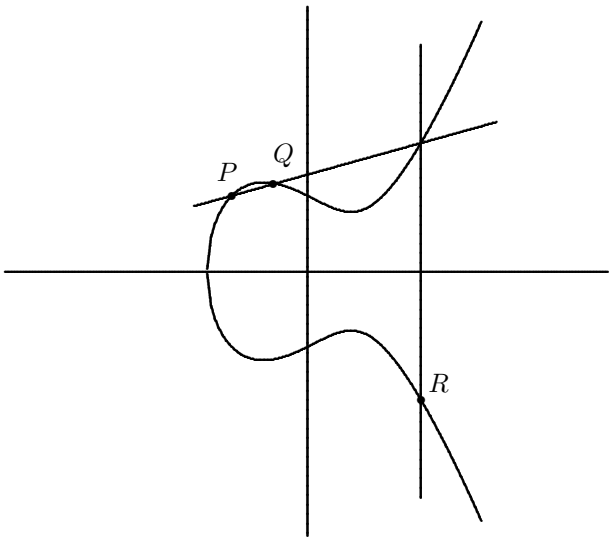
5　楕円曲線暗号

原理的には有限群を 1 つ決めると暗号が決まった。ここでは楕円曲線が作る群に基づく暗号を紹介する。楕円曲線暗号の強さについて 2010 年に富士通研究所が解析した結果によると,「楕円曲線暗号が RSA 暗号と比較して，従来考えていたよりも，数千倍程度相対的に高い強度であることが考えられる」。「従来 RSA 暗号/1024 ビットと楕円暗号/160 ビットがほぼイコールと考えられていたが，今回の成果で，楕円暗号/140 ビットでほぼイコールであることが判明した」とのことである。ここではこの楕円曲線暗号を簡単に紹介する。

最初に楕円曲線について述べる。**楕円曲線** (*elliptic curve*) は**楕円** (*ellipse*) に関連して研究されるようになった曲線であるが，2 つは別物である。楕円は $\dfrac{x^2}{a^2}+\dfrac{y^2}{b^2}=1$ で表される曲線であり，楕円曲線は $y^2=x^3+ax+b$ で表される曲線である。ただしここで $x^3+ax+b=0$ が重解を持たないことを要求する。そのためには判別式 $4a^3+27b^2$ が 0 でなければよいことが知られている。この条件が満たされているときこの曲線を楕円曲線と呼ぶ。楕円の長さを求めようとすると，$\displaystyle\int\sqrt{x^3+ax+b}\,dx$ という不定積分を求めることが必要になる。この積分は楕円積分と呼ばれ初等関数 (解析学 I で学んだ範囲の関数：整関数，有理関数，無理関数，指数関数，対数関数，三角関数，逆三角関数) では表すことができないことが分かっている。このことに関連して楕円曲線が研究されたが，楕円曲線は面白い (不思議な) 性質を持っていることが分かった。その 1 つとして曲線上の点に対して演算が定義されてそれが群になることである。複素数の世界 $\left\{(x,y)\in\mathbb{C}^2\,\middle|\,y^2=x^3+ax+b\right\}$ と実数の世界 $\left\{(x,y)\in\mathbb{R}^2\,\middle|\,y^2=x^3+ax+b\right\}$ が考えられる。理論的には複素数の世界がすっきりしているのだが，ここでは視覚化可能な実数の世界で考える。曲線上の点に加えて**無限遠点** (*the point at infinity*) $\mathcal{O}$ を加えて $E(\mathbb{R})=\left\{(x,y)\in\mathbb{R}^2\,\middle|\,y^2=x^3+ax+b\right\}\cup\{\mathcal{O}\}$ とする。次図は $a=-1, b=1$ の場合の図である。



P, Q が無限遠点ではないお互いに異なる点とする。P と Q を通る直線と楕円曲線の交点を R' とし，この点を x 軸に関して対称移動した点を R とする。このとき

$$R = P + Q$$

と定義する。曲線は 3 次曲線なので直線とは一般的には 3 点で交わる。しかし交わらない場合もある。P と Q を通る直線と曲線が交わらないときは

$$\mathcal{O} = P + Q$$

と定義する。$P = Q$ のときは P を通る接線を考え，それと曲線の交点を R' とし，x 軸に関して対称移動した点を R とし，

$$R = P + P$$

と定義する。また無限遠点に関しては

$$P = P + \mathcal{O} = \mathcal{O} + P$$

と定義する

この定義は幾何的にされたものだが，代数に翻訳しよう。$P = (x_1, y_1), Q = (x_2, y_2), R = (x_3, y_3)$ とする。$x_1 \neq x_2$ のときは $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ とおくと

