高校生にわかるか、楕円曲線暗号

林　雄一郎

1　はじめに

ABC 予想を証明した望月新一氏の IUT（宇宙際タイヒミューラー）理論についての解説本「宇宙と宇宙をつなぐ数学」（加藤文元著）を読んでいたら、楕円曲線暗号のことが書かれていた。この暗号は楕円曲線を利用した公開鍵暗号で、RSA 暗号（2012 年第 1 回数実研での拙著「ＲＳＡ暗号と素因数分解」）よりも短い鍵長で十分な暗号強度を持ち、現在、IC カード、データ通信、デジタル通貨などの暗号に利用されている。これを数学の効用というコンテクストで生徒にアピールするトピック教材として使えるだろうか。

2　有限の数の体系

コンピュータの記憶量は有限である。この中で数の計算を自由に行うには有限の数の体系が必要となる。つまり、数の四則演算を有限の数の体系の中で行うのである。

まず、ある演算と数の体系モデルでもある「群」を考える。群は結合法則、単位元、逆元の存在する体系である。例えば、整数の集合は加法について、単位元は0 で$a+0=a$、a の逆元は$-a$ で$a+\left(-a\right)=0$ となるから加法群であり、交換法則$a+b=b+a$ も成り立つ。

一般に交換法則の成り立つ群は可換群（アーベル群）と呼ばれる。さらに、有理数の集合を考える。このような数の体系を「(数) 体」という。有理数の体系は、加法について加法群となる。a の逆元は$-a$ と記す。0 を除く集合では乗法について可換群となる。$a\neq 0$ の乗法の逆元は$a^{-1}=1/a$ と記す。加法と乗法を結びつける分配法則が成り立つ。減算は$a-b=a+\left(-b\right)$、割り算は$b\neq 0$ のとき$a/b=a\cdot b^{-1}$ とすれば四則演算が自由に行われる。例えば、集合$F_2=\left\{0,1\right\}$ は以下の演算規則で体となる。

$$0+0=0,0+1=,1+0=1,1+1=0,0\times 0=0,1\times 0=0\times 1=0,1\times 1=1$$

加法、乗法について結合法則が成り立ち、その演算を取り持つ分配法則も成り立つと仮定する。0 は加法の単位元、１は乗法の単位元である。加法について、$0,1$の逆元はそれぞれ$0,1$である。また、乗法については１の逆元は１である。よって演算規則で四則演算が集合$\left\{0,1\right\}$ で閉じている。このような有限個の元からなる体は有限体と呼ばれる。

以下、素数 p を固定して考える。整数を素数 p で割った余りは$0,1,2,\cdots,p-1$のいずれかとなる。余り k となる整数の集合を剰余類といい$\bar{k}$ と書く。a,b が同じ剰余類の元のとき

$a \equiv b \bmod p$ と書く。剰余類の集合 $F_p = \left\{\bar{0}, \bar{1}, \cdots, \overline{p-1}\right\}$ は集合を元とする集合である。F_p に和と積を次のように定義する。$\bar{a}+\bar{b} = \overline{a+b}, \bar{a}\cdot\bar{b} = \overline{ab}$ のとき $\left(\bar{a}+\bar{b}\right)+\bar{c} = \bar{a}+\left(\bar{b}+\bar{c}\right)$ $\bar{a}+\bar{0} = \bar{0}+\bar{a} = \bar{a}, \bar{a}+\left(\overline{-a}\right) = \bar{0}$ が成り立つ。$\bar{0}$ は零元、$-\bar{a} = \overline{-a}$ は $\bar{a}$ の逆元である。F_p は加法群になる。また、 $\left(\bar{a}\bar{b}\right)\bar{c} = \bar{a}\left(\bar{b}\bar{c}\right), \bar{a}\bar{b} = \bar{b}\bar{a}$ 、$\bar{a}\bar{1} = \bar{1}\bar{a} = \bar{a}$ $\bar{1}$ は乗法の単位元となる。$GCM\left(a,p\right) = 1$ だから $ax + py = 1$ を満たす解 x, y がある。$ax \equiv 1 \bmod p$ となり、$\bar{a}\bar{x} = \bar{1}$ $\bar{x}$ は $\bar{a}$ の逆元である。例えば、F_5 では $\bar{2}\cdot\bar{3} = \bar{1}$ より $\bar{2}$ と $\bar{3}$ は互いに逆元同士である。$F_p - \left\{\bar{0}\right\}$ は積について可換群となる。F_p は有限体である。

