素数位数を有する楕円曲線の構成とその計算量評価

堀内　啓次[†]　布田　裕一[††]　境　隆一[†††]　金子　昌信[††††]
笠原　正雄[†]

Construction of Elliptic Curves with Prime Order and Estimation of Its Comprexity

Keiji HORIUCHI[†], Yuichi FUTA[††], Ryuichi SAKAI[†††], Masanobu KANEKO[††††], and Masao KASAHARA[†]

あらまし　楕円暗号において，楕円曲線の群の位数は重要なパラメータである．特に，その位数が素数であることが望ましい．楕円曲線の位数を計算する方法としてSchoofのアルゴリズム及びそれを改良したElkies, Atkinのアルゴリズムが知られている．本論文ではSchoofの改良アルゴリズムを用いた素数位数を有する楕円曲線の効率的な構成法を示す．更に，楕円曲線の位数分布及び位数が素数である確率を導出した後，素数位数を有する楕円曲線の構成に必要な計算量を評価する．また，法 p の条件による計算時間の違いについて考察する．

キーワード　楕円曲線，素数位数，計算量

1. まえがき

近年における情報化社会の急速な発展により，情報通信システムを介した情報交換の重要性がますます高まっている．これに伴い，情報内容や個人情報の保護を目的とした情報セキュリティ技術の研究が活発になわれている．こうした流れの中，昨今，特に注目されている方式として楕円曲線を利用した暗号方式（楕円暗号）を挙げることができる．楕円曲線を利用することによる有利な点はその離散対数問題を解く準指数時間のアルゴリズムが存在しないことである．

楕円暗号に対する攻撃法として，Baby-Step Giant-Step を用いた攻撃 M.O.V Reduction を用いた攻撃 [1]，及び，anomalous な楕円曲線に対する攻撃 [2] が挙げられる．素体 $\mathbb{F}_p$ 上の楕円曲線の $\mathbb{F}_p$ 有理点を考える場合，これらの攻撃に対して安全であるための条件は，$\#\mathrm{E}(F_p)$ が $p, p+1$ でないこと，及び，その最大素因数が十分大きいことである．一方，楕円暗号の効率を上げるためには，法 p のサイズを小さくすることが効果的である．したがって，一定の安全性を保ちつつ暗号化及び復号の計算効率を上げるためには素数位数の楕円曲線がより好ましい．素対 $\mathbb{F}_p$ 上の楕円曲線の位数を求める方法として，Schoofのアルゴリズム [3] が知られており，Elkies, Atkinらはこのアルゴリズムを改良している [4]～[6]．このアルゴリズムはSEAのアルゴリズムと呼ばれており，実用的な時間での位数計算が可能である．最近，伊豆，小暮らはSEAアルゴリズムで用いるパラメータを適切に設定することにより，高速な位数計算を実装している [7]．

本論文では，**2.** でSEAのアルゴリズムに基づいて，素数位数を有する素体 $\mathbb{F}_p$ 上の楕円曲線を効率的に構成する手法を考察する．**2.2** ではアルゴリズムの分岐点での分岐確率を導出し，その証明を与える．また，**3.** で楕円曲線の位数分布を明らかにし，位数が素数である確率を導出する．更に，**4.** で素数位数を有する楕円曲線の構成に必要な計算量を求め考察する．また，法 p の条件による計算時間の変化を **2.** 及び **3.** での解析結果に基づいて調べる．

[†] 京都工芸繊維大学工芸学部電子情報工学科，京都市
Department of Electronics and Information Science, Kyoto Institute of Technology, Matsugasaki, Sakyo-ku, Kyoto-shi, 606–8585 Japan
[††] 松下電器産業株式会社マルチメディア開発センター，門真市
Multimedia Development Center, Matsushita Electric Industrial Co., Ltd., 1006 Kadoma, Kadoma-shi, 571–8501 Japan
[†††] 大阪電気通信大学工学部，寝屋川市
Department of Applied Electronics, Osaka Electro Communication University, Neyagawa-shi, 572–8530 Japan
[††††] 九州大学大学院数理学研究科，福岡市
Graduate School of Mathematics, Kyushu University, 6–10–1 Hakozaki, Higashi-ku, Fukuoka-shi, 812–8581 Japan

2. 素数位数をもつ楕円曲線の構成法

本章では，楕円曲線の位数計算法である Schoof のアルゴリズム，及びその改良アルゴリズムである SEA アルゴリズムについて，必要最小限の概要を **2.1** で紹介する．また，**2.2** で SEA アルゴリズムの分岐点での分岐確率を導出し証明を与える．更に，**2.3** で素数位数を有する楕円曲線の効率的な構成法を示す．Schoof のアルゴリズム及び SEA アルゴリズムの詳細に関しては付録を参照されたい．なお，以下において，素数位数を有する楕円曲線を EPO（elliptic curve with prime order）と略記する．

2.1 Schoof 及び SEA 改良アルゴリズム

Schoof のアルゴリズムは，固有方程式 $\phi_p^2 - t\phi_p + n = 0$ のトレース t を楕円曲線の l 等分多項式を用いて，$t \pmod l$ を求めることにより t ($|t| \leqq 2\sqrt{p}$) を求め，楕円曲線の位数 $\#E(\mathbb{F}_p) = p + 1 - t$ を求めるアルゴリズムである．ただし，$t \bmod l$ の算出は素数 $l = 2, 3, 5, 7, \cdots$ の順に行う．

