アルゴリズム 69－8
（1999．9．2）

楕円曲線法の高速化について

伊豆 哲也 (izu@flab.fujitsu.co.jp)
富士通研究所セキュアコンピューティング研究部
〒211-8588 川崎市中原区上小田中 4-1-1

概略: 合成数の素因数分解アルゴリズムのうち, 楕円曲線法 (ECM) と呼ばれる方法についてまとめる. ECM は素因数依存型アルゴリズムのうち最良のものであり, 合成数のサイズが大きくても適用できる可能性がある. ECM のアルゴリズムそのものは単純であるが, 実際に計算する上ではさまざまな高速化手法が欠かせない. 本稿では曲線の生成法を中心として, さまざまな高速化方法を紹介する.

Fast Computation on Elliptic Curve Method of Integer Factorization

IZU Tetsuya (izu@flab.fujitsu.co.jp)
FUJITSU Laboratories Ltd.
4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki, 211-8588, Japan
Email: izu@flab.fujitsu.co.jp

Abstract: In this artcle, we survey the technique to compute the Elliptic Curve Method(ECM) of integer factorization.

1 はじめに

整数の素因数分解問題は古くから知られている. エラトステネスのふるい法をはじめさまざまな方法が考案されてきたが, 効率さの面からは不十分であった. 計算機の普及によって巨大整数が手軽に扱えるようになると, アルゴリズム的にも計算量的にも興味深い手法が考案されるようになり, さらにはセキュリティ技術へ応用 (RSA 暗号など) されたこともあって, 素因数分解問題に対して広い関心が寄せられるようになった. 特に最近では巨大整数の素因数分解に成功したというニュースをたびたび耳にするようになり, 1999 年だけを見ても, 2 月に RSA-140 が解かれたり, 4 月に (特殊) 数体ふるい法による記録が大幅に更新されたりしている (211 桁, 従来は 186 桁).

素因数分解問題に対しては入力の準指数時間を必要とするアルゴリズムしか知られていない. 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 n に依存するタイプと p に依存するタイプに大別できる. 前者では, 連分数法,2 次ふるい法, 数体ふるい法, 後者では $p-1$ 法, 楕円曲線法などが有名であり, それぞれの (最悪または平均) 計算量は次のようになる:

◇合成数 n に依存	
2 次ふるい法	$L_n[1/2, 1.020]$
数体ふるい法 (汎用)	$L_n[1/3, 1.901]$
数体ふるい法 (特殊)	$L_n[1/3, 1.526]$
◇素因数 p に依存	
試行割算法	$O(p)$
ρ 法	$O(\sqrt{p})$
$p-1$ 法	$O(p_{max})$
楕円曲線法	$L_p[1/2, 1.414]$

(p_{max} は $p-1$ の最大素因数). ここで関数 $L_x[u,v]$ は

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

と定義する. この関数は,

$$L_x[0,v] = \exp(v\log\log x) = (\log x)^v$$

$$L_x[1,v] = \exp(v\log x) = x^v$$

となることより, 多項式関数と指数関数の橋渡しをしている (準指数関数).

本稿は, p に依存するアルゴリズムとして最速である楕円曲線法の高速化手法を考察することが目的である. アルゴリズムの概略を示した後, 具体的な高速化手法について検討する. また, 素因数分解に関する最近のトピックを付録にまとめた. なお表から分かる通り数体ふるい法が (漸近的には) 最速であるが, n の桁数が大きくても p が小さい場合には, 楕円曲線法が有効であることに注意されたい.

2 楕円曲線法

本節では楕円曲線についてまとめた後, 楕円曲線法のアルゴリズムについて説明する. 楕円曲線法は $p-1$ 法の拡張であるため, $p-1$ 法の概略を述べた後に楕円曲線法について述べる.

2.1 楕円曲線

素数 $p>3$ に対し $K=GF(p)$ とおく. $a,b\in K, 4a^3+27b^2\neq 0$ を満たす a,b に対し, 方程式

$$E_p(a,b): y^2 = x^3+ax+b$$

で定められる曲線を (Weierstrass 型) 楕円曲線という. K 上でこの方程式を満たす点集合と, 無限遠点と呼ばれる仮想的な点 $\mathcal{O}$ を併せた点集合を $E(K)$ とかき, その個数を $\#E(K)$ 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である.

