二次曲線に基づく公開鍵暗号について

内山 成憲

NTT 情報通信研究所

uchiyama@sucaba.isl.ntt.co.jp

1 はじめに

$a\ (>0), b \in \mathbf{Z}$, $D = a^2 - 4b \neq 0$ に対して

$$L_0(a,b) = 2,\ L_1(a,b) = a,\ L_{n+1}(a,b) = aL_n(a,b) - bL_{n-1}(a,b)\ (n \geq 1),$$

$$F_0(a,b) = 0,\ F_1(a,b) = 1,\ F_{n+1}(a,b) = aF_n(a,b) - bF_{n-1}(a,b)\ (n \geq 1)$$

で定まる数列の組 $(L_n(a,b), F_n(a,b))$ は a, b に関する同伴 Lucas 数列と呼ばれるが[1]，これらは二次方程式 $t^2 - at + b = 0$ の二つの根を α，β とすると，それぞれ次のように書ける

$$L_n(a,b) = \alpha^n + \beta^n,\ F_n(a,b) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{1}$$

この数列の組は多数の面白い性質を持っているが [6]，その中でもとりわけ重要な性質として，次の加法定理を持つ

$$\begin{aligned} 2L_{m+n} &= L_mL_n + DF_mF_n, \\ 2F_{m+n} &= F_mL_n + L_mF_n \end{aligned} \tag{2}$$

これらは，よく見ると三角関数の加法定理と似ていることが分かる．実際，三角関数は単位円 S^1 をパラメータ表示しているが $(L_n(a,b), F_n(a,b))$ は，(1) により，二次曲線 $x^2 - Dy^2 = 4b^n$ 上の点とみなすことが出来，特に $b = 1$ として，二次曲線 $C_D : x^2 - Dy^2 = 4$ を取れば，これは Pell 方程式と呼ばれるもので，二次形式による自然数の表現に関する研究などとの関係からよく知られている二次の不定方程式であるが，$(\pm L_n(a,1), \pm F_n(a,1))$ は，この二次曲線上の有理整数点であって，つま

[1]特に $(F_n(1,-1))_{n\geq 0}$ は，Fibonacci 数列である．

り，$C_D(Z)$ のパラメータ表示を与えると考えることも出来る．また，(2) で与えられる加法定理を用いることによって $C_D(Z)$ には加法が定義され，単位元が $(2,0)$，点 (x,y) の逆元が $(x,-y)$ である abel 群となる．

さて，この Lucas 数列は，いわゆる $N+1$ 法と言われる素数判定法や，$p+1$ 法といった素因数分解にも用いられているが [2] [7]，ここでは RSA 型の公開鍵暗号として知られる Lucas 数列を用いた公開鍵暗号 LUC [8] [9] について（これは上述のように二次曲線上の加法を用いているともみなせるが），その整数論的性質を調べ，低指数攻撃が可能な事や RSA との関係について述べる．

まず最初に Section 2 で，二次曲線 C_D の有限体 $\mathbf{F}_q$- 有理点の全体 $C_D(\mathbf{F}_q)$ や，自然数 n を法とした剰余類環 Z/nZ- 有理点の全体 $C_D(Z/nZ)$ について述べる．

次に，Section 3 で LUC の定義をし，Section 2 で得られた結果を用いて LUC の幾つかの表現を与え，Section 4 で RSA との関係や LUC への低指数攻撃ついて述べる．

2 二次曲線 C_D

ここでは，r を自然数，p を奇素数として $q=p^r$ とおき，さらに，n を奇数として Section 1 で定めた $C_D(\mathbf{F}_q)$，$C_D(Z/nZ)$ について考察する．但し，p，n ともに D と互いに素であるとする．最初に，$C_D(Z)$ が abel 群であることから $C_D(\mathbf{F}_q)$，$C_D(Z/nZ)$ がともに有限 abel 群になることに注意しておく．