3　有限体 F_p 上で定義された楕円曲線上の加法

複素数 C 上の楕円曲線とは　$y^2 = x^3 + ax + b$ ・・・①　（$a, b \in C$）で表される曲線（Weierstrass 型）上の点に無限遠を加えた点の集合 $E\left(C\right)$ をいう。ただし、右辺＝0 は重根を持たない（特異点なし）とする。以下、複素数体 C の代わりに実数体 R 上で考える。

例えば、　$y^2 = x^3 - 2x + 1$ ・・・②　のグラフ（図 1）は x 軸に対称となる。

$E\left(R\right)$ 上の点に加法演算を次のように幾何学的に定義する。いま、P(x1,y1), Q(x2,y2)の和となる点 R＝P＋Q は、P, Q を結ぶ直線と①との交点を x 軸に対称に反転した①上の点を $R\left(X_r, Y_r\right)$ とするのである（図 2)。

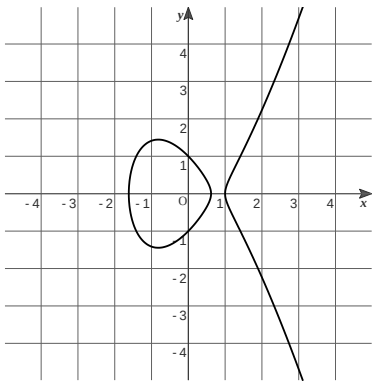

図 1

（３－１）実数体上の楕円曲線

まず、この座標 X_r, Y_r を求めることにする。

ア　$P \neq Q, x_p \neq x_q$ のとき

PQ と①の交点 S の座標を(X,Y)とする。このとき次式が成り立つ。

$y_p^{\,2} = x_p^{\,3} + ax_p + b$ ・・・③

$y_q^{\,2} = x_q^{\,3} + ax_q + b$ ・・・④

$\lambda = \left(y_q - y_p\right) / \left(x_q - x_p\right)$ とおくと

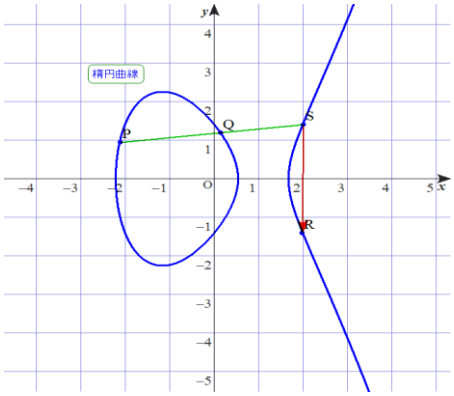

図 2

直線 PQ の方程式は $\left(y - y_p\right)\left(x_q - x_p\right) = \left(y_q - y_p\right)\left(x - x_p\right)$ ・・・⑤

③、④　から　　$\lambda\left(y_p + y_q\right) = a + x_p^{\,2} + x_p x_q + x_q^{\,2}$　　・・・⑥

他方、点 S は楕円曲線と PQ 上の点だから

$Y^2 = X^3 + aX + b$ 、　$Y - y_p = \lambda\left(X - x_p\right)$　この 2 式から

$$X^3 - \lambda^2 X^2 + \left(a - 2\lambda y_p\right)X + b - y_p^{\,2} + 2\lambda y_p x_p - \lambda^2 x_p^{\,2} = 0$$

x_p, x_q, X はこの 3 次方程式の解である。解と係数の関係から

$x_p + x_q + X = \lambda^2$　よって　$X = \lambda^2 - x_p - x_q$　点 R の座標を(X_r ,Y_r)とすると

$X_r = \lambda^2 - x_p - x_q$　$Y_r = -Y = -y_p - \lambda\left(X_r - x_p\right) = -\lambda X_r - \mu$ ・・・⑦

ただし、$\mu = \left(y_p x_q - y_q x_p\right) / \left(x_q - x_p\right)$　である。

イ　$P = Q$ のとき　　$y_p = y_q = 0$ ならば点 P での接線は x 軸に垂直となり①との交点 S は無限遠点 O となる。このとき $P + O$ に対応する直線 PO は y 軸に平行だから①との交点は点 P の x 軸に関する対称点でありそれを反転した点はまた P となるから $P + O = P$ となる。　$O + O = O$ と定める。$P = Q, y_p \neq 0$ ならば点 P での接線と①との交点 S を反転した点が R となる。$2P = R$　　⑥で $x_q \to x_p, y_q \to y_p$ とすると

