

# Condition on composite numbers easily factored with elliptic curve method

Masaaki Shirase

Future University Hakodate, Hakodate, Japan,  
shirase@fun.ac.jp

**Abstract.** For a composite integer  $N$  that we would like to factor, we consider a condition for the elliptic curve method using  $N$  as a scalar value to succeed and show that if  $N$  has a prime factor  $p$  such that  $p = (DV^2 + 1)/4$ ,  $V \in \mathbb{Z}$ ,  $D \in \{3, 11, 19, 35, 43, 51, 67, 91, 115, 123, 163, 187, 235, 267, 403, 427\}$ , we can find a non-trivial divisor of  $N$  (multiple of  $p$ ) in a short time. In the authors' implementation on PARI/GP, a 1024-bit  $N$  was factored in a few seconds when  $p$  was 512 bits.

**Keywords:** Prime factorization, Elliptic curve method, Class polynomial, Residue ring

## 1 Introduction

RSA, which is the most popular public key cryptography, is based on the hardness of prime factorization. Prime factorization experiments are hence important to decide the key length of practical RSA systems.

Representative prime factorization methods [3] include the number field sieve (NFS), the quadratic sieve (QS), Lenstra elliptic curve method (ECM) [8], the  $p - 1$  method, and the  $\rho$  method. The NFS, QS and ECM are subexponential time algorithms, while the  $p - 1$  method and the  $\rho$  method are exponential time algorithms. It is said that the NFS is considered to be the best algorithm for factoring a composite number  $N$  when  $N$  is a product of two large primes as in the case of the public key of RSA and that the ECM is suitable for moderately large composite numbers.

### 1.1 Easily Factored Composite Numbers

Let  $p$  and  $q$  be primes of several hundreds of bits or more. Then, factoring  $N = pq$  is hard. The largest such composite number  $N$  that has been factored and that does not fall into any of the special cases listed below is 768 bits long [1]. However, it is known that such large  $N$ s can be easily factored in a short time in the following special cases:

1. When  $p - 1$  has only small prime factors, the  $p - 1$  method can easily factor  $N$ ,

2. When  $|p - q|$  is a small integer, Fermat's method can be used to factor  $N$ .

This paper will add to this list the following.

3. When  $p$  has the form

$$p = (DV^2 + 1)/4, V \in \mathbb{Z} \quad (1)$$

for some non-square number  $D \in \mathbb{Z}$ , an improved version of ECM can be used to factor  $N$ .

This paper will show that the set of such  $D$ s includes  $\{3, 11, 19, 35, 43, 51, 67, 91, 115, 123, 163, 187, 235, 267, 403, 427\}$ .

**Remark 1** *The authors think that the results in this paper are NOT a threat against practical RSAs. To see that this is the case, let us consider the probability that a given integer is a square. For a square  $m^2$ , the following one is  $(m + 1)^2$ , and the difference between them is*

$$(m + 1)^2 - m^2 = 2m + 1 (= 2\sqrt{m^2} + 1).$$

Then, the probability that a large enough integer  $n$  is a square is about

$$\frac{1}{2\sqrt{n} + 1} \doteq \frac{1}{2\sqrt{n}}. \quad (2)$$

Next, we consider the probability that a given prime  $p$  has the form (1). Modifying the expression of Eq. (1), we get

$$V^2 = (4p - 1)/D. \quad (3)$$

If  $p$  has the form (1), the right term of (3) has to be a square, and its probability is

$$\frac{1}{2\sqrt{(4p - 1)/D}} \doteq \frac{1}{2\sqrt{(4p)/D}} = \frac{\sqrt{D}}{4\sqrt{p}}$$

from (2). In the case of a 1024-bit RSA, the probability that  $p$  has the form (1) is less than  $1/2^{253}$ , because  $p \doteq 2^{512}$  and  $D < 2^{10}$ .

## 1.2 Notation

This paper uses the following notations, where  $n$  is a natural number and  $p$  is a prime.

$$\begin{aligned} \mathbb{Z}_n &:= \{0, 1, 2, \dots, n - 1\} . \\ \mathbb{F}_p &:= \mathbb{Z}_p = \{0, 1, 2, \dots, p - 1\} . \\ a_p &:= a \bmod p \text{ for } a \in \mathbb{Z}, \text{ or for } a \in \mathbb{Z}_n \text{ (} p \text{ is a prime factor of } n \text{)} . \\ E_p &: y^2 = x^3 + A_p x + B_p \text{ for } E : y^2 = x^3 + Ax + B . \\ P_p &:= (x_p, y_p) \in E_p \text{ for } P = (x, y) \in E . \end{aligned}$$

$\mathcal{O}_p$  := the point at infinity of  $E_p$ .  
 $H_D(j)$  : the class polynomial of discriminant  $D$ .  
 $H_{D,n}(j)$  : a polynomial generated by reducing all coefficients of  $H_D(j) \pmod n$ .  
 $\mathcal{Q}_n^\tau$  :=  $\mathbb{Z}_n[X]/(X^2 - \tau)$  .  
 $\mathcal{R}_n^D$  :=  $\mathbb{Z}_n[j]/(H_{D,n}(j))$  .  
 $\mathcal{S}_n^{D,\tau}$  :=  $\mathcal{R}_n^D[X]/(X^2 - \tau) = \mathbb{Z}_n[j, X]/(H_{D,n}(j), X^2 - \tau)$  .

## 2 Preliminary

### 2.1 Elliptic Curves over a General Field

This section briefly introduces the definitions and properties of elliptic curves over a general field. Readers can refer to [10, 5] for details.

#### 2.1.1 Addition on Elliptic Curves

Let  $\mathbb{K}$  be a field and  $E$  an elliptic curve over  $\mathbb{K}$  given by the Weierstrass normal form,

$$E/\mathbb{K} : y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{K}, \quad 4A^3 + 27B^2 \neq 0. \quad (4)$$

Then, the set  $E(\mathbb{K})$  is defined as

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

where  $\mathcal{O}$  is the point at infinity.  $P + Q \in E(\mathbb{K})$  can be defined geometrically or using the addition formula for any point  $P, Q \in E(\mathbb{K})$ . In addition, the negative of a point  $P = (x_1, y_1) \neq \mathcal{O}$ ,  $-P$ , is defined as  $-P = (x_1, -y_1)$ , and  $-\mathcal{O} = \mathcal{O}$ . Then,  $E(\mathbb{K})$  forms a group under the operation ‘+’ with the identity  $\mathcal{O}$ .

Scalar multiplication  $mP$  is defined by repeatedly performing ‘+’, i.e.,

$$mP = P + P + \dots + P \quad (m \text{ terms}) \in E(\mathbb{K})$$

for  $P \in E(\mathbb{K})$  and  $m \in \mathbb{N}$ . In the affine coordinate system,  $mP$  has coordinates such as

$$mP = \left( \frac{a_m}{d_m^2}, \frac{b_m}{d_m^3} \right), \quad (5)$$

([10, Exer. III.3.7]) and

$$mP = \mathcal{O} \Leftrightarrow d_m = 0. \quad (6)$$

#### 2.1.2 $J$ -invariant and Twist

For an elliptic curve  $E/\mathbb{K}$  given by Eq. (4),

$$j = 4 \cdot 1728A^3 / (4A^3 + 27B^2) \quad (7)$$

is called the  $j$ -invariant of  $E$ .

**Lemma 2** *Given  $j_0 \in \mathbb{K}$ , an elliptic curve having  $j$ -invariant  $j_0$  is constructed as shown in Table 1.*

**Table 1.** Elliptic curve having  $j$ -invariant  $j_0$ .

$y^2 = x^3 + \frac{3j_0R^2}{1728 - j_0}x + \frac{2j_0R^3}{1728 - j_0}$	$(R \neq 0)$ when $j_0 \neq 0, 1728$
$y^2 = x^3 + R$	when $j_0 = 0$
$y^2 = x^3 + Rx$	when $j_0 = 1728$

$\therefore$ ) Refer to [5, Sec. 9.4].  $\square$

Some of the literature has stated that elliptic curves having  $j$ -invariant  $j_0$  are constructed as in Table 1 only for  $R = 1$ . However, we easily see that such elliptic curves can also be constructed for other  $R$ s from the definition of the  $j$ -invariant (7).

Let  $E$  and  $E'$  be elliptic curves defined over  $\mathbb{K}$ . If  $E'$  is isomorphic to  $E$  over  $\overline{\mathbb{K}}$  that is the algebraic closure of  $\mathbb{K}$ ,  $E'$  is called a twist of  $E$ . If  $E'$  is isomorphic to  $E$  over  $\mathbb{K}$ ,  $E'$  is called a trivial twist of  $E$ . The set of twists of  $E$  mod  $\mathbb{K}$ -isomorphism is denoted by  $Twist(E/\mathbb{K})$ .

It is known that if  $E$  and  $E'$  are defined over  $\mathbb{K}$  and have the same  $j$ -invariant, then  $E'$  is a twist of  $E$ .

## 2.2 Elliptic Curves over a Finite Field

Let  $E$  be an elliptic curve over a finite field  $\mathbb{F}_p (p \geq 5)$  given by Eq. (4). An integer  $t$  satisfying  $\#E(\mathbb{F}_p) = p+1-t$  is called the trace (of Frobenius), where  $\#$  denotes the number of elements. When  $\#E(\mathbb{F}_p) = p$ , which means  $E$  has trace 1,  $E$  is called anomalous. If  $E'$  is a twist of  $E$  of degree 1, then  $\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p)$ . If  $E'$  is a twist of  $E$  of degree  $\geq 2$ , then  $\#E(\mathbb{F}_p) \neq \#E'(\mathbb{F}_p)$  in general.

Let  $E$  be an elliptic curve over a finite field  $\mathbb{F}_p (p \geq 5)$  given by Eq. (4). An integer  $t$  satisfying  $\#E(\mathbb{F}_p) = p+1-t$  is called the trace (of Frobenius), where  $\#$  denotes the number of elements. When  $\#E(\mathbb{F}_p) = p$ , which means  $E$  has the trace 1,  $E$  is called anomalous.