2.1 $C_D(\mathbf{F}_q)$

まず，$r=1$ の場合の $C_D(\mathbf{F}_p)$ について．

この群がどんな群であるかを見る前に，位数を求めてみる．一般に与えられた有限体上の曲線の位数を，初等的な方法で求めることは難しいと思われるが，この場合は比較的容易に求まる．

$$\#C_D(\mathbf{F}_p)=\sum_{y=0}^{p-1}\left\{\left(\frac{4+Dy^2}{p}\right)+1\right\}=p+1+\sum_{y=1}^{p-1}\left(\frac{4+Dy^2}{p}\right)$$

すなわち，この最右辺の指標和の部分をきちんと求めてやれば良い．但し，$\left(\frac{-}{p}\right)$ は Legendre 記号を表すものとする．

これは， Euler の規準を用いて

$$\begin{aligned}\sum_{y=1}^{p-1}\left(\frac{4+Dy^2}{p}\right) &\equiv \sum_{y=1}^{p-1}(4+D)^{\frac{p-1}{2}} \pmod p\\ &\equiv \sum_{y=1}^{p-1}\sum_{i=0}^{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{i}4^{\frac{p-1}{2}-i}D^i y^{2i} \pmod p\\ &\equiv -4^{\frac{p-1}{2}}-D^{\frac{p-1}{2}} \pmod p\\ &\equiv -1-\left(\tfrac{D}{p}\right) \pmod p\end{aligned}$$

すなわち

$$\sum_{y=1}^{p-1}\left(\frac{4+Dy^2}{p}\right)\equiv -1-\left(\frac{D}{p}\right) \pmod p$$

が成り立つことが分かる．ここで左辺の指標和の取り得る値の範囲などを考えると，等号が成立して

$$\sum_{y=1}^{p-1}\left(\frac{4+Dy^2}{p}\right)=-1-\left(\frac{D}{p}\right)$$

となり， $C_D(\mathbf{F}_p)$ の位数は次で与えられる．

Lemma 2.1

$$\#C_D(\mathbf{F}_p)=p-\left(\frac{D}{p}\right) \tag{3}$$

が成り立つ．

次に，この有限 abel 群は一体どんな群であろうか？有理整数環上の場合からの類推から，この場合は $\mathbf{F}_p(\sqrt{D})$ の乗法群 $\mathbf{F}_p(\sqrt{D})^*$ への，中への同型写像が存在することが予想されるが，実際，次が成立する．

Theorem 2.1 単射準同型

$$C_D(\mathbf{F}_p)\ni(x,y)\longmapsto\frac{x+\sqrt{D}y}{2}\in\mathbf{F}_p(\sqrt{D})^*$$

が存在する．

即ち， Lemma 2.1 と合わせれば，次が得られる．

Theorem 2.2 $C_D(\mathbf{F}_p)$ に対して

$\left(\frac{D}{p}\right)=1$ の時

$$C_D(\mathbf{F}_p)\cong\mathbf{F}_p^*,$$

$\left(\frac{D}{p}\right)=-1$ の時

$$C_D(\mathbf{F}_p)\cong\mathbf{F}_{p^2}^*/\mathbf{F}_p^*$$

が成り立つ．

従って，$C_D(\mathbf{F}_p)$ は，位数が $p+1$ か $p-1$ の巡回群である．

一般の場合も $C_D(\mathbf{F}_q)$ は乗法群 $\mathbf{F}_q(\sqrt{D})^*$ への，中への同型が得られ，$\sqrt{D}$ が $\mathbf{F}_q$ に属するか，しないかに従って，位数が $q-1$ か $q+1$ の巡回群になる．

以上のことから次が分かる [4].