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

であり，$P = Q$ のとき，即ち $x_1 = x_2$ かつ $y_1 = y_2$ のとき $\lambda = \dfrac{3x_1^2 + a}{2y_1}$ とおくと

$$x_3 = \lambda^2 - 2x_1$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

である。また $P \neq Q$ かつ $x_1 = x_2$ のときは

$$R = \mathcal{O}$$

であり，$R = (x_3, y_3)$ の形には書けない。

この演算に関し $E(\mathbb{R})$ は群になる。結合法則以外の証明は簡単だが，結合法則の証明は難しい。

ここで考えた楕円曲線の作る群 $E(\mathbb{R})$ は一般に無限群であり，有限群にはならない。そこで，実数「$\mathbb{R}$」の有限の対応物を考える。それを有限体という。素数 p と自然数 n に対し $q = p^n$ とおく。この q に対し q 個の元からなる有限体と呼ばれる F_q が唯 1 つ存在して次の性質を持つことが知られている。

(1) 加法が定義されていて，F_q は可換群をなす。加法の単位元を 0 と書く。
(2) 乗法が定義されていて，$F_q - \{0\}$ は可換群をなす。乗法の単位元を 1 と書く。
(3) 分配法則 $[a(b + c) = ab + ac]$ が成立する。

この性質を満たすとき**体** (*field*) と呼ぶことにする。有限体の一般論は専門書にまかせて，ここでは例を見る。$n=1$ の場合，即ち $q=p$ の場合 $F_q=F_p$ は剰余類群 $\mathbb{Z}_p$ である。$\mathbb{Z}_p$ に加法と乗法が定義されていて，前の 3 つの性質を満たすことはすでに調べてある。よって $\mathbb{Z}_p$ は体である。

次に $p=2, n=2$ の場合を考えよう。$\mathbb{Z}_2$ の元は $[0],[1]$ と書いたが，以下簡単のために $0,1$ と書くことにする。$\mathbb{Z}_2$ では $1+1=0$ 等が成立する。$\mathbb{Z}_2$ 係数の 2 次式 $f(x)$ で $\mathbb{Z}_2$ に解を持たないものを考える。$f(x)=x^2$ は $f(0)=0$ となって不適だが，例えば $f(x)=x^2+x+1$ とすると，$f(0)=1, f(1)=1$ で条件を満たす。実数に i ($f(x)=x^2+1$ の解) を付け加えて複素数を作ったように $\mathbb{Z}_2$ に $f(x)=0$ の解を付け加える F_4 を作る。α を $f(x)=0$ の解とする。即ち $\alpha^2+\alpha+1=0$ が成立している。$\mathbb{Z}_2$ に α を加えたものを F_4 とする。F_4 が体のとき，$\alpha+1$ も F_4 の元でなくてはならない。このとき $\alpha\neq\alpha+1$ が成立する。即ち

$$F_4=\{\,0,1,\alpha,\alpha+1\,\}$$

となる。F_2 では $2=1+1=0$ なので $\alpha+\alpha=2\alpha=0$ となる。$-1=1$ なのでまた $\alpha\cdot\alpha=\alpha^2=-\alpha-1=\alpha+1$ となる。その他どの元の演算も結果は F_4 の元になり，体になることが分かる。

一般の $q=p^n$ 場合は最初に $\mathbb{Z}_p$ を考える。次に Z_p に係数を持つ n 次多項式 $f(x)$ で**既約** (*irreducible*)，即ち $\mathbb{Z}_p$ 係数で因数分解されないものをとってくる。$f(x)=0$ の解を α とするとき，$\mathbb{Z}_p$ に α を加えると，q 個の元から構成される体 F_q が得られることが知られている。多項式のとり方により F_q の構造が変わるようにも思えるが，とり方によらず一通りに決まることが証明されている。

我々が対象とするのは $q=p^n$ としたときの，有限体上の楕円曲線

$$E(F_q)=\left\{\,(x,y)\in F_q^2 \;\middle|\; y^2=x^3+ax+b\,\right\}\cup\{\,\mathcal{O}\,\}$$

である。代数的な和はこの $E(F_q)$ 上でも**ほとんどの場合**前述の式で同様に定義され群になる。

修正が必要なのは次の場合である。$q=p^n$ のとき p をこの体の**標数**と呼ぶ。標数 2 および 3 以外は同様に定義されるが，$p=2$ または 3 のときは修正が必要である。その理由を述べておく。楕円曲線は一般的には

