SCIS2000 The 2000 Symposium on Cryptography and Information Security
Okinawa, Japan, January 26-28, 2000

素因数分解に適した楕円曲線の生成法

Generating Elliptic Curves Suitable for Factorization

伊豆 哲也 (IZU Tetsuya) *
izu@flab.fujitsu.co.jp

あらまし 楕円曲線法は, 素因数依存型の素因数分解アルゴリズムの中で最良であり, 合成数のサイズが大きくても素因数を見つけられる可能性がある. 楕円曲線法で素因数を見つけるには, 位数が小さな素因数の積となっていることが望ましい [Mon87,KTK97]. 本稿では Yoshimura の提案した曲線の構成法 [Yos99] を拡張することによって, ある 4 次体上で $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ と同型なねじれ部分群を持つ楕円曲線の生成法を与え, この曲線を素体へ reduction することによって, 位数が 36 の倍数となる楕円曲線の構成法を示す. また, 本構成法を楕円曲線法に適用した場合の効果を考察し, 実験結果とともにその性能を報告する.

キーワード 素因数分解, 楕円曲線法 (ECM), 位数, ねじれ部分群

1 はじめに

整数の素因数分解問題に対する効率的な解法, つまり入力値の多項式時間アルゴリズム, は知られていない. この事実は RSA 暗号をはじめとする情報セキュリティ技術に広く応用されており, 世間の素因数分解問題への関心が高まっている. 巨大整数の素因数分解記録が新聞報道されるようになったのも, その一端といえる.

素因数分解したい合成数を n, その素因数を p とするとき, 素因数分解アルゴリズムは, その計算量が合成数 n に依存するタイプと素因数 p に依存するタイプに大別できる. 前者では 2 次ふるい法, 数体ふるい法, 後者では $p-1$ 法, 楕円曲線法が有名で, それぞれの (最悪または平均) 計算量と分解記録は 表 1 のようになる. なお表中の C は合成数, P は素数, それに続く数字は 10 進での桁数をあらわす. また関数 $L_x[u,v]$ は

$$L_x[u,v] = \exp\left((v+o(1))(\log x)^u(\log\log x)^{1-u}\right)$$

と定義される関数で,

$$\begin{aligned} L_x[0,v] &= \exp(v\log\log x) = (\log x)^v \\ L_x[1,v] &= \exp(v\log x) = x^v \end{aligned}$$

となることから多項式関数と指数関数の橋渡しをしており (準指数関数), u が小さい方が漸近的な計算量的において優れている. 表から分かる通り, 素因数分解アルゴリズムは準指数時間アルゴリズムしか知られていない. その中で数体ふるい法は漸近的に最速の方法であるが, n の桁数が大きくても p の桁数が小さい場合には, 楕円曲線法が有効である.

楕円曲線法 (Elliptic Curve Method, ECM) は, 1987 年に Lenstra Jr. によって提案されたアルゴリズムである ([Len87]). $p-1$ 法が既約剰余類群 $GF(p)^*$ の構造を利用していた代わりに, ECM は楕円曲線上の有理点のなす加法群 $E(GF(p))$ の構造を利用する. これらの方法で素因数分解できるのは, 群の位数 (要素の個数) が小さな素因数の積で表されるときである. 合成数 n が与えられたときに, $p-1$ 法では $GF(p)^*$ の位数が固定されてしまうのに対し, 楕円曲線法では楕円曲線の係数を変化させることで, 加法群 $E(GF(p))$ の位数も変化するため, 他のパラメータを変化させないですむことから, 計算量を抑えられる要因となっている.

しかし群の位数が小さな素因数の積で表せるような楕円曲線を生成することは, 一般には難しい. そこで群の位数があらかじめ小さい因子 d を持っているような楕円曲線を使用することで, 群の位数の最大素因子を小さくしようという試みがなされている ([Mon87]). 代数体 K 上の楕円曲線 E/K の有理点群 $E(K)$ の構造に関して, K が有理数体や 2 次体の場合には, 有理点群 $E(K)$ のねじれ部分群の分類が分かっており ([Maz78,Kam90,Kam92,KeMo88]), これらのねじれ部分群を有するような楕円曲線を代数体上で構成し, その曲線を $GF(p)$ に reduction することによって, d が既知の, つまり ECM に適した楕円曲線を生成する方法がいくつか提案されている ([AM93,Yos99,Izu99b]).