集合 $E(K)$ は以下で定義する加法によって加法群となる: $P=(x,y)$ の逆元は $(x,-y)$ 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 ($P_1\neq\pm P_2$):

$$x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2$$

$$y_3 = \frac{y_2-y_1}{x_2-x_1}(x_1-x_3) - y_1$$

2 倍算 ($P_1=P_2$):

$$x_3 = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1$$

$$y_3 = \frac{3x_1^2+a}{2y_1}(x_1-x_3) - y_1$$

とする. 加法の単位元は $\mathcal{O}$ である.

加法群の位数 $\#E(K)$ については

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

となることが知られている (Hasse の定理).

2.2 $p-1$ 法

$p-1$ 法は Pollard によって考案された素因数分解アルゴリズムである. p を素数とする. フェルマーの小定理により $\gcd(a,p)=1$ である任意の整数 a に対し $a^{p-1}\equiv 1 \pmod p$ が成立する. よって整数 M が $p-1$ の倍数ならば $a^M\equiv 1 \pmod p$ となる. 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 $\gcd(a^M-1,n)=p$ 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, $\gcd(a^M-1,n)$ 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. $p-1$ 法 の計算量は, $p-1$ の最大の素因数 p_{max} に依存する.

M はどのように定めればよいだろうか. 実際には p も $p-1$ も未知なので, M が $p-1$ の倍数になる可能性を高めるには, M が大きさの割にたくさんの素数で割れるように定めた方が都合よい.

そこであらかじめ限界値 L_1 を定めておき, M は L_1 以下の比較的小さな素数の積

$$M = \prod_{p_i \leq L_1} p_i^{e_i} \quad p_i^{e_i} \leq \mathsf{LIMIT} < p_i^{e_i+1}$$

と定めるのが普通である. ただし具体的な M の値を求める必要はない. ここで LIMIT は M を決めるためのパラメータである. ただし $p-1$ 法は p_{max} が大きい場合には効果がないので, $\gcd(a^M-1, n) = 1$ であれば, M を選び直すしかない. ここまでを $p-1$ 法の第 1 段階という.

しかし $p-1$ が

$$p-1 = q \prod_{p_i \leq \mathrm{BOUND}} p_i^{e_i} \quad L_1 < q \leq L_2$$

のように 1 つだけ大きな素因数を持つ (つまり p_{max} が比較的小さい) 場合ならば, 次のような工夫ができる. いま $r \equiv a^M \bmod n$ とすると

$$r^q \equiv a^{qM} \equiv (a^M)^q \equiv 1 \pmod{p}$$

となる. したがって $L_1 < q \leq L_2$ の範囲の素数 q に対して r^q をチェックしていけばよい. この工夫を $p-1$ 法の第 2 段階という.

しかし p_{max} が巨大だったり, 大きな素因数を複数持ったりするときには, $p-1$ 法は無力である. これは n が与えられたときに乗法群 $(\mathbf{Z}/p\mathbf{Z})^*$ 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のである. この欠点を克服したのが次の楕円曲線法である.

2.3 楕円曲線法

楕円曲線法 (Elliptic Curve Method,ECM) は, 1987 年に Lenstra によって提案された素因数分解法である [Lenstra87]. ECM は $p-1$ 法が既約剰余類群 $GF(p)^*$ の構造を利用していた代わりに, 楕円曲線上の有理点のなす加法群 $E(GF(p))$ の構造を利用しており, 楕円曲線の係数を変化させることによってこの群の位数が適当に変化するため, M を変化させる必要がなくなっている.

素数 p に対し有限体 $K = GF(p)$ 上で定義される楕円曲線 $E_p(a,b)$ を考える. その位数 $\#E = \#E_p(a,b)$ に関して

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

が成立する (この式は $p-1$ 法におけるフェルマー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 $\mathbf{Z}/n\mathbf{Z}$ 上で考えることにする. 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 $E_n(a,b)$, 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. M が $\#E_p(a,b)$ の倍数になっている場合には, $E_p(a,b)$ でも $E_n(a,b)$ でも $MP = \mathcal{O}$ となるので, 計算が不可能となり, そこから p を求められる可能性がある. また $p-1$ 法の第 2 段階と同様に, ECM でも第 2 段階を考えることができる.