If  $E'$  is a trivial twist of  $E$ ,  $\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p)$ . If  $E'$  is not a trivial twist but a twist of  $E$ ,  $\#E(\mathbb{F}_p) \neq \#E'(\mathbb{F}_p)$  in general. From [5, Sec. 9.5.8], it is known that

$$\#Twist(E) = \begin{cases} 2 & \text{if the } j\text{-invariant of } E \neq 0, 1728 \\ 4 & \text{if the } j\text{-invariant of } E = 1728 \\ 6 & \text{if the } j\text{-invariant of } E = 0. \end{cases} \quad (8)$$

The following theorem is important.

**Theorem 3 (Lagrange's Theorem for  $E(\mathbb{F}_p)$ )** *Let  $E/\mathbb{F}_p$  be an elliptic curve over the finite field  $\mathbb{F}_p$ , and  $n = \#E(\mathbb{F}_p)$ . Then, any point  $P \in E(\mathbb{F}_p)$  satisfies*

$$nP = \mathcal{O}.$$

$\therefore$ ) Refer to [2, Sec. 2.1.1]

**Table 2.** Class polynomials  $H_D(j)$  of degree 1 for  $p = (DV^2 + 1)/4$  possibly prime

$D$	$H_D(j)$
3	$j$
11	$j + (2^5)^3$
19	$j + (2^5 \cdot 3)^3$
43	$j + (2^6 \cdot 3 \cdot 5)^3$
67	$j + (2^5 \cdot 3 \cdot 5 \cdot 11)^3$
163	$j + (2^6 \cdot 3 \cdot 5 \cdot 23 \cdot 29)^3$

**Table 3.** Class polynomials  $H_D(j)$  of degree 2 for  $p = (DV^2 + 1)/4$  possibly prime

$D$	$H_D(j)$
35	$j^2 + 117964800j - 134217728000$
51	$j^2 + 5541101568j + 6262062317568$
91	$j^2 + 10359073013760j - 3845689020776448$
115	$j^2 + 427864611225600j + 130231327260672000$
123	$j^2 + 1354146840576000j + 148809594175488000000$
187	$j^2 + 4545336381788160000j - 3845689020776448000000$
235	$j^2 + 823177419449425920000j + 11946621170462723407872000$
267	$j^2 + 19683091854079488000000j + 531429662672621376897024000000$
403	$j^2 + 2452811389229331391979520000j$ $-108844203402491055833088000000$
427	$j^2 + 15611455512523783919812608000j$ $+155041756222618916546936832000000$

### 2.3 CM Method and Class Polynomial

The following proposition, called the CM method, is useful for constructing  $E/\mathbb{F}_p$  with a specified the trace  $t$ .

**Proposition 4 (The CM Method)** *Let a non-square integer  $D \in \mathbb{Z}$  and a prime  $p$  satisfy  $4p - t^2 = DV^2$  for  $(0 \neq)t, V \in \mathbb{Z}$  and let  $H_D(j)$  be the class polynomial of discriminant  $D$ . Then, an elliptic curve  $E$  over  $\mathbb{F}_p$  having  $j$ -invariant  $j_0$ , which is a root of  $H_D(j)$ , or a twist  $E'$  over  $\mathbb{F}_p$  of  $E$  has trace  $t$ .*

*If  $E$  is constructed as in Table 1 using  $j_0$ , then the probability that  $E$  has trace  $t$  is*

$$\left. \begin{array}{l} 1/6 \text{ if } D = 3, \\ 1/4 \text{ if } D = 1, \\ 1/2 \text{ otherwise.} \end{array} \right\} \quad (9)$$

$\therefore$ ) Refer to [2]. The probability (9) is obtained from (8),  $\square$

Table 2 gives a set of  $D$ s such that  $p = (DV^2 + 1)/4$  is possibly a prime and the class polynomial  $H_D(j)$  is linear, and Table 3 gives a set of  $D$ s such that  $p = (DV^2 + 1)/4$  is possibly a prime and the class polynomial  $H_D(j)$  is quadratic [9]. For  $n \in \mathbb{N}$  and a class polynomial  $H_D(j)$ , we denote a polynomial over  $\mathbb{Z}_n$  generated by reducing all coefficients of  $H_D(j) \bmod n$  by  $H_{D,n}(j)$ .

**Remark 5** Solving  $H_D(j) = 0$  over  $\mathbb{Q}$  using a mathematical software, *Mathematica*, for each  $H_D(j)$  in Table 3, we see that

$$\begin{aligned} \text{root of } H_{35}(j) &\in \mathbb{Q}(\sqrt{5}), & \text{root of } H_{51}(j) &\in \mathbb{Q}(\sqrt{17}), \\ \text{root of } H_{91}(j) &\in \mathbb{Q}(\sqrt{13}), & \text{root of } H_{115}(j) &\in \mathbb{Q}(\sqrt{5}), \\ \text{root of } H_{123}(j) &\in \mathbb{Q}(\sqrt{41}), & \text{root of } H_{187}(j) &\in \mathbb{Q}(\sqrt{17}), \\ \text{root of } H_{235}(j) &\in \mathbb{Q}(\sqrt{5}), & \text{root of } H_{267}(j) &\in \mathbb{Q}(\sqrt{89}), \\ \text{root of } H_{403}(j) &\in \mathbb{Q}(\sqrt{13}), & \text{root of } H_{427}(j) &\in \mathbb{Q}(\sqrt{61}). \end{aligned}$$

If  $p = (DV^2 + 1)/4$  is prime, we can prove that  $H_{D,p}(j)$  is reducible in  $\mathbb{F}_p$ . For example, consider the case of  $D = 35$ . We can see that  $V$  must be odd for  $p$  to be prime; therefore, replacing  $V$  with  $2V + 1$ , we have  $p = 35V^2 + 35V + 9$ . The computation of the Legendre symbol is as follows.

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{35V^2 + 35V + 9}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Therefore, 5 is a square in  $\mathbb{F}_p$ , the roots of  $H_{35,p}(j)$  are in  $\mathbb{F}_p$ , and  $H_{35,p}(j)$  is reducible in  $\mathbb{F}_p$ . As well, we can see that  $H_{D,p}(j)$ s are reducible in  $\mathbb{F}_p[j]$  for other all  $D$ s.

## 2.4 Elliptic Curves over $\mathbb{Z}_N$ and Factoring

Let  $N$  be a composite number we would like to factor. This subsection remarks on elliptic curves over  $\mathbb{Z}_N$  and describes relationships between elliptic curves over  $\mathbb{Z}_N$  and factoring  $N$ , the ECM, and results by Kunihiko et al. [6]. The method described in Sec. 3 is based on the ECM and uses an elliptic curve over  $\mathbb{Z}_N$ .

**Remark 6** Let  $E$  be an elliptic curve over  $\mathbb{Z}_N$ . Although  $\mathbb{Z}_N$  is not a field, we consider the set  $E(\mathbb{Z}_N)$  of  $\mathbb{Z}_N$ -points on  $E$ . For  $P, Q \in E(\mathbb{Z}_N)$ , when a division  $\alpha/\beta$  appearing in a computation of  $P+Q$  is computable, in other words,  $\gcd(N, \beta) = 1$ , we can compute  $P+Q \in E(\mathbb{Z}_N)$ .

Let  $p$  be a prime factor of  $N$  and  $E$  an elliptic curve over  $\mathbb{Z}_N$ ,

$$E : y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}_N.$$

We denote  $E_p$  to be the elliptic curve over  $\mathbb{F}_p$ ,

$$y^2 = x^3 + A_p x + B_p,$$

where

$$A_p := A \bmod p \text{ and } B_p := B \bmod p.$$

For example, we have

$$E_5/\mathbb{F}_5 : y^2 = x^3 + 2x + 4$$

for

$$E/\mathbb{Z}_{35} : y^2 = x^3 + 17x + 19.$$

When  $N$  is factored into  $N = p_0 \cdot p_1 \cdot \dots \cdot p_i$ ,  $E(\mathbb{Z}_N)$  is represented as

$$E(\mathbb{Z}_N) = E(\mathbb{F}_{p_0}) \times E(\mathbb{F}_{p_1}) \times \dots \times E(\mathbb{F}_{p_i}).$$

Each  $E(\mathbb{F}_{p_i})$  forms a group, and  $E(\mathbb{Z}_N)$  also forms a group.

Let  $N$  be a composite number,  $N = \prod_{i=1}^k p_i$ ,  $p_i \neq 2, 3$ , and  $E$  be an elliptic curve over  $\mathbb{Z}_N$ . An elliptic curve  $E$  is called super-anomalous if

$$\#E_{p_i}(\mathbb{F}_{p_i}) = p_i$$

holds for all  $i$ s. If  $E$  is super-anomalous, we have

$$\#E(\mathbb{Z}_N) = N.$$

If  $E$  is not super-anomalous but  $\#E(\mathbb{Z}_N) = N$ , then  $E$  is called pseudo super-anomalous [7].

**Remark 7** Let  $p$  be a prime factor of  $N$ . Let the coordinates of  $kP$  be

$$kP = \left( \frac{a_k}{d_k^2}, \frac{b_k}{d_k^3} \right)$$

for  $P \in E(\mathbb{Z}_N)$ , and let  $d_{k,p} := d_k \bmod p$ . If  $kP_p = \mathcal{O}_p$ , then  $d_{k,p} = 0$  ( $\Leftrightarrow d_k$  is a multiple of  $p$ ). In other words, if  $g = \gcd(N, d_k)$  and  $g \neq 0$ , then  $g$  is a non-trivial divisor of  $N$  (multiple of  $p$ ).

Remark 7 is essential for the ECM and the proposed method to work.

#### 2.4.1 Elliptic Curve Method (ECM)

The ECM (more precisely stage 1 of the ECM) factors  $N$  as follows [8].

1. Construct an elliptic curve  $E : y^2 = x^3 + Ax + B$  over  $\mathbb{Z}_N$  and pick a point  $P \in E(\mathbb{Z}_N)$ .
2. Set

$$L := (\text{the least common multiple from } 2 \text{ to } B_1) \quad (10)$$

(for an optimal integer  $B_1$ , for example, listed as in [4]).

3. Compute  $LP = (a_L/d_L^2, b_L/d_L^3)$  over  $\mathbb{Z}_N$ .
4. Compute  $\gcd(N, d_L)$ . If  $\gcd(N, d_L) \neq 0, 1$ , return it. Otherwise go back to step 1. (Or go to stage 2 if  $\gcd = 1$ .)