本稿では, Yoshimura によって提案された, 2 次体 $\mathbf{Q}(\sqrt{-3})$ 上で $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ と同型なねじれ部分群を

* (株) 富士通研究所, 〒 211-8588 神奈川県川崎市中原区上小田中 4-1-1, FUJITSU Laboratories Ltd., 4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki, Kanagawa, 211-8588, Japan

方法	計算量	記録	分解日時	対象
2 次ふるい法	$L_n[1/2, 1.020]$	C129(P64)	1994 年 4 月	RSA129
数体ふるい法 (汎用)	$L_n[1/3, 1.901]$	C155(P78)	1999 年 8 月	RSA155
数体ふるい法 (特殊)	$L_n[1/3, 1.526]$	C211(P93)	1999 年 4 月	$10^{211}-1$
$p-1$ 法	$O(p_{max})$	(P32)		$2^{977}-1$
楕円曲線法	$L_p[1/2, 1.414]$	(P54)	1999 年 12 月	$(6^{43}-1)^{42}-1$

表 1: 素因数分解法の計算量と分解記録の比較

持つ楕円曲線の構成法 ([Yos99]) を拡張することによって, ある 4 次体上で $\mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ と同型なねじれ部分群を持つ楕円曲線が生成できることを示す. そしてこの曲線を reduction することによって, 素体上で位数が 36 の倍数となる楕円曲線 $E/GF(p)$ を構成する. 最後に ECM に適用した場合の効果を考察し, 実験結果とともに報告する.

本稿の構成は以下の通りである : 第 2 節で必要な数学的知識を準備をした後に, 第 3 節で具体的な曲線の構成法を示す. 第 4 節では楕円曲線法の概略と, それに適した楕円曲線について説明する. そして第 5 節で提案する曲線の構成法を楕円曲線法に適した場合の効果を考察し, 実験結果とともに報告する.

2 準備

本節では楕円曲線に関する数学的事項を整理する. 詳細は専門書 ([Sil91] など) を参照されたい.

以下素数 $p > 3$ に対し, 要素数 p の有限体を $GF(p)$ とかく.

2.1 楕円曲線

K を代数体または素体 $GF(p)$ とする. このとき $4a^3 + 27b^2 \neq 0$ を満たす $a, b \in K$ に対し

$$E/K : y^2 = x^3 + ax + b$$

で与えられる曲線を K 上の **楕円曲線 (elliptic curve)** といい, この式を楕円曲線の定義方程式と呼ぶ. K 上で定義方程式を満たす点を **有理点 (rational point)** といい, 楕円曲線上のすべての有理点と, **無限遠点 (infinite point)** と呼ばれる仮想的な有理点 $\mathcal{O}$ を併せた点集合を $E(K)$ とかく. $E(K)$ の点の個数を **曲線の位数 (order of a curve)** といい, $\#E(K)$ であらわす. 無限遠点 $\mathcal{O}$ は (x, y) のような成分表示が不可能な点として特徴付けられる.

有理点集合 $E(K)$ は加法群の構造を持つ. 加法の具体的な計算式は, 以下のような K 上の四則演算によって与えられる: $P = (x, y)$ の逆元を $(x, -y)$ とする. 曲線上の 2 点 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ に対して $P_3 = P_1 + P_2 = (x_3, y_3)$ とおく. ここで P_3 は

加算 ($P_1 \neq \pm P_2$):

$$\begin{aligned} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 &= \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) - y_1 \end{aligned}$$

2 倍算 ($P_1 = P_2$):

$$\begin{aligned} x_3 &= \left(\frac{3x_1^2 + \alpha}{2y_1}\right)^2 - 2x_1 \\ y_3 &= \frac{3x_1^2 + \alpha}{2y_1}(x_1 - x_3) - y_1 \end{aligned}$$

とする. 加法の単位元は $\mathcal{O}$ となる.

群として考えたときの $E(K)$ を有理点群と呼ぶ. 有理点群の任意の点 $P \in E(K)$ に対し, $nP = \mathcal{O}$ を満たす正の最小の整数 n を **点の位数 (order of a point)** と呼ぶ. 点の位数は曲線の位数の約数となる.

2.2 有理点群の構造

代数体上で定義される楕円曲線 E/K の有理点群の構造は次の定理によって与えられる.

定理 2.1 (Mordell-Weil) 代数体 K 上で定義された楕円曲線 E/K の有理点群 $E(K)$ は有限生成アーベル群である. すなわち

$$E(K) \cong E(K)_{tor} \oplus \mathbf{Z} \oplus \ldots \oplus \mathbf{Z}$$

と表すことができる. ここで $E(K)_{tor}$ は点の位数が有限である点の集合である.

部分群 $E(K)_{tor}$ を $E(K)$ の **ねじれ部分群 (torsion subgroup)** という. 特に K が有理数体または 2 次体の場合には, ねじれ部分群の分類が知られている.