$p-1$ 法で素因数 p が見つけられるのは $p-1$ が smooth な場合であり, 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 を大きく設定し直すしかなかった. しか ECM では素因数 p が見つけられるのは $\#E_p(a,b)$ 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.

2.4 アルゴリズムの詳細

本節では実際の計算を行う上での高速化手法について述べる.

2.4.1 Montgomery 型楕円曲線

ECM では加算公式の計算量を減らすために, Weierstrass 型でなく, Montgomery 型楕円曲線

$$E_p(a,b) : by^2 = x^3 + ax^2 + x \quad (a^2-4)b \neq 0$$

を使用する [Montgomery87]. この型の曲線での加算公式は以下のようになる. ただし点 $P_0 = (x_0, y_0)$ の逆元を $-P_0 = (x_0, -y_0)$ とする (y 座標は使用しないので省略する):

加算:

$$x_2 = \frac{1}{x_2'} \frac{(x_0x_1 - 1)^2}{(x_0 - x_1)^2}$$

ただし $P_0=(x_0,y_0)$, $P_1=(x_1,y_1)$, $P_2=P_0+P_1=(x_2,y_2)$, $P_2'=P_0-P_1=(x_2',y_2')$.

2 倍算:

$$x_2=\frac{(x_0^2-1)^2}{4x_0(x_0^2+ax_0+1)}$$

ただし $P_0=(x_0,y_0)$, $P_2=2P_0=(x_2,y_2)$.

2.4.2 射影座標

前節の座標系での加法公式では逆元計算が必要となるため, 高速化させるには逆元計算をほとんど必要としない射影座標を使用する. Montgomery 型に対しては通常の射影座標が最適であり [Takeuchi-Koyama99], 上記のような y 座標を使用しない加法公式を用いる場合, Montgomery 型が最適である [Izu99a].

計算式は上の式に $x=X/Z, y=Y/Z$ を代入すれば良いが, ここでは省略する. 詳細は [Montgomery87] を参照されたい. Montgomery 型曲線を射影座標系で用いた場合, 加算は 6 回の乗余剰算で, 2 倍算は 5 回の乗算剰余で計算できる. しかし P_0 と P_1 の和を求めるのに P_2, P_2' が必要であることに注意しなければならない.

2.4.3 M の設定

ECM によって n の素因数 p が見つかるのは, 楕円曲線の位数 $\#E_p(a,b)$ が M の約数となるときである. しかし $\#E_p(a,b)$ はランダムに変化するため, 効率的に M を設定することは難しい. そこで M は $p-1$ 法と同様に, ある限界値 L_1 に対し

$$M=\prod_{p_i\le L_1} p_i^{e_i}\quad p_i^{e_i}\le \mathrm{LIMIT}<p_i^{e_i+1}$$

と設定するのが普通である. 楕円曲線での点のスカラー倍では $(M_1M_2)P=M_1(M_2P)$ が成立するので, 実際に M の値を計算する必要はない.

2.5 第 1 段階

与えられた楕円曲線 $E_n(a,b)$, 点 P, 整数 M に対し, 定数倍算 MP を計算する部分を第 1 段階という.

2 進展解法の利用: Montgomery 型楕円曲線において点のスカラー倍算を計算する場合, 加算に P_2' にあたる情報が必要となり, 通常の定数倍算で使用する加算鎖 (2 進展開法など) はそのままでは適用できない. そこで常に mP と $(m+1)P$ の 2 点を記憶しながら計算を進めていく方法が必要となる.

M の 2 進展開

$$M=2^{k-1}+m_1 2^{k-2}+\ldots+m_{k-2}2^1+m_{k-1}$$

に対し, 射影座標で表された点 P を用いて, 点列 $\{S_i\},\{T_i\}$ を

$$\begin{aligned} S_i &= (2^i+m_1 2^{i-1}+\ldots+m_{i-1}2^1+m_i)P \\ T_i &= S_i+P \end{aligned}$$

と定義する ($S_0=P, T_0=2P$). このとき $i=1,2,\ldots$ に対して以下の計算を行う:

$k_{i+1}=0$ のとき $S_{i+1}=2S_i, T_{i+1}=S_i+T_i$,

$k_{i+1}=1$ のとき $S_{i+1}=S_i+T_i, T_{i+1}=2T_i$.

