Elliptic Curve Method with Complex Multiplication Method

相川 勇輔（Yusuke AIKAWA）*

北海道大学大学院理学院数学専攻/産業技術総合研究所

1 はじめに

本稿で述べる研究内容は縫田光司氏（産業技術総合研究所/JST さきがけ）と白勢政明氏（公立はこだて未来大）との共同研究に基づく．

数学的な問題意識の中のみで研究されてきた対象の，数学以外の学問領域への応用が見出されたならば，それは驚くべきことであり，このような交流はお互いにとって喜ばしいことである．暗号理論はまさにその好例である．本稿ではその交流のほんの一側面を紹介するとともに，筆者らの研究によって構成された素因数分解アルゴリズム [1] について報告する．そのアルゴリズムは，代表的な素因数分解アルゴリズムである楕円曲線法に特殊な楕円曲線生成法である CM 法を組み合わせたものとなっている．

なぜ素因数分解か．RSA 暗号など現代の公開鍵暗号技術の多くは素因数分解の計算困難性を安全性の根拠におく．したがって，それらの安全性を見積もる上で，素因数分解アルゴリズムの研究は決定的に重要である．純粋に数学的関心の範疇で素因数分解問題は歴史上古くから考えられてきたが，今日のように広い関心を惹きつけるになった背景にはこのような事情がある．しかしながら一般の合成数に対する素因数分解については準指数時間アルゴリズムしか未だ知られていない．分解したい合成数を N，その素因数を p としたとき，素因数分解アルゴリズムはその計算量が N の大きさに依存するタイプのものと p の大きさに依存するタイプのものに大別できる．前者の代表的なものでは数体ふるい法がよく知られており，本稿で中心的役割を果たす楕円曲線法（§3.3）は後者の代表例となっている．ところが，本稿でも紹介する Pollard の $p-1$ 法（§3.2）のように，特定の条件を満たす合成数を高速に素因数分解する方法が知られているため，同じ大きさを持つ合成数であってもその素因数分解の計算量（つまり公開鍵としての強度）は均一でない．したがって暗号技術の実運用においては “素因数分解されやすい合成数”を公開鍵として使用することは避けるべきであり，そのような合成数の種類を明らかにすることは重要な意味を持つ．

そのような中で本稿では，特殊な形をした素数を素因数に持つ合成数 N に対する N の大きさに関する多項式時間素因数分解アルゴリズムを提案する．これは冒頭でも述べたように，Lenstra Jr. による楕円曲線法 [5] と特殊な楕円曲線生成法である CM 法を組み合わせたものとなっている．

N を合成数とし p をその素因数とすると，楕円曲線法は，§3.3 でも詳しく解説するが，$\mathbb{Z}/N\mathbb{Z}$ 上の楕円曲線と有理点の組みをたくさん生成し，その中に $\mathbb{F}_p$ への還元がスムースな位数（つまりその素因数が全て小さい素数である位数）を持つものがあると期待するものであった．このアルゴリズムでは大量の有理点のスカラー倍演算が必要な上，そのスカラー倍演算の程度（有理点を何倍するか）を上手に選ぶ必要があった．

先行研究 [8] のアルゴリズムでは発想を逆転させる．すなわち，$\mathbb{F}_p$ への還元が良い位数を持つ楕円曲線を予めひとつ生成することで，この 2 つの問題点を同時に克服することを試みた．[8] では素数 p が，その類多項式が 2 次以下となるよう判別式 $-D$ を用いて $4p = 1 + Dv^2 (v \in \mathbb{Z})$ と書ける場合，CM 法を用いて $\mathbb{F}_p$ 上での位数が p となる楕円曲線 E を生成するというアイデアを用いた．そうすることで，

* *e-mail*:yusuke@math.sci.hokudai.ac.jp

もし有理点を得ることができれば，その N 倍が $E(\mathbb{F}_p)$ の中で単位元となり，あとは楕円曲線法と同様の手続きで N の非自明な素因数が得られる．ではどのようにして有理点を見つけるのか？ 元々の楕円曲線法では先に有理点の座標を決めてからそれを解に持つように楕円曲線の定義方程式を調整するという巧みな方法をとっていた．しかし，CM 法を用いる場合には後から楕円曲線を調整することができない．そこで [8] では，楕円曲線の定義方程式の解を添加して拡大した係数環を導入することでこの問題点を回避した．本稿においてもこのテクニックを踏襲する．すると新たな問題が生じる．拡大した係数環を用いる場合，$\mathbb{F}_p$ への還元が ∞ となる有理点から N の非自明な素因数を得る際に，元々の楕円曲線法と同じ方法は適用できず，別途計算を行う必要がある．先行研究においては類多項式が 2 次以下となる判別式で表される素数に対してのアルゴリズムの構成を与えたが，その計算は複雑かつアドホックでありそのまま 3 次以上への拡張は困難であった．