SEA アルゴリズムは，$t \pmod l$ を求める部分に，

（1） $\left(\frac{t^2-4p}{l}\right) = 1$ のとき Elkies のアルゴリズム

（2） $\left(\frac{t^2-4p}{l}\right) = -1$ のとき Atkin のアルゴリズム

を適用する．また，$t \pmod l$ が確定した時点で Isogeny Cycle 法 [8] を適用し，$t \pmod{l^2, l^3, \cdots}$ を求める．以下 $(\frac{t^2-4p}{l})$ が $1, 0, -1$ の場合をそれぞれ Case-Elkies, Case-Schoof, Case-Atkin と呼ぶことにする．なお，Case-Atkin の手法は $t \pmod l$ の候補を求めるものであり，$t \pmod l$ は確定しない．

2.2 SEA アルゴリズムにおける分岐確率の導出

ここで，SEA アルゴリズムにおいて Case-Elkies, Case-Schoof へ分岐し，$t \pmod l$ が確定する確率を求めておく．各 l において Case-Elkies, 及び Case-Schoof への分岐確率を $P_{El}(l)$ と表記する．トレース t 及び素数 p をランダムに与えたとき，次の定理が成立する．

[定理 1] SEA アルゴリズムにおいて，$l = 2$ の場合，すべての素数 p に対して $P_{El}(l) = 1$ となる．l が奇素数 の場合，ランダムに与えた t 及び素数 p に対して，$P_{El}(l) = 1/2$ である． □

（証明）

i) $l = 2$ のとき

$\left(\frac{t^2-4p}{l}\right) = \left(\frac{t^2}{l}\right) = 1$ または 0（$t = 0$ のとき）

より，確率は 1 である．

ii) l が奇素数のとき

t を固定，$p = 0, 1, \cdots, l-1 \pmod l$ とすると $t^2 - 4p$ は $0, 1, \cdots, l-1 \pmod l$ のすべての値をとり得る．$\left(\frac{t^2-4p}{l}\right) = 1$ または 0 となる組合せの数は $(l+1)/2$ である．$p \not\equiv 0 \pmod l$ であるので，それを除くと $(l-1)/2$ である．したがって，p を $1, 2, \cdots, l-1 \pmod l$ の中でランダムに選ぶとき，$\left(\frac{t^2-4p}{l}\right) = 1$ または 0 となる確率は，$\frac{\frac{l-1}{2}}{l-1} = \frac{1}{2}$ である．これは任意の t に対して成り立つ． □

t をランダムに与え，p を固定した場合の確率は p の条件により変わる．このとき，次の定理が成立する．

[定理 2] $\left(\frac{p}{l}\right) = 1$ のとき，ランダムに与えた t に対して，$P_{El}(l) = \dfrac{l+1}{2l}$ となる．

$\left(\frac{p}{l}\right) = -1$ のとき，ランダムに与えた t に対して，$P_{El}(l) = \dfrac{l-1}{2l}$ となる． □

（証明）

分岐確率 $P_{El}(l)$ を求めるためには，$\left(\frac{p}{l}\right) = 1$ となる素数 p, l に対し，

$$\#\left\{t \in \mathbb{F}_l \;\middle|\; \left(\frac{t^2-4p}{l}\right) = 1 \text{ or } 0\right\} \tag{1}$$

を評価すればよい．

$\left(\frac{p}{l}\right) = 1$ であるから，$4p = s^2 \pmod l$ を満たす $s \in \mathbb{F}_l^*$ が存在する．任意の $s_1, s_2 \in \mathbb{F}_l (s_1 \neq s_2)$ に対し，$r \in \mathbb{F}_l$ を $rs_1 \equiv s_2 \pmod l$ とすると，

$$\left(\frac{t^2-s_1^2}{l}\right) = \left(\frac{t^2-s_1^2}{l}\right)\left(\frac{r^2}{l}\right) = \left(\frac{(tr)^2-s_2^2}{l}\right) \tag{2}$$

と変形される．ゆえに，$s_1, s_2 \in \mathbb{F}_l (s_1 \neq s_2)$ に対し，

$$\#\left\{t \in \mathbb{F}_l \;\middle|\; \left(\frac{t^2-s_1^2}{l}\right) = 1\right\} = \#\left\{t \in \mathbb{F}_l \;\middle|\; \left(\frac{t^2-s_2^2}{l}\right) = 1\right\}$$

が成り立つ．一方 $u = t + s, v = t - s$ とおくと，

$$\begin{aligned}\#\left\{t \in \mathbb{F}_l,\, s \in \mathbb{F}_l^* \;\middle|\; \left(\frac{t^2-s^2}{l}\right)\right\} &= \#\left\{u, v \in \mathbb{F}_l \;\middle|\; \left(\frac{u}{l}\right)\left(\frac{v}{l}\right) = 1\right\} - (l-1) \\ &= \frac{(l-1)^2}{2} - (l-1)\end{aligned} \tag{3}$$

したがって，任意の $s \in \mathbb{F}_l^*$ に対して，

$$\#\left\{t \in \mathbb{F}_l \,\middle|\, \left(\frac{t^2-s^2}{l}\right)=1\right\} = \frac{l-1}{2}-1=\frac{l-3}{2} \tag{4}$$

となり，これより，$\left(\frac{p}{l}\right)=1$ となる素数 l,p に対し，

$$\#\left\{t \in \mathbb{F}_l \,\middle|\, \left(\frac{t^2-s^2}{l}\right)=1 \text{ or } 0\right\} = \frac{l-3}{2}+2=\frac{l+1}{2} \tag{5}$$

が成り立つ．したがって $P_{El}(l)=\frac{l+1}{2l}$ となる．同様に $\left(\frac{p}{l}\right)=-1$ のとき，$P_{El}(l)=\frac{l-1}{2l}$ となる． □

2.3 EPO の構成法

本節では，SEA アルゴリズムを用いた EPO の効率的な構成法を示す．EPO の構成法の概要は次のとおりである．まず，ランダムに選んだ楕円曲線に対して，SEA アルゴリズムを適用する．ここで，SEA アルゴリズムの各 l において Case-Elkies または Case-Schoof へ分岐し，$t \pmod l$ が確定した場合，この時点で，位数が l を因数にもつか否かの判定が可能である．位数が l を因数にもつと判定されれば，即座に楕円曲線を選び直し．これを EPO が得られるまで繰り返す(注1)．なお，twist された楕円曲線も同時に判定を行う．以下にアルゴリズムの詳細を示す．