補助情報 P_2' は常に P に等しいため, 常に Z 座標の値は 1 であり, 乗法の計算回数を減らすことができる [Angrew-Mullin-Vanstone93,Izu99b]. k ビットの整数 M による定数倍算に必要な乗算剰余の計算回数は $10k$ 回である.

2.5.1 第 2 段階

ECM の第 1 段階で素因数 p を見つけられるのは $\#E_p(a,b)|M$ となっている場合である. しかし p を求める確率を少しでも高めるために,

$$E_p(a,b)=q\prod_{p_i\le L_1} p_i^{e_i}\quad p_i\le L_1<q\le L_2$$

となっている場合への工夫がなされている. これ以降の部分を ECM の第 2 段階と呼ぶ.

以下, $Q=MP\neq\mathcal{O}$ として考える.

standard continuation 最も簡単なチェック法は, $L_1<q\le L_2$ を満たすすべての素数 q に対して qQ を計算し, $\gcd(Z(qQ),n)$ をチェックしていく方法である. このままでは gcd の計算回数が膨大なので, 実際には

$$\gcd\left(\prod_q Z(qQ),n\right)$$

を計算すれば良い．しかしこの方法は基本的には全数検索なので，効率は悪い．

Montgomery continuation $p-1$ 法の第2段階と同様の手法を用いるのが Montgomery continuation である．$L_1 < q \leq L_2$ を満たす q に対し

$$q = 420t \pm s \quad 0 \leq s < 210$$

となる (t,s) が一意に決まる．ここで q は大きな素数なので $\gcd(q,s)=1$ と仮定する．

第1段階で得られた曲線上の点 Q を用いて $Q_i = iQ$ とおく．仮定より $Q_q = qQ = \mathcal{O}$ となるので，$Z(Q_q) = Z((420t \pm s)Q) \equiv 0 \pmod{p}$ が成立する．したがって加法公式から

$$Z(420tQ)X(\pm sQ) - X(420tQ)Z(\pm sQ) \equiv 0 \pmod{p}$$

を得る．ここで $X(\pm sQ) = X(sQ)$，$Z(\pm sQ) = Z(sQ)$ だから，変形して

$$x(Q_{420t}) - x(sQ) \equiv 0 \pmod{p}$$

が成立することがわかる．

したがって Q が得られた段階で

$$Q_{420t} \ : \ \left\lfloor \frac{L_1}{420} \right\rfloor = t_1 \leq t \leq t_2 = \left\lceil \frac{L_2}{420} \right\rceil,$$
$$Q_s \ : \ 1 \leq s < 210, \ \gcd(s,210) = 1$$

を求めておき，積

$$u = \prod_{t_1 \leq t \leq t_2} \prod_{\substack{1 \leq s < 210, \\ \gcd(s,210)=1}} (x(Q_{420t}) - x(Q_s))$$

を計算しておけば，$\gcd(u,n)$ により素因数 p が求められる可能性がある．

なお $210 = 2 \times 3 \times 5 \times 7$ という数は，s の個数が少なくて済む，つまり $\phi(n)/n$ が小さい数から選ばれている．もっと大きな値（例えば $2310 = 2 \times 3 \times 5 \times 7 \times 11$, $30030 = 2 \times 3 \times 5 \times 7 \times 11 \times 13$ など）を用いると高速化が可能となる．

この方法は基本的には Shanks の Baby Step Giant Step 法なので，記憶容量との兼ね合いで効率が決まる．なお，Montgomery continuation を用いた場合の L_1, L_2 の最適値が [Silverman-Wagstaff93] に報告されている．