定理 2.2 (Mazur) 有理数体 $\mathbf{Q}$ 上で定義される楕円曲線 E/K のねじれ部分群 $E(K)_{tor}$ は, 以下の *15* 個のうちのいずれかの群と同型になる:

$$\begin{cases} \mathbf{Z}/\mu\mathbf{Z} & \mu = 1, \ldots, 10, 12 \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mu\mathbf{Z} & \mu = 1, 2, 3, 4 \end{cases}$$

定理 2.3 (Kamienny-Kenku-Momose) *2次体* $K = \mathbf{Q}(\sqrt{m})$ 上で定義される楕円曲線 E/K のねじれ部分群 $E(K)_{tor}$ は, 以下の *26* 個のうちのいずれかの群と同型になる*:*

$$\begin{cases} \mathbf{Z}/\mu\mathbf{Z} & \mu = 1, \ldots, 16, 18 \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mu\mathbf{Z} & \mu = 1, 2, 3, 4, 5, 6 \\ \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mu\mathbf{Z} & \mu = 1, 2 \\ \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z} \end{cases}$$

ただし $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mu\mathbf{Z}$ は $m = -3$ のとき, $\mathbf{Z}/4\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}$ は $m = -1$ のときにしか現れない.

Mazur の定理 (定理 2.2), Kamienny-Kenku-Momose の定理 (定理 2.3) は, 与えられた楕円曲線の有理点群のねじれ部分群を分類している. これとは反対に, 与えられたねじれ部分群を持つ楕円曲線をどうやって構成するかという問題が考えられる. すべてを書き尽くすことは難しいが, 定理 2.2 に対して [Kub76],[Mon87],[AM93], 定理 2.3 に対してはさらに [Rei86],[Yos99],[Izu00] などによって, それぞれのねじれ部分群に対する構成例が示されている.

2.3 有限体上の楕円曲線

ECM にとって, 次の 2 つの定理は重要である. これらの定理によって, 楕円曲線の係数を変化させたときに, その位数が "適当に" 変化することが保証される.

定理 2.4 (Hasse-Weil) 有限体 $GF(p)$ 上で定義された楕円曲線 $E/K : y^2 = x^3 + ax + b$ の有理点群 $E(K)$ の位数を $\#E(K)$ とすると

$$p + 1 - 2\sqrt{p} \leq \#E(K) \leq p + 1 + 2\sqrt{p}$$

が成立する.

定理 2.5 (Deuring) E の係数 a, b が $K = GF(p)$ を動くとき, $t = \#E(K) - (p + 1)$ は $-2\sqrt{p} \leq t \leq 2\sqrt{p}$ の区間に一様に分布し, この範囲のすべての整数値をとりうる.

2.4 分割多項式

体 K の代数閉体を $\overline{K}$ とかく. 有理点群 $E(\overline{K})$ 上の点で, ℓ 倍すると無限遠点 $\mathcal{O}$ となる点を **ℓ-ねじれ点 (l-torsion point)** といい, その集合を $E[\ell]$ とかく. $E[\ell]$ 上の点が零点集合となるような 2 変数多項式を **分割多項式 (division polynomial)** といい, 具体的な式は以下の漸化式によって与えられる:

$$\begin{aligned} \psi_1 &= 1, \ \psi_2 = 2y, \\ \psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2, \\ \psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 \\ &\qquad - 4abx - 8b^2 - a^3), \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \\ &\qquad (m \geq 2), \\ \psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)/(2y) \\ &\qquad (m \geq 3). \end{aligned}$$

3 ある 4 次体上で $Z/6Z \times Z/6Z$ と同型なねじれ部分群を持つ楕円曲線

本節では Yoshimura の結果を拡張し, ある 4 次体上で $\mathbf{Z}/6\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$ と同型なねじれ部分群を持つ楕円曲線の生成法を示す.

3.1 Yoshimura の結果

Yoshimura は [Yos99] において, 2 次体 $\mathbf{Q}(\sqrt{-3})$ 上で $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ と同型なねじれ部分群を持つ楕円曲線の族の構成例を与えた. その構成法は以下の通りである:

定理 3.1 (Yoshimura) $\mathbf{Q}$ 上の楕円曲線 $y^2 = x^3 - 2160$ 上の無限位数の点 $P = (16, 44)$ について, 点 P の m-倍点を $mP = (x_m, y_m)$ とする. このとき

$$t_m = -\frac{x_m}{12}, \quad r_m = \frac{t_m^3 + 8}{9}$$

とおけば, 楕円曲線

$$E_{t_m} : y^2 = x^3 + a_m x + b_m$$

は $\mathbf{Q}(\sqrt{-3})$ 上で $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$ に同型なねじれ部分群を持つ. ただし

$$\begin{aligned} a_m &= -\frac{1}{3}(3r_m - 2)(3r_m^3 - 6r_m^2 + 12r_m - 8) \\ b_m &= -\frac{2}{27}(3r_m^2 - 12r_m + 8) \\ &\qquad \times (9r_m^4 - 24r_m^2 + 24r_m - 8) \end{aligned}$$

とする. さらに

$$\begin{aligned} x_0 &= -\frac{4r_m}{3} + \frac{t_m^6 + 16t_m^3 - 44}{81} \\ y_0 &= \frac{r_m y_m}{81} \end{aligned}$$

とおけば, 点 $P_0 = (x_0, y_0)$ は $E_{t_m}/\mathbf{Q}(\sqrt{-3})$ 上の無限位数の点となる.

