 \tilde{z}_1 \tilde{z}_2}{\tilde{x}_1 \tilde{x}_2\,(\tilde{x}_1 \tilde{z}_2 - \tilde{x}_2 \tilde{z}_1)^2};$$

combined they imply

$$\begin{aligned}
\frac{\tilde{x}_3\,\tilde{x}_4}{\tilde{z}_3\,\tilde{z}_4} &= \frac{\tilde{b}^2(\tilde{x}_2^2\,\tilde{y}_1^2 - \tilde{x}_1^2\,\tilde{y}_2^2)^2 \tilde{z}_1^2 \tilde{z}_2^2}{\tilde{x}_1^2 \tilde{x}_2^2\,(\tilde{x}_1\,\tilde{z}_2 - \tilde{x}_2\,\tilde{z}_1)^4} = \frac{(\tilde{x}_2^2\,\tilde{b}\,\tilde{y}_1^2 \tilde{z}_1\,\tilde{z}_2 - \tilde{x}_1^2\,\tilde{b}\,\tilde{y}_2^2 \tilde{z}_2\,\tilde{z}_1)^2}{\tilde{x}_1^2 \tilde{x}_2^2\,(\tilde{x}_1\,\tilde{z}_2 - \tilde{x}_2\,\tilde{z}_1)^4} \\
&= \frac{\big(\tilde{x}_2^2 \tilde{z}_2\,(\tilde{x}_1^3 + \tilde{a}\,\tilde{x}_1^2 \tilde{z}_1 + \tilde{x}_1 \tilde{z}_1) - \tilde{x}_1^2 \tilde{z}_1\,(\tilde{x}_2^3 + \tilde{a}\,\tilde{x}_2^2 \tilde{z}_2 + \tilde{x}_2 \tilde{z}_2)\big)^2}{\tilde{x}_1^2 \tilde{x}_2^2\,(\tilde{x}_1\,\tilde{z}_2 - \tilde{x}_2\,\tilde{z}_1)^4} \qquad (10) \\
&= \frac{\tilde{x}_1^2 \tilde{x}_2^2\,\big((\tilde{x}_1 \tilde{x}_2 - \tilde{z}_1 \tilde{z}_2)(\tilde{x}_1 \tilde{z}_2 - \tilde{x}_2 \tilde{z}_1)\big)^2}{\tilde{x}_1^2 \tilde{x}_2^2\,(\tilde{x}_1\,\tilde{z}_2 - \tilde{x}_2\,\tilde{z}_1)^4} = \frac{(\tilde{x}_1\,\tilde{x}_2 - \tilde{z}_1\,\tilde{z}_2)^2}{(\tilde{x}_1\,\tilde{z}_2 - \tilde{x}_2\,\tilde{z}_1)^4}.
\end{aligned}$$

The latter equation will enable us to compute $\tilde{x}$ and $\tilde{z}$ for the sum of two points once they are known for the difference.

If $Q = P$ then (cf. (2), (5), and (9)), dropping the subscripts,

$$\lambda = \frac{3x^2 + az^2}{2yz} = \frac{\tilde{b}^{-2}\big(3(\tilde{x} + \frac{1}{3}\tilde{a}\,\tilde{z})^2 + (1 - \frac{1}{3}\tilde{a}^2)\tilde{z}^2\big)}{2\tilde{y}\tilde{z}\,\tilde{b}^{-1}} = \frac{3\tilde{x}^2 + 2\tilde{a}\,\tilde{x}\tilde{z} + \tilde{z}^2}{2\tilde{b}\,\tilde{y}\tilde{z}}$$

so by (3) and (9)

$$\frac{\tilde{x}_3}{\tilde{z}_3} = \tilde{b}\lambda^2 - 2\frac{\tilde{x}}{\tilde{z}} - \tilde{a} = \frac{\tilde{b}(3\tilde{x}^2 + 2\tilde{a}\,\tilde{x}\tilde{z} + \tilde{z}^2)^2 - 8\tilde{b}^2\,\tilde{x}\tilde{y}^2\tilde{z} - 4\tilde{a}\,\tilde{b}^2\,\tilde{y}^2\tilde{z}^2}{4\tilde{b}^2\,\tilde{y}^2\tilde{z}^2}$$