それに対し，本研究では以下のことを行った．まず用いられている数学的理論を整理することにより類多項式の次数に関する制限を外せることの理論的根拠を与えた．さらに，先行研究におけるアドホックな構成が本質的に終結式の計算を行っていることを看破することによって，判別式が高次の類多項式を持つ場合へアルゴリズムの構成を一般化した．それにとどまらず，先行研究が $4p = 1 + Dv^2$ という形の素数を扱っていたのに対し，$4p = t^2 + Dv^2$ という形をしていても $p + 1 - t$ がスムースとなる場合へアルゴリズムを拡張した．まとめると，本稿では次の 2 つのアルゴリズムを与え，それによって得られた素因数分解の数値例を提示する．

- $4p = 1 + Dv^2$ という形の素数を素因数に持つ合成数 N と判別式 $-D$ とその類多項式 $H_{-D}(X)$ の入力に対し N の素因数を 確率 $\frac{1}{4}$ で出力する N の長さに関する多項式時間アルゴリズム．
- 素数 p が $4p = t^2 + Dv^2$ という形をしており $p + 1 - t$ が smooth になるとき，このような p を素因数にもつ合成数 N と判別式 $-D$ とその類多項式 $H_{-D}(X)$ の入力に対し N の素因数を確率 $\frac{1}{4}$ で出力する N の長さに関する多項式時間アルゴリズム．

本稿は以下のように構成される．まず §2 において本研究の動機を明確にするために公開鍵暗号の一つである RSA 暗号について解説する．§3 では楕円曲線法について解説を行うが，そのために楕円曲線の基本的事項をまとめ，楕円曲線法の基本的アイデアとなった $p - 1$ 法についても解説を行う．特殊な楕円曲線生成法である CM 法は §4 で解説を行う．最後に §5 においてこれらを組み合わせた素因数分解アルゴリズムを提案する．本アルゴリズムを用いた数値例は §6 で与える．

2 RSA 暗号

暗号技術の重要な役割の一つは “守秘”である．送信者 S はメッセージ m をその内容を第三者には秘密にしたまま受信者 R に送ろうとしており，この m を盗聴したい第三者の攻撃者 A はこの二者の間の通信を傍受することができる，という状況を考える．もし S がこのメッセージ m をそのまま R へ送れば A はその内容を知ることができるので，S はメッセージ m を暗号文 c に変換（この変換に必要なパラメータを**暗号化鍵**とよぶ）してから R へ送信し，R は暗号文 c をメッセージ m に変換（この変換に必要なパラメータを**復号鍵**とよぶ）しその内容を知る，という手続きを行う必要がある．この暗号化鍵と復号鍵が同じものを**共通鍵暗号**という．原始的な例だが，“アルファベットを一文字ずらす”という鍵で構成される共通鍵暗号方式を考える[*1]．送信者が「LOVE」というメッセージを秘密に送信したいとする．このときこの文字列を鍵を用いて一文字ずらし「MPWF」と暗号化し送信する．それを受け取った者は鍵を用いてメッセージ「LOVE」を復元する．このような共通鍵暗号は，はるか昔から用いられてきた暗号であるが，S と R がどのようにして鍵を共有するかという問題が常につきまとう．もし鍵の受け渡しの途中で鍵が A に漏洩してしまえば，解読が困難な暗号を用いたとしても A は暗号文 c をたちまちメッセージ m に変換しその内容を知ることができてしまう．

この問題を解消したのが 1970 年代に編み出された**公開鍵暗号** [4] である．公開鍵暗号では暗号化鍵と復号鍵が異なり，前者から後者を求めることが困難であることが求められる．すると受信者が復号鍵

[*1] このようにアルファベットを一定数ずらすことで構成されるものをシーザー暗号という．

を秘密にしてさえおけば，暗号化鍵は公開しておいてもメッセージの漏洩は避けることができ，秘密裏に鍵を共有しておく必要がなくなる．そこで，公開鍵暗号では暗号化鍵を**公開鍵**とよび，復号鍵を**秘密鍵**とよぶ．公開鍵暗号の構成には数学的問題の困難性が利用される．素因数分解の困難性を利用した RSA 暗号，離散対数問題の困難性を利用した ElGamal 暗号，そして楕円曲線の離散対数問題を利用した楕円曲線暗号がその代表例である．