Brent continuation (The birthday paradox continuation) Brent は birthday paradox に基づく方法を提案している [Brent86]．点 Q は $qQ = \mathcal{O}$ を満たすので，Q のスカラー倍点は高々 q 通りしかない．したがって点列 $\{Q_i | Q_i$ は Q のスカラー倍, $1 \leq i \leq S\}$ がランダムであれば，$\{Q_i\}$ は q 通りの中からランダムに選ばれた S 個の点とみなすことができる．しかし，楕円曲線上の任意の点の x 座標と，その逆元の点の x 座標は等しいので，$\{Q_i\}$ の x 成分の集合は $(q+1)/2$ 通りの値の中からランダムに選ばれた S 個の値とみなせる．点列 $\{Q_i\}$ を，適当な関数 f を用いて $Q_{i+1} = f(Q_i)$ と定めて計算し，そして

$$u = \prod_{i=1}^{S-1} \prod_{j=i+1}^{S} (x_i - x_j)$$

を計算すれば，$\gcd(u,n)$ から p を求められる可能性がある．

Brent は関数 f の例として

$$Q_{i+1} = f_B(Q_i) = (s+ti)^e Q, \quad s,t : \text{乱数}$$

を提案している．また Kuwakado-Koyama は

$$Q_i = f_K(Q_{i-1}) = r_i^3 Q \quad r_i : \text{乱数}$$

を提案している [Kuwakado-Koyama96].

n が平方因子を持つ場合 n が平方因子を持つ場合に効果的な高速化手法が [Peralta-Okamoto96] で提案されている．これは $n = pa^2$ とあらわされるときに，Legendre 記号が

$$\left(\frac{x}{n}\right) = \left(\frac{x}{pa^2}\right) = \left(\frac{x}{p}\right)$$

となることを利用し，第2段階における mod p での合同数の探索部分を高速化させる手法である．

3 曲線の選択

ECM によって素因数 p が見つかるのは $\#E_p(a,b)$ が smooth になる場合であるが，実際にはこうなることは希である．このため使用する曲線の選択法が全体の効率を左右する．

Hasse の定理により $\#E_p(a,b)$ 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．ECM に

よって素因数 p が見つかるのは, $\#E_p(a,b)|M$ となる場合である. ここで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ると仮定すると, ランダムに動く部分のサイズは p から p/d に減少するので, $\#E_p(a,b)|M$ になりやすいことが期待できるこれは数ビット程度の貢献でしかないが, 実際の効果は大きい [Silverman-Wagstaff93].

実際には $d=8,12,16$ となる曲線の構成法が提案されている. 以下では $d=8,12$ となる曲線について述べる.

3.1 $d=8$

Montgomery は簡単な計算により $d=8,16$ となる曲線の生成法を示している [Montgomery87].

$B=A+2$ のとき点 $P=(1,1)$ は $E=E(A,A+2)$ 上の点で, 位数は 4 である. 実際 $2P=(0,0)$, $3P=(1,3)$, $4P=\mathcal{O}$ となる. つまり $E(A,A+2)$ は $\mathbf{Z}/4\mathbf{Z}$ と同型な部分群を持つ.

他方で, 適当な数 $u\neq 0,\pm 1$ に対して $A=u+\frac{1}{u}$ とおくと,

$$x^3+Ax^2+x=x(x+u)\left(x+\frac{1}{u}\right)$$

となり, $E=E(u+\frac{1}{u},B)$ は 3 つの位数 2 の点 $(0,0),(-u,0),(-\frac{1}{u},0)$ を持つ. つまり $E(u+\frac{1}{u},B)$ は $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ と同型な部分群を持つ.

よって, $A=u+\frac{1}{u}$ かつ $B=A+2=u+\frac{1}{u}+2$ とおくと, 曲線の位数は少なくとも 8 で割り切れることになる. (x_0,y_0) を曲線上の点とすると

$$y_0^2=\frac{x_0^2}{(u+1)^2}(u+x_0)\left(u+\frac{1}{x_0}\right)$$

より, $(u+x_0)(u+\frac{1}{x_0})$ が平方剰余でなければならない. これは, 例えば適当な数 r を用いて $u=\frac{x_0^2-r^2}{x_0(r^2-1)}$ とすることで

$$(u+x_0)\left(u+\frac{1}{x_0}\right)=\frac{r^2(x_0^2-1)^2}{x_0^2(r^2-1)^2}$$

となり, 実現可能である.