Assume that  $E$  is (fortunately) constructed such that all prime factors of  $\#E_p(\mathbb{F}_p)$  are equal to or less than  $B_1$  in step 1 of the ECM for a prime factor  $p$  of  $N$ . Accordingly,  $LP_p = \mathcal{O}_p$  from Lagrange's theorem, and if  $\gcd \neq 0$ , step 4 of the ECM returns a non-trivial divisor of  $N$  (see Remark 7).

By selecting an optimal  $B_1$ , the ECM is a subexponential time algorithm in  $p$ , where  $p$  is the smallest prime factor of  $N$ .

**Remark 8** Note that even if an optimal  $B_1$  is selected the ECM is a subexponential (not polynomial) time algorithm. According to [4], when  $N$  is expected to have an 80-digit prime factor, the optimal  $B_1$  is 25,000,000,000 and the expected number of iterations of the ECM is 265,557. Note that the digits of  $L$  computed from (10) number 25,234,114,168 for this  $B_1$ .

### 2.4.2 Results of Kunihiro et al.

Kunihiro et al. [6] showed two interesting relationships between an elliptic curve over  $\mathbb{Z}_N$  and factoring  $N$  as follows:

1. If  $\#E(\mathbb{Z}_N)$  were known, then  $N$  would be easy to factor.
2. If the discrete logarithm problem on  $E(\mathbb{Z}_N)$  could be solved, then  $N$  would be easy to factor.

## 3 Proposed Method

The ECM constructs an elliptic curve  $E$  over  $\mathbb{Z}_N$  for the  $N \in \mathbb{N}$  we would like to factor and computes  $LP$  for some  $P \in E(\mathbb{Z}_N)$  and  $L \in \mathbb{N}$  to find a divisor of  $N$ , where  $L = \text{lcm}(2, \dots, B_1)$  for an optimal  $B_1$  as in [4]. The table also shows the expected number of iterations of the ECM.

This section describes a theorem that states an integer  $N$  satisfying a certain condition can be factored by computation of  $NP$  with relatively few iterations. We use the theorem to construct algorithms for factoring  $N$  in a short time.

### 3.1 Basic Idea

The following theorem describes a condition for the ECM to succeed with a computation of  $NP$ .

**Theorem 9** Let  $N$  be an integer and  $p$  a prime factor of  $N$  having the form (1),

$$p = (DV^2 + 1)/4, \quad D, V \in \mathbb{Z},$$

where  $D$  is non-square. Let  $H_D(j)$  be the class polynomial of discriminant  $D$ , and  $E/\mathbb{Z}_N$  an elliptic curve having the  $j$ -invariant  $j_0$  given by Eq. (4), where  $j_0$  is a root of  $H_D(j)$ . Moreover, for any point  $(\mathcal{O} \neq)P \in E(\mathbb{Z}_N)$ , compute

$$NP = (a_N/d_N^2, b_N/d_N^3)$$

and  $g = \text{gcd}(N, d_N)$ . Then, if  $g \neq 0$ ,  $g$  is a non-trivial divisor of  $N$  (multiple of  $p$ ) with the probability,

$$\begin{cases} 1/6 & \text{if } D = 3, \\ 1/4 & \text{if } D = 1, \\ 1/2 & \text{otherwise.} \end{cases}$$



∴) From Proposition 4 for  $t = 1$ ,  $E_p$  is anomalous with probability as in (9), and from Lagrange's theorem, we have  $pP_p = \mathcal{O}_p$ . Accordingly,  $NP_p = \mathcal{O}_p$  because  $p$  is a divisor of  $N$ , and from Remark 7, if  $g = \gcd(N, d_N)$  is not zero, then  $g$  is a non-trivial divisor of  $N$ .  $\square$

**Remark 10** *If  $E/\mathbb{Z}_N$  is super-anomalous or pseudo super-anomalous, we have  $NP = \mathcal{O} \in E(\mathbb{Z}_N)$  from Lagrange's theorem, in other words,  $d_N = 0$  from Eq. (6). Accordingly, we have  $\gcd(N, d_N) = 0$  and cannot apply Theorem 9.*

**Problem 11** *Even if the composite number  $N$  has a prime factor of the form (1), the following problems appears to apply to Theorem 9.*

- (i) *How do we construct  $H_D(j)$ ?*
- (ii) *How do we find a root of  $H_D(j)$  over  $\mathbb{Z}_N$ ? (If we have a root  $j_0$  of  $H_D(j)$ , then, from Lemma 2, it is easy to construct an elliptic curve having the  $j$ -invariant  $j_0$ .)*
- (iii) *How do we pick a point  $P \in E(\mathbb{Z}_N)$ ?*

We can use the  $D$ s in Tables 2 or 3 to overcome (i). Therefore, we only need to consider how to overcome (ii) and (iii).

### 3.2 Case of $D = 3$

The case of  $D = 3$  is the easiest. In this case, we can see that  $H_3(j) = j$  from Table 2 and its root is 0 and that we can overcome (ii) of Problem 11. To apply Theorem 9, we can construct an elliptic curve having the  $j$ -invariant 0. Such an elliptic curve has the form,

$$E : y^2 = x^3 + B$$

from Table 1. Therefore, we pick  $x_0, y_0 \in \mathbb{Z}_N$  at random and set  $B = y_0^2 - x_0^3$ ; accordingly, we have

$$(x_0, y_0) \in E(\mathbb{Z}_N),$$

which overcomes (iii). The above enables the following algorithm to be constructed.

---

#### Algorithm 1

---

Input: A composite number  $N$  having a prime factor  
such that  $p = (3V^2 + 1)/4$

Output: Non-trivial divisor of  $N$  (multiple of  $p$ )

---

1. Select  $x_0, y_0 \in \mathbb{Z}_N$  at random, set  $B = y_0^2 - x_0^3$ ,  
and construct  $E/\mathbb{Z}_N : y^2 = x^3 + B$ .
  2. Set  $P = (x_0, y_0)$ . (Note  $P \in E(\mathbb{Z}_N)$ .)
  3. Compute  $NP = (a_N/d_N^2, b_N/d_N^3)$ .
  4. Compute  $g = \gcd(N, d_N)$ .
  5. If  $g \neq 0$ , then  $g \neq 1$  with probability  $1/6$  and return it.  
If  $g = 0, 1$ , then fail or goto step 1.
-

### 3.3 Case in which $H_D$ is Linear and $D \neq 3$

The purpose of this subsection is that for

$$D \in \{11, 19, 43, 67, 163\}$$

for which  $H_D(j)$  is linear, we consider how to overcome (ii) and (iii) of Problem 11 and use Theorem 9 to construct an algorithm for factoring  $N$  having a prime factor such that

$$p = (DV^2 + 1)/4, \quad V \in \mathbb{Z}.$$

When  $H_D(j)$  is linear, it is easy to find a root  $j_0$  of  $H_D(j)$  over  $\mathbb{Z}_N$ , in other words, to overcome (ii). It is also easy to construct an elliptic curve having the  $j$ -invariant  $j_0$ . For  $D \in \{11, 19, 43, 19, 43, 67, 163\}$  and  $0 \neq R \in \mathbb{Z}_N$ , we may set

$$\left. \begin{aligned} A^{D,R} &:= 3j_0 \cdot R^2 / (1728 - j_0) \pmod{N} \\ B^{D,R} &:= 2j_0 \cdot R^3 / (1728 - j_0) \pmod{N} \end{aligned} \right\} \quad (11)$$

and construct an elliptic curve  $E^{D,R}/\mathbb{Z}_N$  as follows.

$$E^{D,R} : y^2 = x^3 + A^{D,R}x + B^{D,R}$$

Then, from Lemma 2, the elliptic curve  $E^{D,R}/\mathbb{Z}_N$  has the  $j$ -invariant  $j_0$ .

However, it is not easy to choose a point  $P \in E^{D,R}(\mathbb{Z}_N)$ , in other words, to overcome (iii) of Problem 11. The authors propose that we choose a point  $P \in E^{D,R}$  over a residue ring of  $\mathbb{Z}_N[X]$ , named  $\mathcal{Q}_N^\tau$ . Taking  $x_0 \in \mathbb{Z}_N$  at random, we set

$$\tau = x_0^3 + A^{D,R}x_0 + B^{D,R},$$

and construct the residue ring,

$$\mathcal{Q}_N^\tau = \mathbb{Z}_N[X]/(X^2 - \tau). \quad (12)$$

Note that a representative of  $\mathcal{Q}_N^\tau$  has the form,

$$a_0 + a_1X, \quad a_0, a_1 \in \mathbb{Z}_N.$$

**Remark 12** In  $\mathcal{Q}_N^\tau$ , we have

$$(x_0, X) (= (x_0 + 0X, 0 + X)) \in E^{D,R}(\mathcal{Q}_N^\tau)$$

because  $X^2 - \tau = 0$ , equivalently  $X^2 = \tau$ , holds and

$$X^2 = \tau = x_0^3 + A_{D,R}x_0 + B^{D,R}$$

holds.

The following proposition is a modification of Theorem 9 by using computation on  $\mathcal{Q}_N^\tau$  for  $D \in \{11, 19, 43, 67, 163\}$ .

**Proposition 13** *Let  $N$  be a composite number having a prime factor,*

$$p = (DV^2 + 1)/4, \quad D \in \{11, 19, 43, 67, 163\}, V \in \mathbb{Z}.$$

*Choosing  $(0 \neq)R \in \mathbb{Z}_N$ , we construct an elliptic curve  $E^{D,R}$  over  $\mathbb{Z}_N$  (using Eq. (11)). Choosing  $x_0 \in \mathbb{Z}_N$  at random, we compute*

$$\tau = x_0^3 + A^{D,R}x_0 + B^{D,R} \in \mathbb{Z}_N, \quad (13)$$

*and construct the residue ring  $\mathcal{Q}_N^\tau$  (using Eq. (12)). Moreover, for  $P = (x_0, X) \in E^{D,R}(\mathcal{Q}_N^\tau)$ , we compute  $NP$  on  $E(\mathcal{Q}_N^\tau)$ . Let the coordinates of  $NP$  be*

$$NP = \left( \frac{a_{N,0} + a_{N,1}X}{(d_{N,0} + d_{N,1}X)^2}, \frac{b_{N,0} + b_{N,1}X}{(d_{N,0} + d_{N,1}X)^3} \right) \in E^{D,R}(\mathcal{Q}_N^\tau),$$

*( $a_i, b_i, d_i \in \mathbb{Z}_N$ ). Then, for  $g = \gcd(N, d_{N,0}^2 - d_{N,1}^2\tau)$ , if  $g \neq 0$ ,  $g$  is a non-trivial divisor of  $N$  (multiple of  $p$ ) with probability  $1/4$ .*

Refer to Appendix A for the arithmetic on  $\mathcal{Q}_N^\tau$  and for the proof of Proposition 13. The following algorithm is obtained using Proposition 13.

