L-037

擬似的 2 次拡大環上の楕円曲線法
ECM over dummy quadratic residue rings

森下　拓也†　趙　晋輝†‡
Morishita Takuya　Jinhui Chao

1. 序論

桁数が大きな素因数分解問題は, RSA 暗号や Paillier 暗号をはじめとする多くの公開鍵暗号形式の安全性の根拠となっているため, 暗号系の安全性を分析する上で素因数分解アルゴリズムの研究は欠かすことができない.

主要な素因数分解アルゴリズムとして, 数体篩法 (以下, NFS) と楕円曲線法 (以下, ECM) の二つが存在する. NFS はその計算量が合成数の桁数に依存するのに対して, ECM の計算量は合成数の最小素因数に依存しており, まず ECM により中規模程度の素因数を求めた後, NFS により残りの素因数を導くことで効率的な素因数分解を行うことができる.

これまで, ECM の高速化や成功率の改善に関して多くの研究が行われてきた. 成功率を高めるために, 有理数体上で定義された Montgomery 曲線や Edwards Curve といった位数の大きい Torsion group を持つ楕円曲線を利用する手法が広く知られている[2]. しかしながら, 有理数体上の楕円曲線は, Mazor の定理により Torsion group は多くは存在していないため, 改善には限界があった.

一方で, 代数体上の曲線は有理数体上の曲線よりも大きい位数の Torsion group が多く存在していることが知られており, これらの曲線を利用することで更なる成功率の向上が期待される. しかし, 代数体上の曲線 Torsion group を保ったまま ECM に適用する場合, 素因数の形によっては Torsion group の位数を保った状態では利用できていなかった. そのため, 4 次数体上の曲線[1]や円分体上の曲線[7] において特定の形の素因数に有効であることが示されているが, 任意の素因数を含む素因数分解への適用は成功していない.

本研究では, 有理数体の剰余環上で定義されている ECM を, 擬似的に 2 次拡大剰余環上へ拡張し, 2 次数体上の曲線を ECM に適用することを可能とする, 任意の素因数に対して有効な素因数分解アルゴリズムを提案すると共に, 有理数体上の曲線を用いた ECM との素因数分解成功率の比較実験を行った.

2. 準備

2.1 楕円曲線

体 K 上で定義される楕円曲線 E/K とは, 以下の方程式で与えられた代数曲線のことである.

$E/K: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad a_i \in K$

楕円曲線の K-有理点群とは, この方程式を満たす点(x, y) に無限遠点∞ を加えた集合のことであり, $E(K)$ と表す. また, 楕円曲線上の加算について可換群の構造を満たしている.

† 中央大学理工学研究科情報工学専攻　Department of Information and System Engineering, Graduate School of Science and Engineering, Chuo University
‡ 中央大学理工学部　Department of Information and System Engineering, Faculty of Science and Engineering, Chuo University

2.2 Torsion group

有理点群 $E(K)$ において, 位数がある自然数 n になる集合

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty\}$$

を n-Torsion group という. $\overline{K}$ は K の代数的閉包である.

代数体 K 上で定義される楕円曲線の有理点群 $E(K)$ は有限生成な可換群となり,

$$E(K) \cong Z^r \times E_{tor}(K)$$

と表せる. ここで, $E_{tor}(K)$ は有限な n のすべてに対して $E[n]$ の K 上部分群全体であり, $E(K)$ の Torsion group という. K が有理数 または 2 次数体のとき, K 上の楕円曲線 E 上の Torsion group は有限群に分類できることが知られている.

2.2.1 Mazor の定理

有理数体 Q 上の 楕円曲線の Torsion subgroup は, 以下の有限群のいずれかに同型である.

$$\begin{cases} Z/nZ & (1 \le n \le 10, n = 12) \\ Z/2Z \times Z/2nZ & (1 \le n \le 4) \end{cases}$$

2.2.2 Kenku-Momose の定理

2 次数体 $Q(\sqrt{-d})$ 上の楕円曲線の Torsion group は, 以下の有限群のいずれかに同型である[4].