$\lambda \to \left(3x_p{}^2 + a\right) / 2y_p = \lambda^*$　となる。

あるいは、①から　$2yy' = 3x^2 + a$　x, y に x_p, y_p を代入すれば得る。

このときの μ を計算する。　③× $x_q{}^2$ ―④× $x_p{}^2$

$$\left(y_p x_q - y_q x_p\right)\left(y_p x_q + y_q x_p\right) = x_p{}^2 x_q{}^2\left(x_p - x_q\right) + a x_p x_q\left(x_q - x_p\right) + b\left(x_q{}^2 - x_p{}^2\right)$$

$$\mu = \left(y_p x_q - y_q x_p\right) / \left(x_q - x_p\right) = \left(-x_p{}^2 x_q{}^2 + a x_p x_q + b\left(x_q + x_p\right)\right) / \left(y_p x_q + y_q x_p\right)$$

$Q \to P$ のとき　$\mu \to \left(-3x_p{}^3 - a x_p + 2y_p{}^2\right) / 2y_p = \mu^*$

また、　$Q \to P$ のとき　$X_r = \lambda^2 - x_p - x_q \to \lambda^{*2} - 2x_p = X_r{}^*$

$$Y_r \to -\lambda^* X_r{}^* - \mu^* = -X_r{}^*\left(3x_p{}^2 + a\right) / 2y_p - \left(-3x_p{}^3 - a x_p + 2y_p{}^2\right) / 2y_p = Y_r{}^*$$

よって、　$2P = R$ の座標は $\left(X_r{}^*, Y_r{}^*\right)$　・・・⑧　となる。

（３－２）　有限体上の楕円曲線

次に、① を有限体 $F_p\left(p \neq 2,3\right)$ 上で考える。　$\bar{a}, \bar{b} \in F_p$　をとり、$mod\ p$ で①を還元すると　$\bar{y}^2 = x^3 + \bar{a}\bar{x} + \bar{b}$　・・・⑨　となる。この式は F_p 上で定義された楕円曲線という。これを満たす有理点 $P\left(x, y\right) \in F_p \times F_p$ に無限遠点 $O\left(\infty, \infty\right)$ を合わせた点の全体を $E\left(F_p\right)$ とおくと、この集合の点の個数 N_p（楕円曲線の位数）は有限個となり a, b, p で定まる。

このとき、⑦、⑧の計算は有限体 F_p 上で行うことになる。座標値は F_p の元であり、この計算は、有限体上の法 p とする合同計算となる。もちろん体だから四則演算が自由にできる。これを繰り返すとある点 P の n 倍（スカラー積）の点 $R = nP$ を計算できる。

例　体 $F_5 = \left\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\right\}$ 上で定義された楕円曲線　$y^2 = x^3 - \bar{2}x + \bar{1}$　の有理点は

$O,\left(\bar{0},\bar{1}\right),\left(\bar{0},\bar{4}\right),\left(\bar{1},\bar{0}\right)$ の 4 個である。よって、$N_5 = 4$

例　F_{23} 上の楕円曲線 $y^2 \equiv x^3 + x + 1 \bmod 23$ において点 $P\left(3,10\right),Q\left(9,7\right)$ は有理点となる。これは代入すればわかる。⑧を用いて

$$\lambda = \left(7-10\right)/\left(9-3\right) = -3/6 = -1/2 \equiv 11 \bmod 23$$

（Q $2\cdot 12 = 24 \equiv 1 \bmod 23$ だから 2 の逆数 $1/2 \equiv 12$ 、$-12 \equiv 11 \bmod 23$）

$$X_r = 11^2 - 3 - 9 = 109 \equiv 17 \bmod 23$$

$$Y_r = -10 - 11\left(-6-3\right) = 89 \equiv 20 \bmod 23$$　よって、　$P+Q = \left(17,20\right)$

次に、$2P$ の座標を求める。⑨を用いて

$$\lambda^* = \left(3\times 3^2 + 1\right)/2\times 10 \equiv 5/20 = 1/4 \equiv 6 \bmod 23$$

$$X_r^* = 6^2 - 2\times 3 = 30 \equiv 7 \bmod 23$$

$$Y_r^* = -7\cdot\left(3\cdot 3^2+1\right)/2\cdot 10 - \left(-3\cdot 3^3 - 1\cdot 3 + 2\cdot 10^2\right)/2\cdot 10 = -78/5 \equiv 12 \bmod 23$$