and therefore, using the equation of the curve again,

$$(11)\quad \frac{\tilde{x}_3}{\tilde{z}_3} = \frac{(\tilde{x}^2 - \tilde{z}^2)^2}{4\tilde{z}\,(\tilde{x}^3 + \tilde{a}\,\tilde{x}^2\tilde{z} + \tilde{x}\tilde{z}^2)} = \frac{(\tilde{x} + \tilde{z})^2\,(\tilde{x} - \tilde{z})^2}{4\tilde{x}\tilde{z}\big((\tilde{x} - \tilde{z})^2 + 4\,\tilde{x}\tilde{z}\,(\frac{\tilde{a}+2}{4})\big)}\,.$$

Note that neither $\tilde{y}_1$, $\tilde{y}_2$ nor $\tilde{b}$ appears in (10) or (11).

4.4 Scalar multiplication in the Montgomery model. We can now describe how any point in $\tilde{E}(\mathbf{Z}/n\mathbf{Z})$ can be doubled and how the sum of two distinct points in $\tilde{E}(\mathbf{Z}/n\mathbf{Z})$ can be computed if their difference is known, with $\tilde{E}$ as in (6). Finally, we present the resulting scalar multiplication. For any $(\tilde{x} : \_ : \tilde{z}) \in \tilde{E}(\mathbf{Z}/n\mathbf{Z})$ we keep track of $\tilde{x} - \tilde{z}$ and $\tilde{x} + \tilde{z}$ as well, at the cost of two additions.

4.4.1 ***Doubling.*** Let $(\tilde{x} : \_ : \tilde{z}) \in \tilde{E}(\mathbf{Z}/n\mathbf{Z})$, and assume that $\frac{1}{4}(\tilde{a} + 2)$ has been pre-computed. To compute $2(\tilde{x} : \_ : \tilde{z}) \in \tilde{E}(\mathbf{Z}/n\mathbf{Z})$ first compute $4\tilde{x}\tilde{z}$ as $(\tilde{x} + \tilde{z})^2 - (\tilde{x} - \tilde{z})^2$ in two squarings and one addition. Since

$$2(\tilde{x} : \_ : \tilde{z}) = \Big((\tilde{x} + \tilde{z})^2(\tilde{x} - \tilde{z})^2 : \_ : 4\tilde{x}\tilde{z}\,\big((\tilde{x} - \tilde{z})^2 + 4\,\tilde{x}\tilde{z} \cdot \tfrac{1}{4}(\tilde{a} + 2)\big)\Big)$$

by (11), doubling of a point can be done in four additions, two squarings and three multiplications, all of them modulo n.

4.4.2 ***Computing the sum given the difference*** (cf.[11]). Let $(\tilde{x}_i : \_ : \tilde{z}_i) \in \tilde{E}(\mathbf{Z}/n\mathbf{Z})$ for $i = 1, 2, 4$ such that $(\tilde{x}_1 : \_ : \tilde{z}_1) - (\tilde{x}_2 : \_ : \tilde{z}_2) = (\tilde{x}_4 : \_ : \tilde{z}_4)$ in $\tilde{E}(\mathbf{Z}/n\mathbf{Z})$. To compute $(\tilde{x}_1 : \_ : \tilde{z}_1) + (\tilde{x}_2 : \_ : \tilde{z}_2) \in \tilde{E}(\mathbf{Z}/n\mathbf{Z})$ first compute $t_1 = (\tilde{x}_1 - \tilde{z}_1)(\tilde{x}_2 + \tilde{z}_2)$ and $t_2 = (\tilde{x}_1 + \tilde{z}_1)(\tilde{x}_2 - \tilde{z}_2)$ in two multiplications. Put

$$\begin{aligned}(\tilde{x}_3 : \_ : \tilde{z}_3) &= (\tilde{z}_4(t_1 + t_2)^2 : \_ : \tilde{x}_4\,(t_1 - t_2)^2) \\ &= (4\,\tilde{z}_4\,(\tilde{x}_1\tilde{x}_2 - \tilde{z}_1\tilde{z}_2)^2 : \_ : 4\,\tilde{x}_4\,(\tilde{x}_1\,\tilde{z}_2 - \tilde{x}_2\,\tilde{z}_1)^2)\end{aligned}$$

which equals $(\tilde{x}_1 : \_ : \tilde{z}_1) + (\tilde{x}_2 : \_ : \tilde{z}_2)$ by (10); this takes two additions, two squarings, and two multiplications. It follows that the sum can be computed in four additions, two squarings, and four multiplications, all modulo n.

