IEICE TRANS. FUNDAMENTALS, VOL.E102–A, NO.1 JANUARY 2019

PAPER *Special Section on Cryptography and Information Security*

Elliptic Curve Method Using Complex Multiplication Method

Yusuke AIKAWA[†a)], **Koji NUIDA**[††b)], ***Nonmembers***, ***and*** **Masaaki SHIRASE**[†††c)], ***Member***

SUMMARY In 2017, Shirase proposed a variant of Elliptic Curve Method combined with Complex Multiplication method for generating certain special kinds of elliptic curves. His algorithm can efficiently factorize a given composite integer when it has a prime factor p of the form $4p = 1 + Dv^2$ for some integer v, where $-D$ is an auxiliary input integer called a discriminant. However, there is a disadvantage that the previous method works only for restricted cases where the class polynomial associated to $-D$ has degree at most two. In this paper, we propose a generalization of the previous algorithm to the cases of class polynomials having arbitrary degrees, which enlarges the class of composite integers factorizable by our algorithm. We also extend the algorithm to more various cases where we have $4p = t^2 + Dv^2$ and $p + 1 - t$ is a smooth integer.

key words: *integer factorization, elliptic curve method, complex multiplication method, class polynomials*

1. Introduction

The security of a large fraction of the currently known public key cryptosystems, such as RSA cryptosystem, is based on the computational hardness of integer factorization. Accordingly, study and improvement of integer factorization algorithms are valuable in order to closely evaluate the actual security level of those cryptosystems in real environments. Now we note that, there are integer factorization algorithms (such as Pollard's $p - 1$ method) that work efficiently when the input composite integer satisfies a certain condition depending on each algorithm. By virtue of such special-purpose integer factorization algorithms, the strength of composite integers as secret keys are not uniform even if their bit lengths are equal. From the point of view, it is meaningful to determine the class of easy-to-factorize integers in order to avoid a use of weak keys in practically implemented cryptosystems.

Along this direction of research, recently Shirase [7] proposed a special-purpose efficient integer factorization algorithm, which is a modification of celebrated Elliptic Curve Method (invented by Lenstra Jr. [6]; ECM, in short) combined with Complex Multiplication method (CM method, in short), the latter being an algorithm to generate an elliptic curve having a certain special property, which was first used in context of a primality proving [1]. To explain the idea of [7], let $N = pq$ be a public integer to be factorized and let p and q be the secret distinct prime factors. Shirase's algorithm intends to use an elliptic curve E over the ring $\mathbb{Z}/N\mathbb{Z}$ with the property that its reduction modulo p becomes an elliptic curve obtained by CM method over $\mathbb{F}_p$. When p is of a certain special form, this curve satisfies with very high probability that the group $E(\mathbb{F}_p)$ of rational points over $\mathbb{F}_p$ has order precisely p, therefore the scalar multiplication $N \cdot P$ for a rational point P over $\mathbb{Z}/N\mathbb{Z}$ has the unit element as the $E(\mathbb{F}_p)$-component since N is a multiple of p. Then it is naively expected that a prime factor of N could be derived from the coordinates of the point $N \cdot P$ in a way analogous to the original ECM*.

However, in fact there are two hurdles against realizing the aforementioned idea. Roughly speaking, one is to handle CM method over $\mathbb{F}_p$ without knowing the corresponding prime factor p of N. The other is to find a rational point P of the obtained elliptic curve over $\mathbb{Z}/N\mathbb{Z}$; this in general requires to solve a quadratic equation modulo the composite integer N, which is difficult when the factorization of N is not known. Shirase [7] resolved these problems by introducing a certain extension of the coefficient ring $\mathbb{Z}/N\mathbb{Z}$, but this solution causes another problem as a side effect. That is, though the way of deriving a prime factor of N from the coordinates of the finally obtained rational point is easy in the original ECM, the same procedure is no longer effective for the present case since the coefficient ring is not $\mathbb{Z}/N\mathbb{Z}$ but a more complicated extension ring. Actually, Shirase proposed a concrete solution for this final process only for restricted cases. More precisely, the condition for the prime p in CM method (and hence in Shirase's algorithm) is closely related to a special kind of polynomial called a

Manuscript received March 22, 2018.
Manuscript revised July 8, 2018.