$$\begin{cases} Z/nZ & (1 \le n \le 16,\ n = 18) \\ Z/2Z \times Z/2nZ & (1 \le n \le 6) \\ Z/3Z \times Z/3nZ & (n = 1,2\ for\ d = 3) \\ Z/4Z \times Z/4Z & (for\ d = 1) \end{cases}$$

2.3 楕円曲線法(ECM)

合成数 $N = pq$ (p, q は異なる素数) を分解するとき, 剰余環 Z/NZ 上で定義した楕円曲線を用いて ECM を実行する. このとき, 有理点集合 $E(Z/NZ)$ は群構造を成していないため, 任意の点で計算を行うことができない. しかし, 点の計算に失敗したとき, その点の座標における分母は, Z/NZ 上の零因子となっており, p, q のいずれかを含んでおり, 素因数分解に成功する. したがって, ECM が成功するのは合成数に含まれる最小の素因数の大きさに依存している.

ECM は, 有理点集合 $E(Z/NZ)$ の位数が小さい素数の積となっているときに成功する. 素数の上限を B とすると, そのような $E(Z/NZ)$ を B–smooth という.

以下に, ECM のアルゴリズムを示す[3].

図 1　ECM のアルゴリズム

入力 :合成数 N　出力 : 素因数 または 失敗
1: 素数の上限を B とする.
2: L=$\prod {p_i}^{a_i}$ (p_i は B より小さいすべての素数, $a_i = \lfloor (\log B)/(\log p_i) \rfloor$).
3: $P_i = (s_i, t_i) \in \mathrm{E}(Z/NZ)$を選ぶ.
4: $Q = L * P_i$を計算する.
5: Qの計算に失敗した場合, 分母とN の Gcd を求める.
6: Gcd が 1 もしくはN でなければ, Gcd を素因数として出力する.

3. 代数体上の楕円曲線を用いた ECM

3.1 課題と現状

前章で述べた ECM の成功条件を常に満たす曲線は珍しく, またそのような曲線を構成することは困難である. しかし, 位数の大きい Torsion group を持つ曲線を構成すれば, Z/NZ 上において曲線の位数が B-smooth となる確率は向上する. また, Torsion group の位数が大きいほど素因数分解成功率は向上するため, 前章の定理から 2 次数体上の曲線は有理数体上の曲線よりも ECM の成功率の向上が期待できる.

しかし, 2 次数体上の曲線 $E/Q(\sqrt{-d})$ を ECM に適用するためには, 通常, 剰余環上の曲線 $E/(Z/NZ)$ への reduction を行う必要があった. そして, $E(Q)$ の Torsion group を保ちながら reduction を行うためには, ”拡大に用いた既約多項式の根が合成数の素因数各々に対して平方剰余でなければならない”という制約が存在する. これにより平方非剰余となる素因数を含む合成数に対しては効果がないことが既存研究で示されている[1].

3.2 提案手法

本研究では, 2 次数体上で位数の大きい Torsion group を持つ楕円曲線$E/Q(\sqrt{-d})$に対して, 剰余環上ではなく擬似的に定義した 2 次拡大環$\mathrm{Z}/N\mathrm{Z}(\sqrt{-d})$上に曲線を reduction することで, 平方非剰余となる素因数を含む合成数においても有効な ECM による素因数分解を提案する.

4. 比較実験

4.1 $N = pq$に対する比較

p, q を同じサイズでランダムな素数とし, 合成数 $N = pq$ の素因数分解を考える. 本研究では, 数式ソフト Magam を用いて以下の 3 種の楕円曲線で, ECM の成功率比較を行った.

(1) 有理数体 Q 上で$\mathrm{Z}/12\mathrm{Z}$ に同型な Torsion group を持つ曲線.
(2) 2 次数体 $Q(\sqrt{-1})$ 上で$\mathrm{Z}/4\mathrm{Z} \times \mathrm{Z}/4\mathrm{Z}$ に同型な Torsion group を持つ曲線[5].
(3) 2 次数体 $Q(\sqrt{-3})$ 上で $\mathrm{Z}/3\mathrm{Z} \times \mathrm{Z}/6\mathrm{Z}$ に同型な Torsion group を持つ曲線[6].