Notice that we need only three multiplications if $\tilde{z}_4 = 1$, and that $\tilde{b}$ does indeed not enter into any of the formulas.

4.4.3 ***Scalar multiplication.*** Let $P_1 = (\tilde{x}_1 : \_ : \tilde{z}_1) \in \tilde{E}(\mathbf{Z}/n\mathbf{Z})$, and let $m > 2$ be some odd positive integer. To compute $mP_1 \in \tilde{E}(\mathbf{Z}/n\mathbf{Z})$ we proceed as follows.

Let $(P_2, P_3) = (P_1, P_1 + P_1)$ be a pair of points in $\tilde{E}(\mathbf{Z}/n\mathbf{Z})$, computed using (4.4.1), let r be such that $2^r < m < 2^{r+1}$ and let $2^{r+1} - m = \sum_{i=0}^{r-1} m_i 2^i$ with $m_i \in \{0,1\}$. For $i = r-1, r-2, \ldots, 0$ in succession replace (P_2, P_3) by $(P_2 + P_3, P_3 + P_3)$ if $m_i = 0$ and by $(P_2 + P_2, P_2 + P_3)$ if $m_i = 1$; now because the difference $P_3 - P_2 = P_1$ throughout this computation, it can be carried out using just (4.4.1) and (4.4.2). As a result we have that the final P_3 equals $mP_1 \in \tilde{E}(\mathbf{Z}/n\mathbf{Z})$.

This takes $8 \log_2 m$ additions, $4 \log_2 m$ squarings and $7 \log_2 m$ multiplications; the latter can be reduced to $6 \log_2 m$ if $\tilde{z}_1 = 1$. Notice that for $i = 0$ (and therefore $m_0 = 1$ since m is odd) the computation of $P_2 + P_2$ can be omitted, and that $P_2 + P_2 = P_3$ if $m_{r-1} = 1$.

To compute mP_1 for even m we apply this procedure to P_1 and the odd part of m, followed by one or more doublings as in (4.4.1).

5 CURVE SET-UP AND FIRST PHASE

In this section we describe how we carry out Steps (i) and (ii) of Algorithm (3.5).

5.1 Curve setup. We follow Suyama's suggestion [16] to obtain a random curve and point on that curve. Let $u, v \in \mathbf{Q}$ be such that $uv(u^2-1)(9u^2-1) \neq 0$ and let $\tilde{a} = (-3u^4 - 6u^2 + 1)/(4u^3)$ and $\tilde{b} = (u^2-1)^2/(4uv^2)$. For p not dividing $\tilde{b}(\tilde{a}+2)(\tilde{a}-2)$ the equation (6) defines an elliptic curve, and for this choice of $\tilde{a}$ and $\tilde{b}$ the order of $\tilde{E}_{\tilde{a},\tilde{b}}(\mathbf{F}_p)$ will be divisible by 12. To obtain a non-trivial point $(\tilde{x}_0 : \_ : 1)$ on $\tilde{E}_{\tilde{a},\tilde{b}}$ over $\mathbf{Z}/n\mathbf{Z}$, one takes $\tilde{x}_0 = (3u/4) \bmod n$; this implies that u must be chosen such that

$$u\left(\tilde{x}_0^3 + \tilde{x}_0^2 \frac{-3u^4 - 6u^2 + 1}{4u^3} + \tilde{x}_0\right) = \frac{9 - 6u^2}{64}$$

is a square. This can for instance be achieved by putting $u = 6s/(s^2+6)$ for some randomly selected $s \in \mathbf{Z}/n\mathbf{Z}$ (cf. [11], also for other choices of initial points). Since explicit values for $\tilde{y}_0$ and $\tilde{b}$ are not needed, v can be left unspecified.