[†]The author is with Department of Mathematics, Hokkaido University, Sapporo-shi, 060-0810 Japan.
[††]The author is with Graduate School of Information Science and Technology, The University of Tokyo/Information Technology Research Institute, National Institute of Advanced Industrial Science and Technology, Tokyo, 113-8656 Japan.
[†††]The author is with Future University Hakodate, Hakodate-shi, 041-8655 Japan.
a) E-mail: yusuke@math.sci.hokudai.ac.jp
b) E-mail: nuida@mist.i.u-tokyo.ac.jp
c) E-mail: shirase@fun.ac.jp
DOI: 10.1587/transfun.E102.A.74

*One may think that, when an elliptic curve E with complex multiplication by $\mathbb{Q}(\sqrt{-D})$ is used in ECM for a general input N, the reduction of E modulo p may frequently become supersingular, see Theorem 13.12, [5], which is not suitable for ECM since $\#E(\mathbb{F}_p) = p + 1$ always holds in this case. We emphasize, however, that the present work focuses on special-purpose integer factorization rather than general-purpose integer factorization such as the original ECM, and the "certain special form" of p, that is $4p = t^2 + Dv^2$, in our target case mentioned above guarantees that the supersingular curve never appear in our case.

class polynomial, and Shirase's algorithm is designed in an ad hoc manner specific to the case where the corresponding class polynomial has degree at most two. This restricts the availability of the algorithm for various choices of p, and it is nontrivial to extend the construction to more general cases where the degree of the class polynomial is higher.

1.1 Our Contributions

In this paper, we revisit the aforementioned ad hoc construction of the algorithm in the previous paper [7], and propose a generalization of the construction that works for any case of the class polynomial (possibly having degree higher than two) associated to a special prime factor p of the input integer N. Although our proposed algorithm still has an intrinsic limitation for the possibility of the prime factor p inherited from that of CM method, our generalization indeed enlarges the class of the effective inputs N significantly. Technically, in the previous paper [7] a certain polynomial is computed in order to derive a prime factor of N from the scalar multiplication $N \cdot P$ of a rational point P. In this paper, we reveal that this polynomial can be written as the resultant of the class polynomial and another polynomial that can also be systematically calculated from the coordinates of $N \cdot P$. This fact enabled us to extend the original algorithm to the case of an arbitrary class polynomial.

Moreover, in contrast to the previous paper [7] which dealt with only the case of primes p for which CM method provides an elliptic curve E with $E(\mathbb{F}_p)$ of order precisely p, we also point out that our algorithm can be similarly applied to the case where $E(\mathbb{F}_p)$ derived by CM method has smooth order, in a way analogous to the original ECM. This further enlarges the possible choices of the prime factor p for which our proposed algorithm works efficiently.

1.2 Notation and Terminology

We collect here notation and terminology which is used throughout this paper.

- Let C be an integer. We say that an integer N is C-smooth if $N|C!$. Moreover, for integers, we use the term "smooth" roughly when the biggest prime factor is small.
- For a set S, $\#S$ denotes the number of elements in S.
- For a field K, $\overline{K}$ denotes the algebraic closure of K.
- There is the natural morphism $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ and this induces the morphism between the polynomial rings: $\mathbb{Z}[T] \to \mathbb{Z}/N\mathbb{Z}[T]$. For $f(T) \in \mathbb{Z}[T]$, $f_N(T) \in \mathbb{Z}/N\mathbb{Z}[T]$ denotes the image of $f(T)$ under this morphism.
- Let K be a field. For $f(T), g(T) \in K[T]$, we denote the resultant of $f(T)$ and $g(T)$ by $\mathrm{Res}(f(T), g(T))$. We recall that $f(T)$ and $g(T)$ have a common root in K if and only if their resultant is zero in K.
- Let $D \in \mathbb{Z}$ be a positive integer with no odd square factor such that $D \equiv 3 \bmod 4$ or $D \equiv 4, 8 \bmod 16$. Then the negative integer $-D$ is called a discriminant. Throughout this paper, in order to avoid a case analysis, we work under the following assumption.

  Assumption 1: $D \neq 3, 4$

  The excluded case $D = 3, 4$ are included in [7].
- For a discriminant $-D$, the field

$$K := \mathbb{Q}(\sqrt{-D}) := \{a + b\sqrt{-D} | a, b \in \mathbb{Q}\}$$

  is called an imaginary quadratic field. The largest subring of K is called the ring of integers of K, which is denoted by $\mathcal{O}_K$. An order of K is a subring of $\mathcal{O}_K$ such that $\mathbb{Z} \subsetneq \mathcal{O} \subset \mathcal{O}_K$.

2. Elliptic Curves

We collect the basic properties of elliptic curves which are necessary for this paper into this section, for details see [9], [11], and give a quick review on the Elliptic Curve Method (ECM, in short) which is a factorization method for integers introduced by Lenstra, Jr in [6]. The group of rational points of an elliptic curve plays a crucial role in this method.

2.1 Elliptic Curves and Its Rational Points

Let K be a field. We assume that the characteristic of K is neither 2 nor 3 throughout this paper. Algebraic curves E over K defined by the equation

$$E : Y^2 = X^3 + AX + B \ (A, B \in K, 4A^3 + 27B^2 \neq 0) \quad (1)$$

are called elliptic curves over K. When we emphasize the coefficient field K, we write E/K. For an elliptic curve E/K, we define the set of rational points:

$$E(K) := \{(x, y) \in K \times K | y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

where the point ∞ denotes the point at infinity. Elliptic curves have a marked property: $E(K)$ carries a structure of abelian group with the unit element ∞. This group is often called the Mordell-Weil group of E.