点 P_0 は ECM における開始点である.

簡単な計算によって, 定理 3.1 の楕円曲線 E_{t_m} は以下のような性質を持つことがわかる. ただし添字の m を省略して $t = t_m$ のように表記する.

命題 3.2 定理 *3.1* の楕円曲線 E_t に関し以下が成立する.
(1) $E_t(\mathbf{Q})$ は $\mathbf{Z}/6\mathbf{Z}$ に同型なねじれ部分群を持つ. 実際, 点

$$P_1 = \left(\frac{-t^6 - 16t^3 + 44}{81}, \frac{-4t^6 - 28t^3 + 32}{81}\right)$$

は 6 分点である.

(2) $E_t(\mathbf{Q}(\sqrt{-3}))$ は $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$ に同型なねじれ部分群を持つ. 実際, 点

$$\begin{aligned}Q_1 &= \left(\frac{-t^6+6t^4-4t^3+18t^2+12t-4}{81}+\right.\\ &\quad \frac{-6t^4+18t^2-12t}{81}\alpha,\\ &\quad \left.\frac{-6t^7+18t^5-24t^4+36t^2-24t}{243}+\right.\\ &\quad \left.\frac{-2t^7-6t^5-8t^4+36t^3-12t^2-8t}{243}\alpha\right)\end{aligned}$$

は (P_1 によって生成されない) 3 分点である (ここで $\alpha=\sqrt{-3}$).

なお Mazur の定理により, $E_t(\mathbf{Q})$ は (2) のようなねじれ部分群を持ち得ないことがわかる.

3.2 分割多項式 $\psi_6(x,y)$ の分解体の計算

定理 3.1 の楕円曲線 E_t に対する分割多項式 $\psi_6(x,y)$ を考察する. 6 分点に着目するために

$$\psi(x)=\psi_6(x,y)/(\psi_2(x,y)\psi_3(x,y))$$

とおくと, $\psi(x)$ は x の 12 次式で, その根は 6 分点の x 座標に一致する. 楕円曲線 $E_t/\mathbf{Q}(\sqrt{-3})$ 上の 6 分点は, 命題 3.2 の記号を用いると, $P_1, P_1+Q_1, P_1+2Q_1, 3P_1+Q_1, 3P_1+2Q_1, 5P_1, 5P_1+Q_1, 5P_1+2Q_1$ の 8 点であるが, このうち x 座標が異なる点は 4 点であり, これは $\psi(x)$ が $\mathbf{Q}(\sqrt{-3})$ 上で

$$\psi=f_1^{(1)}f_2^{(1)}f_3^{(1)}f_4^{(1)}g_1^{(2)}g_2^{(2)}h^{(4)}$$

と因数分解できることに対応する (右肩の添字は次数を表す).

方程式 $h^{(4)}(x)=0$ の分解体と解が得られたとすると, $\psi(x)$ はその分解体上で 1 次因子の積に分解でき, 楕円曲線 E_t は $\mathbf{Z}/6\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$ に同型なねじれ部分群を持つことになる. よって $h^{(4)}(x)=0$ の分解体を求めたい. ここで $h^{(4)}(x)$ は 4 次式であるから, 解の公式を適用することが可能である. 細かい計算は省略するが, $\alpha=\sqrt{-3}$, $\beta=\sqrt{\frac{t(t^3+8)}{9}}$ とおくと, 4 次体 $\mathbf{Q}(\alpha,\beta)$ において $h^{(4)}(x)$ は根

$$\begin{aligned}x &= \frac{-t^6+3t^5+3t^4-22t^3+24t^2+24t-4}{81}\\ &\quad+\frac{t^5-t^4+8t^2-8t}{27}\alpha\\ &\quad+\frac{t^3+3t^2-6t+2}{9}\beta+\frac{t^3-3t^2+2}{9}\alpha\beta\end{aligned}$$

を持つ.

以上をまとめて, 次の命題を得る.

命題 3.3 (Izu) 定理 3.1 の楕円曲線 E_t は, $\alpha=\sqrt{-3}$, $\beta=\sqrt{\frac{t(t^3+8)}{9}}$ とおくとき, 4 次体 $K=\mathbf{Q}(\alpha,\beta)$ 上で x 軸と 3 点で交わり, その定義方程式は

$$\begin{aligned}E_t: y^2 &= \left(x-\frac{-t^6+20t^3+8}{81}\right)\\ &\quad\times\left(x-\frac{(t^6-20t^3-8)+(t^4+8t)\beta}{162}\right)\\ &\quad\times\left(x-\frac{(t^6-20t^3-8)-(t^4+8t)\beta}{162}\right)\end{aligned}$$