Corollary 2.1 有限体上の二次曲線 $C_D(\mathbf{F}_q)$ における離散対数問題は，高々 $\mathbf{F}_{q^2}^*$ におけるそれに帰着される．

2.2 $C_D(Z/nZ)$

n の素因数分解を $n=\prod_{i=1}^{s} p_i^{e_i}$ とすると，中国人剰余の定理により

$$C_D(Z/nZ) \cong \prod_{i=1}^{s} C_D(Z/p_i^{e_i}Z)$$

が成り立つことが分かる．つまり $C_D(Z/p^eZ)$ に対して調べればよい．この群の位数は，剰余類環 Z/p^eZ から Z/pZ への自然な写像を考えることによって求められ，また，Theroem 2.1 と同様の準同型写像が環 $(Z/p^eZ)[\sqrt{D}]$ の単数群に対して作れることから，次が成り立つ [2].

Theorem 2.3 位数は

$$\#C_D(Z/p^eZ) = p^{e-1}\left(p-\left(\frac{D}{p}\right)\right)$$

であり，

$$C_D(Z/p^eZ) \cong Z/p^{e-1}(p-(\tfrac{D}{p}))Z$$

が成り立つ．

特に，$(\frac{D}{p}) = 1$ であれば，$C_D(Z/p^eZ)$ は p^e を法とした既約剰余類群 $(Z/p^eZ)^*$ に同型であることが分かる．

ここで，$C_D(Z/nZ)$ の位数を $\varphi_D(n)$ とすれば，これは Lehmer-Euler の関数と呼ばれるもので，Lucas 数列における Euler の totient 関数 $\varphi(n) = \sum_{1\le d\le n,(d,n)=1} 1$ に対応するものであって，二次体 $K=Q(\sqrt{D})$ との関係を考えると次が成り立つ．

Corollary 2.2 奇数 n の素因子がすべて，二次体 $Q(\sqrt{D})$ で分解するとき

$$\varphi_D(n) = \varphi(n)$$

が成り立つ．

また，二次体 K の整数環を Z_K とするとき， φ_K を K における Euler 関数，即ち，Z_K において，そのイデアル I を法とした既約剰余類群の位数を $\varphi_K(I)$ で表すことにすると，次が成り立つ.

Corollary 2.3 Z_K の単項イデアル (n) に対して

$$\varphi_K((n)) = \varphi(n)\varphi_D(n)$$

が成り立つ.

これは， (n) が K でどう分解されるかを見れば，簡単に分かる.

さて， $C_D(Z/nZ)$ などについて調べ終った段階で， Lucas 数列による素数判定法や $p+1$ 法を，ここでの立場から見直してみると，奇数 N に対して， Pocklington-Lehmer の $N-1$ 法の Lucas 数列を用いた analogy が Lucas 数列を使った $N+1$ 法になり， $p-1$ 法の analogy が $p+1$ 法となることが， $(Z/NZ)^*$ の代わりに， $(\frac{D}{N}) = -1$ (Jacobi 記号) なる D をとった時の $C_D(Z/NZ)$ を用いたものだと考えれば，理解しやすいように思われる [2].

今まで，性質を調べるために，二次体の単数群への埋め込みを利用したが， Section 1 で述べたように，二次形式の自己同型群への埋め込み，すなわち， Z 上の 2×2- 型の行列で，行列式が 1 となるものの全体のなす群 $SL_2(Z)$ への埋め込みによれば，次が成り立つ

Theorem 2.4

$$C_D(Z) \ni (x,y) \longmapsto \begin{pmatrix} \frac{x-ay}{2} & -y \\ y & \frac{x+ay}{2} \end{pmatrix} \in SL_2(Z)$$

なる単射準同型が存在する．ここで， $D = a^2 - 4$ であった.

すなわち，次が言える.

Corollary 2.4 $C_D(Z/nZ)$ は， $SL_2(Z/nZ)$ の部分群と見なせる.

また，この $SL_2(Z/nZ)$ に対しては次が成り立つことも知られている.