Let E_1 and E_2 be elliptic curves. An isogeny between E_1 and E_2 is a group homomorphism between $E_1(\overline{K})$ and $E_2(\overline{K})$ which is given by rational functions, i.e. an isogeny $\alpha : E_1(\overline{K}) \to E_2(\overline{K})$ can be described by

$$\alpha(x, y) = \left(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)}\right)$$

where f_i and g_i $(i = 1, 2)$ are in $\overline{K}[X, Y]$. In the case $E_1 = E_2$, an isogeny is called an endomorphism and set $\mathrm{End}_K(E) := \{\alpha : E(\overline{K}) \to E(\overline{K}) | \alpha \text{ is an endomorphism of } E\}$. This carries a structure of ring in the natural way, so we call it the ring of endomorphisms of E.

Example 2: Let E/K be an elliptic curve. For $n \in \mathbb{Z}$, the map

$$[n] : E(\overline{K}) \to E(\overline{K}); P \mapsto nP$$

gives the endomorphism of E, that is, can be described by rational functions. We give formulas for these functions in §2.2. Then this induces the natural injection $\mathbb{Z} \hookrightarrow \mathrm{End}(E); n \mapsto [n]$.

Let E be an elliptic curve over $\mathbb{C}$. It is known that $\mathrm{End}_{\mathbb{C}}(E)$ is either $\mathbb{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$. We say that $E/\mathbb{C}$ has complex multiplication by an order $\mathcal{O}$ if $\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}$.

For the elliptic curve over a field K defined by the Eq. (1), we define the j-invariant of E as follows:

$$j_E := 1728\frac{4A^3}{4A^3 + 27B^2} \in K.$$

Assumption 3: In this paper, we treat elliptic curves E with $j_E \neq 0, 1728$. The excluded case $j_E = 0, 1728$ correspond to the elliptic curves with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-1})$ whose discriminants $-D$ are -3 and -4 respectively. For these cases, see [7] since their class polynomials are of degree 1.

For given $j_0 \in K$ with $j_0 \neq 0, 1728$, the elliptic curve E defined by the following equation

$$E : Y^2 = X^3 + \frac{3j_0}{1728 - j_0}X + \frac{2j_0}{1728 - j_0} \tag{2}$$

satisfies $j_E = j_0$.

Proposition 4: For elliptic curves E_1/K and E_2/K, they are isomorphic over the algebraic closure $\overline{K}$ of K if and only if their j-invariants coincide.

This property implies that isomorphic classes of elliptic curves over $\mathbb{C}$ are classified completely by j-invariants. If we work on an arbitrary field K, the condition "isomorphic over K" yields the condition "same j-invariant". However, the converse does not hold. For an elliptic curve E/K, elliptic curves with j-invariant j_E are called twist of E. We identify two twists if they are isomorphic over K.

Proposition 5: Let E be an elliptic curve over a finite field $\mathbb{F}_p$ defined by the Eq. (1) with $j_E \neq 0,\ 1728$ (recall the Assumption 3). Then #{twists of E}/$\sim$=2, where $\sim$ denotes the equivalence relation meaning isomorphic over $\mathbb{F}_p$. Let $c \in \mathbb{F}_p^{\times}$ be a quadratic nonresidue. Then

$$E' : Y^2 = X^3 + c^2AX + c^3B$$

is a twist of E which is not isomorphic over $\mathbb{F}_p$.

2.2 Scalar Multiplications

We describe the map on an elliptic curve E given by multiplication by an integer: for $n \in \mathbb{Z}$, $E(\overline{K}) \to E(\overline{K})$; $P \mapsto nP$. For an elliptic curve $Y^2 = X^3 + AX + B$, we define the division polynomials by

$$\begin{aligned}
\psi_0 &= 0\\
\psi_1 &= 1\\
\psi_2 &= 2Y\\
\psi_3 &= 3X^4 + 6AX^2 + 12BX - A^2\\
\psi_4 &= 4Y(X^6 + 5AX^4 + 20BX^3\\
&\quad -5A^2X^2 - 4ABX - 8B^2 - A^3)\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \ (m \geq 2)\\
\psi_{2m} &= \frac{\psi_m}{2Y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \ (m \geq 3)
\end{aligned}$$

and polynomials by

$$\begin{aligned}
\phi_m &= X\psi_m^2 - \psi_{m+1}\psi_{m-1}\\
\omega_m &= \frac{1}{4Y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).
\end{aligned}$$

Now, we can give the formula for the endomorphism of E given by multiplication by an integer. Let $P = (x, y) \in E(\overline{K})$ be a rational point on E and $n \in \mathbb{Z}$ be a positive integer. Then we have

$$nP = \Big(\frac{\phi_n(x, y)}{\psi_n(x, y)^2}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3}\Big). \tag{3}$$

Moreover, the following holds:

$$nP = \infty \Leftrightarrow \psi_n(x, y) = 0. \tag{4}$$

2.3 Elliptic Curve Method

We start with a composite number N that we want to factor. ECM [6] is a method which finds a prime factor of N in the following procedure.

