大東文化大学紀要41号

虚数乗法をもつ楕円曲線とj-不変量について

永田　清

On CM-type elliptic Curves and j-invariant.

Kiyoshi Nagata

概要

現在の高度情報化社会において，重要な役割を果たす公開鍵暗号の一つである楕円暗号方式について，その構成法と数学的理論の関係を考察する。特に，類体論や楕円曲線の理論がどのように現実的な事柄と結びついていくかを明らかにすることが本論文の目的である。

1. はじめに

1976年にW. DiffieとM. Hellman[1]によって提案された公開鍵暗号方式の考え方は，それまで第3者に知られないように，送受信者間で大切に保管しておかなければならなかった“鍵”と呼ばれる秘密情報の扱いを根本的に変えた。その結果として，多人数で構成される情報ネットワークにおける鍵の管理が1人一つとなり，鍵の配信といった厄介な問題も解決される。また，秘匿通信手段としての暗号が，相手の認証や文書の非否認性などにも応用されるようになった。この方式の基本は，暗号化する鍵と，それをもとに戻す（“復号化”）鍵とを別のものにすることである。それにより一度鍵を掛け暗号化すると，たとえ本人であっても，復号化することができなくなる。復号化できるのは，暗号化鍵とは違う復号化鍵を持っている人だけであり，よって暗号化鍵は公開しても問題がない。この意味で，公開鍵暗号方式と呼ばれるこの方式は，もう一つの大きな利点である“認証”を可能にする。ある情報を自分しか知らない鍵（秘密鍵）で暗号化すると，その情報は公開しているもう一つの鍵（公開鍵）で復号化できるので，誰でもその情報の中身を知ることができる。しかし，秘密鍵と公開鍵は対を成しているので，ある公開鍵で復号化し意味のある情報に戻すことができる暗号文は，対応する秘密鍵で暗号化した情報だけである。つまり，暗号化した人が，確かに対応する秘密鍵の所持者であることが認証される。

DiffieとHellmanのアイデアを実現するには，次のようなパラメータkを含む二つの関数で，

一方のパラメータから他方が簡単には計算できないものを用意する。

$$f(k_e, g(k_d, M)) = M,\ g(k_d, f(k_e, M)) = M$$

ここで，Mは送りたい情報であり，$(k_e,\ k_d)$は鍵の対である。実際は，二つの関数f, gは同じものが使われる場合がほとんどであるが，異なるものでも構わない。ただし，どのような関数を使っているかは公開する。問題は，一方の鍵からもう一方の鍵が“簡単には”計算できないという点である。例えばf, gを計算するために必要な情報とk_eの値が与えられても，有効な時間と計算資源の範囲では，対応するk_dが求められないことが必要である。また，逆に鍵の対を生成するためには，特殊な情報さえあれば，うまくk_eからk_dを計算できるような仕組みを考え出さなければならない。

Diffie と Hellman の論文には示されていなかった具体的な実現方法は，1978年に 3 人の数学者 R. Rivest, A. Shamir および L. Adleman[2]によって提示された。これは，現在でも広く使われている RSA 公開鍵暗号方式と呼ばれるもので，Euler の定理を使っている。扱う対象は二つの大きな素数の積nを法とした剰余環Z/nZの要素であり，計算の難しさを与える問題は，ある要素を与えたときにそのk_e乗根を求めることである。Euler の定理より，$k_e k_d \equiv 1 \bmod \varphi(n)$を満たす$k_d$を求めれば$k_e$乗根を計算することができるが，そのためには Euler 関数の値が必要である。整数nの二つの素因子がわかっていれば Euler 関数値もすぐに計算できるが，そうでない場合は良い方法が見つかっていない。また素因数分解に関しては，数々の方法が知られているが，それらはいくつかの場合にあてはまるnに対して使えるもので，従ってそれらの場合を避ければ，安全であろうと考えられている。