[アルゴリズム 3]（EPO の構成アルゴリズム）
入力：素体 $\mathbb{F}_p$
出力：楕円曲線 $E/\mathbb{F}_p : \#E(\mathbb{F}_p)=$ 素数
[Step 1] 適当な素数 p を選ぶ．
[Step 2] 楕円曲線 $E(\mathbb{F}_p)$ をランダムに選ぶ．
[Step 3] E の位数 $\#E$ を SEA アルゴリズムによって求めるが $t \pmod l$ が求まるたびに $l \mid \#E$ を判定する．この際，twist された楕円曲線 E' に対しても同様の判定を行う．
[Step 4] $\#E, \#E'$ の両者が Step 3 で合成数と判定されれば Step 2 へ戻る．
[Step 5] $\#E$ または $\#E'$ が素数 $(\neq p)$ であれば終了．そうでなければ Step 2 へ戻る．

3. 楕円曲線の位数分布及び EPO の存在確率

楕円曲線を構成する上で，楕円曲線の位数が Hasse の範囲内でどのように分布しているかは，基本的かつ重要な問題である．本章では，楕円曲線の位数分布を導出し，更に，位数が素数である曲線 EPO の存在確率を見積もる．なお，個数を表すときは互いに同型な楕円曲線を同一視する．

3.1 楕円曲線の位数分布

本節では，楕円曲線の位数分布を導出する．

判別式 $D=\sqrt{4p-t^2}$ である位数 $x=p+1-t$ を有する楕円曲線の個数は，Kronecker の類数 $H(D)$ に一致する．また，$H(D)$ 及び楕円曲線の総数は，次式のように表せる [11]．

$$H(D)=\sum_{i=1,i^2|D}^{\sqrt{-D}} h\left(\frac{D}{i^2}\right) \tag{6}$$

$$\text{総数}=\sum_{t=-2\sqrt{q}}^{2\sqrt{q}}\left\{\sum_{i=1,i^2|(t^2-4q)} h\left(\frac{t^2-4q}{i^2}\right)\right\} \tag{7}$$

更に，虚 2 次体の類数 $h(D)$ はあたかも，

$$\sum_{-D<d<0} h(d) \sim \frac{\pi}{18\zeta(3)} D^{3/2} \tag{8}$$

$$h(D) \sim C|D|^{\frac{1}{2}} \tag{9}$$

のように振る舞うことが知られている [10]．ここで，位数分布の平均値を求める．式 (6) と式 (9) より $H(D) \sim C'D^{\frac{1}{2}}$ とし，Hasse の範囲で積分した値が楕円曲線の総数 $2(p-1) \simeq 2p$ であることから $H(D)$ の平均値は，$\frac{1}{\pi}D^{\frac{1}{2}}$ となる [11]．したがって，楕円曲線の位数が x となる確率密度関数は，$\frac{\sqrt{4p-(p+1-x)^2}}{2\pi p}$ となり，ここで，

$$\cos\theta=\frac{p+1-x}{2\sqrt{p}} \tag{10}$$

なる変数変換を行うと，確率密度関数は，

$$\frac{2}{\pi}\sin^2\theta \tag{11}$$

となり，佐藤予想との類似関係が得られる [12]．

素体 $\mathbb{F}_p$ 上での楕円曲線の位数分布と，その平均値を図 1 に示す．これによると位数は Hasse の範囲でほぼ一様に分布していることが確かめられる．この結果より，EPO も偏りなく存在していることが予想できるが，次節で EPO の存在確率を導出する．

(注1)：Lercier によっても独立に提案されている [15]．しかし，筆者らの手法は，更に，計算時間を短縮するために Case-Atikin, Isogeny Cycle の計算は可能な限り後回しにするという手法である．

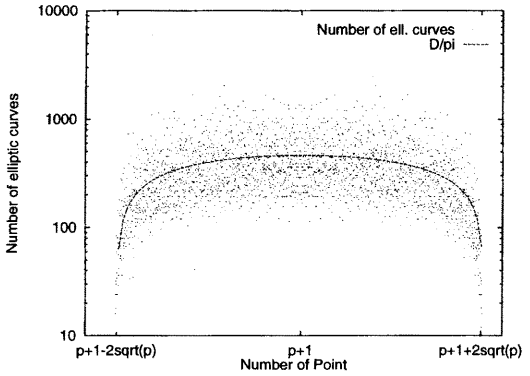


図1 素体 $\mathbb{F}_p$ $(p = 524287)$ での楕円曲線の位数分布
Fig. 1 Distribution of order of ell. cur. over $\mathbb{F}_p$.

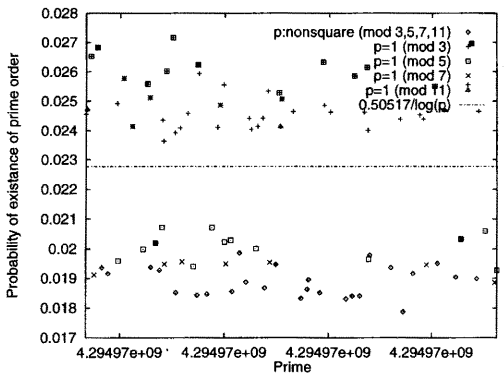


図2 EPO の存在確率
Fig. 2 Probability of existance of ell. cur. with prime order.

表1 $p \equiv 1 \pmod{l}$ である場合の素数位数となる確率 P_p との比
Table 1 Ratio of probability of existance of ell. cur. with prime order and its avarage probability P_p.