In the first phase we attempt to compute $Q = kP$, for some appropriately chosen integer k. As indicated in (3.3), the optimal choice for k (and the total number of trials in (3.5)) depends on the size of the smallest prime factor p of n. Because p is usually unknown in practice, one often simply picks some value for B_1, depending on the size of factors one would hope or expect to find, and defines

$$k = \prod_{\substack{q \text{ prime} \\ q \leq B_1}} q^{t_q} \tag{12}$$

where, unlike (4), $t_q \in \mathbf{Z}_{\geq 0}$ is maximal such that $q^{t_q} \leq B_1$ and the product ranges over the primes only; of course k is not actually computed. For examples of choices for B_1 we refer to Section 7. Putting it all together, we get the following.

5.2 First phase. Let $P \in \tilde{E}_{\tilde{a},\tilde{b}}(\mathbf{Z}/n\mathbf{Z})$ and B_1 be as above. For all $m = q^{t_q}$ as in (12) in succession, use (4.4.3) to compute the point $mP = (\tilde{x} : \_ : \tilde{z}) \in \tilde{E}_{\tilde{a},\tilde{b}}(\mathbf{Z}/n\mathbf{Z})$, then next attempt to compute $\tilde{z}^{-1} \bmod n$ and finally replace P by $(\tilde{x}\,\tilde{z}^{-1} : \_ : 1) \in \tilde{E}_{\tilde{a},\tilde{b}}(\mathbf{Z}/n\mathbf{Z})$.

After P has been replaced successfully by $kP \in \tilde{E}_{\tilde{a},\tilde{b}}(\mathbf{Z}/n\mathbf{Z})$ this way (i.e. if no factor if n has been detected), use (7) and (8) to convert it to a point Q of the form $(x, y) \in E_{a,b}(\mathbf{Z}/n\mathbf{Z})$, with $E_{a,b} = E_{a',b'}$ in the Weierstraß model (1). This finishes the description of the first phase of ECM.

Notice that, during the application of (4.4.3) we can take advantage of the fact that the $\tilde{z}$-coordinate of P equals 1. It is of course possible to do the inversion only once every few ms, instead of per m. In that case, it is advisable to define m as the product of a few prime powers, to avoid the extra $\log_2 q^{t_q}$ multiplications modulo n that are needed per prime power if the $\tilde{z}$-coordinate is not equal to 1 (which would be more expensive, even for moderate q^{t_q}s, than the inversion that would be saved).

6 PHASE TWO

Let $Q = (x, y)$ be the point kP on $E = E_{a,b}$ (as in (1)), as computed in the first phase of ECM (since we will be working with inhomogeneous coordinates in this section, z will always be equal to 1). Assume that n has a factor p such that the order of Q_p in $E(\mathbf{F}_p)$ is at most B_2, for some B_2 that may be up to several orders of magnitude larger than B_1 (cf. Sections 3 and 5). In this section we review the method from [1, § 9.1] that may detect this factor p of n, followed by some implementation details.

6.1 Brent's birthday paradox second phase. Let e, r and $\bar{r}$ be three positive integers that depend on B_2, with e small, $r < \bar{r}$ and $r\bar{r} \approx B_2$ (cf. (6.3)). Let $u, v, \bar{u}$ and $\bar{v}$ be four small randomly chosen positive integers (cf. (6.4)).

(i) Compute $(x_i, y_i) = (ui + v)^e Q$ for $i = 1, 2, \ldots, r$ (cf. (6.4)).

(ii) Compute the polynomial $f = \sum_{j=0}^{r} f_j X^j = \prod_{i=1}^{r} (X - x_i) \bmod n$ (cf. (6.6)).

(iii) Compute $(\bar{x}_j, \bar{y}_j) = (\bar{u}j + \bar{v})^e Q$ for $j = 1, 2, \ldots, \bar{r}$ (cf. (6.4)).

(iv) Compute $d = \prod_{j=1}^{\bar{r}} f(\bar{x}_j) \bmod n$ (cf. (6.7)).

(v) Attempt to factor n by computing $\gcd(n, d)$.