文献[2]を参考に, p,q が 20bit のとき, $B = 256$ とし, p,q が 30bit のとき, $B = 1024$ とした. また, 実験回数はそれぞれ 38635 回, 65536 回ずつ計算を行い, 成功率の平均を求めた. 素数に対する条件は,(i) N を法としてどちらも平方剰余 (ii) 一方が平方剰余, 他方が平方非剰余, (iii) どちらも平方非剰余 , に対して行った. それぞれの場合を (n, n), (n, s), (s, s) と表す. 表 1, 2 に実験結果を示す.

表 1　20bit での実験結果

20bit	(1)	(2)	(3)
(n, n)	48.92%	53.99%	55.21%
(n, s)	49.22%/	53.29%	54.04%
(s, s)	49.81%	52.28%	52.68%

表 2　30bit での実験結果

30bit	(1)	(2)	(3)
(n, n)	19.33%	21.77%	22.80%
(n, s)	19.44%/	21.36%	21.73%
(s, s)	19.52%	20.64%	21.07%

表 1, 2 より素因数が平方非剰余であるすべての場合で, (1) の曲線よりも成功率が向上しているから, 常に有理数体上の曲線よりも有効であることが確認できる.

4.2 素因数の条件を変えた場合の比較

楕円曲線に関する条件を変えずに,

① p, q, r をそれぞれ 20bit の素数とし, $N = pqr$ に対する素因数分解
② p, q をそれぞれ 20bit, 40bit の素数とし, $N = pq$ に対する素因数分解

を(i)すべての素因数が平方剰余, (ii)すべての素数が平方非剰余の場合に対して,それぞれ 38635 回ずつ行った. ① のそれぞれの場合を (n, n, n), (s, s, s) と表し, ②は表 1, 2 と同じにする. 表 3, 4 に結果を示す.

表 3　①の実験結果

N = pqr	(1)	(2)	(3)
(n, n, n)	41.63%	45.30%	46.10%
(s, s, s)	42.07%	44.99%	45.52%

表 4　②の実験結果

N = pq	(1)	(2)	(3)
(n, n)	28.22%	32.59%	33.93%
(s, s)	29.08%	31.23%	32.26%

表 3, 4 よりいずれの場合に対しても, 表 1, 2 と同様に(1)の曲線よりも成功率が向上していることが確認できる. このことから, 2 次数体上の曲線を用いた ECM においても, 有理数体上の曲線と同様, 成功率が合成数ではなく最小の素因数に依存することが確認できた.

5. まとめ

本研究では, 2 次数体上の楕円曲線を擬似的 2 次拡大環上の ECM へ適用することで, 合成数の素因数が平方非剰余の場合であっても成功率が向上することを示した. また, 融資数体上の曲線を用いた計算と同様に, その成功率は最小の素因数に依存することを確認した.

本手法は, 2 次数体に限らず代数体上の楕円曲線に適用可能であるが, 擬似的剰余環の計算量が増えるため拡大次数とのトレードオフが必要と思われる.

今後は, アルゴリズムの高速化, より大きい位数を持つ曲線のパラメタの調査を行っていく予定である.

参考文献

[1] 伊豆 哲也, “素因数分解に適した楕円曲線の生成法”, Proc. of SCIS, SCIC2000-B20.
[2] D. J. Bernstein, P. Birkner, T. Lange and C. Peters “ECM Using Edwards Curves”, The 12th Workshop on Elliptic Curve Cryptography (2008).
[3] Denis A. Rangel “Elliptic curves and factoring”, 2010.
[4] M. A. Kenku, F. Momose , “Torsion points on elliptic curves defined over quadratic fields”, Nagoya Math. J. 109, 1988, pp.125-149.
[5] A. Dujella, M. J. Bokun “On the rank of elliptic curves over Q(i) with torsion group Z/4Z×Z/4Z”, Proc. Japan Acad. Ser. A Math. Sci. 86, 2010 ,pp.93-96.
[6] M. J. Bokun “On the rank of elliptic curves over Q($\sqrt{-3}$) with torsion group Z/3Z×Z/3Z and Z/3Z×Z/6Z”, 2010.
[7] E. Brier, C. Clavier, “New Families of ECM Curves for Cunningham Numbers”, In Proceedings of ANTS, pp.96-109, 2010