Q $5\cdot 14 - 23\cdot 3 = 1, 5\cdot 14 \equiv 1 \bmod 23, -78\cdot\left(1/5\right) \equiv -78\cdot 14 = -1092 \equiv -11 \equiv 12$

なお、Y_r^* の計算は定義に戻って求める方が楽である。

接線の方程式は $y-10 = 6\left(x-3\right)$　　$x=7$ のとき $y = 6\times 7 - 8 = 34$

よって　$Y_r^* = -34 \equiv 12 \bmod 23$　いずれにせよ　$2P = \left(7,12\right)$

4　楕円曲線上の離散対数問題

3 で導入した加法で生じる点の集合を考察する。それらの点はある点 G から出発し、順に　$2G,3G,\cdots$ と計算してゆく。F_p は有限個だから、生成される点 kG は有限個の

$\left(0,0\right),\cdots,\left(p-1,p-1\right)$ に $O\left(\infty,\infty\right)$ を加えた p^2+1 個のいずれかの点である。だから、$nG = O$ となる最小の整数 n がみつかる。そして、次式が成り立つ。これらの点の集合を

$<G>$と書く。　　$(n+1)G = nG + G = O + G = G, (n+2)G = 2G, \cdots$

$P, Q \in <G>$に対し、$P+Q \in <G>$　また、$P+O=P$となりOは単位元である。x座標が同じでy座標の符号が異なり絶対値が等しい点P, Qは$P+Q=O$となる。互いに逆元となる。さらに、加法の結合法則$(P+Q)+R=P+(Q+R), P+Q=Q+P$が成り立つ。よって、このような規則が成り立つ集合は群（加法群、アーベル群）となる。また、どの元もkG（kは非負整数）の形をしているのでGを生成元という。よって、$<G>=\{O, G, 2G, \cdots, (n-1)G\}$となる。集合の個数$n$は位数という。$nG=O$が成り立つ。$<G>$は位数$n$の巡回群という。

$<G>$の任意の元Xに対して、$X=aG$となるaは$0 \le a \le n-1$で一つ定まる。このaをXの離散対数といい、aを求める問題を楕円曲線上の離散対数問題という。

$<G>$は演算が加法だが一般には乗法である。$X=aG$の形は一般には$x \equiv g^a \bmod p$の形となる。一般の離散対数問題はx, g, pが分かっているときaを求めるものである。gの指数を求めるので“対数”というのであろう。この問題はpが大きい場合に計算が困難である。例えば、$X=aG$を満たすaを求めるには、$(0,0), \cdots, (p-1, p-1)$の高々$p^2$個の点について調べなければならないからである。$p$が160ビット程度の大きさのとき、現在最も効率的なアルゴリズムを用い、最新のコンピュータで計算しても現実的な時間で解は求まらないといわれている。これがこの方式による暗号系のセキュリティを保証するものとなっている。ところが、量子コンピュータを用いると素因数分解や離散対数問題は多項式時間で解けることが証明されている（Peter Shor、Quantum Computing,1998）。

ＲＳＡ暗号との比較を考える。ＲＳＡ暗号では巨大素数からなる合成数Nとr（rは$(p-1)(q-1)$と互いに素）を公開鍵として送信者、受信者が使う。通信文（平文）を数値化したものをaとし、閉める鍵rを使って式$a^r \equiv b \bmod N$で求めたbを暗号文とする。受信者はまず$N=p \cdot q$と素因数分解する。これが厄介なことがこの暗号のセキュリティの核心となる。次にrを使い、$rs \equiv 1 \bmod (p-1)(q-1)$を満たす$s$を求める。$s$が秘密鍵（開ける鍵）である。$b$を$s$乗すれば元の通信文$a$を得ることになる。

$$b^s \equiv \left(a^r\right)^s = a^{rs} \equiv a^1 = a \bmod N$$

ＲＳＡ暗号のアイディアは閉める鍵と開ける鍵が異なることにある。

ＲＳＡ暗号のsを求める操作が楕円曲線暗号における離散対数を求める操作に対応する。ＲＳＡ暗号では乗算（累乗計算）だが楕円曲線暗号では加法となる。

離散対数問題は$s = r^x \bmod p$　においてs,r,p　がわかっているときxを求める問題である。$0 \le s \le p-1, 0 \le r \le p-1$　整数の組　(r,s)を楕円曲線上の点Gに対応させることができる。点$G=(r,s)$は$(0,0),\cdots,(p-1,p-1)$のいずれかであるが、既述したように楕円曲線上の点Pは$P=kG$　と書ける。