6.2 Remark. Because $d = \prod_{j=1}^{\bar{r}} \prod_{i=1}^{r} (\bar{x}_j - x_i) \bmod n$, it follows that it is quite likely that $p = \gcd(n, d)$ if some random scalar multiple $(ui+v)^e Q_p$ of Q_p equals some other random scalar multiple $\pm(\bar{u}j + \bar{v})^e Q_p$ (notice that $-(x, y) = (x, -y)$ on the curve, so by using the x-coordinates of the points on the curve we identify points with their negatives). This happens if one of the $(ui + v)^e$ equals one of the $\pm(\bar{u}j + \bar{v})^e$ modulo q, where q is the order of Q_p in $E(\mathbf{F}_p)$. Since $r\bar{r} \approx B_2$ and B_2 is assumed to be $\geq q$, it follows from the 'birthday paradox' that the approach from (6.1) has a fair probability of success.

It is beneficial (and relatively cheap, cf. (6.4)), to choose e as a highly composite integer > 1, because the number of solutions to $w^e \equiv 1 \bmod q$ equals $\gcd(e, q-1)$ and the scalars $(ui+v)^e$ and $(\bar{u}j+\bar{v})^e$ have a higher probability to be equal modulo q for such e than for general e (or $e = 1$).

6.3 Selecting B_2, e, r and $\bar{r}$. From various asymptotic analyses of ECM [1], [11] it appears to be optimal to choose B_2 so that the runtimes of the two phases are approximately equal; for our implementation this led to $B_2 \approx 10 B_1$.

Given B_1 and B_2 as above, we choose e, r and $\bar{r}$ as follows. First, we select e as the largest value from $\{1, 2, 3, 6, 12, 18, 24, 30, 60\}$ (cf. (6.2)) such that $1250 e^2 \leq B_1$. Next, we take the largest integer t such that $2^t - 1 \leq 50e$ and set $r = 2^t - 1$. Finally, we set $\bar{r} = [B_2/r]$ so that $\bar{r} \approx 5r$. Our implementation of (6.1)(iv) uses the fact that r is a 2-power minus 1 and that $\bar{r}$ is considerably larger than r. For our implementation our choices lead to approximately equal runtimes for the two phases of ECM; other implementations might lead to other choices.

6.4 Computing $(x_i, y_i) = (ui + v)^e Q$ for $i = 1, 2, \ldots, r$.
Because the i-th scalar multiplier $(ui + v)^e$ is an e-th power of a linear function of i, the e-th differences of the scalar multipliers are constant. This implies that after an initial $O(e^2 \log(ue + v))$ additions and doublings on the curve, the (x_i, y_i) for $i = 1, 2, \ldots, r$ can be computed in $r \cdot e$ additions on the curve. We selected u and v as random positive integers $\leq [2^{30}/(e+2)]$, so that the $ui + v$ for $i \leq e$ could be represented by single length integers.

In the pre-computation we first set R_i to $(ui + v)^e Q$ for $i = 0, 1, \ldots, e$ (cf. (4.1.2)) and next we do the following for $i = 1, 2, \ldots, e$ in succession: for $j = e, e-1, \ldots, i$ in succession replace R_j by $R_j - R_{j-1}$ on the curve (cf. (4.1.1)). As a result R_i contains the i-th successive difference $\sum_{j=0}^{i} (-1)^j \binom{i}{j} (u(i-j)+v)^e Q$ for $i = 0, 1, \ldots, e$. This computation can be done for the cost mentioned above.

These R_i allow us to compute (x_i, y_i) for $i = 1, 2, \ldots, r$ in succession at a cost of e curve additions per i: for $j = 0, 1, \ldots, e-1$ in succession update R_j by replacing it by $R_j + R_{j+1}$ and next set (x_i, y_i) equal to R_0 (cf. (4.1.1)). Notice that R_e does not get updated, which is intentional because it is the constant e-th difference.

6.5 Remark. Notice that the Weierstraß model is more convenient than the Montgomery model for the computation in (6.4), because in the latter we can only efficiently add points on the curve if their difference is known. Furthermore, all points would have to be normalized to have z coordinate equal to 1 before it makes sense to compute f as in (6.1)(ii). This would lead to r additional inversions modulo n.