ここでは RSA 暗号 [7] について解説を行う．メッセージの受信者 R は大きな素数 p, q [*2]を選び，$N = pq$ を計算する．さらに整数 e で $\gcd\big((p-1)(q-1), e\big) = 1$ となるものをランダムにとる．これらに対して，$\mathbb{Z}/(p-1)(q-1)\mathbb{Z}$ の中での e の逆元 d を計算する．このとき，

$$\text{公開鍵：}(N, e)$$
$$\text{秘密鍵：}d$$

とする．もちろん R は p, q も秘密にしておく．

送信者 S が R へ送りたいメッセージが $0 \leq m \leq N-1$ なる整数 m で表現されているとする．S は公開鍵を用いて暗号文 c を

$$c = m^e \in \mathbb{Z}/N\mathbb{Z}$$

と計算する．この暗号文 c を受け取った R は秘密鍵を用いて $\mathbb{Z}/N\mathbb{Z}$ の中で c^d を計算する．すると，

$$c^d = m \in \mathbb{Z}/N\mathbb{Z}$$

であることが確かめられる．

このような手続きで二者の間でメッセージを秘密裏に共有する方式を RSA 暗号方式という．この方式の中では共通鍵暗号で必要だった鍵の共有という手続きが必要でないことがわかる．しかしながら公開されている合成数 N が簡単に素因数分解できてしまうと，秘密鍵である d が容易に計算できてしまい，暗号文 c を傍受した第三者がメッセージ m を復元できてしまう．このような意味で RSA 暗号の安全性は素因数分解問題に依存している．[*3]従って §1 でも述べたように，RSA 暗号の安全性を評価する上では素因数分解アルゴリズムの研究が欠かすことはできない．例えば，もし何かしらのアルゴリズムで高速に素因数分解されてしまうような “脆弱な素数”が発見されてしまえば，そのような素数を用いて鍵の生成を行ってはならないことが明らかになる．そして，筆者らによる研究はそのような “脆弱な素数”をあぶり出そうという試みである．

3 楕円曲線法

3.1 楕円曲線

体 K を標数が 2 でも 3 でもない体とする．方程式

$$E : y^2 = x^3 + Ax + B \ (A, B \in K, 4A^3 + 27B^2 \neq 0) \tag{3.1}$$

で定義される代数曲線を K 上の**楕円曲線**とよぶ．楕円曲線はその K-有理点集合（以下，状況が明らかな場合は単に有理点とよぶ）

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

が点 ∞ を単位元とする群構造を持つという著しい性質を持つ．この群を楕円曲線 E の Mordell-Weil 群とよぶ．

2 つの有理点 P_1, P_2 に対して $P_1 + P_2$ を具体的に計算する公式が知られている（詳しくは [10] や [11]）．暗号理論への楕円曲線の応用という観点からは，スカラー倍の計算が重要である．スカラー倍計算に対しては，等分多項式を用いた公式が知られているので，それを紹介する．

[*2] 512bit（10 進法で約 150 桁）以上のものを選ぶのが現状では標準である．

[*3] 素因数分解ができれば RSA 暗号は破られるが，その逆については未解決である．つまり，N を素因数分解することなく暗号文を平文に変換する方法があるかどうかは未だわかっていない．

方程式 (3.1) で定義される楕円曲線に対し，次の漸化式で 2 変数多項式の族を定める．

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

これらを等分多項式とよぶ．さらに等分多項式を用いて整数 $m \geq 0$ に対し次のように多項式を定める．

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

以上の多項式を用いて E の有理点 $P = (x, y)$ のスカラー倍は次のように記述できる．n を正の整数とすると，

$$nP = \Big(\frac{\phi_n(x,y)}{\psi_n(x,y)^2}, \frac{\omega_n(x,y)}{\psi_n(x,y)^3}\Big) \tag{3.2}$$

が成り立つ[*4]．このように有理点 P の n 倍点 は等分多項式によって完全に定められ，次が成り立つ：

$$nP = \infty \Longleftrightarrow \psi_n(x,y) = 0. \tag{3.3}$$

このように体上の楕円曲線での群演算において，その計算過程で逆元の計算を必要とする．したがって環上，例えば合成数 N に対して $\mathbb{Z}/N\mathbb{Z}$ 上で楕円曲線を考えた場合は，この加法公式が機能しなくなる．しかし，そのことが楕円曲線法において重要な役割を果たす．なお，環上の楕円曲線の加法公式も知られている [5].