1. Choose several random pairs $(a_i, u_i, v_i) \in \mathbb{Z}/N\mathbb{Z}^{\times 3}$ and define $b_i = v_i^2 - u_i^3 - a_iu_i \in \mathbb{Z}/N\mathbb{Z}$
2. Define elliptic curves $E_i : Y^2 = X^3 + a_iX + b_i$, then $P_i = (u_i, v_i) \in E_i(\mathbb{Z}/N\mathbb{Z})$
3. Choose an integer C and compute $(C!)P_i$ on $E_i(\mathbb{Z}/N\mathbb{Z})$
4. If this computation fails for some i, $\gcd(\psi_{C!}(u_i, v_i), N)$ returns a non-trivial divisor of N. If not, start over with a new choice of a family of elliptic curves or an integer C.

Strong points of this method are that we have a rational point of elliptic curves and the process of leading a prime factor of N is trivial. On the other hand, there is a drawback that the generated elliptic curves do not necessarily have a smooth order. Moreover, it is difficult to choose an appropriate bound C.

Our method resolves these drawbacks instead of losing the advantages. Namely, we generate first an elliptic curve with "good" order and find a rational point later. We utilize the CM method for a generation of such an elliptic curve.

3. Complex Multiplication

In this section, we define the class polynomials of discriminants and state the relationship between primes p of special

form with respect to a discriminant $-D$ and the class polynomial of $-D$ modulo p. After that, we explain the CM method. For details, see [1], [4], [8] and so forth.

3.1 The Class Polynomials

We denote $\mathcal{ELL}(-D)$ by the set of isomorphism classes of elliptic curves over $\mathbb{C}$ with complex multiplication by the ring of integers O_K of $K = \mathbb{Q}(\sqrt{-D})$:

$$\mathcal{ELL}(-D) := \left\{ [E/\mathbb{C}] \mid \mathrm{End}_{\mathbb{C}}(E) \cong O_K \right\}$$

where the notation $[\cdot]$ means an isomorphism class, which is a collection of elliptic curves isomorphic to each others. We can construct an action of $cl(O_K)$ on $\mathcal{ELL}(-D)$, where $cl(O_K)$ denotes the ideal class group of O_K which is one of the important objects in algebraic number theory, see [4] for example. The order of the group $cl(O_K)$ is called the class number of O_K. One of the fundamental theorems in algebraic number theory states that the class number of a ring of integers is finite. On the other hand, the fact that this action is simply transitive yields that the class number of O_K coincides with the order of the set $\mathcal{ELL}(-D)$: $\#cl(O_K) = \#\mathcal{ELL}(-D)$. Therefore, the set $\#\mathcal{ELL}(-D)$ is a finite set. For details, see [8], Ch.II, §1.

If we write

$$\mathcal{ELL}(-D) := \left\{ [E_1],\ [E_2],\ \cdots,\ [E_h] \right\},$$

in virtue of the finiteness, the complex numbers $j_i \in \mathbb{C}$ ($i = 1, 2, \cdots, h$) which are distinct from each others are obtained by taking j-invariants of $[E_i]$. We note that, for elliptic curves, the condition "isomorphic over $\mathbb{C}$" is equivalent to the condition "have same j-invariant". Then we define the class polynomial of the discriminant $-D$ as:

$$H_{-D}(T) := \prod_{i=1}^{h} (T - j_i).$$

The class polynomials have integer coefficients, that is, $H_{-D}(T) \in \mathbb{Z}[T]$, and can be computed by using SAGE [10], for example. The relationship between the class polynomial of a discriminant $-D$ and the quadratic equation $4p = X^2 + DY^2$ for a prime p is stated as the following (see Theorem 3.2 in [1]).

Proposition 6: For a discriminant $-D$ and a prime number p, the followings are equivalent:

1 The equation $4p = X^2 + DY^2$ has the solution in $\mathbb{Z}$.
2 $H_{-D,p}(T)$ splits completely in $\mathbb{F}_p$.

Here, as in the notation in §1.2, $H_{-D,p}(T)$ is the image of $H_{-D}(T)$ under the natural morphism $\mathbb{Z}[T] \to \mathbb{Z}/p\mathbb{Z}[T] = \mathbb{F}_p[T]$.

3.2 CM Method

As mentioned at the introduction, our idea is to apply the procedure of ECM to an elliptic curve having "good" order. Here, we utilize the CM method to generate such an elliptic curve. The CM method is a way to construct an elliptic curve $E/\mathbb{F}_p$ with a specified number of $\mathbb{F}_p$-rational points. To be precise, we suppose that a prime number p has a special form $4p = t^2 + Dv^2$ for some discriminant $-D$ ($D > 4$) and integers $t, v \in \mathbb{Z}$. The integers t^2 and v^2 are uniquely determined by p and $-D$ for $D > 4$. The CM method is a method which generates an elliptic curve $E/\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p + 1 \pm t$ for the above p and t.