５　楕円曲線暗号による通信

ネットではあまり紹介されていないので以下で述べよう。楕円曲線は３の①とする。素数pは2^{180}程度の数を選ぶ。発信者Ａは４で述べた生成元Gを決める。その際、$<G>$の位数nが非常に大きな素数となるように選ぶ。楕円曲線①とGは公開する。

・発信者Ａは秘密鍵$k_A\left(k_A < n\right)$を決め、$P_A = k_A G$を計算する。また、受信者Ｂも秘密鍵$k_B\left(k_B < n\right)$を決め$P_B = k_B G$を計算する。P_A, P_Bはそれぞれ公開鍵とする。

次に、Ａは$k_A P_B$を計算し、同様にＢも$k_B P_A$を計算する。このとき
$k_A P_B = k_A k_B G, k_B P_A = k_B k_A G$だから２つは一致する。これを$K$とおき秘密鍵として共有する（鍵交換）。これはＥＣＤＨ（Elliptic Curve Diffie-Hellman Key Exchange）と呼ばれているものである。この共有鍵を用いることで共通鍵暗号方式（閉めるカギと開けるカギが同じ）でのやり取りができる。まず、発信者Ａは通信文（平文）mを符号化して楕円曲線上の点P_mに対応させる。共有鍵Kを用いた暗号化・復号化は例えば次のようになる。Ａは$C_m = P_m + K$と暗号化しＢに送る。Ｂは$C_m - k_B P_A = P_m + K - K = P_m$と計算する。$P_m$から平文$m$を得れば復号化できる。

・楕円曲線エルガマル暗号（ECElGamal）方式と呼ばれるものの暗号化・復号化は次のように行われる。Ａは乱数を使って整数kを決め次のような暗号のペアC_mを作りこれを暗号文としてＢに送信する。　　$C_m = \{C_{m1}, C_{m2}\}, C_{m1} = kG, C_{m2} = P_m + kP_B$

一方、C_m を受信した受信者Ｂは次のようにしてこれを復号化し P_m を得る。

$$C_{m2} - k_B \cdot C_{m1} = \left(P_m + kP_B\right) - k_B \cdot kG = P_m + kk_BG - k_BkG = P_m$$

Ｂは P_m から平文 m を得る。C_{m1} が漏洩したとしても、$C_{m1} = kG$ と G（公開）から k を得るのは前述したように難しいことがこの暗号のセキュリティを保証している。

・楕円曲線署名（ＥＣＤＳＡ）は次のように行う。Ａの送った通信文 m にＢが電子署名することを考える。m をハッシュ加工して m' とする。$kG = \left(r_x, r_y\right)$ の r_x、秘密鍵 k_B を用いて $S = \left(m' + r_xk_B\right) / k$ を計算し、$\left(r_x, S\right)$ を電子署名とする。これと通信文 m とまとめて署名付き文書としＡに送信する。これを受け取ったＡは公開鍵 $P_B = k_BG$ を用いて $\left(r_x, S\right)$ を確かめる。

$$\left(m'G + r_xP_B\right) / S = k\left(m'G + r_xP_B\right) / \left(m' + r_xk_B\right) = k\left(m' + r_xk_B\right)G / \left(m' + r_xk_B\right) = kG = \left(r_x, r_y\right)$$

が成立すれば署名は正しいと判定する。秘密鍵 k_B を知っているのはＢのみだからである。

６　あとがき

現在、量子コンピュータが開発されつつあるが、これは超高速計算が可能で暗号通信には脅威となっている。そこで夢の暗号系である量子暗号が脚光を浴びている。

例えば、東芝が考案した原理は、暗号鍵を分割して光子に乗せて光ファイバーで送信し、もし途中で盗聴・改竄などがあれば光子の乱れが生じるためそれが検知でき、自動的に別の鍵を発出する仕組みとなっている。この方式は絶対に盗聴・改竄ができないとされている。この暗号システムを応用した量子暗号通信を 2035 年までに実用化するべく現在実証試験中である。これが本格実用となれば、既存の RSA や楕円曲線を用いた素数ベースの暗号系は影をひそめることになるかもしれない。

参考文献　神永正博：現代暗号入門、講談社、2017、 ISBN978-4-06-502035-7