	$p \equiv 1 \pmod{l}$	$p \not\equiv 1 \pmod{l}$
$l = 3$	1.111	0.889
5	1.041	0.986
7	1.021	0.996
11	1.008	0.999

3.2 EPO の存在確率

本節では，EPO の存在確率を導出する．素体 $\mathbb{F}_p$ 上定義された楕円曲線 $E(\mathbb{F}_p$ の位数 $\#E(\mathbb{F}_p)$ が素数 l で割り切れる確率を $P(l)$, 割り切れない確率を $P_{av}(l)$ とする．文献 [13] によると，

$$P(l) = \begin{cases} \frac{1}{l-1} + O(\frac{l}{\sqrt{p}}) & p \not\equiv 1 \pmod{l} \\ \frac{l}{l^2-1} + O(\frac{l}{\sqrt{p}}) & p \equiv 1 \pmod{l} \end{cases} \tag{12}$$

である．ここで，誤差項 $O(\frac{l}{\sqrt{p}})$ は十分小さい値である．式 (12) より，

$$P_{av}(l) \simeq \frac{l-2}{l-1} + \frac{1}{(l-1)^2(l+1)} \tag{13}$$

となる．楕円曲線の位数が素数となる平均確率を P_p, 任意に与えた正整数が素数となる確率を P_{prime} とし，これらの比をとる．

$$\lim_{p\to\infty} \frac{P_p}{P_{prime}} \simeq \frac{\prod_{2\leq l\leq p} P_{av}(l)}{\prod_{2\leq l\leq p}(1-\frac{1}{l})} \tag{14}$$

なお，この値は $l \leq 10^{12}$ において計算すると 0.50516.. に収束するように振る舞う．したがって，P_p は $P_p \simeq 0.50517/\log p$ と近似する．図 2 に，10 進数 9 けた（32 ビット）の素数標数の素体上において，EPO の存在確率を示す．図 2 より明らかに P_p に対し，EPO の存在確率は上下にばらつきがある．これは，表 1 のように $p \pmod{l}$ の値によって EPO の存在確率が変化することによるものと考えられる．したがって，EPO を構成する場合，特に小さな素数 l に対し $p \equiv 1 \pmod{l}$ を満たす素数を法とする素体を選べば効率が良いことがわかる．

4. 計算量評価

2.3 で示した EPO の構成法の計算量評価を行う．また，法 p の種類により SEA アルゴリズムでの Case-Elkies, Case-Schoof への分岐確率及び EPO の存在確率が異なることを示したが，その計算時間の違いについて考察する．

4.1 SEA のアルゴリズムの計算量

本論文では多項式乗算に Karatsuba 法を用いる．このことを考慮すると，最高次数 l の多項式乗算に要する計算時間は $O(l^{2.6}(\log p)^{1.6})$ である．SEA アルゴリズムで用いる最大の l を L とする．法 p が 160 bit の場合，L は 53 となることを SEA アルゴリズムの平均値より確かめており，これを $\log p$ で表すと $L = 0.48 \log p$ と表すことができる．したがって，本論文では，$L = 0.48 \log p$ と仮定した．

4.2 EPO の構成に要する計算量

本節では，EPO の構成に要する計算量を求める．EPO の構成に必要な計算量を求めるにあたって，考慮すべき点は以下のとおりである．

（1） 各 l に対して $t \pmod l$ を求める計算量.

（2） 位数が素数 l で割り切れる確率 $P_{av}(l)$, 及び EPO の存在確率 P_p.

（3） $t \pmod l$ の確定する確率 $P_{El}(l)$.

（4） Schoof のオリジナルアルゴリズムを適用する最大の素数 L_{Sch}.

（5） SEA アルゴリズムで用いる最大の素数 L.

まず,（1）に関して **4.1** より係数 K を用い，計算時間を $K(l^{2.6}(\log p)^{1.6})$ とする.（3）については，法 p はランダムに与えるものとし確率を 1/2 とする.（5）については，$L_{Sch}=5$ とし，以上より，EPO を構成する計算量は，

$$\frac{1}{2P_p}\sum_{2\leqq l<L}\left\{\frac{1-P_{av}(l)}{2}\left(\prod_{2\leqq s\leqq l}\frac{1+P_{av}(s)}{2}\right)\times K(\log p)^{1.6}\sum_{2\leqq k\leqq l}k^{2.6}\right\}+\frac{1}{2P_p}\left(\prod_{2\leqq l\leqq L}\frac{1+P_{av}(l)}{2}\right)K(\log p)^{1.6}\sum_{2\leqq k\leqq L}k^{2.6} \tag{15}$$

で与えられる．ただし，$\sum,\prod$ は素数の範囲を動く．これを SEA アルゴリズムの計算量

$$K(\log p)^{1.6}\sum_{2\leqq k\leqq L}k^{2.6} \tag{16}$$

で割ると SEA アルゴリズムに換算した回数が導出できる．すなわち，EPO を構成する計算量は SEA アルゴリズムをこの回数分計算した計算時間と等しい．以降，この回数を SEA 相当回数と呼ぶ．この値は，式 (15), (16) より，

$$\frac{1}{2P_p}\left(\sum_{2\leqq k\leqq L}k^{2.6}\right)^{-1}\sum_{2\leqq l<L}\left\{\frac{1-P_{av}(l)}{2}\times\left(\prod_{2\leqq s\leqq l}\frac{1+P_{av}(s)}{2}\right)\sum_{2\leqq k\leqq l}k^{2.6}\right\}+\frac{1}{2P_p}\prod_{2\leqq l\leqq L}\frac{1+P_{av}(l)}{2} \tag{17}$$

で与えられる．法 p が 10 進数 16 けた（50 ビット）から 28 けた（85 ビット）の範囲で計算結果と式 (17) とを比較して図 3 に示す．高位ビットに関する比較は表 2 に示す．なお，各法 p に対してアルゴリズム 100 回の平均値をとっている．多少のばらつきはあるが，式 (17) と実測値はほぼ一致しているといえる．