さて，K 上定義された 2 つの楕円曲線 E_1 から E_2 への同種写像とは準同型写像 $\alpha : E_1(\overline{K}) \to E_2(\overline{K})$ であって，有理関数で与えられるものである．さらに逆写像が存在するとき E_1 と E_2 は同型であるという．E 自身から E 自身への同種写像を E の自己準同型とよび，それらのなす環を $\mathrm{End}(E)$ で表す．本稿では $K = \mathbb{C}$ の場合の自己準同型環の構造が重要であるが，それについて述べる前に次の定義を用意する．

定義 3.1. 平方因子を持たない整数 d に対し，体

$$\mathbb{Q}(\sqrt{-d}) = \big\{a + b\sqrt{-d} \mid a, b \in \mathbb{Q}\big\}$$

を**虚二次体**とよぶ．虚二次体の部分環であって $\mathbb{Z}$ を真に含むものを**オーダー**とよぶ．

$\delta \in \mathbb{Q}(\sqrt{-d})$ を

$$\delta = \begin{cases} \frac{1+\sqrt{-d}}{2} & (d \equiv 3 \bmod 4)\\ \sqrt{-d} & (d \equiv 1, 2 \bmod 4) \end{cases}$$

とおく．このとき $\mathbb{Q}(\sqrt{-d})$ のオーダー $\mathcal{O}$ は整数 $f > 0$ が存在して $\mathcal{O} = \mathbb{Z} + f\delta\mathbb{Z}$ という形をしている．これに対してオーダー $\mathcal{O}$ の**判別式**を

$$-D = \begin{cases} -f^2 d & (d \equiv 3 \bmod 4)\\ -4f^2 d & (d \equiv 1, 2 \bmod 4) \end{cases}$$

で定める．あるオーダーの判別式となっている負の整数を単に判別式とよぶ．

[*4] 実は，ψ_m^2 と ϕ_m は X と Y^2 の多項式になることが示せる．従ってこの公式の第一成分は y^2 に $x^3 + Ax + B$ を代入することで x のみの多項式として書ける．

定理 3.2. E を $\mathbb{C}$ 上の楕円曲線とする．このとき次のどちらかが成り立つ．

- $\mathrm{End}(E) = \mathbb{Z}$
- ある虚二次体 $K = \mathbb{Q}(\sqrt{-D})$ とそのオーダー $\mathcal{O}$ が存在し，$\mathrm{End}(E) \cong \mathcal{O}$ となる

定義 3.3. $\mathbb{C}$ 上の楕円曲線 E が $\mathbb{Q}(\sqrt{-D})$ **のオーダー** $\mathcal{O}$ **による虚数乗法を持つ**とは，$\mathrm{End}(E)$ が $\mathcal{O}$ と同型なときをいう．

方程式 (3.1) で定義される楕円曲線 E に対し

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

を E の j **不変量**と呼ぶ．

仮定 3.4. 本稿では $j_E \neq 0, 1728$ なる楕円曲線のみを扱う．

これらの場合はそれぞれ $\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-1})$ [*5]の整数環（極大オーダー）よる虚数乗法を持つ楕円曲線であり，先行研究 [8] に含まれるもの（類多項式が 1 次）であるので本稿では除いて議論を進める．またこれらの判別式はそれぞれ $-3, -4$ なので，判別式としてこれらの値を除いて議論を進める．

逆に $j_0 \in K$ が与えられた時，j_0 を j 不変量とする楕円曲線は次のように構成できる．

命題 3.5. 与えられた $j_0 \in K$ $(j_0 \neq 0, 1728)$ に対し，

$$E : y^2 = x^3 + \frac{3j_0}{1728 - j_0}x + \frac{2j_0}{1728 - j_0}$$

は j_0 を j 不変量とする K 上の楕円曲線である．

さて，この量は次の重要な性質を持つ．

命題 3.6. 2 つの楕円曲線が代数的閉体上同型であることと，それらの j 不変量が等しいことは同値である．

一般の体 K 上で考えた場合，K 上同型であれば定義より明らかに j 不変量は一致するが，その逆は成り立たない．楕円曲線 E に対し，j_E に等しい j 不変量を持つ楕円曲線を E の**ツイスト**とよぶ．

3.2 $p-1$ 法

Pollard によって考案された $p-1$ 法は楕円曲線法の基本的アイデアを与えた重要な素因数分解アルゴリズムであるのでここで簡単な解説を与える．そこで，一つ用語を導入する．

定義 3.7. C を正の整数とする．このとき整数 N が C-**スムース**であるとは，N の最大の素因数が C より小さいときを言う．C を省略して単に，N が**スムース**である，と言った場合は C が小さい整数であるということを暗に意味する．