RSA と並んで，良く使われるタイプの暗号方式が ElGamal 方式[3]と呼ばれるものである。この場合は，合成数ではなく（大きな）素数pを法とする剰余環，つまり標数pの素体を扱う。pより小さい二つの数g, xを適当に選び，$y = g^x \bmod p$を計算する。公開する情報はy, gおよびpであり，xは個人の秘密鍵である。暗号化して送りたい情報（メッセージ）をMとすると，送信者は受信者の公開情報を使って次の二つを計算し，対にして受信者に送る。

$$a = g^k \bmod p,\ b = y^k M \bmod p$$

受信者は，

$$M = b/a^x \bmod p$$

を計算できる。ここでは，素体における離散対数問題の難しさが安全性を保証している。

上記のような方法は，素体でなくても実現できる。一般の可換群において，ある要素とその整数乗（整数倍）を与えたときに，べき指数（倍数）を求めることが難しければ，つまりその群における離散対数問題が難しいなら，ElGamal 方式だけでなく，いくつかの方式による暗号化，認証，署名，鍵交換なども安全性を保証されて実現できる。その中で有力なものが，楕円曲線や超楕円曲線の Jacobi 群であるが，ここでは特に楕円曲線を扱う。

2. 楕円曲線と暗号

有限体上の楕円曲線を用いた暗号方式は，1986年頃V. Miller[4]とN. Koblitz[5]の二人によって独立に提案された。有限体そのものを扱う場合に比べ優れていると思われる点は次のようなものである。

・有限体を一つ決めても，その上に多くの楕円曲線が構成できる
・同程度の安全性[1]を確保するために必要な，鍵のサイズが小さくてすむ
・有限体上の離散対数問題に対し使える“Index Calculus”の技法が楕円曲線に対しては有効に使えない

近年暗号の用途は多種多様にわたり，ICカードのような処理速度やメモリに関してあまり高い性能を期待できないメディアにも実装することが求められている。そのためには，鍵サイズが小さく，演算をおこなう体のサイズも小さい方が望ましい。また，多くの暗号が必要となるが，上記1，2番目の性質はその用件にかなうものである。

“Index Calculus”は，有限体上の離散対数問題を，体の個数の桁に対する準指数時間で解く方法であり，素数全体の集合が自然数の独立な生成系になることを利用し，予め何番目かまでの素数に対する離散対数を求めておいて，$g^r y \bmod p$がそれらの生成する整数になるようなrを求めることによって，$y=g^x \bmod p$となるxを求める方法である[6][7]。Millerは[4]において，楕円曲線を扱う場合にはこの方法が適用できないことを述べている。それは，Mordell–Weil群（より一般にはJacobi群）のランクがあまり大きくならないことによっている。

上記のような利点を持つ楕円曲線暗号ではあるが，素因数分解や有限体の離散対数問題ほど単純でなく，楕円曲線自体が数学的に非常に深い意味を持っているためか，いくつかの問題点も指摘されている。

・位数の大きな曲線の生成
・加法や整数倍算の高速化
・特殊なタイプの曲線を避ける工夫

特に安全性に関して重要なことは，最後に挙げた事柄であろう。現時点では，Supersingular curveとAnomalous curveは避ける必要がある。前者は，MOV攻撃[7]によって比較的小さい有限体の離散対数問題に帰着されてしまい，前述のように準指数時間で楕円離散対数が求まってしまう。後者はかなり特殊なタイプの曲線で，位数の大きな，それも素数位数の曲線を単純に生成しようとしたものであるが，やはり特殊なものであるだけに，特殊な性質を持ち，多項式時間のアルゴリズムが考案されてしまった[8][9]。