---

**Algorithm 2**

---

Input: A composite number  $N$  having a prime factor such that

$$p = (DV^2 + 1)/4, \quad D \in \{11, 19, 43, 67, 163\} \text{ and } D.$$

Output: A non-trivial divisor of  $N$  (multiple of  $p$ )

---

1. Construct an elliptic curve

$$E^{D,R}/\mathbb{Z}_N : y^2 = x^3 + A^{D,R}x + B^{D,R}$$

using  $D$  and some  $(0 \neq)R \in \mathbb{Z}_N$  as (11).

2. Choose  $x_0 \in \mathbb{Z}_N$  at random.

3. Compute  $\tau = x_0^3 + A^{D,R}x_0 + B^{D,R} \in \mathbb{Z}_N$ .

4. Construct  $\mathcal{Q}_N^\tau := \mathbb{Z}_N[X]/(X^2 - \tau)$ .

5. Set  $P = (x_0, X)$ . (Note  $P \in E(\mathcal{Q}_N^\tau)$ .)

6. Compute

$$NP = \left( \frac{a_{N,0} + a_{N,1}X}{(d_{N,0} + d_{N,1}X)^2}, \frac{b_{N,0} + b_{N,1}X}{(d_{N,0} + d_{N,1}X)^3} \right) \in E(\mathcal{Q}_N^\tau)$$

( $a_i, b_i, d_i \in \mathbb{Z}_N$ ).

7. Compute  $g = \gcd(N, d_{N,0}^2 - d_{N,1}^2\tau)$ .

8-1. If  $g \neq 0$ , then  $g \neq 1$  with probability  $1/4$  and return it.

8-2. If  $g = 0, 1$ , fail, or do one of the following.

a) Go to step 1, and change  $R$ .

b) Go to step 2, and change  $x_0$ .

---

### 3.4 Case in which $H_D$ is Quadratic

We will consider how to overcome (ii) and (iii) of Problem 11 for

$$D \in \{35, 51, 91, 115, 123, 187, 235, 267, 403, 427\}, \quad (14)$$

for which  $H_D(j)$  is quadratic. It is generally hard to find the roots of the quadratic polynomial over  $\mathbb{Z}_N$ . Instead, we introduce the residue ring of the polynomial ring  $\mathbb{Z}_N[j]$ ,

$$\mathcal{R}_N^D := \mathbb{Z}_N[j]/(H_{D,N}(j)),$$

where  $H_{D,N}(j)$  is a polynomial with coefficients in  $\mathbb{Z}_N$  obtained by reducing all coefficients of  $H_D(j)$  mod  $N$ . In addition,  $j$  as an element in  $\mathcal{R}_N^D$  satisfies  $H_{D,N}(j) = 0$ , and hence,  $j$  is a root of  $H_{D,N}(j)$  in  $\mathcal{R}_N^D$ . The representative in  $\mathcal{R}_N^D$  has the form,

$$a_0 + a_1j, \quad a_0, a_i \in \mathbb{Z}_N.$$

For  $R \in \mathbb{Z}_N$ ,  $3R^2j$ ,  $2R^3j$ , and  $1728 - j$  are elements in  $\mathcal{R}_N^D$ , and if  $1728 - j$  is regular, we have

$$\frac{3R^2j}{1728 - j}, \quad \frac{2R^3j}{1728 - j} \in \mathcal{R}_N^D.$$

(Note that if  $1728 - j \in \mathcal{R}_N^D$  is non-regular, we can easily find a non-trivial divisor of  $N$  by computing  $\gcd(N, 1728 - j)$ , and thereby factor  $N$ .) We see that the  $j$ -invariant of the elliptic curve,

$$E^{D,R}/\mathcal{R}_N^D : y^2 = x^3 + \underbrace{\frac{3R^2j}{1728 - j}}_{=:A^{D,R}}x + \underbrace{\frac{2R^3j}{1728 - j}}_{=:B^{D,R}} \quad (15)$$

is  $j$ , which is a root of  $H_{D,N}(j)$  in  $\mathcal{R}_N^D$  from Lemma 2.

To pick a point  $P \in E^{D,R}$ , we choose  $x_0 \in \mathbb{Z}_N (\subset \mathcal{R}_N^D)$  at random, set

$$\tau = x_0^3 + A^{D,R}x_0 + B^{D,R},$$

construct the residue ring  $\mathcal{S}_N^{D,\tau}$  of  $\mathcal{R}_N^D[X]$ ,

$$\begin{aligned} \mathcal{S}_N^{D,\tau} &= \mathcal{R}_N^D[X]/(X^2 - \tau) \\ &= \mathbb{Z}_N[j, X]/(H_{D,N}(j), X^2 - \tau), \end{aligned}$$

and consider  $E^{D,R}$  over  $\mathcal{S}_N^{D,\tau}$ . The representative of  $\mathcal{S}_N^{D,\tau}$  has the form,

$$\alpha_0 + \alpha_1X, \quad \alpha_i \in \mathcal{R}_N^D$$

or

$$(a_0 + a_1j) + (a_2 + a_3j)X, \quad a_i \in \mathbb{Z}_N.$$

**Remark 14** *We have*

$$(x_0, X)(= (x_0 + 0X, 0 + X)) \in E^{D,R}(\mathcal{S}_N^{D,\tau})$$

because  $X^2 - \tau = 0$ , equivalently  $X^2 = \tau$ , in  $\mathcal{S}_N^{D,\tau}$ . Therefore, we can pick a point in  $E^{D,R}(\mathcal{S}_N^{D,\tau})$ .

Let  $H_{D,N}(j)$  be represented as  $H_{D,N}(j) = s + tj + j^2$  ( $s, t \in \mathbb{Z}_N$ ), and define a map  $\phi_N$ ,

$$\phi_N : \left. \begin{array}{l} \mathcal{S}_N^{D,\tau} \rightarrow \mathbb{Z}_N \\ (a_0 + a_1j) + (a_2 + a_3j)X \mapsto c \end{array} \right\}, \quad (16)$$

where  $c$  is computed as follows,

1. Compute  $b_0, b_1 \in \mathbb{Z}_N$  such as  $b_0 + b_1j = (a_0 + a_1j)^2 - (a_2 + a_3j)^2\tau \in \mathcal{R}_N^D$ .
2. Compute  $c = b_0^2 + b_1^2s - b_0b_1t \in \mathbb{Z}_N$ .

The following proposition is a modification of Theorem 9 on  $\mathcal{S}_N^{D,\tau}$  for

$$D \in \{35, 51, 91, 115, 123, 187, 235, 267, 403, 427\}.$$

**Proposition 15** *Let  $N$  be a composite number having a prime factor such that*

$$D \in \left. \begin{array}{l} p = (DV^2 + 1)/4, \\ \{35, 51, 91, 115, 123, 187, 235, 267, 403, 427\}, \\ V \in \mathbb{Z}. \end{array} \right\}$$

*Pick an element  $(0 \neq)R \in \mathbb{Z}_N(\subset \mathcal{R}_N^D)$  and construct an elliptic curve over  $\mathcal{R}_N^D$  (using Eq. (15)),*

$$E^{D,R}/\mathcal{R}_N^D : y^2 = x^3 + A^{D,R}x + B^{D,R}.$$

*Choose  $x_0 \in \mathbb{Z}_N(\subset \mathcal{R}_N^D)$  at random and compute*

$$\tau = x_0^3 + A^{D,R}x_0 + B^{D,R} \in \mathcal{R}_N^D. \quad (17)$$

*For the point  $P = (x_0, X) \in E^{D,R}(\mathcal{S}_N^{D,\tau})$ , compute  $NP$  on  $E^{D,R}(\mathcal{S}_N^{D,\tau})$ . Let the coordinates of  $NP$  be*

$$NP = \left( \frac{(a_{N,0} + a_{N,1}j) + (a_{N,2} + a_{N,3}j)X}{((d_{N,0} + d_{N,1}j) + (d_{N,2} + d_{N,3}j)X)^2}, \frac{(b_{N,0} + b_{N,1}j) + (b_{N,2} + b_{N,3}j)X}{((d_{N,0} + d_{N,1}j) + (d_{N,2} + d_{N,3}j)X)^3} \right) \in E^{D,R}(\mathcal{S}_N^{D,\tau}).$$

*Finally, compute  $g = \gcd(N, \phi_N((d_{N,0} + d_{N,1}j) + (d_{N,2} + d_{N,3}j)X))$ . Then, if  $g \neq 0$ ,  $g$  is a non-trivial divisor of  $N$  (multiple of  $p$ ) with probability  $1/4$ .*

Refer to Appendix B for the arithmetic on  $\mathcal{R}_N^D$  and  $\mathcal{S}_N^{D,\tau}$  and the proof of Proposition 15. The following algorithm is constructed using Proposition 15.

---

**Algorithm 3**

---

Input: A composite number  $N$  having a prime factor having the form

Eq. (1) with  $D$  as in Eq. (14), the class polynomial  $H_D(j)$

Output: A non-trivial divisor of  $N$  (multiple of  $p$ )

---

1. Construct  $\mathcal{R}_N^D := \mathbb{Z}_N/(H_D(j))$ .

2. Construct

$$E^{D,R}/\mathcal{R}_N^D : y^2 = x^3 + A^{D,R}x + B^{D,R}$$

as (11) for some  $(0 \neq)R \in \mathbb{Z}_N$ .

3. Take  $x_0 \in \mathbb{Z}_N (\subset \mathcal{R}_N^D)$  at random.

4. Compute  $\tau = x_0^3 + A^{D,R}x_0 + B^{D,R} \in \mathcal{R}_N^D$ .

5. Construct  $\mathcal{S}_N^{D,\tau} := \mathcal{R}_N^D[X]/(X^2 - \tau)$ .

6. Set  $P = (x_0, X)$ . (Note  $P \in E(\mathcal{S}_N^{D,\tau})$ .)

7. Compute

$$NP =$$

$$\left( \frac{(a_{N,0} + a_{N,1}j) + (a_{N,2} + a_{N,3}j)X}{((d_{N,0} + d_{N,1}j) + (d_{N,2} + d_{N,3}j)X)^2}, \frac{(b_{N,0} + b_{N,1}j) + (b_{N,2} + b_{N,3}j)X}{((d_{N,0} + d_{N,1}j) + (d_{N,2} + d_{N,3}j)X)^3} \right) \in E^{D,R}(\mathcal{S}_N^{D,\tau}).$$

8. Compute  $g = \gcd(N, \phi_N((d_{N,0} + d_{N,1}j) + (d_{N,2} + d_{N,3}j)X))$ .

9-1. If  $g \neq 0$ , then  $g \neq 1$  with the probability  $1/4$  and return it.