合成数 N が $N = pq$ と素数の積であるとし，N の素因数を見つけたい．素因数の一つの p に対し $p-1$ が C-スムースであると仮定する．また簡単のために $p-1$ は平方因子を持たないと仮定する．このとき $p-1$ は $C!$ の約数となるので，

$$a^{C!} \equiv 1 \bmod p$$

が成り立つ．さらに運良く

$$a^{C!} \not\equiv 1 \bmod q$$

であったとする．このとき $\gcd(a^{C!} - 1, N)$ は p を出力し合成数 N の非自明な素因数が見つかる．

[*5] これらの虚 2 次体の単数群が特殊なものであるから例外的に扱う必要がある．

以上の手続きで合成数の素因数を見つける方法を $p-1$ **法**とよぶ．しかし，この方法には N が与えられた時点で群 $\mathbb{F}_p^\times$ が固定されてしまうという問題点がある．従って $p-1$ がスムースでなければ，C の値を変化させるくらいしか我々に出来ることはなく，その値が大きくなればなるほど計算は困難となる．そこで，様々な位数を持った群で上述のような計算ができるような状況があればこの問題点を解消できる．楕円曲線はこれを実現した．

3.3 楕円曲線法

この $p-1$ 法の問題点を楕円曲線を用いることで鮮やかに回避したのが Lenstra Jr. による**楕円曲線法** [6] である．まずそのアイデアを見る．

合成数を $N=pq$（p と q は異なる奇素数）とし，環 $\mathbb{Z}/N\mathbb{Z}$ 上で楕円曲線 E を考える．このとき，

$$E(\mathbb{Z}/N\mathbb{Z}) \cong E(\mathbb{F}_p) \oplus E(\mathbb{F}_q) \tag{3.4}$$

が成り立つ．

さて $E(\mathbb{Z}/N\mathbb{Z})$ 上で公式 (3.2) を用いた有理点 P のスカラー倍を観察する．するとその計算過程では $\mathbb{Z}/N\mathbb{Z}$ の逆元の計算を必要とする．したがって分母にくるべき数 d が逆元を持たない場合は計算失敗となる．では $\mathbb{Z}/N\mathbb{Z}$ で逆元を持たない数とは何か．それは p と q の少なくとも一方を素因数とする数である．そこで，

$$\begin{cases} d \equiv 0 \bmod p \\ d \not\equiv 0 \bmod q \end{cases} \tag{3.5}$$

であったとする．このとき，P のスカラー倍nP の計算が (3.4) の左辺で失敗したとしよう．P に対応する (3.4) の右辺の点を (P_p, P_q) と書けば，仮定 (3.5) は (3.3) より $nP_p=\infty$ かつ $nP_q\neq\infty$ を意味する．この観察を利用する．つまり，$\#E(\mathbb{F}_p)|n$ となる n を選ぶことができれば $nP_p=\infty$ となり，$E(\mathbb{Z}/N\mathbb{Z})$ 内で計算した nP の分母にくるべき値と N の最大公約数を取ったとき非自明な値が返ってくる．この $\#E(\mathbb{F}_p)$ こそが $p-1$ 法における値 $p-1$ にあたるものである．そこで，スムースな位数を持つことを期待して次々に楕円曲線を生成していけばよい．

しかしながら，一般に $\mathbb{Z}/N\mathbb{Z}$ 上の楕円曲線 E とその有理点 P の組みをランダムに生成することは難しい．この問題点は次のようにして巧みに回避できる．まずランダムに $\mathbb{Z}/N\mathbb{Z}$ の元の 3 つ組み（a,u,v）をとる．これらを用いて $b\in\mathbb{Z}/N\mathbb{Z}$ を $b=v^2-u^3-au \bmod N$ と定めれば，$\mathbb{Z}/N\mathbb{Z}$ 上の楕円曲線 $E: y^2=x^3+ax+b$ と有理点 $P=(u,v)\in E(\mathbb{Z}/N\mathbb{Z})$ が得られる．

まとめると，楕円曲線法とは以下の手続きで合成数の素因数を見つける方法である．

- **Step1**:いくつものランダムな $\mathbb{Z}/N\mathbb{Z}$ の組み (a_i,u_i,v_i) から上述のように楕円曲線とその有理点の組みの族 (E_i,P_i) を生成する．
- **Step2**:正整数 C を選び $(C!)P_i$ を計算していく．
- **Step3**:ある i で計算に失敗したらその分母に来るべき整数と N の最大公約数は N の非自明な素因数を返す．全ての i で計算が実行できたら，楕円曲線の族を生成しなおすか C を選び直して同様の計算を実行する．

4 CM 法

本節の内容について詳しくは [2]，[9]ChIII 等を参照されたい．

また，本節以降の便利のため，次の記号を導入する．多項式 $f(X)\in\mathbb{Z}[X]$ に対して，その係数を $\bmod n$ して得られる多項式を $f_n(X)\in\mathbb{Z}/N\mathbb{Z}[X]$ で表す．