Under this assumption, since the class polynomial $H_{-D,p}(T)$ splits completely in $\mathbb{F}_p$, we can take a root $j_0 \in \mathbb{F}_p$ of $H_{-D,p}(T)$. Then we construct an elliptic curve $E_{j_0}/\mathbb{F}_p$ with j-invariant j_0 as in (2) and write $\#E_{j_0}(\mathbb{F}_p) = p + 1 - a$ ($|a| \leq 2\sqrt{p}$). We recall that Hasse's theorem shows $|\#E(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}$. For the following proposition, we refer to §4.2 in [1].

Proposition 7: In the above setting, we have the equality $a = \pm t$. Thus if we let E'_{j_0} be a twist of E_{j_0} which is not isomorphic to E_{j_0} over $\mathbb{F}_p$, either E_{j_0} or E'_{j_0} have the order $p + 1 - t$.

4. Our Proposed Algorithms

4.1 The Setting

Let $-D$ be a discriminant and $N = pq$ be a composite number. Throughout this section, we assume that a prime number p has the form: $4p = t^2 + Dv^2$ for some $t, v \in \mathbb{Z}$. For the class polynomial $H_{-D}(T_1)$, we define a ring:

$$R_N^{-D} := \mathbb{Z}/N\mathbb{Z}[T_1]/(H_{-D,N}(T_1)).$$

For a random element $c \in \mathbb{Z}/N\mathbb{Z}$, put $A^{-D,c}(T_1) := \frac{3c^2T_1}{1728-T_1}$ and $B^{-D,c}(T_1) := \frac{2c^3T_1}{1728-T_1}$, and we define an elliptic curve $E^{-D,c}$ over the ring R_N^{-D} as follows:

$$E^{-D,c} : Y^2 = X^3 + A^{-D,c}(T_1)X + B^{-D,c}(T_1). \tag{5}$$

Then we have $j_{E^{-D,c}} = T_1$.

By the assumption about the form of p, we can take a root j_0 of the class polynomial $H_{-D,p}(T_1)$ in $\mathbb{F}_p$ (see Proposition 6). By substituting T_1 for j_0 in the equation of $E^{-D,c}$, we obtain the elliptic curve over $\mathbb{F}_p$

$$E^{-D,c}_{T_1=j_0} : Y^2 = X^3 + A_p^{-D,c}(j_0)X + B_p^{-D,c}(j_0)$$

with j-invariant j_0. Then the CM method implies that

$$\#E(\mathbb{F}_p) = p + 1 \pm t.$$

The next thing that we have to do is to find a rational point of $E^{-D,c}$. We will construct a rational point of $E^{-D,c}$ by extending the coefficient ring R_N^{-D}. We choose a random element $x_0 \in \mathbb{Z}/N\mathbb{Z}$ and define a polynomial

$$\tau(T_1) := x_0^3 + A^{-D,c}(T_1)x_0 + B^{-D,c}(T_1). \tag{6}$$

Set

$$S_N^{-D,\tau(T_1)} := R_N^{-D}[T_2]/(T_2^2 - \tau(T_1)).$$

Then we obtain a rational point naturally:

$$P := (x_0, T_2) \in E^{-D,c}(S_N^{-D,\tau(T_1)}).$$

Using the formula (3), we can write

$$nP = \Big(\frac{\phi_n(x_0,T_2)}{\psi_n^2(x_0,T_2)}, \frac{\omega_n(x_0,T_2)}{\psi_n^3(x_0,T_2)}\Big) \in E^{-D,c}(S_N^{-D,\tau(T_1)})$$

and in $S_N^{-D,\tau(T_1)}$

$$\psi_n(x_0,T_2) = g_{n,0}(T_1) + g_{n,1}(T_1)T_2,$$

where $g_{n,i}(T_1) \in \mathbb{Z}/N\mathbb{Z}[T_1]$ with $\deg(g_{n,i}(T_1)) < \deg(H_{-D}(T_1))$ $(i = 0, 1)$.

4.2 The Fundamental Fact and Algorithms

In the above setting, we state the key fact for the algorithms.

Theorem 8: Notation as above. Suppose that $t = 1$. Moreover, we assume that $\#E(\mathbb{F}_p) = p$ and $\tau_p(j_0) \in \mathbb{F}_p$ is a quadratic residue. Then, we have

$$\gcd(\mathrm{Res}(H_{-D,N}(T), g_{N,0}^2(T) - g_{N,1}^2(T)\tau(T)), N) \neq 1.$$

Proof : By the assumption, there exists $\sigma \in \mathbb{F}_p$ such that $\sigma^2 = \tau_p(j_0)$. Then, the homomorphism

$$S_N^{-D,\tau(T_1)} \to \mathbb{F}_p;\ T_1 \mapsto j_0,\ T_2 \mapsto \sigma$$

induces $E^{-D,c}(S_N^{-D,\tau(T_1)}) \to E^{-D,c}(\mathbb{F}_p)$. We denote the image of $P \in E^{-D,c}(S_N^{-D,\tau(T_1)})$ under this morphism by $P_p \in E^{-D,c}_{T_1=j_0}(\mathbb{F}_p)$.