Theorem 2.5

$$\#SL_2(Z/nZ) = n^3 \prod_{p|n}(1 - \frac{1}{p^2})$$

二次曲線 C_D 上の加法が，すなわち Lucas 数列における加法が，行列の乗法から得られるということは，三角関数からの analogy としてみても，自然に理解出来ると思われる.

この Section の最後にもう一つだけ注意しておくと，上述の，行列の乗法と， Lucas 数列の加法との関係からも分かるが， Lucas 数列 $(L_m(a,1))_{m\geq 0}$ は， a の m 次の多項式で書ける [5]. 実際，次が成り立つ.

Theorem 2.6 X を不定元として， $T_m(X)$ を m 番目の第一種の $Tchebychev$ 多項式とすれば，次が成り立つ.

$$L_m(a,1) = 2T_m(\frac{a}{2}) \tag{4}$$

ここで， $T_m(X)$ は， cos の m 倍角の公式を与える多項式で，次で定義されるものである.

$$T_m(X) = \sum_{i=0}^{[\frac{m}{2}]} \binom{m}{2i} X^{m-2i}(X^2-1)^i \tag{5}$$

[ ] は Gauß 記号を表すものとする.

3 公開鍵暗号 LUC

ここでは， P. Smith 等によって提案されている RSA 型の公開鍵暗号 LUC について説明する.

$n = pq$ （p,q は大きな素数）， e を $p\pm 1, q\pm 1$ と互いに素な自然数とし

$$ed \equiv 1 \pmod{l.c.m.(p\pm 1, q\pm 1)}$$

（符号はすべての組合せを取る）

で d を定める.

この時， RSA 暗号と同様に (n,e) を公開鍵， (p,q,d) を秘密鍵として，次のように，暗号化と復号を定める.

平文 m に対し， Lucas 数列 L_k を用いて

$$c \equiv L_e(m,1) \pmod{n}$$

で暗号化.

復号は

$$m \equiv L_d(c,1) = L_d(L_e(m,1),1) \pmod{n}$$

で与えられる.

これで復号出来ることは，加法定理を少し変形した

$$L_{l+k}(a,1) = L_l(a,1)L_k(a,1) - L_{l-k}(a,1) \ \ (l \geq k) \tag{6}$$

を用いて帰納的に

$$L_{kl}(a,1) = L_k(L_l(a,1),1)$$

が成立することが分かり，上の場合は ed が $L_k \bmod n$ の周期を法として 1 と合同なので

$$L_{de}(m,1) \equiv L_1(m,1) \pmod{n} \tag{7}$$

が成立することから分かる.

ここで，少しこのアルゴリズムについて， Section 2 で調べてきたこと用いて見直して見ると，次のように書ける.

Proposition 3.1 上述の LUC の暗号化，復号は，二次曲線 $C_D(Z/nZ)$ を使って表現すれば次のようになる.

暗号化*:*

$$\begin{array}{ccccc}
(Z/nZ)^* \ni & m \bmod n & \longrightarrow & (m,1) & \in C_{m^2-4}(Z/nZ) \\
 & & & \downarrow e \text{ 倍} & \\
(Z/nZ)^* \ni & c \bmod n & \longleftarrow & (L_e(m,1), F_e(m,1)) & \in C_{m^2-4}(Z/nZ)
\end{array}$$

復号*:*

$$\begin{array}{ccccc}
(Z/nZ)^* \ni & c \bmod n & \longrightarrow & (c,1) & \in C_{c^2-4}(Z/nZ) \\
 & & & \downarrow d \text{ 倍} & \\
(Z/nZ)^* \ni & m \bmod n & \longleftarrow & (L_d(c,1), F_d(c,1)) & \in C_{c^2-4}(Z/nZ)
\end{array}$$

また，行列の言葉で言い直せば次のようになる.