4.1 類多項式

$-D$ を判別式とする．すると，判別式 $-D$ をもつオーダー $\mathcal{O}\subset\mathbb{Q}(\sqrt{-D})$ がある．この $\mathcal{O}$ による虚数乗法をもつ楕円曲線の $\mathbb{C}$ 上での同型類の集合を $\mathcal{ELL}(-D)$ と書く．このとき次が言える．

命題 4.1. $\mathcal{ELL}(-D)$ は有限集合である．

そこで $\mathcal{ELL}(-D) = \{E_1, \cdots, E_h\}$ と書き下せば，それらの j 不変量をとることによって有限個の相異なる複素数 $j_1, \cdots, j_h \in \mathbb{C}$ が得られる．このとき，多項式

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

を判別式 $-D$ の**類多項式**という．類多項式は整数係数を持つという著しい性質をもち，したがって係数を $\bmod p$ することによって $\mathbb{F}_p$ 係数の多項式 $H_{-D,p}(X)$ が得られる．

次の定理が成り立つ．

定理 4.2. 判別式 $-D$ とし，p を $-D$ を割らない素数とする．次は同値．

- $4p = t^2 + Dv^2$ *(*$\exists t \in \mathbb{Z}$ s.t. $t \not\equiv 0 \bmod p$, $\exists v \in \mathbb{Z}$*)*.
- $\left(\frac{-D}{p}\right) = 1$ であって $H_{-D,p}(X)$ は $\mathbb{F}_p$ において一次式のみの積に分解する．ただし，$\left(\frac{\cdot}{p}\right)$ は平方剰余記号．

4.2 CM 法

素数 p がある判別式 $-D$ を用いて $4p = t^2 + Dv^2 (t, v \in \mathbb{Z})$ と書けるとする（$D > 4$ のとき[*6]，整数 t^2, v^2 は p, D から一意的に定まる）．CM 法はここに現れる p と t に対し，$\mathbb{F}_p$ 上の楕円曲線 E であって $\#E(\mathbb{F}_p) = p + 1 - t$ なる楕円曲線を構成する方法である．

この仮定の下で定理 4.2 により $-D$ の類多項式 $H_{-D,p}(X)$ は $\mathbb{F}_p$ の中で一次式の積に分解できるので，$\mathbb{F}_p$ 内に根を持つ．そのひとつを j_0 とする．この j_0 を j 不変量にもつ $\mathbb{F}_p$ 上の楕円曲線 E_{j_0} を命題 3.5 のように構成する．$\#E_{j_0}(\mathbb{F}_p) = p + 1 - a$ ($|a| < 2\sqrt{p}$[*7]) と書くと次が成り立つ．

命題 4.3. この状況下で

$$a = \pm t$$

が成り立つ．従って E'_{j_0} を E_{j_0} のツイストで $\mathbb{F}_p$ 上同型でないものとすると，そのどちらかは位数 $p + 1 - t$ をもつ．

5 提案アルゴリズム

5.1 設定

$N = pq$ を相異なる二つの素数の積とし，素数 p が判別式 $-D$ を用いて $4p = t^2 + Dv^2 (t, v \in \mathbb{Z})$ と書けると仮定する．$-D$ の類多項式 $H_{-D}(X)$ に対し

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

とおく．ランダムに選んだ $c \in \mathbb{Z}/N\mathbb{Z}$ に対して $A^{-D,c}(X) = \frac{3c^2X}{1728-X}, B^{-D,c}(X) = \frac{2c^3X}{1728-X}$ とおき，R_N^{-D} 上の楕円曲線を次のように定義する：

$$E^{-D,c} : y^2 = x^3 + A^{-D,c}(X)x + B^{-D,c}(X). \tag{5.1}$$

このとき $j_{E^{-D,c}} = X$ である．j_0 を $H_{-D,p}(X)$ の根とし，$\mathbb{F}_p$ 上の楕円曲線を

$$E_{j_0}^{-D,c} : y^2 = x^3 + A_p^{-D,c}(j_0)x + B_p^{-D,c}(j_0)$$

[*6] 仮定 3.4 とその直後の文章に注意．

[*7] Hasse の定理による．詳しくは [10]，[11] など．

で定義すれば，その j 不変量は j_0 であるから CM 法により

$$\#E_{j_0}^{-D,c}(\mathbb{F}_p) = p + 1 - t \text{ or } p + 1 + t$$

である．

係数環を拡大することにより $E^{-D,c}$ の有理点を構成する．さらにランダムに選んだ $x_0 \in \mathbb{Z}/N\mathbb{Z}$ に対し，