Moreover, the assumption $\#E^{-D,c}(\mathbb{F}_p) = p$ yields $NP_p = \infty \in E^{-D,c}_{T_1=j_0}(\mathbb{F}_p)$. Thus, by (4), we have

$$\psi_N(x_0,\sigma) = g_{N,0}(j_0) + g_{N,1}(j_0)\sigma = 0 \in \mathbb{F}_p$$

and then

$$\tau_p(j_0) = \frac{g_{N,0}(j_0)^2}{g_{N,1}(j_0)^2} \in \mathbb{F}_p.$$

Since j_0 is a root of $H_{-D,p}(T)$ in $\mathbb{F}_p$, this means that two polynomials $H_{-D,p}(T)$ and $g_{N,0}(T)^2 - g_{N,1}(T)^2\tau(T)$ have a common root in $\mathbb{F}_p$. Therefore, we have

$$\gcd(\mathrm{Res}(H_{-D,N}(T), g_{N,0}^2(T) - g_{N,1}^2(T)\tau(T)), N), N) \equiv 0 \bmod p,$$

so we are done. □

This theorem leads Algorithm 1. On the other hand, the following theorem leads Algorithm 2.

Theorem 9: Notation as above. Suppose that $p + 1 - t$ is C-smooth. Put $M = C!$. Moreover, we assume that $\#E(\mathbb{F}_p) = p + 1 - t$ and $\tau_p(j_0) \in \mathbb{F}_p$ is a quadratic residue. Then, we have

$$\gcd(\mathrm{Res}(H_{-D,M}(T), g_{M,0}^2(T) - g_{M,1}^2(T)\tau(T)), N) \neq 1.$$

Proof : The same discussion as above is valid if we add slight modifications. □

We discuss the success conditions and success probabilities for our proposed algorithms. Algorithm 1 fails when $t \neq \pm 1$, and Algorithm 2 fails when $p + 1 \pm t$ is not a divisor of $C!$. Also when $t = \pm 1$ in Algorithm 1 or when $p + 1 \pm t$ is a divisor of $C!$ in Algorithm 2, these may fail depending on how to select $c \in \mathbb{Z}/N\mathbb{Z}$ or $x_0 \in \mathbb{Z}/N\mathbb{Z}$, but its probability is not so high. So, if one selects c or x_0 sufficiently many times, the algorithms succeed with high probability. Conversely, if these do not succeed, it is highly probable that the above conditions for t are not satisfied.

In detail, if c is chosen at random, it is expected that the order of $E(\mathbb{F}_p)$ will be randomly determined from two ways $p + 1 \pm t$, one of which is appropriate and the other is inappropriate. So, there is a possibility that the algorithm fails with a probability of $\frac{1}{2}$ with respect to how to select c. Therefore, the expected value of the number of times to choose c before the algorithm succeeds is considered to 2.

Also, if x_0 (and c) is chosen at random, for each of the roots $j_1, \ldots, j_h$ of $H_{-D}(T)$, the probability that $\tau_p(j_i)$ is not a quadratic residue is expected to be $\frac{1}{2}$. The algorithms fail when this happens for all j_i. So, assuming that the behaviors whether $\tau_p(j_i)$ is a quadratic residue are independent of each other, the probability that this causes a failure of the algorithms is thought to be $(\frac{1}{2})^h$. Therefore, for each c, the expected value of the number of times to choose x_0 before the algorithm succeeds is less than or equal to 2, and when h is large this expected value is close to 1.

On the other hand, for solving the equation $4p = X^2 + DY^2$, there is a faster algorithm given by Cornacchia, which is easy to describe, see [2], [3]. As our proposed algorithm with input discriminant $-D$ is effective only when a prime factor p of N satisfies $4p = X^2 + DY^2$ for some X, Y, the attack by our algorithm will be avoidable by, for example, checking (in the key generation phase) whether or not the equation $4p = X^2 + DY^2$ has a solution and then by discarding the prime p if a solution exists.

Here, we describe the process of our proposed algorithm in step by step by using a small example. We give an example of Algorithm 2 only, since the structure of Algorithm 1 is almost the same as Algorithm 2.

Example 10: We attempt to factor $N = 793 = 61 \cdot 13$ using Algorithm 2 with $C = 5$. Since $4 \cdot 61 = 2^2 + 15 \cdot 4^2$ and $61 + 1 - 2 = 60$ is a divisor of $C! = 120$, if we choose the discriminant $-D = -15$, Algorithm 2 should be successful.