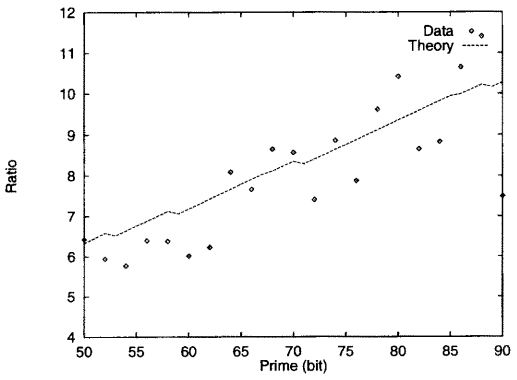


図 3 EPO の構成時間の SEA 相当回数
Fig. 3 Ratio of computational times for finding ell. cur. with prime order and SEA algorithm.

表 2 大きなビットサイズの標数 p での EPO 構成時間の SEA 相当回数
Table 2 Ratio of computational times for finding ell. cur. with high prime order and SEA algorithm.

法 p	SEA 相当回数（実測値）	SEA 相当回数（理論値）
160 bit	15.87 回	17.03 回
170 bit	16.94 回	17.93 回

図 3 より，SEA 相当回数は法 p のビットサイズに対し，ほぼ比例の関係があり，法 p のサイズが 92 ビットならば SEA 相当回数は 10.4 回，160 bit であれば SEA 相当回数は 17.0 回と十分実用的な値となっている．

4.3 EPO の構成に適した標数 p

以下の二つの確率

（1） EPO の存在確率

（2） Case-Elkies, Schoof への分岐確率

は，法 p の条件によって変化する．本節では，これらの確率が EPO の構成アルゴリズムにどのような影響を与えるのかを調べる．**2.2** で示したように，法 p が $p\equiv 1 \pmod l$ の条件を満たすとき，（1）の確率が高くなる．**3.2** で示したように，$\left(\frac{p}{l}\right)=1$ の条件を満たすとき，（2）の確率が高くなる(注2)．ランダムに楕円

(注2)：法 p に条件を与えることにより，楕円暗号の安全性に差を生ずるという研究報告は，筆者らの知る限りではなされていない．この問題の解明は今後に残された課題の一つである．

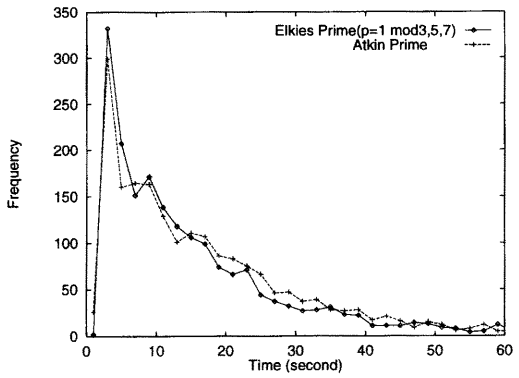


図4 EPOの構成に要する時間の分布
Fig. 4 Distribution of computation time for finding ell. cur. with prime order.

曲線を選ぶ際，EPOでなければ，楕円曲線を選び直す必要がある．しかしCase-Atkinでは，位数が素数であるか否かの判定が行えないためCase-Elkies, Schoofへ多く分岐させた方が効率が良い．また，Case-Elkiesへ分岐した場合のみIsogeny Cycleが使用できるため，これによる効率の向上も可能である．

図4に法 $p = 2^{60} + 7035 \equiv 1 \pmod{3,5,7}$ 及び $p = 2^{60} + 7081 \not\equiv 1 \pmod{3,5,7}$ としたときの素数位数を有する楕円曲線の構成アルゴリズムを2000回実行した場合の計算時間の分布を示す．図4より，法 p のタイプでの計算時間の分布の差が確認できる．また，平均時間はそれぞれ15.57(s), 18.91(s)であり，法 p を変えるだけで約20 %の計算時間の短縮が可能である．

5. むすび

本論文で提案したEPOの効率的な構成法に関し，楕円曲線の位数分布，EPOの存在確率を導出し，EPO構成に必要な計算量の評価を行った．その結果，計算量的に十分実用的であることがわかった．また，法 p の条件を選択することにより，計算時間が20%程度短縮された．

文献

[1] A.J. Menezes, T. Okamoto, and S.A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," IEEE Trans. Info. Theory, vol.39, pp.1639–1646, 1993.

[2] T. Satoh and K. Araki, "Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves," Public Release Ver.2 (97-10-21), 1997.

[3] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p," Mathematics of Computation vol.44, no.170, pp.483–494, 1985.

[4] R. Schoof, "Counting points on elliptic curve over finite fields," Journal de Théorie des Nombres de Bordeux 7, pp.219–254, 1995.

[5] N.D. Elkies, "Elliptic and modular curves over finite fields and related computational issues," Amer. Math. Soc./IP Stud, Adv. Math., 7, 21-76, Providence RI: Amer. Math. Soc., 1998.

[6] F. Morain, "Calcul du nombre de points sur une courbe elliptique dans un corps fini: Aspects algorithmiques," Journal de Théorie des Nombres de Bordeux 7, pp.255–282, 1995.

[7] 伊豆哲也，小暮 淳，野呂正行，横山和弘，"安全な楕円曲線暗号パラメーター設計（Schoofアルゴリズム改良），" SCIS'98, 1998.

[8] J.-M. Couveignes and F. Morain, "Schoof's algorithm and isogeny cycles," Lecture Notes in Compute Science 877, pp.43–58, Springer-Verlag, 1994.