となり, $\mathbf{Z}/6\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$ に同型なねじれ部分群を持つ. 実際, 点

$$P_1 = \left(\frac{-t^6-16t^3+44}{81},\frac{-4t^6-28t^3+32}{81}\right)$$

および

$$\begin{aligned}P_2 &= \left(\frac{-t^6+3t^5+3t^4-22t^3+24t^2+24t-4}{81}\right.\\ &\quad+\frac{t^5-t^4+8t^2-8t}{27}\alpha\\ &\quad+\frac{t^3+3t^2-6t+2}{9}\beta+\frac{t^3-3t^2+2}{9}\alpha\beta,\\ &\quad\frac{t^8-5t^7+16t^5-44t^4+64t^2-32t}{81}\\ &\quad+\frac{-t^8-5t^7+18t^6-16t^5}{243}\alpha\\ &\quad+\frac{-44t^4+144t^3-64t^2-32t}{243}\alpha\\ &\quad+\frac{t^6-3t^5+22t^3-24t^2+4}{27}\beta\\ &\quad\left.+\frac{-t^6-3t^5-22t^3-24t^2+36t-4}{81}\alpha\beta\right)\end{aligned}$$

は 6 分点で, ねじれ部分群の生成元となっている.

3.3 $GF(p)$ への reduction

命題 3.3 の楕円曲線 E_t の導出過程を見てみると, この構成法は, 代数体だけでなく, 素体 $GF(p)$ でも適用可能であることがわかる. ただし $GF(p)$ において $-3, t(t^3+8)/9$ の平方根が存在することが必要で, -3 が平方剰余であるための必要十分条件は

$$\left(\frac{-3}{p}\right)=1 \iff p\equiv 1 \pmod 3,$$

$t(t^3+8)/9$ が平方剰余であるための必要十分条件は

$$\left(\frac{t(t^3+8)}{p}\right)=1$$

で与えられる. ただし $\left(\frac{\cdot}{p}\right)$ は Legendre 記号を表す.

p,t が与えられたときに, $p, t(t^3+8)$ がそれぞれ平方剰余となる割合はそれぞれ 1/2 程度だから, p,t の対全体に対し曲線が生成できる場合は 1/4 程度の割合になることが期待できる.

	$\mathcal{O}$	P_2	$2P_2$	$3P_2$	$4P_2$	$5P_2$
$\mathcal{O}$	$\mathcal{O}$	$(890, 744)$	$(847, 525)$	$(39, 0)$	$(847, 484)$	$(890, 265)$
P_1	$(790, 549)$	$(420, 677)$	$(929, 253)$	$(526, 391)$	$(750, 556)$	$(832, 660)$
$2P_1$	$(241, 234)$	$(882, 590)$	$(49, 58)$	$(416, 852)$	$(881, 148)$	$(995, 711)$
$3P_1$	$(871, 0)$	$(636, 68)$	$(6, 123)$	$(99, 0)$	$(6, 886)$	$(636, 941)$
$4P_1$	$(241, 775)$	$(995, 298)$	$(881, 861)$	$(416, 157)$	$(49, 951)$	$(882, 419)$
$5P_1$	$(790, 460)$	$(832, 349)$	$(750, 453)$	$(526, 618)$	$(929, 756)$	$(420, 332)$

表 2: P_1, P_2 が生成するねじれ部分群の例

3.4 数値例

本節では $GF(p)$ 上での数値例を示す. 素数 $p = 1009$ に対しては $\left(\frac{-3}{p}\right) = 1$ となるので, $GF(1009)$ では -3 の平方根が存在する. 実際 $\sqrt{-3} = 260, 749$ である.

次に開始点 P_0 と楕円曲線 E_{t_m} を定める. $P, 2P, \cdots$ と順に計算していくと, $m = 3$ のときに $3P = (217, 919)$, $t = t_3 = 66$, $\sqrt{\frac{t(t^3+8)}{9}} = 54, 955$ となる. このとき楕円曲線 E_t は

$$\begin{aligned} y^2 &= x^3 + 961x + 66 \\ &= (x - 99)(x - 39)(x - 871) \end{aligned}$$

で与えられ, $P_0 = (89, 593)$ となる.

楕円曲線 E_t のねじれ部分群の生成元 P_1, P_2 は

$$P_1 = (790, 549), \quad P_2 = (890, 744)$$

となり, P_1, P_2 の生成するねじれ部分群は 表 2 のようになる.
この曲線の位数は $\#E_t = 972$ で 36 の倍数であり, さらに開始点 P_0 の位数 81 の倍数にもなっている.

4 楕円曲線法への適用

本節では, 楕円曲線の族 E_t の楕円曲線法への適用について述べる. 楕円曲線法は $p-1$ 法の拡張であるので, まず $p-1$ 法について述べ, 続いて楕円曲線法を説明する. 楕円曲線法の実装上のテクニックなどは [Mon87],[KiMa94],[Izu99a] などに詳しい. また楕円曲線法の分解記録については [ECM-NET] を参照されたい.