6.6 Computing $f = \sum_{j=0}^{r} f_j X^j = \prod_{i=1}^{r} (X - x_i) \bmod n$.

This computation can trivially be carried out during the computation of the (x_i, y_i) for $i = 1, 2, \ldots, r$. Initially set $f = 1$. Right after (x_i, y_i) has been computed, simply replace f by $(X - x_i) \cdot f \bmod n$ using $i - 1$ modular multiplications and additions. In this way only the f_i for $i = 0, 1, \ldots, r$ have to be kept, but not the (x_i, y_i), which saves some storage.

Clearly, the runtime of this method is quadratic in r. There exist various methods to compute the f_i that are asymptotically much faster. For the relatively small r that we have been using they are probably not competitive with the above straightforward approach, and we did not implement them. If our implementation is going to be used for very large B_2 values, however, then it might be a good idea to change this. See [12] for an independent ECM implementation that incorporates this and other improvements.

6.7 Computing $d = \prod_{j=1}^{\bar{r}} f(\bar{x}_j) \bmod n$.

Each $f(\bar{x}_j) \bmod n$ can be computed using about $\frac{1}{2}r + \log_2 r$ modular multiplications (and some additions) if we first pre-condition f. To pre-condition the monic polynomial f of degree $r = 2^t - 1$ we used Algorithm A from [13]. If the degree r equals 1 pre-conditioning does not change the polynomial. Otherwise, write $f = \sum_{j=0}^{r} f_j X^j$ of degree $r = 2s - 1 > 1$ as $(X^s + f_{s-1} - 1)g + h$ with $g = X^{s-1} + \sum_{j=0}^{s-2} f_{s+j} X^j$ and $h = X^{s-1} + \sum_{j=0}^{s-2} (f_j - (f_{s-1} - 1) f_{s+j}) X^j$ both monic; replace f_{s-1} by $f_{s-1} - 1$, replace $f_{2s-2}, \ldots, f_s$ by the coefficients $g_{s-2}, \ldots, g_0$ of the recursively pre-conditioned polynomial g, and similarly replace $f_{s-2}, \ldots, f_0$ by the coefficients $h_{s-2}, \ldots, h_0$ of the pre-conditioned h. All computations are carried out modulo n.

To evaluate $f(\bar{x}_j) \bmod n$, first compute $\bar{x}_j^{2^i}$ for $0 \le i < t$ then next evaluate $f(\bar{x}_j) \bmod n$ as $(\bar{x}_j^s + f_{s-1})\, g(\bar{x}_j) + h(\bar{x}_j) \bmod n$ which can be done by recursively evaluating $g(\bar{x}_j) \bmod n$ and $h(\bar{x}_j) \bmod n$.

7 PARAMETER CHOICE AND EXAMPLES

The implementation described in this paper was originally written at the Digital Equipment Corporation's Systems Research Center (DEC SRC) for application on small multi-processor workstations, where each processor would run its own copy of the program. This put severe constraints on the size of the program, also because the total available memory was fairly limited. For this reason it was decided to use the second phase from [1] instead of the one from [11]. Using this set-up many 'most-wanted', 'more-wanted', and 'other' numbers from the list of unfactored numbers from the Cunningham tables have now been factored [2]. For further details we refer to [8]; the results can be found in the updates to [2] that are regularly published by S. S. Wagstaff, Jr.

A portable version of the DEC SRC implementation was included in the second author's long integer package [5]. Using this version of the program many numbers from the 'RSA Partition Challenge List' have been factored, see below; for further results and run times we refer to [14]. This portable version of the implementation was included in Magma, more or less unchanged and including the underlying arithmetic from [5].

As mentioned in (3.3) the optimal number of trials and first phase bound B_1 depend on the size of the prime factor p one attempts to find. In the table we give some choices that are close to optimal for a 60% probability of success (cf. [8]).