9-2. If  $g = 0, 1$ , then fail or do one of the following.

a) Go to step 2, and change  $R$ .

b) Go to step 3, and change  $x_0$ .

---

### 3.5 Implementation

The implementation of  $\mathbb{Z}_N$  is essentially the same as that of the finite field  $\mathbb{F}_p$ . However, the inversion  $a^{-1}$  in  $\mathbb{Z}_N$  is computable only in the case of  $\gcd(N, a) = 1$ .

To implement Algorithm 2, we need to implement the residue ring  $\mathcal{Q}_N^r = \mathbb{Z}_N[X]/(X^2 - \tau)$ , which is done in the same way as the implementation of the quadratic extension  $\mathbb{F}_{p^2} = \mathbb{F}_p[X]/(X^2 - \tau)$ . Refer to Lemma 16 for the computability of the inversion in  $\mathcal{Q}_N^r$ .

To implement Algorithm 3, we need to implement the residue ring  $\mathcal{S}_N^{D,\tau}$ , which is done in the same way as the implementation of the fourth extension  $\mathbb{F}_{p^4} = \mathbb{F}_p[j, X]/(H_{D,N}(j), X^2 - \tau)$ . The computability of the inversion in  $\mathcal{S}_N^{D,\tau}$  is given by (18) and (19).

The authors implemented Algorithms 1, 2, and 3 using PARI/GP. These implementations were not intended to be fast but confirming that they worked correctly. Thus, they didn't use the projective coordinate system that is usually used to make elliptic curve cryptosystems fast.

Although the authors didn't exactly measure the run time of the implementations, they returned a non-trivial divisor of  $N$  in several seconds in almost all cases for  $N = pq$  of 1024 bits and  $p$  of 512 bits. (Of course,  $N$  has to have a prime factor such that  $p = (DV^2 + 1)/4$  for  $V \in \mathbb{Z}$ ,  $D \in \{3, 11, 19, 35, 43, 51, 67, 91, 115, 123, 163, 187, 235, 267, 403, 427\}$ .)

## 4 Conclusion

This paper has shown that a composite number  $N$  having a prime factor  $p = (DV^2 + 1)/4$  for  $D \in \{3, 11, 19, 35, 43, 51, 67, 91, 115, 123, 163, 187, 235, 267, 403, 427\}$ ,  $V \in \mathbb{Z}$ , for which the class polynomial is linear or quadratic, can be factored by using the proposed algorithms. Algorithm 1 is for  $D = 3$ , Algorithm 2 is for  $D \in \{11, 19, 43, 19, 43, 67, 163\}$ , and Algorithm 3 is for  $D \in \{35, 51, 91, 115, 123, 187, 235, 267, 403, 427\}$ .

These algorithms are based on the ECM, and the computation of  $NP$  can find a non-trivial divisor of  $N$  for an elliptic curve  $E/\mathbb{Z}_N$  and  $P \in E$  in a short time. In the case of  $D \neq 3$ , we have to consider  $E$  on  $\mathcal{Q}_N^\tau$  or  $\mathcal{S}_N^{D,\tau}$  to construct  $E$  and/or to choose a point  $P \in E$ . The properties of  $\mathcal{Q}_N^\tau$  and  $\mathcal{S}_N^{D,\tau}$  are described in the appendix.

Each algorithm contains the statement, “if  $\gcd \neq 0, \dots$ .” Although the probability of  $\gcd = 0$  is experimentally found to be small, the derivation of this probability is left as a future subject. Another subject is to deal with  $D$  such that  $H_D(j)$  is third or higher degree. The authors think that an elliptic curve over  $\mathbb{Z}_N[j]/(H_D(j))$  can be used for such  $D$ s, as was done in this paper; however, the implementation of  $\mathbb{Z}_N[j]/(H_D(j))$  may become more complicated.

## Acknowledgments

This work was supported by the Japan Society for the Promotion of Science (JSPS KAKENHI Grant Number 16K00188).

## References

1. K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann. Factorization of a 768-bit RSA modulus. In T. Rabin ed., *Advances in Cryptology – CRYPTO 2010*, LNCS 6223, pp. 333–350. Springer, Berlin, Heidelberg, 2010. doi:10.1007/978-3-642-14623-7.
2. H. Cohen and G. Frey eds. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall/CRC, 2005.
3. R. Crandall and C. Pomerance. *Prime Numbers: A Computational Perspective*. Springer, 2005.
4. *ECMNET*. <https://members.loria.fr/PZimmermann/records/ecm/params.html>. Last access 2016/12/09.
5. S. D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012.
6. N. Kunihiko and K. Koyama. Equivalence of counting the number of points on elliptic curve over the ring  $z_n$  and factoring  $n$ . In K. Nyberg ed., *Advances in Cryptology – EUROCRYPT’98*, LNCS 1403, pp. 47–58. Springer, 1998. doi:10.1007/BFb0054112.
7. N. Kunihiko and K. Koyama. Tow discrete log algorithms for super-anomalous elliptic curves and their applications. *IEICE TRANS. on Fundamentals.*, E83-A(1):10–16, 2000.

8. H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126(3):649–673, 1987. doi:10.2307/1971363.
9. F. Leprévost, J. Monnerat, S. Varrette, and S. Vaudenay. Generating anomalous elliptic curves. *Information Processing Letters*, 93:225–230, 2005. doi:10.1016/j.ipl.2004.11.008.
10. J. H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag New York, 1985. doi:10.1007/978-0-387-09494-6.

## A On Proposition 13

This section gives a proof of Proposition 13. Proposition 13 relates to an elliptic curve over  $\mathcal{Q}_N^\tau$ . We also need to know the properties of  $\mathcal{Q}_p^\tau$  to prove Proposition 13, where  $p$  is a prime factor of  $N$ .

Section A.1 explains the arithmetic on  $\mathcal{Q}_n^\tau$  for a general integer  $n$ . Section A.2 explains the properties of  $\mathcal{Q}_p^\tau$ . Finally, Sec. A.3 gives the proof of Proposition 13.

### A.1 Arithmetic on $\mathcal{Q}_n^\tau$

Let  $\mathbb{Z}_n[X]$  be a set of polynomials with coefficients in  $\mathbb{Z}_n$  for  $(2 \leq) n \in \mathbb{N}$ . Then,  $\mathbb{Z}_n[X]$  forms a ring. Consider the residue ring of  $\mathbb{Z}_n[X]$ ,

$$\mathcal{Q}_n^\tau := \mathbb{Z}_n[X]/(X^2 - \tau)$$

for  $\tau \in \mathbb{Z}_n$ . We may take a representative of  $\mathcal{Q}_n^\tau$  as

$$a_0 + a_1X, \quad A_i \in \mathbb{Z}_n.$$

For  $a_0 + a_1X, b_0 + b_1X \in \mathcal{Q}_n^\tau$ , addition, subtraction, and multiplication are defined as follows.

$$\begin{aligned} (a_0 + a_1X) \pm (b_0 + b_1X) &= (a_0 + b_0) \pm (a_1 + b_1)X \\ (a_0 + a_1X) \cdot (b_0 + b_1X) &= a_0b_0 + (a_0b_1 + a_1b_0)X + a_1b_1 \underbrace{X^2}_{=\tau} \\ &= (a_0b_0 + a_1b_1\tau) + (a_0b_1 + a_1b_0)X \end{aligned}$$

The following lemma describes multiplicative inversion in  $\mathcal{Q}_n^\tau$ .

**Lemma 16** For  $a_0 + a_1X \in \mathcal{Q}_n^\tau$ , we have

$$a_0 + a_1X \text{ is regular in } \mathcal{Q}_n^\tau \Leftrightarrow \gcd(n, a_0^2 - a_1^2\tau) = 1.$$

Let  $b_0 + b_1X$  be the multiplicative inversion of a regular  $a_0 + a_1X$ . Then,  $b_0$  and  $b_1$  are given by

$$b_0 = \frac{a_0}{a_0^2 - a_1^2\tau} \quad \text{and} \quad b_1 = \frac{-a_1}{a_0^2 - a_1^2\tau}.$$



∴) We have

$$\begin{cases} a_0b_0 + a_1b_1\tau = 1 \\ a_0b_1 + a_1b_0 = 0 \end{cases}$$

because  $(a_0 + a_1X) \cdot (b_0 + b_1X) = 1 (= 1 + 0X)$ . Solving this as a simultaneous equation with  $b_0$  and  $b_1$  as variables, we see that

$$b_0 = \frac{a_0}{a_0^2 - a_1^2\tau} \text{ and } b_1 = \frac{-a_1}{a_0^2 - a_1^2\tau}.$$

Therefore, we have

$$\begin{aligned} a_0 + a_1X \text{ is regular in } \mathcal{Q}_n^\tau &\Leftrightarrow a_0^2 - a_1^2\tau \text{ is regular in } \mathbb{Z}_n \\ &\Leftrightarrow \gcd(n, a_0^2 - a_1^2\tau) = 1. \end{aligned}$$

□

## A.2 About $\mathcal{Q}_p^\tau$

Consider the residue ring of the polynomial ring  $\mathbb{F}_p[X]$  with coefficients in  $\mathbb{F}_p$ ,

$$\mathcal{Q}_p^\tau := \mathbb{F}_p[X]/(X^2 - \tau)$$

for  $\tau \in \mathbb{F}_p$ .

When  $\tau$  is a non-square in  $\mathbb{F}_p$ , the following holds.

$$\mathcal{Q}_p^\tau \simeq \mathbb{F}_{p^2} \text{ (ring isomorphism)}$$

We have the following lemma for when  $\tau$  is a square in  $\mathbb{F}_p$ .