[9] J.-M. Couveignes, L. Dewaghe, and F. Morain, "Isogeny cycles and the Schoof-Elkies-Atkin algorithm," LIX Research Report LIX/RR/96/03, 1996.

[10] D.B. Zagier, 片山孝次訳，数論入門，岩波書店，1990.

[11] 境 隆一，笠原正雄，"楕円曲線の位数分布と素数位数を有する楕円曲線について，" SITA96, 1996.

[12] 三井孝美編，"佐藤の予想，" 岩波数学辞典（第3版），205S, p.550.

[13] H.W. Lenstra, Jr., "Factoring Integers with Elliptic Curves," Annals of Mathematics 126, pp.649–673, 1987.

[14] R. Lercier and F. Morain, "Counting the number of points on elliptic curve over finite fields: Strategies and performances," EUROCRYPT' 95, pp.79–94, 1995.

[15] R. Lercier, "Algorithmique des courbes elliptiques dans les corps finis," Thése, École Polytechnique-LIX, 1997.

[16] J.-M. Couveignes, L. Dewaghe, and F. Morain, "Isogeny cycles and the Schoof-Elkies-Atkin algorithm," LIX Research Report LIX/RR/96/03, 1996.

[17] 布田裕一，境 隆一，笠原正雄，"Schoofのアルゴリズムに関する 基礎的考察，" 第19回情報理論とその応用シンポジウム，pp.649–652, 1996.

[18] 堀内啓次，布田裕一，境 隆一，笠原正雄，"素数位数を有する楕円曲線の構成とその計算量評価について，" 第二回代数曲線とその応用シンポジウム，1998

付録

1. SEAアルゴリズム

Elkies, Atkinによって改良されたSchoofのアルゴリズムを示す．文献[6], [14]にこのアルゴリズムを

Schoof, Elkies, Atkin の頭文字をとって，SEA アルゴリズムとある．ここでもそれにならってそのように記述する．

1.1 準　　備

必要となる定義，定理をまとめる．本論文では以下の式で定義される楕円曲線を用いる．

$$E : Y^2 = X^3 + AX + B \quad (A, B \in \mathbb{F}_p) \quad \text{(A·1)}$$

［定義 3］（フロベニウス自己準同型写像 ϕ_p）

フロベニウス自己準同型写像 ϕ_p を以下のように定義する．

$$\phi_p : (X, Y) \mapsto (X^p, Y^p) \quad \text{(A·2)}$$

□

このフロベニウス自己準同型写像は，以下の固有方程式と呼ばれる方程式を満たす．

$$\phi_p^2 - \mathrm{tr}(\phi_p) \cdot \phi_p + n(\phi_p) = 0 \quad (\mathrm{tr}(\phi_p) \in \mathbb{Z}) \quad \text{(A·3)}$$

ここで，$\mathrm{tr}(\phi_p), n(\phi_p)$ はそれぞれ，ϕ_p のトレース及び，ノルムであり，$n(\phi_p) = p$ である．簡単のため，以降 $\mathrm{tr}(\phi_p)$ を t で表すことにする．

［定理 4］（Hasse-Weil の定理）

E を素体 $\mathbb{F}_p$ 上定義された楕円曲線とする．このとき，E 上の $\mathbb{F}_p$ に座標成分を有する点の個数 $\#E(\mathbb{F}_p)$ は

$$\#E(\mathbb{F}_p) = p + 1 - t \quad \text{(A·4)}$$

$$-2\sqrt{p} \leqq t \leqq 2\sqrt{p} \quad \text{(A·5)}$$

を満たす．□

［定義 5］（j-不変量）

式 (A·1) の楕円曲線に対して，j-不変量を以下の式で定義する．

$$j = 1728\frac{4a^3}{4a^3 + 27b^2} \quad \text{(A·6)}$$

楕円曲線 E の j-不変量を $j(E)$ で表す．□

j-不変量に対応する楕円曲線は以下のようになる．

$$E/\mathbb{F}_p : y^2 = x^3 + 3\frac{j}{1728 - j}x + 2\frac{j}{1728 - j} \quad \text{(A·7)}$$

ただし，$p > 3$ とする．

［定義 6］（twist された楕円曲線）

式 (A·1) のような楕円曲線 $E/\mathbb{F}_p$ に対して以下の方程式で定義される 楕円曲線 E' を twist された楕円曲線と呼ぶ．

$$E' : y^2 = x^3 + ac^2x + bc^3 \quad \text{(A·8)}$$

ただし，$\left(\frac{c}{p}\right) = -1$ である．□

［定理 7］ twist された楕円曲線の $\mathbb{F}_p$-有理点の個数は，

$$\#E'(\mathbb{F}_p) = p + 1 + t \quad \text{(A·9)}$$

である．□

上の定理より，1 回の Schoof のアルゴリズムを行うことで二つの楕円曲線の位数を求めることができる．等分多項式は以下の漸化式により定義される．

［定義 8］（ 等分多項式 ）

$$\begin{cases} \Psi_{2n}(X, Y) = \Psi_n\left(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2\right) \\ \qquad\qquad /2Y \\ \Psi_{2n+1}(X, Y) = \Psi_{n+2}\Psi_n^3 - \Psi_{n+1}^3\Psi_{n-1} \end{cases} \quad \text{(A·10)}$$

$$\Psi_{-1}(X, Y) = -1, \quad \Psi_0(X, Y) = 0$$

$$\Psi_1(X, Y) = 1, \quad \Psi_2(X, Y) = 2Y$$

$$\Psi_3(X, Y) = 3X^4 + 6AX^2 + 12BX - A^2$$

$$\Psi_4(X, Y) = 4Y\left(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3\right)$$

□

また，等分多項式を

$$\begin{aligned} f_n(X) &= \Psi_n(X, Y) \quad (n : \text{odd}) \\ f_n(X) &= \Psi_n(X, Y)/Y \quad (n : \text{even}) \end{aligned} \quad \text{(A·11)}$$