3.2 $d=12$

Montgomery は, 任意の Montgomery 型楕円曲線において $4|\#E(A,B)$ となることを導いた. 実際, x^2+Ax+1 の判別式 $A^2-4=(A+2)(A-2)$ が $GF(p)$ で平方剰余ならば, 曲線は x 軸で 3 点と交わるので, E は $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ と同型な部分群を持つ. $(A+2)(A-2)$ が平方非剰余ならば $B(A\pm 2)$ のどちらかが平方剰余で, 点 $(\pm 1,\sqrt{(A\pm 2)/B})$ の位数が 4 となる.

一方で Suyama は位数 3 の点の構成法を提案した. これらの結果を合わせることで $d=12$ の曲線の構成が可能となる.

曲線上の点 $P=(x_0,y_0)$ に対し $P_3=3P=(x_3,y_3)$ とおくと

$$\begin{aligned} x_3 &= \frac{x_0(x_0^4-6x_0^2-4Ax_0-3)^2}{(3x_0^4+4ax_0^3+6x_0^2-1)^2}\\ y_3 &= \frac{(x_0^4-6x_0^2-4Ax_0-3)g(x_0)}{By_0(3x_0^4+4Ax_0^3+6x_0^2-1)^3}\\ & g(x_0)\text{ は }x_0\text{の 11 次式}\end{aligned}$$

となる. したがって, 方程式 $3x^4+4Ax^3+6x^2-1=0$ の根 u と適当な数 v を用いて

$$A=\frac{-3u^4-6u^2+1}{4u^3},\quad B=\frac{(u^2-1)^2}{4uv^2}$$

とおけば. 点 (u,v) は曲線上の点でその位数は 3 となる (ただし A,B の条件から $uv(u^2-1)(9u^2-1)\neq 0$ でなければならない). このとき曲線の位数は 12 で割り切れる.

このとき y_0^2 の非平方部分は

$$g(x_0)=\left(4u^3x_0^3-(3u^4+6u^2-1)x_0^2+4u^3x_0\right)$$

となる. $g(x_0)$ を平方数にする実現方法はさまざま提案されている.

(1) Suyama-Montgomery [Motgomery87]

$$\begin{aligned} x_0 &= \frac{3}{4}u,\quad u=\frac{6r}{r^2+6},\\ g(x_0) &= \frac{u^2}{16}\left(\frac{r^2-6}{r^2+6}\right)^2\end{aligned}$$

(2) Montgomery-Brent [Motgomery87]

$$\begin{aligned} x_0 &= u^3,\quad u=\frac{r^2-5}{4r},\\ g(x_0) &= \frac{u^2(u+1)^2(u-1)^2}{4}\left(\frac{r^2+5}{r}\right)^2\end{aligned}$$

(3) Montgomery-Kida
[Motgomery87,Kida-Makino94]

$$x_0 = \frac{3u^2+1}{4u}, \quad u = \frac{2r}{3r^2-1},$$
$$g(x_0) = \frac{(u+1)^2(u-1)^2}{16u^2}\left(\frac{3r^2+1}{3r^2-1}\right)^2$$

4 まとめ

本稿では, 素因数分解アルゴリズムのうち楕円曲線法における高速化手法を考察した. 楕円曲線法は計算量が素因数に依存するタイプのうち最速であり, 合成数そのもののサイズが大きくても楕円曲線法が有効に働く場合がある.

参考文献

[Angrew-Mullin-Vanstone93] Angrew,G.B., Mullin,R.C., Vanstone,S.A., *An Implementation of Elliptic Curve Cryptosystems Over $F_{2^{155}}$*, IEEE J.of selected areas in communications, 11(1993),804-813.

[Brent86] Brent,R.P., *Some Integer Factorization Algorithms using Elliptic Curves*, Australian Computer Science Communications 8(1986),149-163.

[Izu99a] 伊豆 哲也, 楕円曲線暗号演算の計算法について, Proc. of 1999 SCIS, 275-280.

[Izu99b] 伊豆 哲也, 楕円曲線上のスカラー倍演算について, preprint.

[Kida-Makino94] 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.

[Koyama-Sizuya95] 小山謙二, 静谷啓樹, 素因数分解と離散対数アルゴリズム, 暗号・ゼロ知識証明・数論, 共立出版,1995.

[Kuwakado-Koyama96] 桑門 秀典, 小山 謙二, 改良楕円曲線法と素因数分解の実行結果, Proc. of 1996 SCIS, SCIS96-3A.