**Lemma 17** *Let  $\tau$  be a square element in  $\mathbb{F}_p$ ,  $\tau = \sigma^2$  ( $\sigma \in \mathbb{F}_p$ ), and  $F(X) \in \mathcal{Q}_p^\tau$ . Then, the map*

$$\begin{aligned} \psi : \mathcal{Q}_p^\tau &\rightarrow \mathbb{F}_p \\ f(X) &\mapsto f(\sigma) \end{aligned}$$

*is a surjective homomorphism. Therefore, we have*

$$\mathcal{Q}_p^\tau / \ker \psi \simeq \mathbb{F}_p \text{ (ring isomorphism)}$$

*from the homomorphism theorem of rings.*

∴) To show the map  $\psi$  is well-defined, we have to show

1.  $\psi(f(X)) \in \mathbb{F}_p$  for any  $f(X) \in \mathcal{Q}_p^\tau$ ,
2. the value of  $\psi(f(X))$  is independent of the selection of the representative; in other words,  $\psi(X^2 - \tau) = 0$  holds because  $\mathcal{Q}_p^\tau = \mathbb{F}_p[X]/(X^2 - \tau)$ .

The polynomial  $f(X)$  has coefficients in  $\mathbb{F}_p$  and  $\sigma \in \mathbb{F}_p$ ; then  $\psi(f(X)) = f(\sigma) \in \mathbb{F}_p$ . In addition, we see that

$$\psi(X^2 - \tau) = \sigma^2 - \tau = 0$$

from the definition of  $\psi$ .

The map  $\psi$  is clearly a ring homomorphism. For any  $\alpha \in \mathbb{F}_p$ , we have  $\alpha (= \alpha + 0X) \in \mathbb{F}_p[X]/(X^2 - \tau)$  and

$$\psi(\alpha) = \alpha.$$

Thus,  $\psi$  is surjective.

From the above, we see that  $\psi$  is a surjective homomorphism.  $\square$

**Remark 18** From Lemma 17, if  $\tau$  is a square in  $\mathbb{F}_p$ , we may consider  $\mathcal{Q}_p^\tau$  as another (redundant) representation of  $\mathbb{F}_p$  because

$$\mathcal{Q}_p^\tau / \ker \psi \simeq \mathbb{F}_p.$$

The elements in  $\mathcal{Q}_p^\tau$  and  $\mathbb{F}_p$  correspond to each other as follows.

$$\begin{array}{ccc} \mathcal{Q}_p^\tau & \leftrightarrow & \mathbb{F}_p \\ \hline a_0 + a_1X & \mapsto \psi(a_0 + a_1X) = a_0 + a_1\sigma & \\ (\alpha - a\sigma) + aX & \leftrightarrow & \alpha \end{array}$$

where  $a \in \mathbb{F}_p$  is a random element.

The following lemma describes a property of  $a_0 + a_1X \in \mathcal{Q}_p^\tau$  corresponding to  $0 \in \mathbb{F}_p$ .

**Lemma 19** Let  $\tau$  be a square in  $\mathbb{F}_p$  and  $\sigma^2 = \tau$ . Then, if  $a_0 + a_1X \in \mathcal{Q}_p^\tau$  corresponds to  $0 \in \mathbb{F}_p$  in the way of Remark 18,  $a_0^2 - a_1^2\tau = 0$ .

$\cdot$ ) If  $a_0 + a_1X \in \mathbb{Z}_N[X]/(X^2 - \tau)$  corresponds to  $0 \in \mathbb{F}_p$ , we have  $\psi(a_0 + a_1X) = 0$  from Remark 18. Accordingly, we have

$$\begin{aligned} a_0^2 - a_1^2\tau &= a_0^2 - a_1^2\sigma^2 \\ &= (a_0 + a_1\sigma)(a_0 - a_1\sigma) \\ &= \underbrace{\psi(a_0 + a_1X)}_{=0} (a_0 - a_1\sigma) \\ &= 0. \end{aligned}$$

$\square$

Lemma 19 ensures that we can derive 0 given  $\tau$  and  $a_0 + a_1X \in \mathcal{Q}_p^\tau$  corresponding to  $0 \in \mathbb{F}_p$ , even if we don't know  $\sigma$  such that  $\tau = \sigma^2$ .

### A.3 Proof of Proposition 13

First, we should make a few preparations. Let  $E : y^2 = x^3 + Ax + B$  be an elliptic curve over  $\mathbb{Z}_N$ , and let  $P$  be a point on  $E(\mathcal{Q}_N^\tau)$  such that

$$P = (x_0 + x_1X, y_0 + y_1X) \in E(\mathcal{Q}_N^\tau), \quad x_i, y_i \in \mathbb{Z}_N.$$

Define

$$\begin{cases} A_p := A \bmod p, & B_p := B \bmod p \\ x_{i,p} := x_i \bmod p, & y_{i,p} := y_i \bmod p, \end{cases}$$

and  $E_p/\mathbb{F}_p : y^2 = x^3 + A_px + B_p$ . Then, the point

$$P_p = (x_{0,p} + x_{1,p}X, y_{0,p} + y_{1,p}X)$$

is on  $E_p$ .

**Remark 20** Let  $E$  be an elliptic curve over  $\mathbb{Z}_N (\subset \mathcal{Q}_N^\tau)$ ,  $p$  a prime factor of  $N$ , and  $\tau \in \mathbb{Z}_N$ . Moreover, assume that  $\tau_p := \tau \bmod p$  is a square in  $\mathbb{F}_p$ . Let the coordinates of  $kP$  be

$$kP = \left( \frac{a_{k,0} + a_{k,1}X}{(d_{k,0} + d_{k,1}X)^2}, \frac{b_{k,0} + b_{k,1}X}{(d_{k,0} + d_{k,1}X)^3} \right)$$

for  $P \in E(\mathcal{Q}_N^\tau)$ , where  $a_{k,i}, b_{k,i}, d_{k,i} \in \mathbb{Z}_N$ ,  $i = 0, 1$ . Then, if  $kP_p = \mathcal{O}_p$ , we have  $d_{k,0,p}^2 - d_{k,1,p}^2 \tau_p = 0$  in  $\mathbb{F}_p$  from Lemma 19, because  $d_{k,0,p} + d_{k,1,p}X$  corresponds to 0 in  $\mathbb{F}_p$  by Eq. (6). In other words,  $d_{k,0}^2 - d_{k,1}^2 \tau$  is a multiple of  $p$ . Therefore,

$$g = \gcd(N, d_{k,0}^2 - d_{k,1}^2 \tau)$$

is a non-trivial divisor of  $N$  (multiple of  $p$ ) if  $g \neq 0$ .

#### Proof of Proposition 13

Upon reducing both sides of Eq. (13) mod  $p$ , we get

$$\tau_p = x_{0,p}^3 + A_p^{D,R} x_{0,p} + B_p^{D,R}.$$

Assume that  $\tau_p$  is a square in  $\mathbb{F}_p$ , whose probability is  $1/2$ . Then, we can regard  $P_p$  as a point in  $E^{D,R}(\mathbb{F}_p)$  from Remark 18. Moreover, assume that  $E^{D,R}$  is anomalous, whose probability is  $1/2$  from Proposition 4 for  $t = 1$ . Then, we have  $pP_p = \mathcal{O}_p$  from Lagrange's theorem. We see that  $NP_p = \mathcal{O}_p$ , because  $N$  is a multiple of  $p$ . Let  $g = \gcd(N, d_{N,0}^2 - d_{N,1}^2 \tau)$ . If  $g \neq 0$ , then  $g$  is a non-trivial divisor (multiple of  $p$ ) from Remark 20. In addition, the probability of finding a non-trivial divisor of  $N$  under the assumption  $g \neq 0$ , which is "the probability that  $\tau_p$  is a square in  $\mathbb{F}_p$ "  $\times$  "the probability that  $E^{D,R}$  is anomalous", is equal to  $1/4$ .  $\square$

## B On Proposition 15

This section gives a proof of Proposition 15. Proposition 15 relates to an elliptic curve over  $\mathcal{S}_N^{D,\tau} = \mathcal{R}_N^D/(X^2 - \tau)$ , where  $\mathcal{R}_N^D = \mathbb{Z}_N[j]/H_{D,N}(j)$  and  $H_{D,N}[j]$  is a quadratic class polynomial. We also need to know the properties of  $\mathcal{R}_p^D$  and  $\mathcal{S}_p^{D,\tau}$  to prove Proposition 15, where  $p$  is a prime factor of  $N$ .

Sections B.1 and B.2 respectively describe arithmetic on  $\mathcal{R}_n^D$  and  $\mathcal{S}_n^{D,\tau}$  for a general  $n \in \mathbb{N}$ . Sections B.3 and B.4 explain  $\mathcal{R}_p^D$  and  $\mathcal{S}_p^{D,\tau}$ , respectively. Finally, Sec. B.5 proves Proposition 15.

### B.1 Arithmetic on $\mathcal{R}_n^D$

Here, we consider the case in which  $H_{D,n}(j)$  is quadratic. We may take  $a_0 + a_1j$ ,  $a_i \in \mathbb{Z}_n$  as a representative in  $\mathcal{R}_n^D(= \mathbb{Z}_n[j]/(H_{D,n}(j)))$ . Addition and subtraction in  $\mathcal{R}_n^D$  are defined as

$$(a_0 + a_1j) \pm (b_0 + b_1j) = (a_0 + b_0) \pm (a_1 + b_1)j$$

for  $a_0 + a_1j, b_0 + b_1j \in \mathcal{R}_n^D$ ,  $a_i, b_i \in \mathbb{Z}_n$ .