$\log_{10} p$	# trials	B_1
12	50	125
13	53	250
14	57	500
15	62	830
16	68	1500
17	75	2500
18	85	4200
19	100	6500
20	120	10000
21	145	15000
22	175	22000
23	210	32000
24	250	45000
25	300	65000
26	400	85000
27	500	115000
28	650	155000
29	750	205000
30	950	275000

In practice there is not much difference between 50 trials with $B_1 = 125$ and 25

trials with $B_1 = 250$, or 12 trials with $B_1 = 500$; they all have a fair probability to find factors of up to about 12 digits. To cast out the small factors one usually runs a few trials, say 30, with small B_1's starting at for instance 1000 and growing by a small factor like 1.02 per trial. If the remaining cofactor is still composite, and one is willing to invest more time in its factorization, the table can be used to decide how that time can best be spent. Notice that finding factors of about 25 or more digits requires on average a considerable effort.

To give an example, we tried to factor the randomly chosen 26-digit number:

$$2\,80215\,16895\,80271\,82839\,42993$$

several times, using $B_1 = B_0 \times 1.02^{k-1}$ at the k-th trial, for various choices of B_0 (and with changing random seeds to initialize the random generator). Each time we found the 11-digit factor $9\,38749\,82749$ (and thereby the prime 15-digit prime cofactor $29849\,82374\,98757$): for $B_0 = 100$ at the 19^{th} trial, another attempt with $B_0 = 100$ only at the 64^{th} trial; for $B_0 = 300$ at the first trial, and at another attempt only at the 13^{th} trial; for $B_0 = 500$ first at $k = 15$ but later at $k = 4$; and for $B_0 = 1000$ at $k = 4$ and later at $k = 1$. In all cases the factor was detected in the second phase, except for the 15^{th} trial with $B_0 = 500$ where it was found in the first phase.

A similar experiment with a 30-digit number (the product of the 14-digit prime $2513\,08345\,13221$ and the 17-digit prime $15\,85659\,19182\,38809$) led to the following: 100 trials with $B_0 = 100$ and $B_0 = 500$ were unsuccessful; a later attempt with $B_0 = 500$ had success at $k = 28$; for $B_0 = 1000$ success at the 11^{th} and later at the 7^{th} trial; for $B_0 = 2500$ success at the 6^{th} and later at the 5^{th} trial. In all cases the 14-digit factor was found, in the second phase.

A more challenging example is provided by the factorization of $2^{213} - 1$. Using trial division we found the prime factors 7 and 66457, with a 59-digit composite cofactor. Using ECM with $B_0 = 1000$ we found, in four separate attempts, the prime factors $2\,28479$, $485\,44121$, and $2128\,85833$ all at the first trial, and the 19-digit prime $2849\,88197\,21147\,40679$ at the 125^{th} trial, with $B_1 = 11408 \approx 1.02^{124} \times 1000$. Notice that finding a 19-digit factor after 125 trials with bounds ranging from 1000 to 11408 agrees reasonably with the table given above.
The resulting factorization is:

$$\begin{aligned} 2^{213} - 1 \;=\; & 7 \times 66457 \times 2\,28479 \times 485\,44121 \times 2128\,85833 \times \\ & \times 2849\,88197\,21147\,40679 \times 4205\,26857\,41913\,96793\,. \end{aligned}$$

The factorization of $2^{217} - 1$ was slightly harder to find. The prime factors 127, 5209 and 62497 were found using trial division, and the 10-digit prime factor $21474\,83647$ was found at the third ECM trial with initial bound $B_0 = 1000$. Of the remaining 46-digit composite cofactor a 22-digit prime factor was found at the 182^{th} trial with

$B_0 = 1000$ and $B_1 = 35220 \approx 1.02^{181} \times 1000$, which again agrees reasonably well with the table. The resulting factorization is:

$$\begin{aligned} 2^{217} - 1 &= 127 \times 5209 \times 62497 \times 2147483647 \times \\ &\quad \times 6268703933840364033151 \times 378428804431424484082633 \ . \end{aligned}$$

In other attempts to factor $2^{213} - 1$ and $2^{217} - 1$ we used $B_1 = (k-1) \times 120 + 2600$ at the k-th trial and found the smallest 19-digit prime factor of $2^{213} - 1$ at $k = 18$ and $B_1 = 4640$; with $B_1 = (k-1) \times 169 + 3090$ we found the 22-digit prime factor of $2^{217} - 1$ at $k = 55$ and $B_1 = 12216$.