Firstly we choose $c = 1$ in $\mathbb{Z}/793\mathbb{Z}$ and construct an elliptic curve $E^{-15,1}$ over the ring $R_{793}^{-15} = \mathbb{Z}/793\mathbb{Z}[T_1]/(H_{-15,793}(T_1))$ as (5) where the class polynomial of -15 is:

$$H_{-15}(T_1) = T_1^2 + 191025T_1 - 121287375 \in \mathbb{Z}[T_1].$$

Algorithm 1
Input: a composite integer N a discriminant $-D$, the class polynomial $H_{-D}(T)$ of $-D$
Output: a prime factor of N
1. Choose a random element $c \in \mathbb{Z}/N\mathbb{Z}$
2. Define an elliptic curve over R_N^{-D} by the Eq. (5)
3. Choose a random element $x_0 \in \mathbb{Z}/N\mathbb{Z}$ and define $\tau(T_1)$ as (6)
4. Take the rational point $P = (x_0, T_2) \in E^{-D,c}(S_N^{-D,\tau(T_1)})$
5. Compute NP
6. Compute $\gcd(\mathrm{Res}(H_{-D,N}(T), g_{N,0}^2(T) - g_{N,1}^2(T)\tau(T)), N)$
6-1. If it is non-trivial divisor of N, we are done.
6-2. If not, start over with a new choice of $c \in \mathbb{Z}/N\mathbb{Z}$ or $x_0 \in \mathbb{Z}/N\mathbb{Z}$

Algorithm 2
Input: a composite integer N, $M = C!$ for a bound C a discriminant $-D$, the class polynomial $H_{-D}(T)$ of $-D$
Output: a prime factor of N
1. Choose a random element $c \in \mathbb{Z}/N\mathbb{Z}$
2. Define an elliptic curve by the Eq. (5)
3. Choose a random element $x_0 \in \mathbb{Z}/N\mathbb{Z}$ and define $\tau(T_1)$ as (6)
4. Take the rational point $P = (x_0, T_2) \in E^{-D,c}(S_N^{-D,\tau(T_1)})$
5. Compute MP
6. Compute $\gcd(\mathrm{Res}(H_{-D,M}(T), g_{M,0}^2(T) - g_{M,1}^2(T)\tau(T)), N)$
6-1. If it is non-trivial divisor of N, we are done.
6-2. If not, start over with a new choice of $c \in \mathbb{Z}/N\mathbb{Z}$ or $x_0 \in \mathbb{Z}/N\mathbb{Z}$

Since we can write $4 \cdot 61 = 2^2 + 15 \cdot 4^2$, the polynomial $H_{-15,61}(T_1)$ splits completely in $\mathbb{F}_{61}$ as follows:

$$\begin{aligned} H_{-15,61}(T_1) &= T_1^2 + 34T_1 + 23 \\ &= (T_1 + 5)(T_1 + 29) \in \mathbb{F}_{61}[T_1] \end{aligned}$$

So, by the CM method, if we substitute a root $-5 = 56$ of $H_{-15,61}(T_1)$ in $\mathbb{F}_{61}$ for T_1 in the coefficients of $E^{-15,1}$, the order of $E^{-15,1}_{T_1=56}(\mathbb{F}_{61})$ should be $61 + 1 \pm 2 = 60$ or 64 since its j-invariant is equal to 56. Indeed, $\#E^{-15,1}_{T_1=56}(\mathbb{F}_{61}) = 60$.

Secondly, we take $x_0 = 4$ and define $\tau(T_1)$ as (6). Then, $\tau_{61}(56) = 49 \in \mathbb{F}_{61}$ is a quadratic residue in $\mathbb{F}_{61}$. By extending the coefficient ring, we obtain a rational point over the ring $S_{793}^{-15,\tau(T_1)} = \mathbb{Z}/793\mathbb{Z}[T_1, T_2]/(H_{-15,793}(T_1), T_2 - \tau(T_1))$:

$$P = (4, T_2) \in E^{-15,1}(S_{793}^{-15,\tau(T_1)}).$$

Finally, Algorithm 2 should succeed since $\#E^{-15,1}_{T_1=56}(\mathbb{F}_{61}) = 60$ is 5-smooth. Indeed, we compute the division polynomial $\psi_{5!}$ by using the recurrence relation in §2.2,

$$\begin{aligned} \psi_{5!}(4, T_2) &= g_{5!,0}(T_1) + g_{5!,1}(T_1)T_2 \\ &= (549T_1 + 61)T_2 \in S_{793}^{-15,\tau(T_1)} \end{aligned}$$

and we compute

$$g_{5!,0}^2(T_1) - g_{5!,1}^2(T_1)\tau(T_1) = 488T_1 + 488 \in \mathbb{Z}/793\mathbb{Z}[T_1].$$

So, we obtain

$$\mathrm{Res}(H_{-15,793}(T_1), 488T_1 + 488) = 61.$$

Therefore, the computation of the step 6 in Algorithm 2 outputs

$$\begin{aligned} \gcd(\mathrm{Res}(H_{-15,793}(T_1), 488T_1 + 488), 793) &= \gcd(61, 793) \\ &= 61. \end{aligned}$$

Algorithm 2 succeeds since 61 is a divisor of 793.