Proposition 3.2 上述の LUC の暗号化，復号は次で書ける.

$$\text{暗号化}: \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \equiv \begin{pmatrix} 0 & -1 \\ 1 & m \end{pmatrix}^e + \begin{pmatrix} 0 & -1 \\ 1 & m \end{pmatrix}^{-e} \pmod{n},$$

$$\text{復号}: \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} \equiv \begin{pmatrix} 0 & -1 \\ 1 & c \end{pmatrix}^d + \begin{pmatrix} 0 & -1 \\ 1 & c \end{pmatrix}^{-d} \pmod{n}$$

また， (7) は次で書ける.

$$\begin{pmatrix} 0 & -1 \\ 1 & m \end{pmatrix}^{ed} \equiv \begin{pmatrix} 0 & -1 \\ 1 & m \end{pmatrix} \pmod{n}$$

4 RSA と LUC

RSA と LUC の帰着関係については [1] で簡単に触れられているが，ここでも [1] に沿った方針で互いの関係を述べ，最後に LUC に対する攻撃について，低指数攻撃についてだけ簡単に述べる.

まず RSA 問題と LUC 問題を次で定義しておく.

RSA 問題とは， RSA で用いる公開鍵 (n,e) と， $c \bmod n \in (Z/nZ)^*$ の組 (n,e,c) が与えられた時， $m \bmod n$ で， $c \equiv m^e \pmod n$ を満たすものを求める問題.

また， LUC 問題とは， LUC で用いる公開鍵 (n,e) と， $c \bmod n \in (Z/nZ)^*$ の組 (n,e,c) が与えられた時， $m \bmod n$ で， $c \equiv L_e(m,1) \pmod n$ を満たすものを求める問題とする.

$n = pq$， e を LUC の共通鍵とする． e に関しては LUC の方が条件が多いため，LUC で使えるものは RSA でも使えるが， RSA の指数は必ずしも LUC で使えるとは限らないことに注意しておく.

すると， (1) からただちに，次が成り立つことが分かる.

Lemma 4.1 $m \in (Z/nZ)^*$， $Z \ni k \geq 0$ に対して

$$2m^k \equiv L_k(m+m^{-1},1) + (m-m^{-1})F_k(m+m^{-1},1) \pmod n, \tag{8}$$

$$m^k + m^{-k} \equiv L_k(m+m^{-1},1) \pmod n \tag{9}$$

$P \equiv m + m^{-1} \pmod n$ と表せる平文 P の LUC による暗号文 $C \equiv L_e(P,1) \pmod n$ が与えられているとする．すると， (9) により

$$m^e + m^{-e} \equiv C \pmod n$$

となり， $m^e \bmod n$ を多項式時間で求めることが出来れば，入力 (n,e,C) の LUC 問題は， RSA 問題に帰着される．これは，例えば $m^e - m^{-e} \bmod n < \sqrt{n}$ の範囲であれば， $(m^e - m^{-e})^2 \equiv C^2 - 4 \pmod n$ なる合同式が，二次方程式を解くことで得られるので，次が成り立つ.

Proposition 4.1 (cf.[1]) *LUC* 問題の入力 (n,e,c) において， $c \bmod n$ を $c \equiv L_e(m+m^{-1},1) \pmod n$, $m^e - m^{-e} \bmod n < \sqrt{n}$, $(m \bmod n \in (Z/nZ)^*)$ となるものの全体に制限した *LUC* 問題は， *RSA* 問題に多項式帰着される.

逆に， e を RSA の暗号化指数とする．先に述べたように，これは必ずしも LUC で使えるとは限らないが， e に対する条件式から， RSA の指数のうち 1/4 は LUC に

