SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

位数が $4k$ の有限体上楕円曲線の点の位数の判定法
Determining the evenness of order of points on elliptic curves on finite fields with order of $4k$

白勢 政明 *
Masaaki SHIRASE

キーワード 楕円曲線, Montgomery 曲線, 位数, 指標, Half Point

あらまし

位数が $4k$(k は奇素数) である有限体 $\mathbb{F}_p$ 上楕円曲線 E に対して，点 P の位数は 1，2，4，k，$2k$，$4k$ のどれかになる．一般に暗号では位数 k の点を用いるが，その他の位数の点の使用は脆弱性の原因になるかもしれない．$\mathcal{O}$ でない P に対して $kP = \mathcal{O}$ となるならば点 P の位数は k と確かめられるが，この計算のコストは高い．本稿では，$E(\mathbb{F}_p)$ の 2 次の指標 ($E(\mathbb{F}_p)$ から $\{1, -1\}$ への準同型写像) と half point 計算 ($P = 2Q$ となる点を計算すること) による点の位数が k かどうかを判定する効率的なアルゴリズムを提案する．

$\#E(\mathbb{F}_p) = 4k$ の時，位数 2 を持つ点を $(0, 0)$ にする座標変換により，$E/\mathbb{F}_p$ を

$$E/\mathbb{F}_p:\ y^2 = x^3 + ax^2 + bx \tag{1}$$

という形にすることができる．暗号高速実装に適している Montgomery 曲線 $By^2 = x^3 + Ax^2 + x$ も B が $\mathbb{F}_p$ 上平方元の時は (1) の形にできる．以降では，$E/\mathbb{F}_p$ は (1) で与えられるとする．

$P \in E(\mathbb{F}_p)$ の half point $Q \in E(\mathbb{F}_p)$ が存在する時，P の座標と E の係数 a, b から Q を計算することができる [1]．なお，計算過程で平方根計算が必要となる．

写像 $\phi:\ E(\mathbb{F}_p) \to \{1, -1\}$ を次のように定義する．

$$\begin{array}{ccc} \mathcal{O} & \mapsto & 1 \\ (0,0) & \mapsto & b^{(p-1)/2} \\ (x_1, y_1) & \mapsto & x_1^{(p-1)/2} \quad (x_1 \neq 0) \end{array}$$

すると，ϕ は準同型となる [2]．($P, Q \in E(\mathbb{F}_p)$ に対して $\phi(P + Q) = \phi(P) \cdot \phi(Q)$ が成り立つ．)

* 公立はこだて未来大学, 北海道函館市亀田中野町 116-2, Future Universuty Hakodate, 116-2 Kamedanakano, Hakodate, Hokkaido (shirase@fun.ac.jp)

$\#E(\mathbb{F}_p) = 4k$ (k は奇素数) の時，Sylow の定理より，

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} \tag{2}$$

または

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} \tag{3}$$

となる．(2) の場合，点 $P \in E(\mathbb{F}_p)$ の位数が k であるかどうかの判定法は [2] で与えられている．(3) の場合，

アルゴリズム 1 の出力が $1 \Leftrightarrow P$ の位数は k

となることを，$E(\mathbb{F}_p)$ が (3) という構造を持つこと，half point の性質，ϕ の準同型性，を使って示す．

アルゴリズム 1 (点の位数判定)

入力 $(\mathcal{O} \neq) P \in E(\mathbb{F}_p)$
出力 0 か 1

1. P の位数が 2 か 4 ならば，0 を返す
2. $\phi(P) = -1$ ならば，0 を返す
3. P の half point $Q \in E(\mathbb{F}_p)$ を 1 つ計算する
4. $\phi(Q) = -1$ ならば，0 を返す
5. 1 を返す

参考文献

[1] J. Miret, R. Moreno, A. Rio, and M. Valls, “Determining the 2-Sylow subgroup of an elliptic curve over a finite field,” Math. Comp. 74 (2005), 411-427

[2] 白勢政明,“偶数位数を持つ有限体上楕円曲線の 2 次の指標,” 応用数理学会 2019 年度年会

[3] 白勢政明,“有限体上の楕円曲線の指標と点の位数の偶奇性,” ISEC2019-66