4.1 $p-1$ 法

素数 p と互いに素な整数 a に対し, $a^{p-1} \equiv 1 \pmod{p}$ が成立する (Fermat の小定理). よって整数 m が $p-1$ の倍数ならば, $a^m \equiv 1 \pmod{p}$ が成立する. このとき $a^m - 1$ は p の倍数となるので, p が n の素因数であれば $\mathsf{gcd}(a^m - 1, n) = p$ となることが期待できる. 入力された n に合わせて適当に m を定め, $\mathsf{gcd}(a^m - 1, n)$ を計算することによって素因数 p を見つける方法を $p-1$ 法という.

p が見つけられるのは $(p-1)|m$ となる場合である. つまり $p-1$ 法 の計算量は $p-1$ の最大の素因数 p_{max} に依存する. $\mathsf{gcd}(a^m - 1, n) = 1$ のときは m を大きな値に選び直せば良いが, それでも p_{max} が巨大な場合には $p-1$ 法は無力である. これは n が与えられたときに既約剰余類群 $(GF(p)^*$ が固定されてしまい, $p-1$ 法は原理的に $a^{p-1} \equiv 1 \pmod{p}$ を利用しているため, 素因数 p を見つけるためには m を大きくするしかないからである. この欠点を克服したのが楕円曲線法である.

4.2 楕円曲線法

楕円曲線法 (Elliptic Curve Method,ECM) は, 1987 年に Lenstra Jr. によって提案された素因数分解法である [Len87].

素数 p に対し有限体 $K = GF(p)$ 上で定義される楕円曲線 $E_{(a,b)}(K)$ を考える. その位数 $\#E = \#E_{(a,b)}(K)$ と曲線上の任意の点 P に関して

$$E_{(a,b)}(K) \text{ 上の任意の点 } P \text{ に対し } \quad \#EP = \mathcal{O}$$

が成立する (この式は $p-1$ 法における Fermat の小定理に対応する). n を素因数分解する場合, p は未知である. そこで楕円曲線を環 $R = \mathbf{Z}/n\mathbf{Z}$ 上で考える. このとき点の加算を計算するには mod n での逆元計算が必要となるため, 任意の点に対する加算は計算できない. しかし逆元計算に失敗した場合には, その数と n の gcd から p が求められるので, 素因数分解を考える上では都合がよい. 従って素因数分解したい合成数 n に対し, 楕円曲線 $E_{(a,b)}(R)$, 曲線上の点 P, 整数 m を適当に定め, 曲線上で点 mP を計算する. $\#E_{(a,b)}(K)|m$ となっている場合には, $E_{(a,b)}(K)$ でも $E_{(a,b)}(R)$ でも $mP = \mathcal{O}$ となるので, 計算が不可能となり, そこから n の因数そしては素因数 p を求められる. これが楕円曲線法である.

$p-1$ 法で素因数 p が見つけられるのは $p-1$ が小さな素数の積に分解できる場合 (smooth) で, このためある m について素因数が見つけられない場合には, m を (もっと大きな整数に) 設定し直すしかなかった. し

かし ECM で素因数 p を見つけられるのは $\#E_{(a,b)}(K)$ が smooth な場合であり, ある m について素因数が見つけられない場合には a, b を設定し直せばよく, m を変える必要がない. これが ECM の最大の長所である.

4.3 曲線の生成

ECM によって素因数 p が見つかるのは, 素体上での位数 $\#E_{(a,b)}(GF(p))$ が smooth になる場合である. したがってどのような曲線を使用するかが全体の効率を左右する. Hasse-Weil の定理と Deuring の定理から, $\#E_{(a,b)}(GF(p))$ は p 程度の大きさのランダムな数と見なすことができる. したがって曲線をランダムに選んだ場合に $\#E_{(a,b)}(GF(p))$ が smooth になることは希であろう. また smooth になる曲線を構成することも一般には難しい.

しかし位数があらかじめ小さな因数 d を持つような曲線のみを使用すれば, ランダムに動く部分のサイズが p から p/d に減少するので, 素因数分解に成功する確率を高めることができる ([KTK97]). これは数ビット程度の貢献でしかないが, 実際上の効果は大きく, 例えば $d = 16$ のときに, 効率は 1.5 倍程度向上するとの実験結果が報告されている ([SW93]).

Suyama ははじめにこの点に着目し, 分割多項式 ψ_3 を使用することによって $d = 12$ となる曲線の構成法を提案した ([Mon87]). さらに Atkin-Morain は楕円曲線の Kubert-form を利用して, $d = 16$ となる構成法を示した. [ECM-NET],[KiMa94] などで使用されている ECM のプログラムでは, $d = 12$ となる曲線が使用されている (この理由は定かでないが, 位数が 2 のべきで割り切れるという特殊性が嫌われているのではないかと推測する).

4.4 命題 3.3 の適用

Yoshimura は Kubert-form と分割多項式の両者を使用することによって $d = 18, 20, 24$ となる曲線を構成した ([Yos99]). 同様に命題 3.3 で得られた曲線の生成法を利用することによって, $d = 36$ となる曲線を ECM で利用することができる.