5. Numerical Examples

Here we show some examples of discriminants $-D$ and prime factors p for which our generalized algorithm can factorize the integer $N = pq$ while the previous algorithm in [7] is not effective.

- $-D = -23$ ($\deg H_{-D}(X) = 3$)
  $p = 570942088504121$, $t = 1210134$
  $4p = t^2 + D \times 9961456^2$
  $p + 1 - t = 570942087293988 \mid 2000!$
  $q = 883478470161233$
  $N = p \times q = 504415042902280115530654941193$
- $-D = -56$ ($\deg H_{-D}(X) = 4$)
  $p = 804161$, $t = 450$
  $4p = t^2 + D \times 232^2$
  $p + 1 - t = 803712 = 2^7 \times 3 \times 7 \times 13 \times 23$
  $N = p \times q = 488391904291$
- $-D = -131$ ($\deg H_{-D}(X) = 5$)
  $p = 6338253001150313676073094416 63$
  $4p = 1 + D \times 139116657084339^2$
  $q = 868610670601296908562434196197$
  $N = p \times q = 550547418976985666816226779885$
  $030828558826986967578267955611$

6. Conclusion

In this paper, we have given a generalization and an extension of the previous algorithms proposed by Shirase [7]. To be precise, we have proposed efficient algorithms which can factorize a composite integer when it has a prime factor p of the form $4p = 1 + Dv^2$ or $4p = t^2 + Dv^2$ with the condition that $p + 1 - t$ is a smooth integer, where $-D$ is a discriminant whose the class polynomial has arbitrary degree. Therefore, we should avoid using secret prime numbers having the above property. For given a prime number p and a discriminant $-D$, using Cornacchia's algorithm we can check whether or not p has the above property with respect to $-D$.

Experimental evaluations of our algorithms are left as a future research subject. For example, are these algorithms applicable up to what degrees of the class polynomials?, and so on.

Acknowledgements

The first author was supported by National Institute of Advanced Industrial Science and Technology (AIST) during this work. The second author was supported during this work by JST CREST Grant Number JPMJCR14D6, Japan. The third author was supported during this work by JSPS

KAKENHI Grant Number 16K00188.

References

[1] A.O.L. Atkin and F. Morain, "Elliptic curves and primality proving," Math. Comp., vol.61, no.203, pp.29–68, 1993.
[2] J.M. Basilla, "On the solution of $x^2 + dy^2 = m$," Proc. Japan Acad. Ser. A Math. Sci., vol.80, no.5, pp.40–41, 2004.
[3] H. Cohen, A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics, vol.138, Springer-Verlag, Berlin, 1993.
[4] D.A. Cox, Primes of the Form $x^2 + ny^2$, Second Edition, John Wiley & Sons, Hoboken, NJ, 2013.
[5] S. Lang, Elliptic Functions, Second Edition, Graduate Texts in Mathematics, vol.112, Springer-Verlag, New York, 1987.
[6] H.W. Lenstra, Jr., "Factoring integers with elliptic curves," Ann. of Math., vol.126, no.3, pp.649–673, 1987.
[7] M. Shirase, "Condition on composite numbers easily factored with elliptic curve method," IACR Cryptology ePrint Archive, 2017/403. https://eprint.iacr.org/2017/403, accessed March 19, 2018.
[8] J.H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, vol.151, Springer-Verlag, New York, 1994.
[9] J.H. Silverman, The Arithmetic of Elliptic Curves, Second Edition, Graduate Texts in Mathematics, vol.106, Springer, Dordrecht, 2009.
[10] W. Stein et al., Sage Mathematics Software (Version 8.1). The Sage Development Team, 2017, http://www.sagemath.org/, accessed March 20, 2018.
[11] L.C. Washington, Elliptic Curves: Number Theory and Cryuptography, Second Edition, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008.

Yusuke Aikawa received the B.S. and M.S. degree in Mathematics from Hokkaido University in 2013 and 2015, respectively. He is currently studying toward the Ph.D. degree at the Department of Mathematics, Hokkaido University. During Aug. 2017–March 2018, he was supported by National Institute of Advanced Industrial Science and Technology (AIST).

Koji Nuida received the Ph.D. degree in Mathematical Science from The University of Tokyo, Japan, in 2006. Currently, he is mainly working as an associate professor at Graduate School of Information Science and Technology, The University of Tokyo, Japan. His research interest is mainly in mathematics and mathematical cryptography.

Masaaki Shirase received the M.S. and Ph.D. degrees in Information Science from JAIST (Japan Advanced Institute of Science and Technology) in 2003 and 2006, respectively. He is currently an Associate Professor in the School of Systems Information Science at Future University Hakodate. His research interests are algorithm and implementation of cryptography.