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \tag{1}$$

で定義される。標数 2 では $2=0$ になり，$\dfrac{1}{2}$ が存在 せず，標数 3 では $3=0$ になり $\dfrac{1}{3}$ が存在しない。例えば $a_2=0$ とするためには x を $x-\dfrac{1}{3}a_2$ と変形すれば，対応する項を 0 にできるが，標数 3 では $\dfrac{1}{3}$ が存在しないためこの様な操作ができない。この様な事情で標数 3 の場合は

$$y^2=x^3+ax^2+bx+c$$

の形に，標数 2 の場合は

$$y^2+xy=x^3+px^2+b,\qquad \text{または } y^2+py=x^3+ax+b$$

までしか変形ができない。このとき，それぞれの場合の加法の式は前述のものとは若干形が異なる。

(1) 式 (1) において $a_1=a_3=0$ のとき (標数 3) ：1 行目が $P\neq Q$，2 行目が $P=Q$

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-a_2-x_1-x_2 \qquad y_3=-y_1+\frac{y_2-y_1}{x_2-x_1}(x_1-x_3)$$

$$x_3=\left(\frac{3x_1^2+2a_2x_1+a_4}{2y_1}\right)^2-a_2-2x_1 \qquad y_3=-y_1+\frac{3x_1^2+2a_2x_1+a_4}{2y_1}(x_1-x_3)$$

(2) 式 (1) において $a_3 = a_4 = 0$ で $a_1 = 1$ のとき (標数 2)：1 行目が $P \neq Q$，2 行目が $P = Q$

$$x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + \frac{y_1 + y_2}{x_1 + x_2} + x_1 + x_2 + a_2 \qquad y_3 = \frac{y_1 + y_2}{x_1 + x_2}(x_1 + x_3) + x_3 + y_1$$

$$x_3 = x_1^2 + \frac{a_6}{x_1^2} \qquad y_3 = x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right) x_3 + x_3$$

(3) 式 (1) において $a_1 = a_2 = 0$ のとき (標数 2)：1 行目が $P \neq Q$，2 行目が $P = Q$

$$x_3 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2 \qquad y_3 = \frac{y_1 + y_2}{x_1 + x_2}(x_1 + x_3) + y_1 + a_3$$

$$x_3 = \frac{x_1^4 + a_4^2}{a_3^2} \qquad y_3 = \frac{x_1^2 + a_4}{a_3}(x_1 + x_3) + y_1 + a_3$$

点 P に対し $2P = P + P$ と書く。$3P = 2P + P$，$4P + 3P + P$，同様に $kP = (k-1)P + P$ と帰納的に定義する。有限体上の楕円曲線を用いて次のような暗号を考える。ここでは標数が 2，3 ではない場合を考える。標数が 2 または 3 の場合は定義方程式 $f(x)$ を変えれば同様に考えることができる。

暗号化のために，$q = p^n$ を決める。$f(x) = x^3 + ax + b$ を決める。点 $P \in E(F_q)$ および自然数 k を決める。$Q = kP$ を計算する。

秘密鍵： k
公開鍵： $q = p^n$, $y^2 = x^3 + ax + b$, P, Q

暗号化 (送信側)： 平文 $X \in E(F_q)$ とする。適当な乱数 r を発生させる。$A = rP$ と，$B = X + rQ$ を計算し，(A, B) を暗号文として送信する。
復号化 (受信側)： $B - kA$ を計算する。

$$B - kA = X + rQ - krP = X + rkP - krP = X$$

となるので復号化できる。

楕円曲線暗号の安全性の根拠は P および Q を知っても k を知ることは困難であろうという，離散対数問題の困難性に基づいている。同じことであるが，P および A を知っていても r を知ることは困難であると考えられている。r を知ることができれば，$X = B - rQ$ なので平文 X を得ることができる。r は乱数で発生させるので，たまたま解読しやすい数字だという可能性は 0 ではない。しかし，その場合も，解読できるのは特定の平文 X だけであり，別の乱数 r' を用いて暗号化された文章が解読可能というわけではない。しかし k を得た人間は任意の暗号文を解読することができる。一般的には安全と思われているが，解読方法が知られているのタイプの楕円曲線もあるので，実装の場合は更なる知識が必要になる。

楕円曲線暗号に関しては原理的な話だけで，実装アルゴリズム等の話はしていない。これから広く使われる可能性のある暗号として簡単にふれた。