しかし, $d \leq 16$ となる曲線の構成法は Mazur の定理に登場するねじれ部分群を利用しているため, すべての p に対して適用可能であるのに対し, $d > 16$ となる曲線の構成法は Kamienny-Kenku-Momose の定理に登場するねじれ部分群を利用しているため, 適切な条件を満たす p に対してしか適用できないというデメリットが生じてしまう. それでも適用できる場合には従来よりも d の値を大きくできるので, 素因数分解する上での効率が向上することが期待できる. また, 同様の構成法を用いることによって, p に対する条件は網羅することも可能であるので, 大きな欠点にはならないと考える.

5 実験結果

本節では命題 3.3 で得た楕円曲線の性質に関する実験結果を報告する.

楕円曲線の生成法として, 比較のために以下の 4 種類の方法を用いた:

$E^{(1)}$: ランダムに係数を決定,
$E_t^{(12)}$: $d = 12$ となる曲線 ([KiMa94])
$E_t^{(18)}$: $d = 18$ となる曲線 (定理 3.1)
$E_t^{(36)}$: $d = 36$ となる曲線 (命題 3.3)

5.1 実験 1 : 位数の smoothness

合成数 $n = \prod_p p^{e_p}$ に対し, その smoothness を $S(n) = \sum_p e_p log(p)$ と定める. n が smooth であるためには, 大雑把に言って $S(n)$ の値が小さいほうが望ましく, おなじ程度の大きさの n ならば $S' = e_2 \log 2 + e_3 \log 3$ が大きいほうが良い.

以下では $10000 < p < 20000$ を満たす 1033 個の素数 p に対し, 各曲線族に対して 5 種類の楕円曲線 $E/GF(p)$ を生成し, その位数および S' を計算した. $E_t^{(12)}$ では $t = 4, 54, 49/4, 2166/625, 14884/1089$, $E_t^{(18)}, E_t^{(36)}$ では $m = 1, 2, 3, 4, 5$ とし, 条件を満たさないものはスキップした. 結果を表 3 にまとめる. 表中の Sum1 は本数の単純合計を, Sum2 は重みつき本数の合計を表す.

S' の値を比較すると, E_1, E_2, E_3, E_4 の順で S' は大きくなっていて, ECM において通常使用される E_2 に比べ, E_4 の S' は約 17 % 増えている. これは指数が 0,1 となる曲線が存在しない効果であるといえる. しかし計算した曲線の対象本数について考えると, E_1, E_2 は (ほぼ) すべての曲線で生成できているのに対し, E_3 はその 1/2, E_4 ではさらにその 1/2 程度の場合でしか生成できていない. これは E_1, E_2 の生成法がすべての p に対して有効であるのに対し, E_3 は $p \equiv 1 \pmod 3$ となる場合, E_4 はさらに $t(t^3 + 8)$ が $GF(p)$ の平方数となる場合に限られるためで, 対象本数の比は 3.3 節の考察結果と一致している.

5.2 実験 2 : ECM への適用

次に命題 3.3 の楕円曲線を ECM で使用した場合の効果を考える. 素因数分解をする時点では n しかわからないため, その素因数を p とするとき, -3 が $GF(p)$ で平方剰余であるかを判定することができない. そこで本実験では, あらかじめ素因数 p が既知である合成数を使用する.

実験で用いる合成数 $n_1 = p_1 \cdot q$, $n_2 = p_2 \cdot q$ は以下の通り:

$p_1 = 499123818241$(P12)
$p_2 = 774017083691$(P12)

指数	$E^{(1)}$		E_t^{12}		$E_t^{(18)}$		$E_t^{(36)}$	
e	$p=2$	$p=3$	$p=2$	$p=3$	$p=2$	$p=3$	$p=2$	$p=3$
0	1715	2874	0	0	0	0	0	0
1	1331	1442	0	2816	670	0	0	0
2	969	577	1320	1499	766	1499	476	753
3	511	171	1585	557	518	699	349	353
4	325	74	1009	196	285	244	209	118
5	146	16	589	57	168	80	135	39
6	85	7	305	23	79	19	56	11
7	34	3	173	16	44	13	32	9
8	24	1	82	-	14	5	13	-
9	15	-	52	-	10	-	10	-
10	7	-	14	-	-	-	-	-
11	2	-	21	-	5	-	3	-
12	1	-	14	-	-	-	-	-
Sum1	5165	5165	5164	5164	2559	2559	1283	1283
Sum2	8011	3556	19080	8804	6775	6716	4297	3361
S'	1.831		4.434		4.718		5.199	

表 3: 実験 1 の結果

$$q \quad = \quad 992474642815068364143371\,(\mathrm{P24})$$

このとき $\left(\frac{-3}{p_1}\right)=1$, $\left(\frac{-3}{p_1}\right)=-1$ となっている.