と記述することにより，以下の定理が成立する．

［定理 9］ $P = (X, Y) \in E\left(\overline{\mathbb{F}_p}\right)$ で $P \notin E[2]$ の点に対し

$$nP = O \Longleftrightarrow f_n(X) = 0 \quad \text{(A·12)}$$

ここで $\overline{\mathbb{F}_p}$ は $\mathbb{F}_p$ の代数閉包，$E[n]$ は位数が n あるいはその約数である点全体の集合を表し，この集合の任意の要素の n 倍点は無限遠点となる．□

［定理 10］ 点 $P = (X, Y) \in E\left(\overline{\mathbb{F}_p}\right)$ を n 倍した点

$nP(nP \neq O)$ は Ψ_n を用いて，

$$nP=\left(X-\frac{\Psi_{n+1}\Psi_{n-1}}{\Psi_n^2}, \frac{\Psi_{n+2}\Psi_{n-1}^2-\Psi_{n-2}\Psi_{n+1}^2}{4Y\Psi_n^3}\right) \quad (A\cdot 13)$$

と表される． □

1.2 アルゴリズムの主要部

[アルゴリズム 1]（SEA アルゴリズム）
入力：楕円曲線 $E/\mathbb{F}_p : Y^2 = X^3 + AX + B$
出力：$\#E(\mathbb{F}_p)$
[Step 1] $l \leftarrow 2, L \leftarrow 1$ とする．
[Step 2] $\Phi_l(X, j(E)) = \Phi(X) = 0$ の $\mathbb{F}_p$ 上の解を求める．その解の個数が 2, 1 のとき，Case-Elkies として，$L \leftarrow L \times l$ とし，STEP 3 へ．0 のとき，Case-Atkin として，STEP 4 へ．
[Step 3] Elkies のアルゴリズム を行う．(Case-Elkies)
[Step 4] $l \leqq L_{Sch}$ のときは，Schoof のオリジナルアルゴリズムを行う．それ以外は，Atkin のアルゴリズムを行う．(Case-Atkin)
[Step 5] $L > 4\sqrt{p}$ であれば STEP 7 へ．
[Step 6] $l \leftarrow (l$ の次の素数$)$ とし，STEP 2 へ．
[Step 7] 素数 l に対するトレース $t \pmod l$ のすべてのデータから，match and sort アルゴリズムを行い，位数 $\#E(\mathbb{F}_p)$ を求める．終了．

□

1.3 モジュラー多項式

SEA アルゴリズムでは，モジュラー多項式 $\Phi_l(F, J)$ を用いる．これは SEA アルゴリズムとは独立にあらかじめ求めることができる．一般にはモジュラー多項式は二つの j-不変量の関係式を表すが，ここでは，Atkin によって定義されたもの [6] を表す．こちらのほうが係数が小さくなる．詳しい特性，求める方法などについては文献 [6] の 2 節を参照されたい．本論文では $X_0(l)$ 上と $X_0^*(l)$ 上 の モジュラー多項式もともに $\Phi_l(F, J)$ で表す．

1.4 Atkin のアルゴリズム

ここでは Atkin のアルゴリズム [14] について述べる．Atkin のアルゴリズムでは $t \pmod l$ の値が数個の候補値として求まる．
[アルゴリズム 2]（Atkin のアルゴリズム）
入力：楕円曲線 $E/\mathbb{F}_p : Y^2 = X^3 + AX + B, l$
$\Phi_l(X, j(E)) = \Phi(X)$
出力：$t \pmod l$ の候補値
[Step 1] $(X^{p^r} - X, \Phi(X))$ が 1 でない r を求める．
[Step 2] 1 の原始 r 乗根を ζ とし，$t = [(\zeta + \zeta^{-1} + 2) \cdot p]^{1/2} \pmod l$ から $t \pmod l$ を求める．

□

1 の原始 r 乗根は $\phi(r)$ 個あり，可能な値の個数もそれと等しい．t がとり得る値の個数は Case-Atkin が多くなるほど大きくなる．この候補の値から正しい値を見つけるアルゴリズムは match and sort アルゴリズムと呼ばれる．Baby steps and Giant steps のアルゴリズムと中国人の剰余定理に基づいて構成される．詳しくは [15] を参照されたい．

1.5 Elkies のアルゴリズム

Elkies はフロベニウス写像 ϕ_p の固有方程式を解く際に用いる等分多項式 $f_l(X)$ の代わりにそのファクター $g_l(X)$ を用いることによって，アルゴリズムを高速化している [5]．以下では $g_l(X)$ について簡単に説明する．求める方法など詳しくは文献 [6] の **3.** を参照されたい．

楕円曲線 $E = \mathbb{C}/(\omega_1\mathbb{Z} + \omega_2\mathbb{Z})$- に対して，

$$g_l(X) = \prod_{k=1}^{(l-1)/2} (X - \wp(k\omega_1/l)) \quad (A\cdot 14)$$

とおく．この式は l 等分点の一部の X 座標を解としてもつ多項式である．l が Elkies 素数（Case-Elkies となる素数）であるとき，この式は $\mathbb{F}_p(X)$ に還元できる（係数を $\mathbb{F}_p$ に属するようにできる）．更に，l 等分点は固有方程式の解（フロベニウス写像の固有値）に対する解空間に対応する．このことにより，等分多項式 $f_l(X)$ の代わりにこの $g_l(X)$ を用いて固有方程式の解を求めることが可能になる．

等分多項式 $f_l(X)$ の次数が $(l^2-1)/2$ であるのに対し，$g_l(X)$ のそれは $(l-1)/2$ である．$g_l(X)$ を用いることにより，アルゴリズムの高速化が可能になる．