上記の問題を解決するための一つの手段が，虚数乗法の理論を使った楕円曲線の構成法である。

[1] ここでの“安全性”は，絶対的なものではなく単純な攻撃で必要な回数などを意味する

3. 楕円曲線の構成

まず楕円曲線の一般論を簡単に復習しておこう。ここでは，標数が2や3でない体 k を固定し，k の代数閉包を $\bar{k}$ とする。このとき，

$$E : y^2 = x^3 + Ax + B,\ A,\ B \in k,\ \Delta = -16(4A^3 + 27B^2) \neq 0$$

を k 上の楕円曲線という。この式を満たす2点 $P_1(x_1,\ y_1)$，$P_2(x_2,\ y_2)$ に対し，この2点を通る直線と E との3番目の交点を $P'_3(x_3, -y_3)$ としたとき，$P_1 + P_2 = P_3 = (x_3,\ y_3)$ で和を定義することにより，E は可換群となる。この群は楕円曲線の Mordell-Weil 群を呼ばれるが，特に混乱する恐れがないときは，単に楕円曲線 E と呼ぶことにする。また，x，y 成分が共に k の元である点全体も部分群をなし，これを $E(k)$ と書く。

楕円曲線の別の表し方として，複素平面 $\mathbb{C}$ 上の格子点によるものを考える。虚2次体 $K = \mathbb{Q}(\sqrt{-D})$ を一つ決めると，K のイデアル類群 $C_K = I_K/P_K$ の代表系と K の元で基本領域 $H/SL_2(\mathbb{Z})$ に入るもの（"簡約された2次無理数"）とが次のように1対1に対応する。

$$\bar{A} = {}_{\mathbb{Z}}\left\langle a, \frac{-b+\sqrt{-D}}{2} \right\rangle \in C_k \leftrightarrow \tau = \frac{-b+\sqrt{-D}}{2a} \in H/SL_2(\mathbb{Z})$$

ただし，a，b は $-D = b^2 - 4ac$ となる c が存在して，$|b| \leqq |a| \leqq c$ で，どちらかの等号が成立するのは $b > 0$ のとき，となるような整数である。

ここで，格子 $L = \mathbb{Z} + \tau\,\mathbb{Z}$ と置くと，$E_L = \mathbb{C}/L$ が一つの楕円曲線となる。E_L の自己準同型環 End (E_L) は，格子 L を不変にする $\mathbb{C}$ の要素であり，$z \in \mathbb{C}$ が $zL \subseteq L$ を満たせば，$z \in L \subset K$ となる。また，

$$z\begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} s & t \\ u & v \end{pmatrix}\begin{pmatrix} 1 \\ \tau \end{pmatrix} (s, t, u, v \in \mathbb{Z})$$ より，z は $$\det\begin{pmatrix} X-s & t \\ u & X-v \end{pmatrix} = 0$$ の根であり，よって代数的整数となる。逆に，$z = \dfrac{-b+\sqrt{-D}}{2}$ つまり O_K の有理整数でない基底とすれば，

$$z\tau = \frac{1}{4a}(D(b-1) - (D+b)\sqrt{-D})$$ であり，また $D \equiv -b^2 \bmod 4a$ を使えば，$z\tau$ の分子は

$$D(b-1) - (D+b)\sqrt{-D} \equiv b(b-1)(-b+\sqrt{-D}) \bmod 4a$$

となる。よって，$z\tau \in L$ が示され，End $(E_L) = O_K$（K の整数環）となる。

このように，自己準同型環が虚2次体 K の整数環（または，その部分環）となる楕円曲線を，虚数乗法を持つ楕円曲線，または CM（Complex Multiplication）曲線という。

格子によるものと，x，y の2変数多項式表示によるものは，Weierstrass の $\wp$ 関数によって関係付けられる。格子 $L = \mathbb{Z} + \tau\mathbb{Z}$ に対し，Eisenstein 級数

$$G_{2k}(L) = \sum_{(m,n) \neq (0,0)} \frac{1}{(m\tau+n)^{2k}} \quad (k = 1, 2, \ldots)$$

を定義し，Weierstrass の $\wp$ 関数を

$$\wp_L(z)=\frac{1}{z^2}+\sum_{0\neq\omega\in L}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)$$