前節と同様に 4 種類の曲線の生成法を用い, 5000 本の曲線に対して素因数を得られた回数を集計した. ただし $L_1=1000$ とし, 第 2 段階は適用しなかった. 結果を表 4 にまとめる.

	$E^{(1)}$	$E_t^{(12)}$	$E_t^{(18)}$	$E_t^{(36)}$
n_1	47	82	103	113
n_2	29	64	53	68

表 4: 実験 2 の結果

表からわかる通り, n_1 では成功回数に予想通りの差が見られた. これは $GF(p_1)$ で -3 が平方剰余であり, $E_t^{(36)}$ による曲線の生成法の効果が反映されていると考えられる. これに対し n_2 では E_2, E_4 の間に優劣が見えにくく, E_3 はこれらに比べ劣っている. これも $GF(p_2)$ で -3 が平方非剰余であるためと考えられる. $GF(p_2)$ で $t(t^3+8)$ が平方剰余になる割合を $1/2$ と仮定しよう. すると $E_t^{(36)}$ の生成法は半々の割合で $d=6$ と $d=18$, 平均して $d=12$ の曲線を生成していることになっていると考えられ, $E_t^{(12)}$ と $E_t^{(36)}$ の結果が一致することの説明がつく. 同様に $E_t^{(18)}$ の生成法は $d=6$ の曲線を生成していると考えられ, 他に比べて性能が悪いことの説明がつく.

6 まとめと課題

本稿では, Yoshimura の結果を拡張し, ある 4 次体上で $\mathbf{Z}/6\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$ と同型なねじれ部分群を持つ楕円曲線の生成法を示し, その reduction を考えることによって, この生成法が ECM に適用できることを, 実験結果とともに述べた. その結果, p がある条件を満たす場合には, 従来の生成法よりも効率が良いことが判明した.

今後の課題としては以下が考えられる: (1) 大規模な素因数分解実験, (2) より大きな d を持つ楕円曲線の生成法の探索, (3) ECM による分解記録の更新.

謝辞

本稿をまとめるにあたり, 横山和弘博士, および同僚の方々から, 貴重なコメントとアドバイスを頂いたことに感謝いたします.

参考文献

[AM93] Atkin, A.O., Morain., F., *Finding Suitable Curves for the Elliptic Curve Method of Factorization*, Math. of Comp., 60(1993), 399-405.

[ECM-NET] `http://www.loria.fr/~zimmerma/records/`

[Izu99a] 伊豆哲也, 楕円曲線法の高速化について, 情報処理学会アルゴリズム研究会報告集,1999-AL-69-8, 53-60.

[Izu99b] 伊豆哲也, 楕円曲線法の高速化について, 電子情報通信学会情報セキュリティ研究会報告集,ISEC99-60, 59-66.

[Izu00] 伊豆哲也, $\mathbf{Q}(\sqrt{-1})$ 上で $\mathbf{Z}/4\mathbf{Z}\times\mathbf{Z}/4\mathbf{Z}$ に同型なねじれ部分群を持つ楕円曲線法の生成法について, preprint.

[Kam90] Kamienny, S., *Torsion points on elliptic curves*, Bull, Amer. Math. Soc. (N.S.) 23, no.2(1990), 371-373.

[Kam92] Kamienny, S., *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. 109 no.2(1992), 221-229.

[KeMo88] Kenku, M.A., Momose, F., *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 109 (1988), 125-149.

[KiMa94] 木田祐司, 牧野潔夫, UBASIC による コンピュータ整数論, 日本評論社,1994.

[Kub76] Kubert, D.S., *Universal bounds on the torsion of elliptic curves*, Proc. of London Math. Soc. 3, 33(1976), 193-237.

[KTK97] 國廣昇, 鶴岡行雄, 小山謙二, 適切な位数を持つ楕円曲線に基づく素因数分解, Proc. of 1997 SCIS, SCIS97-15-B.

[Len87] Lenstra Jr.,H.W., *Factoring Integers with Elliptic Curves*, Annals of Math. 126(1987),649-673.

[Mon87] Montgomery,P.L., *Speeding the Pollar and Elliptic Curve Methods for Factorizations*, Math. of Comp. 48(1987),243-264.

[Rei86] Reichert,M.A., *Explicit Determination of Nontrivial Torsion Structure of Elliptic Curves over Quadratic Number Fields*, Math. of Comp., 61(1993),445-462.

[Sil91] Silverman,J.H., *The Arithmetic of Elliptic Curves*, GTM 106, Springer,1991.

[SW93] Silverman,R.D., Wagstaff Jr.,S.S., *A Practical Analysis of the Elliptic Curve Factoring Algorithm*, Math. of Comp. 61(1993),445-462.

[Yos99] 吉村俊介, *2*次体上定義された楕円曲線を用いた素因数分解の高速化, 大阪府立大学大学院修士論文,1999.