$$\tau(X) := x_0^3 + A^{-D,c}(X)x_0 + B^{-D,c}(X) \in R_N^{-D} \tag{5.2}$$

とおく．

$$S_N^{-D,\tau(X)} := R_N^{-D}[Y]/\big(Y^2 - \tau(X)\big)$$

とおけば，

$$P = (x_0, Y) \in E^{-D,c}\big(S_N^{-D,\tau(X)}\big)$$

となり，有理点を構成できた．このとき公式 (3.2) により自然数 n に対し

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

と書くことができ，さらに環 $S_N^{-D,\tau(X)}$ の中で

$$\psi_n(x_0, Y) = g_{n,0}(X) + g_{n,1}(X)Y$$

と書くことができる[*8]．ここで，$g_{n,i}(X) \in \mathbb{Z}/N\mathbb{Z}[X]$ であり $\deg\big(g_{n,i}(X)\big) < \deg\big(H_{-D}(X)\big)(i = 0, 1)$ である．

5.2 基本的命題と提案アルゴリズム

以上の設定の下で，後述するアルゴリズムが機能する根拠を与える命題を述べ証明を与える．

命題 5.1. 記号を上記のものとし，$t = 1$ とする．さらに $\#E_{j_0}^{-D,c}(\mathbb{F}_p) = p$ かつ $\tau_p(j_0) \in \mathbb{F}_p$ が平方剰余であると仮定する．このとき，

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

である．

証明. 仮定より $\sigma \in \mathbb{F}_p$ であって $\sigma^2 = \tau_p(j_0)$ なるものが存在する．このとき，$N = pq$ なので準同型写像

$$S_N^{-D,\tau(X)} \to \mathbb{F}_p$$

が X に j_0，Y に σ を代入することで得られる．この写像は $E^{-D,c}(S_N^{-D,\tau(X)}) \to E^{-D,c}(\mathbb{F}_p)$ を導く．$P \in E^{-D,c}(S_N^{-D,\tau(X)})$ のこの写像による像を $P_p \in E^{-D,c}(\mathbb{F}_p)$ と書く．

さらに仮定より $\#E_{j_0}^{-D,c}(\mathbb{F}_p) = p$ なので $NP_p = \infty \in E_{j_0}^{-D,c}(\mathbb{F}_p)$ である．従って，

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

である．よって，

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

[*8] 添え字の n はスカラー倍に対応する n のことで，本稿で用いている係数を mod n して得られる多項式の記号とは異なるので注意されたい．

であるが，j_0 は $H_{-D,p}(X)$ の $\mathbb{F}_p$ 内の根であることに注意すると，これは2つの多項式 $H_{-D,p}(X)$ と $g_{N,0}(X)^2 - g_{N,1}(X)^2\tau(X)$ が $\mathbb{F}_p$ に共通根を持つということを意味する．従って

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

となり命題の結論が得られる． □

この命題の仮定を吟味する．$\#E_{j_0}^{-D,c}(\mathbb{F}_p) = p$ となるかどうかは $c \in \mathbb{Z}/N\mathbb{Z}$ の選び方に依存しており，$\frac{1}{2}$ の確率で仮定を満たす楕円曲線が得られる．一方で，$\tau_p(j_0) \in \mathbb{F}_p$ が平方剰余かどうかは $x_0 \in \mathbb{Z}/N\mathbb{Z}$ の選び方に依存し，こちらも $\frac{1}{2}$ の確率で仮定を満たす元が得られる．このことから $c, x_0 \in \mathbb{Z}/N\mathbb{Z}$ をランダムに選んだとき $\frac{1}{4}$ の確率で命題の仮定を満たす状況が整う．

命題 5.2. 記号を上記のものとし，$p+1-t$ が C-スムースであるとし，素因数の最大の指数を e とする．$M = (C!)^e$ とおく．さらに $\#E_{j_0}^{-D,c}(\mathbb{F}_p) = p+1-t$ [*9]かつ $\tau_p(j_0) \in \mathbb{F}_p$ が平方剰余であると仮定する．このとき，

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

である．

証明. 命題 5.1 と同様. □

以上の議論をもとに，アルゴリズム 1 およびアルゴリズム 2 を提案する．

■ 提案アルゴリズム１

入力：$4p = 1 + Dv^2$ という形をした素因数 p を持つ合成数 N 判別式 $-D$ とその類多項式 $H_{-D}(X)$
出力：N の非自明な約数（p の倍数）