Let  $H_{D,n}(j)$  be represented as  $H_{D,n}(j) = s + tj + j^2$ . Then, multiplication in  $\mathcal{R}_n^D$  is defined as

$$\begin{aligned} (a_0 + a_1j) \cdot (b_0 + b_1j) &= a_0b_0 + (a_0b_1 + a_1b_0)j + a_1b_1 \underbrace{j^2}_{=-s-tj} \\ &= (a_0b_0 - a_1b_1s) + (a_0b_1 + a_1b_0 - a_1b_1t)j. \end{aligned}$$

For  $a_0 + a_1j \in \mathcal{R}_n^D$ , we have

$$\begin{aligned} \gcd(n, a_0^2 + a_1^2s - a_0a_1t) = 1 &\Leftrightarrow a_0^2 + a_1^2s - a_0a_1t \text{ is regular in } \mathbb{Z}_n \\ &\Leftrightarrow a_0 + a_1j \text{ is regular in } \mathcal{R}_n^D \end{aligned} \quad (18)$$

and

$$(a_0 + a_1j)^{-1} = \frac{a_0 - a_1t}{a_0^2 + a_1^2s - a_0a_1t} - \frac{a_1}{a_0^2 + a_1^2s - a_0a_1t} j.$$

### B.2 Arithmetic on $\mathcal{S}_n^{D,\tau}$

This subsection explains arithmetic on  $\mathcal{S}_n^{D,\tau}$ . For a quadratic class polynomial  $H_{D,n}(j)$ ,  $\mathcal{S}_n^{D,\tau}$  is constructed as

$$\begin{aligned} \mathcal{S}_n^{D,\tau} &= \mathcal{R}_n^D[X]/(X^2 - \tau) \\ &= \mathbb{Z}_n[j, X]/(H_{D,n}(j), X^2 - \tau). \end{aligned}$$

Then, we may take a representative in  $\mathcal{S}_n^{D,\tau}$  as

$$\alpha_0 + \alpha_1X, \quad \alpha_i \in \mathcal{R}_n^D$$

or

$$(a_0 + a_1j) + (a_2 + a_3j)X, \quad a_i \in \mathbb{Z}_n.$$

For  $\alpha_0 + \alpha_1X, \beta_0 + \beta_1X \in \mathcal{S}_n^{D,\tau}$  ( $\alpha_i, \beta_i \in \mathcal{R}_n^D$ ), addition, subtraction, and multiplication are defined as follows.

$$\begin{aligned} (\alpha_0 + \alpha_1X) \pm (\beta_0 + \beta_1X) &= (\alpha_0 + \beta_0) \pm (\alpha_1 + \beta_1)X \\ (\alpha_0 + \alpha_1X) \cdot (\beta_0 + \beta_1X) &= \alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0)X + \alpha_1\beta_1 \underbrace{X^2}_{=\tau} \\ &= (\alpha_0\beta_0 + \alpha_1\beta_1\tau) + (\alpha_0\beta_1 + \alpha_1\beta_0)X \end{aligned}$$

For  $\alpha_0 + \alpha_1X \in \mathcal{S}_n^{D,\tau}$ , we have

$$\alpha_0^2 - \alpha_1^2\tau \text{ is regular in } \mathcal{R}_n^D \Leftrightarrow \alpha_0 + \alpha_1X \text{ is regular in } \mathcal{S}_n^{D,\tau}. \quad (19)$$

Then, we have

$$(\alpha_0 + \alpha_1X)^{-1} = \frac{\alpha_0}{\alpha_0^2 - \alpha_1^2\tau} + \frac{-\alpha_1}{\alpha_0^2 - \alpha_1^2\tau}X.$$

### B.3 About $\mathcal{R}_p^D$

Let  $H_D(j)$  be a class polynomial given in Table 3, and  $H_{D,p}(j)$  be represented as  $H_{D,p}(j) = s + tj + j^2$  ( $s, t \in \mathbb{F}_p$ ). Note that  $H_{D,p}(j)$  is reducible over  $\mathbb{F}_p[j]$  from Remark 5. Let  $j_0, j_1 \in \mathbb{F}_p$  be roots of  $H_{D,p}(j)$ . Then, from Vieta's formulas, we have

$$\left. \begin{aligned} s &= j_0j_1 \\ t &= -j_0 - j_1 \end{aligned} \right\}. \quad (20)$$

**Lemma 21** *Let  $H_D(j)$  be a class polynomial given in Table 3, and  $j_0 \in \mathbb{F}_p$  be a root of  $H_{D,p}(j)$ . Define the map  $\psi_1$ ,*

$$\begin{aligned} \psi_1 : \mathcal{R}_p^D = \mathbb{F}_p[j]/(H_{D,p}(j)) &\rightarrow \mathbb{F}_p, \\ f(j) &\mapsto f(j_0). \end{aligned}$$

*Then,  $\psi_1$  is a surjective homomorphism of a ring. Therefore, we see*

$$\mathcal{R}_p^D / \ker \psi_1 \simeq \mathbb{F}_p$$

*from the homomorphism theorem of rings.*

$\therefore$ ) We can see that  $\psi_1(f(j)) = f(j_0) \in \mathbb{F}_p$ , because  $f(j)$  is a polynomial with coefficient in  $\mathbb{F}_p$  and  $j_0 \in \mathbb{F}_p$ . We have  $f(H_{D,p}(j)) = H_{D,p}(j_0) = 0$ ; then  $\psi_1$  is well-defined. In addition,  $\psi_1$  is clearly a homomorphism. We see that  $\psi_1$  is surjective because for any  $a \in \mathbb{F}_p$  we have  $a (= a + 0j) \in \mathcal{R}_p^D$  and

$$\psi_1(a) = a.$$

From the above,  $\psi_1$  is a surjective homomorphism.  $\square$

**Remark 22** From Lemma 21, we have  $\mathcal{R}_p^D / \ker \psi_1 \simeq \mathbb{F}_p$ . Accordingly, we regard  $\mathcal{R}_p^D$  as a (redundant) representation of  $\mathbb{F}_p$ , and  $\mathcal{R}_p^D$  and  $\mathbb{F}_p$  have the following correspondence.

$$\frac{\mathcal{R}_p^D}{\begin{array}{l} a_0 + a_1 j \\ (b - r j_0) + r j \end{array}} \leftrightarrow \frac{\mathbb{F}_p}{\begin{array}{l} \psi_1(a_0 + a_1 j) = a_0 + a_1 j_0 \\ b \end{array}}$$

where  $r \in \mathbb{F}_p$  is a random value. In particular, if we set  $r = 0$ , we see that  $b \in \mathbb{F}_p$  corresponds to  $b \in \mathcal{R}_p^D$ .

The following lemma describes the properties of  $a_0 + a_1 j \in \mathcal{R}_p^D$  corresponding to  $0 \in \mathbb{F}_p$  in the way of Remark 22.

**Lemma 23** Let  $H_{D,p}(j)$  be  $s + tj + j^2$ . Then, if  $a_0 + a_1 j \in \mathcal{R}_p^D$  corresponds to  $0 \in \mathbb{F}_p$  in the way of Remark 22, we have

$$a_0^2 + a_1^2 s - a_0 a_1 t = 0.$$

( $\because$ ) The roots  $j_0, j_1 \in \mathbb{F}_p$  of  $H_{D,p}(j)$  satisfy Eq. (20). If  $a_0 + a_1 j \in \mathcal{R}_p^D$  corresponds to  $0 \in \mathbb{F}_p$ ,  $\psi_1(a_0 + a_1 j) = a_0 + a_1 j_0 = 0$  from Remark 22. Therefore, we have

$$\begin{aligned} a_0^2 + a_1^2 s - a_0 a_1 t &= a_0^2 + a_1^2 j_0 j_1 + a_0 a_1 (j_0 + j_1) \\ &= \underbrace{(a_0 + a_1 j_0)}_{=0} (a_0 + a_1 j_1) \\ &= 0, \end{aligned}$$

from which the lemma is proved.  $\square$

#### B.4 About $\mathcal{S}_p^{D,\tau}$

Consider

$$\begin{aligned} \mathcal{S}_p^{D,\tau} &:= \mathcal{R}_p^D[X] / (X^2 - \tau) \\ &= \mathbb{F}_p[j, X] / (H_{D,p}(j), X^2 - \tau) \end{aligned}$$

for  $\tau \in \mathcal{R}_p^D$ .

Assume that  $\tau \in \mathcal{R}_p^D$  corresponds to a non-square in  $\mathbb{F}_p$  in the way of Remark 22. Then,  $\overline{X^2 - \tau} \in \mathbb{F}_p[X]$  is irreducible, and we know that

$$\mathbb{F}_p[X] / (X^2 - \tau) \simeq \mathbb{F}_{p^2}.$$

Therefore, we can see that

$$\mathcal{S}_p^{D,\tau} \simeq \mathbb{F}_{p^2}[j] / (H_{D,p}(j)).$$

From Remark 5,  $H_{D,p}(j)$  is reducible in  $\mathbb{F}_p[j]$ , which implies that  $H_{D,p}(j)$  is reducible in  $\mathbb{F}_{p^2}[j]$ . A similar argument to the one of Lemma 21 indicates that the map,

$$\begin{array}{ccc} \psi_2 : \mathcal{S}_p^{D,\tau} \simeq \mathbb{F}_{p^2}[j] / (H_{D,p}(j)) & \rightarrow & \mathbb{F}_{p^2} \\ & & \downarrow \\ & & F(j) \end{array} \quad \begin{array}{c} \rightarrow \\ \mapsto \\ \rightarrow \end{array} \begin{array}{c} \mathbb{F}_{p^2} \\ F(j_0) \end{array}$$

is a surjective homomorphism of rings and

$$\mathcal{S}_p^{D,\tau} / \ker \psi_2 \simeq \mathbb{F}_{p^2}.$$

Therefore, we regard  $\mathcal{S}_p^{D,\tau}$  as a redundant representation of  $\mathbb{F}_{p^2}$ .

When  $\tau \in \mathcal{R}_p^D$  corresponds to a square in  $\mathbb{F}_p$  in the way of Remark 22, the following lemma is satisfied.

**Lemma 24** *Assume that  $\tau \in \mathcal{R}_p^D$  corresponds to a square in  $\mathbb{F}_p$  in the way of Remark 22. Then, there is an element  $\sigma \in \mathbb{F}_p \subset \mathcal{R}_p^D$  such that  $\tau = \sigma^2$  from Remark 22. Then, the map  $\psi_3$  defined as*

$$\begin{aligned} \psi_3 : \mathcal{S}_p^{D,\tau} &\rightarrow \mathcal{R}_p^D \\ F(X) &\mapsto F(\sigma) \end{aligned}$$

is a surjective homomorphism of a ring. Therefore, we have

$$\mathcal{S}_p^{D,\tau} / \ker \psi_3 \simeq \mathcal{R}_p^D$$

from the homomorphism theorem of rings.