The point of all these examples is that the practical behavior of ECM varies wildly, although the theoretically expected behavior can indeed on average be recognized. In large scale factoring projects as reported in [2], for instance, one often tries to make sure that the numbers do not have factors of less than 30 digits before one resorts to general purpose factoring methods like quadratic sieve [6] or the number field sieve [7]. As a result most applications of general purpose methods indeed lead to factors larger than 30 digits, but every now and then a small factor slips through, and leads to a 'disappointing' general purpose factorization.

As a final example we present the factorization of the 100-digit 8681^{th} partition number, the smallest number on the 'RSA Partition Challenge List':

$$\begin{aligned} p(8681) &= 1030444214627572681632914059347968971268885230707 \\ &\quad 0442843814287923536390501575945526803826572461691 \ . \end{aligned}$$

This number has two small prime factors that are trivially found using trial division, and a 7 and an 8-digit prime factor that were both found at the first ECM trial with $B_0 = 500$. The remaining 81-digit number was factored in a 25 and a 56-digit prime at the 25^{th} trial with $B_1 \approx (1.02)^{24} \times 10000$, which is faster than could have been expected for a 25-digit smallest factor:

$$\begin{aligned} p(8681) &= 3 \times 4021 \times 7876147 \times 76181269 \times 2440629475228334940216899 \\ &\quad \times 5833178812250720175038988054295336259561524841357640780 1 \ . \end{aligned}$$

The entire factorization took 50 minutes on a DECstation 5000 workstation.

REFERENCES

[1] R. P. Brent, *Some integer factorization algorithms using elliptic curves,* Research Report CMA–R32–85, The Australian National Univ., Canberra, 1985.

[2] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers*, second edition, Contemp. Math. **22**, Providence: Amer. Math. Soc., 1988.

[3] D. V. Chudnovsky, G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests,* IBM Research Report RC 11262, 1985.

[4] B. Dixon, A. K. Lenstra, *Massively parallel elliptic curve factoring*, Advances in Cryptology, Eurocrypt'92, Lecture Notes in Comput. Sci. **658** (1993), 183–193.

[5] A. K. Lenstra, *LIP, a long integer package*, available for anonymous ftp from `/pub/lenstra` on `flash.bellcore.com`.

[6] A. K. Lenstra, H. W. Lenstra, Jr., *Algorithms in number theory*, Chapter 12 in: J. van Leeuwen (ed.), *Handbook of theoretical computer science*, Volume A, *Algorithms and complexity*, Amsterdam: Elsevier, 1990.

[7] A. K. Lenstra, H. W. Lenstra, Jr., (eds.) *The development of the number field sieve*, Lecture Notes in Math. **1554**, Berlin: Springer–Verlag, 1993.

[8] A. K. Lenstra, M. S. Manasse, *Factoring by electronic mail*, Advances in cryptology, Eurocrypt '89, Lecture Notes in Comput. Sci. **434** (1990), 355–371.

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

[10] H. W. Lenstra, Jr., *Elliptic curves and number-theoretic algorithms*, pp. 99–120 in: A. M. Gleason (ed.), Proceedings of the International Congress of Mathematicians, August 3–11, 1986 (Berkeley, California), Providence: American Mathematical Society, 1987.

[11] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization,* Math. Comp. **48** (1987) 243–264.

[12] P. L. Montgomery, *An FFT extension of the elliptic curve method of factorization,* PhD thesis, Los Angeles, 1992.

[13] M. S. Paterson, L. J. Stockmeyer, *On the number of nonscalar multiplications necessary to evaluate polynomials,* SIAM J. Comput. **2** (1973), 60–66.

[14] RSA Data Security Corporation Inc., sci.crypt, May 18, 1991; information available by sending electronic mail to `challenge-rsa-list@rsa.com`.

[15] J. H. Silverman, *The arithmetic of elliptic curves*, New York: Springer–Verlag, 1986.

[16] H. Suyama, *Informal preliminary report,* October 1985.