以下に Elkies のアルゴリズムを示す．
[アルゴリズム 6]（Elkies のアルゴリズム）
入力：楕円曲線 $E/\mathbb{F}_p : Y^2 = X^3 + AX + B, l, j(E)$
出力：$t \pmod l$
[Step 1] $g_l(X)$ を求める．
[Step 2] $\phi_p P = kP$ が 成立するような $1 \leqq k < l$ を求める．そのため以下の式の値を調べる．この値が 1 となるときの k が ϕ_p の固有値である．

$$\begin{cases} \gcd((X^p - X)f_k^2(X^3 + AX + B) \\ \quad + f_{k-1}f_{k+1}, g_l(X)) \quad (k : \text{even}) \\ \gcd((X^p - X)f_k^2 + f_{k-1}f_{k+1}(X^3 \\ \quad + AX + B), g_l(X)) \quad (k : \text{odd}) \end{cases} \tag{A·15}$$

[Step 3] $t \equiv (k^2 + p)/k \pmod{l}$ を求める．

□

Morain らは Isogeny cycle 法により，Case-Elkies をより効果的に用いることに成功した．同種写像の連鎖を考えることにより，$t \pmod{l^2}, t \pmod{l^3 \cdots}$ を求める多項式の次数を抑え，短時間で計算可能にするものである．これにより，SEA アルゴリズムで用いる最大の素数 L を小さくでき，全体の計算時間が短縮される．詳しくは文献 [8], [15], [16] を参照されたい．

1.6 Schoof のオリジナルアルゴリズム

Case-Atkin が多いとき，match and sort アルゴリズムの計算時間が増大する．そのため可能な限り，Atkin Case を減らす必要がある．ここでは Schoof のオリジナルアルゴリズムについて説明する．これは，改良前の Schoof のアルゴリズムである．計算量のオーダが大きいが l が小さいときは計算時間も小さいため，Case-Atkin に代わって行う．これにより，match and sort アルゴリズムの計算時間を短縮できる．

以下にそのアルゴリズムを示す．

[アルゴリズム 5]（Schoof のオリジナルアルゴリズム）

入力：楕円曲線 $E/\mathbb{F}_p : Y^2 = X^3 + AX + B, l, j(E)$

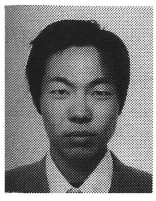
出力：$t \pmod{l}$

[Step 1] $(\phi^2 + p)(X) = t'\phi(X) \pmod{f_l(X)}$ が成立する $1 \leqq t' \leqq (l-1)/2$ を求める．

[Step 2] $(\phi^2 + p)(Y) = t'\phi(Y)$ が成立するとき，t'，しないとき，$-t'$ を出力する．終了．

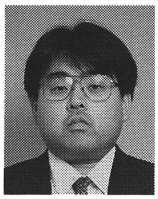
□

（平成 10 年 12 月 28 日受付，11 年 3 月 23 日再受付）



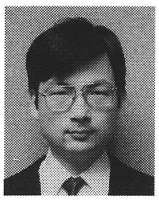
堀内　啓次　（学生員）

平 10 京都工繊大・工芸・電子情報卒．楕円曲線暗号などの研究に従事．



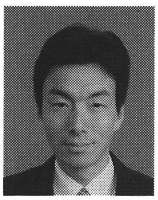
布田　裕一

平 8 京都工繊大・工芸・電子情報卒．平 10 同大大学院工芸科学研究科電子情報工学専攻博士前期課程了．楕円曲線暗号などの研究に従事．



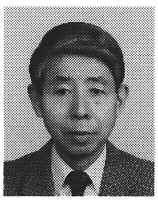
境　　隆一　（正員）

平 2 京都工繊大・工芸・電子卒．平 4 同大大学院工芸科学研究科電子情報工学専攻博士前期課程了．平 7 工芸科学研究科情報・生産科学専攻博士後期課程了．工博．同年阪電通大講師として現在に至る．主に暗号と情報セキュリティ，符号理論の研究に従事．



金子　昌信

昭 58 東大・理・数学卒．昭 60 同大大学院理学研究科数学専攻修士課程了．昭 63 同博士課程了．理博．同年阪大・理・助手．平 2 京都工繊大・工芸・助教授．平 8 九大・数理学研究科・助教授として現在に至る．平 5〜6 ドイツケルン大数学教室客員教授，ドイツマックスプランク数学研究所客員研究員．整数論，特にガロア表現，楕円曲線，モジュラー関数，ベルヌーイ数，ゼータ関数などの研究に従事．平 9 より日本数学会誌「数学」編集委員．日本数学会，アメリカ数学会各会員．



笠原　正雄　（正員）

昭 35 阪府大・工・電気卒．昭 37 阪大大学院工学研究科通信工学専攻修士課程了．昭 40 同博士課程了．工博．同年阪大・工・助手．昭 45 同講師．昭 47 同助教授．昭 62 京都工繊大・工芸・教授として現在に至る．昭 42〜44 米国ベル電話研究所客員研究員．情報理論，符号理論，ディジタル通信システム，情報セキュリティ，音声・画像符号化，技術倫理などの研究に従事．昭 60 本会情報理論研究専門委員会委員長．昭 60 本会評議員．昭 61 本会通信グループ副委員長．平 1 本会情報セキュリティ研究専門委員会委員長．平 7 情報理論とその応用学会長．平 8 本会基礎・境界ソサイエティ会長．平 9 本会代数曲線とその応用研究専門委員会委員長．平 10 本会基礎・境界ソサイエティ編集長．IEEE SIT 東京支部チェアマン．昭 41 年度本会稲田賞．昭 59 年度本会論文賞．昭 61 年度本会著述賞．平 6 年度本会小林記念特別賞，業績賞．著書「情報理論」（共著）など．IEEE（フェロー），情報処理学会，テレビジョン学会，システム制御情報学会各会員．