$\therefore$ ) If the polynomial  $F(X)$  has coefficients in  $\mathcal{R}_p^D$  and  $\sigma \in \mathbb{F}_p \subset \mathcal{R}_p^D$ , we have

$$\psi_3(F(X)) = F(\sigma) \in \mathcal{R}_p^D$$

and

$$\psi_3(X^2 - \tau) = \sigma^2 - \tau = 0.$$

Hence,  $\psi_3$  is well-defined. In addition,  $\psi_3$  is clearly a homomorphism. For any  $\alpha \in \mathcal{R}_p^D$ , we have

$$\alpha (= \alpha + 0X) \in \mathcal{S}_p^{D,\tau}$$

and

$$\psi_3(\alpha) = \alpha.$$

Hence,  $\psi_3$  is surjective, and  $\psi_3$  is a surjective homomorphism.  $\square$

**Remark 25** *When  $\tau \in \mathcal{R}_p^D$  corresponds to a square in  $\mathbb{F}_p$  in the way of Remark 22, we may regard  $\mathcal{S}_p^{D,\tau}$  as a redundant representation of  $\mathbb{F}_p$  because*

$$\mathcal{S}_p^{D,\tau} / \ker \psi_3 \simeq \mathcal{R}_p^D$$

from Lemma 24, and

$$\mathcal{R}_p^D / \ker \psi_1 \simeq \mathbb{F}_p$$

holds from Lemma 21. The correspondence between elements in  $\mathcal{S}_p^{D,\tau}$  and  $\mathbb{F}_p$  is as follows.

$$\begin{array}{ccc} \mathcal{S}_p^{D,\tau} & \leftrightarrow & \mathbb{F}_p \\ \hline (a_0 + a_1j) + (a_2 + a_3j)X & \mapsto & (a_0 + a_1j_0) + (a_2 + a_3j_0)\sigma \\ (b - r_1j) - (r_2 + r_3j)X & \mapsto & b, \end{array}$$

where  $r_1, r_2, r_3 \in \mathbb{F}_p$  are random values.

When  $\tau \in \mathcal{R}_p^D$  corresponds to a square in  $\mathbb{F}_p$  in the way of Remark 22, in order to know which element in  $\mathbb{F}_p$  corresponds to a given element in  $\mathcal{S}_p^{D,\tau}$ , we have to know  $j_0, j_1, \sigma$  in general. However, we can determine whether an element in  $\mathcal{S}_p^{D,\tau}$  corresponds to  $0 \in \mathbb{F}_p$  or not without  $\sigma$ . To show this, we introduce a map  $\phi_p$ , which is a  $p$  version of  $\phi_N$  defined as (16).

Let  $H_{D,p}$  be represented as  $H_{D,p} = s + tj + j^2$  ( $s, t \in \mathbb{F}_p$ ) and  $\tau \in \mathcal{R}_p^D$ . Then, the map  $\phi_p$  is

$$\phi_p : \left. \begin{array}{l} \mathcal{S}_p^{D,\tau} \rightarrow \mathbb{F}_p \\ (a_0 + a_1j) + (a_2 + a_3j)X \mapsto c, \end{array} \right\} \quad (21)$$

where  $c$  is computed as follows.

1. Compute  $b_0, b_1 \in \mathbb{F}_p$  such that  $b_0 + b_1j = (a_0 + a_1j)^2 - (a_2 + a_3j)^2\tau \in \mathcal{R}_p^D$ .
2. Compute  $c = b_0^2 + b_1^2s - b_0b_1t \in \mathbb{F}_p$ .

**Lemma 26** *Assume that  $\tau \in \mathcal{R}_p^D$  corresponds to a square in  $\mathbb{F}_p$  in the way of Remark 22. If  $(a_0 + a_1j) + (a_2 + a_3j)X \in \mathcal{S}_p^{D,\tau}$  corresponds to  $0 \in \mathbb{F}_p$ , we have*

$$\phi_p((a_0 + a_1j) + (a_2 + a_3j)X) = 0.$$

$\therefore$ ) We will compute  $c = \phi_p((a_0 + a_1j) + (a_2 + a_3j)X)$  as follows. Remark 22 enables us to write

$$\tau = \sigma^2 \quad (22)$$

for  $\sigma \in \mathcal{R}_p^D$ , and we have

$$j^2 = -s - tj. \quad (23)$$

Hence, we have

$$\begin{aligned} & (a_0 + a_1j)^2 - (a_2 + a_3j)^2\tau \\ &= (a_0 + a_1j)^2 - (a_2 + a_3j)^2\sigma^2 && \text{from (22)} \\ &= (a_0^2 - a_2^2\sigma^2) + j(2a_0a_1 - 2a_2a_3\sigma^2) + j^2(a_1^2 - a_3^2\sigma^2) \\ &= a_0^2 - a_1^2s - a_2^2\sigma^2 + a_3^2s\sigma^2 + j(2a_0a_1 - 2a_2a_3\sigma^2 - a_1^2t + a_3^2\sigma^2t) && \text{from (23)} \end{aligned}$$

and

$$\begin{cases} b_0 = a_0^2 - a_1^2s - a_2^2\sigma^2 + a_3^2s\sigma^2 \\ b_1 = 2a_0a_1 - 2a_2a_3\sigma^2 - a_1^2t + a_3^2\sigma^2t. \end{cases}$$

Accordingly, we see that

$$\begin{aligned} c &= (a_0^2 - a_1^2s - a_2^2\sigma^2 + a_3^2s\sigma^2)^2 \\ &\quad - (a_0^2 - a_1^2s - a_2^2\sigma^2 + a_3^2s\sigma^2)t \cdot (2a_0a_1 - 2a_2a_3\sigma^2 - a_1^2t + a_3^2\sigma^2t) \\ &\quad + s(2a_0a_1 - 2a_2a_3\sigma^2 - a_1^2t + a_3^2\sigma^2t)^2. \end{aligned}$$



In addition, let  $j_0$  and  $j_1$  be roots of  $H_{D,p}(j)$ ; then Eq. (20) is holds. Using Eq. (20) to eliminate  $s$  and  $t$ , we get

$$c = \left. \begin{aligned} & j_0 j_1 (2a_0 a_1 - a_1^2 (-j_0 - j_1) \\ & \quad - 2a_2 a_3 \sigma^2 + a_3^2 (-j_0 - j_1) \sigma^2)^2 \\ & - (-j_0 - j_1) (2a_0 a_1 - a_1^2 (-j_0 - j_1) - 2a_2 a_3 \sigma^2 + a_3^2 (-j_0 - j_1) \sigma^2) \\ & \cdot (a_0^2 - a_1^2 j_0 j_1 - a_2^2 \sigma^2 + a_3^2 j_0 j_1 \sigma^2) \\ & + (a_0^2 - a_1^2 j_0 j_1 - a_2^2 \sigma^2 + a_3^2 j_0 j_1 \sigma^2)^2. \end{aligned} \right\} \quad (24)$$

If  $(a_0 + a_1 j) + (a_2 + a_3 j)X \in \mathcal{S}_p^{D,\tau}$  corresponds to  $0 \in \mathbb{F}_p$  in the way of Remark 25, we have  $(a_0 + a_1 j_0) + (a_2 + a_3 j_0)\sigma = 0$ , in other words,

$$\sigma = \frac{-(a_0 + a_1 j_0)}{a_2 + a_3 j_0}.$$

Substituting this  $\sigma$  into Eq. (24), we find that  $c = 0$ <sup>1</sup>.  $\square$

## B.5 Proof of Proposition 15

**Remark 27** Let  $p$  be a prime factor of  $N$  and  $\tau \in \mathbb{Z}_N$ . Let the maps  $\phi_N$  and  $\phi_p$  be defined as in (16) and (21), respectively. Moreover, assume that  $\tau_p$  corresponds to a square in  $\mathbb{F}_p$  in the way of Remark 25. Let the coordinates of  $kP$  be

$$kP = \left( \frac{(a_{k,0} + a_{k,1}j) + (a_{k,2} + a_{k,3}j)X}{((d_{k,0} + d_{k,1}j) + (d_{k,2} + d_{k,3}j)X)^2}, \frac{(b_{k,0} + b_{k,1}j) + (b_{k,2} + b_{k,3}j)X}{((d_{k,0} + d_{k,1}j) + (d_{k,2} + d_{k,3}j)X)^3} \right),$$

where  $(a_{k,i}, b_{k,i}, d_{k,i} \in \mathbb{Z}_N, i = 0, 1)$  for  $P \in E(\mathcal{S}_N^{D,\tau})$ , and let  $d_{k,i,p} := d_{k,i} \bmod p$ . Then, if  $kP_p = \mathcal{O}_p$ , an element in  $\mathbb{F}_p$ , which corresponds to  $(d_{k,0,p} + d_{k,1,p}j) + (d_{k,2,p} + d_{k,3,p}j)X$ , is 0 from (6), and we can see that  $\phi_p((d_{k,0,p} + d_{k,1,p}j) + (d_{k,2,p} + d_{k,3,p}j)X) = 0$  in  $\mathbb{F}_p$  from Lemma 26. Therefore, if

$$g = \gcd(N, \phi_N((d_{k,0} + d_{k,1}j) + (d_{k,2} + d_{k,3}j)X))$$

is not 0, then  $g$  is a non-trivial divisor of  $N$  (multiple of  $p$ ).

**Proof of Proposition 15**

Reducing both sides of Eq. (17) mod  $p$ , we get

$$\tau_p = x_{0,p}^3 + A_p^{D,R} x_{0,p} + B_p^{D,R}.$$

Assume that  $\tau_p$  is a square in  $\mathbb{F}_p$ , whose probability is  $1/2$ . Accordingly, we can regard the point  $P_p$  as a point on  $E_p^{D,R}(\mathbb{F}_p)$  from Remark 25. Moreover, assume that  $E_p^{D,R}$  is anomalous, whose probability is  $1/2$  from Proposition 4 for  $t = 1$ . From Lagrange's theorem, we can see that  $pP_p = \mathcal{O}_p$ . Because  $N$  is a multiple of  $p$ ,  $NP_p = \mathcal{O}_p$ . If  $g = \gcd(N, \phi_N((d_{N,0} + d_{N,1}j) + (d_{N,2} + d_{N,3}j)X))$  is not 0, then  $g$  is a non-trivial divisor of  $N$  (multiple of  $p$ ) from Remark 27. In addition, the probability of finding a non-trivial divisor of  $N$  under the assumption  $g \neq 0$ , which is “the probability that  $\tau_p$  is a square in  $\mathbb{F}_p$ ”  $\times$  “the probability that  $E^{D,R}$  is anomalous”, is equal to  $1/4$ .  $\square$

<sup>1</sup> The authors confirmed this using Mathematica.