使えると考えて良い．実際，RSA に対する鍵の選び方と同様に，$g.c.d.(p\pm 1, q\pm 1)$（符号はすべての組合せをとる）は小さくとっておく必要があり，4 つの条件は，ほぼ独立と考えられるので，少なくとも全体の 1/4 は LUC の条件を見たすと考えられる．今，この e が LUC にも適用出来るとする．すると，平文 $m \bmod n$ の RSA による暗号文 $C \equiv m^e \pmod n$ が与えられている時，(9) により

$$C + C^{-1} \equiv m^e + m^{-e} \equiv L_e(m + m^{-1}, 1) \pmod n$$

従って，$P \equiv m + m^{-1} \pmod n$ として，$t^2 - Pt + 1 \equiv 0 \pmod n$ が，多項式時間で解けるような平文 $m \bmod n$ に対しては，RSA は，LUC に帰着される．例えば，$m - m^{-1} \bmod n < \sqrt{n}$ の範囲にあるようなものは多項式で解ける．実際，この範囲にある m に対して，$(m - m^{-1})^2 \equiv P^2 - 4 \pmod n$ であるから，$m - m^{-1} \bmod n < \sqrt{n}$ であれば，二次方程式を解く事になり，多項式時間で解ける．即ち，Proposition 4.1 を言いかえると，次のようになる．

Proposition 4.2 (cf.[1]) *RSA* 問題の入力 (n, e, c) で，e が *LUC* のそれとして使えて，$c \bmod n$ を，$c \equiv m^e \pmod n$（但し，$m - m^{-1} \bmod n < \sqrt{n}$）と表されるものの全体に制限した *RSA* 問題は，*LUC* 問題に多項式帰着される．

最後に，LUC に対する攻撃について簡単に述べる．[1] で，RSA に対する攻撃のいくつかについて，LUC に対しても有効であることが示されているが，ここではそこで触れられていない，低指数攻撃について簡単に述べる．RSA 型の暗号に対する攻撃の一つである Hastad 攻撃 [3] は，同報通信時における攻撃，即ち，同じ平文を複数の相手に送った時に有効な攻撃であるが，その時に利用する暗号文の個数は，暗号化で使う多項式の次数で決まる．LUC の場合，Theorem 2.6 で見たように，公開鍵が (n, e) であれば，平文 $m \bmod n$ に対応する暗号文 c は

$$c \equiv 2^{1-e} \sum_{i=0}^{[\frac{e}{2}]} \binom{e}{2i} m^{e-2i} (m^2 - 4)^i$$

であたえられるので，即ち，LUC は，Hastad 攻撃に対しては，RSA と同じ強度であると言う事が出来る．

5 おわりに

以上では，数論的な性質を中心に述べたが，LUC は RSA と非常によく似ており，一方に対する攻撃はほとんど他方でも使えると思われる．ここでは，低指数攻撃についてのみ簡単に述べたが，他の RSA に対する攻撃法が LUC に対して，どれだけ

有効であるかを調べてみることは重要だと思われるし，また，LUC 特有の性質を使った攻撃が発見されて，それが，RSA に対する新しい攻撃方法への発見へと繋がれば興味深いと思われる.

参考文献

[1] D. Bleichenbacher, W. bosma and A. K. Lenstra, *Some Remarks on Lucas-Based Cryptosystems*, Advances in Cryptrogy-crypto '95, Springer-Verlag (1995), 387 - 396.

[2] D. M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag, 1989.

[3] J. Hastad, *On using RSA with low exponent in a public key network*, Proceedings of Crypto '91, 1991.

[4] A. J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.

[5] W. B. Müller and R. Nöbauer, *Cryptoanalysis of the Dickson-scheme*, Proceedings of Eurocrypto '85, Springer-Verlag (1985), 50 - 61.

[6] P. Ribenboim (吾郷孝視 訳), 素数の世界, 共立出版, 1995.

[7] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, 1994.

[8] P. Smith, *LUC public-key encryption*, Dr. Doob's Journal (January 1993), 44 - 49.

[9] P. Smith and C. Skinner, *A public-key cryptosystem and a digital signature system based on the Lucas-function analogue to discrete logarithms*, Pre-Proceedings Asiacrypto'94, 298 - 306.

[10] S. Uchiyama, *A note on the public-key cryptosystems based on quadratic curves over Z/nZ*, SCIS'97-16D, 1997.