とする。このとき，次の対応がある，

$$z+L\in E_L\leftrightarrow(\wp_L(z),\frac{1}{2}\wp_L'(z))\in E\ :\ y^2=x^3-\frac{g_2}{4}x-\frac{g_3}{4}$$

ただし，$g_2=60G_4(L)$，$g_3=140G_6(L)$。また，楕円曲線の大切な不変量である j- 不変量は，次のように定義される，

$$\Delta=g_2{}^3-27g_3{}^2,\ j=1728\frac{g_2{}^3}{\Delta}=q^{-1}+744+\sum_{1\leq n}c_nq^n\quad(q=e^{2\pi iz})。$$

このとき，代数閉体上の二つの楕円曲線が同型であるための必要十分条件は，j- 不変量が等しいことである。

ここまで楕円関数の一般論を一通り復習したが，暗号などに使うためには有限体を決めて，その上の楕円曲線を考えなければならない。有限体の標数を p とすると，p は虚 2 次体 K において次の条件を満たすように決められる。

(p の条件 1)

K において，相異なる二つの単項イデアルの積に分解する。

つまり，ある整数 A，B があって，$4p = A^2 + B^2D$ となる。

与えられた p が条件を満たすかどうかは，まず p が mod D で平方剰余かどうかを調べ，その場合に条件を満たす A，B が存在するかどうかを調べる。ここで p に対するもう一つの条件を設定する。

(p の条件 2)

p は十分大きく，また $m = p + 1 \pm A$ が大きな素因数を持ち次の(1)，(2)を満たす：

(1) $m \neq p$

(2) $p^n \equiv 1 \mod m$ となる小さな数 n が存在しない

(1)は Anomalous curve にならないための条件，(2)は MOV 攻撃を避けるために設けられた条件である。この条件は，楕円曲線の構成そのものにではなく，安全性にかかわって設けられている。

構成に必要なのは条件 1 であり，次の定理を根拠とする。

定理 I　p を素数とするとき，次の条件は同値である。

(1) p は条件 1 を満たす

(2) イデアル (p) は，K の Hilbert 類体 K_H において完全分解する

(3) Hilbert 多項式 $H_D(X)$ は，素体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ において相異なる一次式の積に完全分解する

この定理を証明する前に，Hilbert 類体と Hilbert 多項式に関する虚数乗法の定理を証明なしで述べておく[10]。

定理Ⅱ　K_H を虚 2 次体 $K = \mathbb{Q}(\sqrt{-D})$ の最大不分岐 Abel 拡大（“Hilbert 類体”）とする。

このとき，$K_H = K(j(\omega_r))$ となる。ここで，ω_r は K の簡約された 2 次無理数の一つであり，K の類数を h_K としたとき，$1 \leqq r \leqq h_K$ である。また，$j(\omega_r)$ の最小多項式（“Hilbert 多項式”）を $H_D(X)$ とすれば，

$$H_D(X) = \prod (X - j(\omega_r)^{\sigma c}),\ j(\omega_r)^{\sigma c} = j(\omega(c_r)^{\sigma c}) = j(\omega(c^{-1}c_r))\ (c, c_r \in C_k)$$

となる。

（定理Ⅰの証明）

p が(1)を満たす有理素数であるとすると，K の単項イデアル群 P_K の元 P_1，P_2 で $(p) = P_1P_2$ となるものが存在する。

K_H/K はイデアル類群 C_K に対応する類体であるから，Aritin 写像による次の同型対応がある。

$$Gal(K_H/K) \cong C_K$$
$$\left(\frac{K_H/K}{P}\right) \leftrightarrow c_P$$

また，

$$<\left(\frac{K_H/K}{P}\right)> = Z_P = \{\sigma \in Gal(K_H/K) : \wp^{\sigma} = \wp, \forall \wp \mid P\}\ (\text{分解群}),\ g = \#Gal(K_H/K)/Z_P$$