[Lenstra87] Lenstra Jr,H.W., *Factoring Integers with Elliptic Curves*, Annals of Math. 126(1987),649-673.

[Montgomery87] Montgomery,P.L., *Speeding the Pollar and Elliptic Curve Methods for Factorizations*, Math. of Comp. 48(1987),243-264.

[Peralta-Okamoto96] Peralta.R., Okamoto,E., *Faster Factoring of Integer of a Special Form*, IEICE Trans. Fundamentals, E79-A,No.4, April,1996, 489-493.

[Silverman-Wagstaff93] Silverman,R.D., Wagstaff Jr.,S.S., *A Practical Analysis of the Elliptic Curve Factoring Algorithm*, Math. of Comp. 61(1993),445-462.

[Takeuchi-Koyama99] Takeuchi,K., Koyama,K., *Fast Computation of Elliptic Curve Cryptosystems*, Proc. of 1999 SCIS, 281-284.

A 素因数分解のトピック

A.1 Cunningham Project

素因数分解を行う動機として, 自分で問題を見つけるよりも, 公開問題として与えられた整数を分解する方が面白いだろう. 世界で注目されている公開問題として Cunningham Project と RSA Challenge がある.

Cunningham projec とは, $b^n \pm 1$, $b = 2,3,5,7,10,11,12$ の型の整数の素因数分解を行うプロジェクトである. Fermat 数,Mersenne 数,repunits などはこの型をしているので, 対象としているかなり範囲は広いと言える. 分解結果は単行本として 1983 年 (第 1 版),1988 年 (第 2 版) に発行されている. 現在は第 3 版を準備中である. Cunningham Project は世界最大規模の公開問題であり, 有名無名をこえて世界中の素因数分解者が挑戦を続けている. しかし整数の型に特殊な条件を課しているため, Cunnningham Project の記録がそのまま素因数分解の記録になるわけではない.

A.2 RSA Challenge

米国の RSA 社によって 1993 年に公開された懸賞つき素因数分解問題が RSA Challenge [1] である. RSA 社は RSA 暗号の考案者たちが設立した会社であり. RSA Challenge は RSA 暗号の安全性を示す目的で始められた.

RSA Challenge は RSA ploblem と partition ploblem の 2 系統の問題からなる. RSA problem と呼ばれる問題では $n = pq$ なる合成数 n を素因数分解することが要求されている. 公開されている n の桁数は 100 桁から 500 桁までの 10 桁きざみの 41 問と, 1997 年 2 月に追加された 155 桁,232 桁,309 桁,617 桁 の 4 問の計 45 問からなり (さらに非公式で追加された 129 桁の問題もある), 桁数をとって RSA-100 のように表記する. このうち既に分解された問題は RSA-100,RSA-110,RSA-120,RSA-129,RSA-130,RSA-140, だけである.

一方の partition problem は $n = p(m)$ なる合成数の素因数分解である. 整数 m の partition number $p(m)$ とは, m を正整数の和で表せる場合の数として定義する. 数列 $p(m)$ は m に関する増加列となるが, 値に規則性は見られない (そうである). $p(m)$ の素因数分解は, m によって簡単な場合もあれば難しい場合もあるが, 桁数が同じ場合,RSA problem よりも難しくはならないことが予想されている. RSA ploblem が専門家向けなのに対し, Partition problem は一般向けといった位置付けになっている.

A.3 円分数

日本で始まったプロジェクトとして, 円分数の素因数分解プロジェクトがある. このプロジェクトは ICU 大学の森本光生先生, 立教大学の木田祐司先生を中心に進められている, 円分数とは $x^m - 1$ であらわされる整数の約数で, 部分的に Cunningham 数と重なっている. 分解結果は単行本として 1987 年 (その 1),1989 年 (その 2),1992 年 (その 3),1999 年 (その 4) に出版されている. また円分数プロジェクトではアルゴリズムの改良が活発に行われており, 上記の単行本には素因数分解アルゴリズムを実装する上での最先端のテクニックが記載されている.

[1] 最近では暗号解読の RSA Challenge の方が有名になっているが, もともとはこちらが先に始まっている.