- 1. ランダムな $c \in \mathbb{Z}/N\mathbb{Z}$ に対し環 R_N^{-D} 上の楕円曲線を方程式 (5.1) で定義する．
- 2. ランダムな $x_0 \in \mathbb{Z}/N\mathbb{Z}$ に対し $\tau(X) \in R_N^{-D}$ を (5.2) で定める．
- 3.$S_N^{-D,\tau(X)}$ を構成し，$P = (x_0, Y) \in E(S_N^{-D,\tau(X)})$ をとる．
- 4.NP を計算する．
- 5-1. 確率 $\frac{1}{4}$ で $\gcd\big(\mathrm{Res}(H_{-D,N}(X), g_{N,0}^2(X) - g_{N,1}^2(X)\tau(X)), N\big)$ は非自明な N の約数を返す．
- 5-2. 上の gcd が 1 を返した場合は失敗．c か x_0 のどちらか，または共に別の値に取り替えて同様の計算を実行．

■ 提案アルゴリズム 2

入力：$4p = t^2 + Dv^2$ という形をした素数 p で $p+1-t$ が C-スムースとなるもの，$M = C!$，p を素因数に持つ合成数 N，判別式 $-D$ とその類多項式 $H_{-D}(X)$
出力：N の非自明な約数（p の倍数）

- 1. ランダムな $c \in \mathbb{Z}/N\mathbb{Z}$ に対し環 R_N^{-D} 上の楕円曲線を方程式 (5.1) で定義する．
- 2. ランダムな $x_0 \in \mathbb{Z}/N\mathbb{Z}$ に対し $\tau(X) \in R_N^{-D}$ を (5.2) で定める．
- 3.$S_N^{-D,\tau(X)}$ を構成し，$P = (x_0, Y) \in E(S_N^{-D,\tau(X)})$ をとる．
- 4.MP を計算する．
- 5-1. 確率 $\frac{1}{4}$ で $\gcd\big(\mathrm{Res}(H_{-D,M}(X), g_{M,0}^2(X) - g_{M,1}^2(X)\tau(X)), N\big)$ は非自明な N の約数を返す．
- 5-2. 上の gcd が 1 を返した場合は失敗．c か x_0 のどちらか，または共に別の値に取り替えて同様の計算を実行．

6 数値例

先行研究 [8] による方式では対応できなかったが，本稿の方式によって対応可能となった合成数に対する実装例をいくつか提示する．実際にどれほど多くの，また巨大な合成数に対して本方式が適用可能

[*9] $p+1+t$ がスムースで $\#E_{j_0}^{-D,c}(\mathbb{F}_p) = p+1+t$ とおきかえてもよい.

なのかの解析については今後の研究課題である.

- $-D = -23$ $(\deg H_{-D}(X) = 3)$
  $p = 570942088504121, t = 1210134$
  $4p = t^2 + D \times 9961456^2$
  $p + 1 - t = 570942087293988 \mid 2000!$
  $q = 883478470161233$
  $N = p \times q = 504415042902280115530654941193$
- $-D = -56$ $(\deg H_{-D}(X) = 4)$
  $p = 804161, t = 450$
  $4p = t^2 + D \times 232^2$
  $p + 1 - t = 803712 = 2^7 \times 3 \times 7 \times 13 \times 23$
  $N = p \times q = 488391904291$
- $-D = -131$ $(\deg H_{-D}(X) = 5)$
  $p = 6338253001150313676073094416 63$
  $4p = 1 + D \times 139116657084339^2$
  $q = 868610670601296908562434196197$
  $N = p \times q = 550547418976985666816226779885030828558826986967578267955611$

参考文献

[1] 相川勇輔, 縫田光司, 白勢政明, 楕円曲線法と CM 法を組み合わせた素因数分解アルゴリズムの改良, 暗号と情報セキュリティシンポジウム (SCIS2018), 2018

[2] A. O. L. Atkin, F. Morain, *Elliptic curves and primality proving*. Math. Comp. 61 (1993), no. 203, 29-68

[3] D. A. Cox, *Primes of the Form $x^2 + ny^2$, Second edition*. John Wiley & Sons, Inc., Hoboken, NJ, 2013.

[4] W. Diffie, M. Hellman, *New directions in cryptography*. IEEE Trans. Information Theory IT-22 (1976), no. 6, 644-654.

[5] H. W. Lenstra, Jr., *Elliptic curves and number-theoretic algorithms*. Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986), 99-120, Amer. Math. Soc., Providence, RI, 1987.

[6] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*. Ann. of Math. (2) 126 (1987), no. 3, 649-673.

[7] R. L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*. Comm. ACM 21 (1978), no.2, 120-126.

[8] 白勢政明, 特別な形の素因数を持つ合成数の楕円曲線法による素因数分解 II, 暗号と情報セキュリティシンポジウム (SCIS2017), 2017.

[9] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves, Second Edition*. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[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.