ここで，g は K のイデアル P が K_H において分解するイデアルの個数を表す。

いま $P = P_1$（または P_2）とすると，$c_P = 1$ であることより，$Z_P = 1$ となり $g = \#Gal(K_H/K)$ が成り立つ。よって，P は K_H において完全分解する。このことは，Hilbert 多項式 $H_D(X)$ が modp で単根のみを持つこと，すなわち(3)，と同値である。

逆に，(p) が K_H で完全分解するなら，(p) を割る K の任意のイデアルは K_H で完全分解しなければならない。ここで，

$$Z_P = 1 \Leftrightarrow \left(\frac{K_H/K}{P}\right) = 1 \Leftrightarrow c_P \in P_K$$

であることより，(1)がいえる。（証明終わり）

定理Ⅰより，条件 1 を満たすように p を選んだとき，Hilbert 多項式は $\mathbb{F}_p$ において K の類数 h_K 個の根を持つ。その一つ j_0 を取り，j_0 が 0 や1728でないとき，

$$E : y^2 = x^3 + 3kx + 2k,\ k = \frac{j_0}{1728 - j_0}$$

とすると，Eはj-不変量が丁度j_0の楕円曲線となり，しかもその位数が条件2で定めたmになることが期待される。この位数に関する部分は楕円曲線のFrobenius写像π_pがイデアルPと同一視されることと，式[11]

$$\#E(F_p) = P + 1 - Tr(\pi_p)$$

から導かれる。

4. 終わりに

暗号などに有用な楕円曲線の構成法を，理論を中心にみてきた。実際の計算においては，イデアルの分解，Hilbert多項式の近似値による計算などを工夫しておこなっている。また，SEA法のように任意に曲線を与え，その位数を高速に計算する方法があり，現在ではそちらが有効とされている。

しかし，代数体の類体論，特に虚数乗法の理論，といった数学的に非常に深い事柄をきれいに結びつけている点で，この方法は興味深く，種数の大きい超楕円曲線に対しても，不変量をうまく使うことで構成法が考えられている。

[1] W. Diffie and M. E. Hellman, "New direction in Cryptography," IEEE Transaction on Information Theory, v. IT-22, n.6, Nov. 1976, pp. 644-654.

[2] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signature and Public-Key Cryptosystems," Communication of the ACM, v.21, n.2, Feb. 1978, pp. 120-126.

[3] T. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," Advances in Cryptology, Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 10-18.

[4] V. Miller, "Use of elliptic curves in cryptography," Advances in Cryptology, Proceedings of CRYPTO 85, Springer-Verlag, 1986, pp. 417-426.

[5] N. Koblitz, "Elliptic curve cryptosystems," Math. Comp., 48, 1987, pp. 203-209.

[6] L. Adleman, "A subexponential algorithm for the discrete logarithm problem with applications to cryptography," Proc. 20th IEEE Found. Comp. Sci. Symp., 1979, pp. 55-60.

[7] J. H. Silverman and Joe Suzuki, "Elliptic Curve Discrete Logarithms and Index Calculus," Proceedings of Asiacrypt 98, Springer-Verlag, 1999, pp. 110-125.

[7] A. J. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", IEEE Transaction on Information Theory, v. 39, n. 5, Sep. 1993, pp. 1639—1646.

[8] T. Satoh and K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves," Comm. Math. Univ. Sancti Pauli, 47, 1998, pp. 81-92.

[9] N. P. Smart, "The discrete logarithm problem on elliptic curves of trace one," Journal of Cryptology, Vol. 12, 1999, pp.193-196.

[10] J. H. Silverman, "Advanced Topics in the Arithmetic of Elliptic Curves," GTM 151, Springer-Verlag, 1994.

[11] J. H. Silverman, "The Arithmetic of Elliptic Curves," GTM 106, Springer-Verlag, 1986.