楕円曲線暗号の計算機実験

2009SE295 若原麻衣
指導教員：小藤俊幸

1　はじめに

現代の情報社会の世の中では，個人情報を守るためや第三者に洩れることなく相互に正確な情報のやり取りを行うために暗号を使うことは必要不可欠である．ここでは授業で習った楕円曲線 [1] を使って暗号化し，数を大きくして手計算ではとうていできないより複雑な暗号にする実験をしたい．

2　有限体 $\mathbb{F}_p$ 上の楕円曲線

5 以上の素数 p と $a, b \in \mathbb{F}_p$ に対して，集合

$$E(p;\, a,\, b) = \left\{(x,\, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 + ax + b\right\} \cup \{\mathcal{O}\} \tag{1}$$

を，$\mathbb{F}_p$ 上の楕円曲線と言う．ここで，$\mathcal{O}$ は無限遠点と呼ばれる特殊な要素であり，$a, b \in \mathbb{F}_p$ は

$$4a^3 + 27b^3 \neq 0 \tag{2}$$

をみたすものとする．

例（楕円曲線 $E(5;\, 1,\, 1)$ 上の点）有限体 $\mathbb{F}_5$ において，$f(x) = x^3 + x + 1$ の $x = 0, 1, 2, 3, 4$ での値，$y = 0, 1, 2, 3, 4$ の y^2 の値を計算すると，

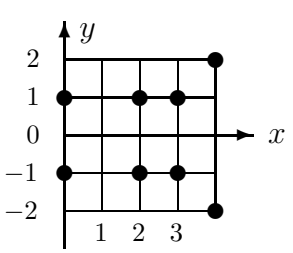
x	0	1	2	3	4
$f(x)$	1	3	1	1	4

y	0	1	2	3	4
y^2	0	1	4	4	1

となる．両者を比較すると，$x = 1$ 以外の x については，$y^2 = f(x)$ となる y が存在することが分かる．例えば，$x = 0$ のとき，$f(x) = 1$ より，$y = 1$ と $y = 4$ で $y^2 = f(x)$ が成り立つ．$E(5;\, 1,\, 1)$ は，9 点からなる

$$E(5;\, 1,\, 1) = \big\{(0,\, 1),\, (0,\, 4),\, (2,\, 1),\, (2,\, 4),\, (3,\, 1),\, (3,\, 4),\, (4,\, 2),\, (4,\, 3)\big\} \cup \{\mathcal{O}\}$$

の集合である．y 座標を $4 = -1, 3 = -2$ と書き直して，$E(5;\, 1,\, 1)$ を xy 平面上に図示すると，下図のようになる．



3　楕円曲線上の点の加法

楕円曲線上の点の加法を以下のように定める．以下，$\mathbb{E} = E(p;\, a,\, b)$ と略記する．

(i) 任意の点 $P \in \mathbb{E}$ と無限遠点 $\mathcal{O}$ との和を

$$P + \mathcal{O} = \mathcal{O} + P = P \tag{3}$$

により定める．すなわち，$\mathcal{O}$ を，この加法に関する 0（単位元）とする．

(ii) 無限遠点 $\mathcal{O}$ 以外の任意の点 $P = (x,\, y) \in \mathbb{E}$ に対して，$P' = (x,\, -y)$ で定まる点は $\mathbb{E}$ の点となる．P と P' の和を

$$P + P' = P' + P = \mathcal{O} \tag{4}$$

と定める．すなわち，P' を $-P$ とする．特に，$P = (x,\, 0)$ のような点があれば（あるとは限らない），$P + P = \mathcal{O}$ である．

定理（加法の定義 **(iii)** ）$P_1 = (x_1,\, y_1) \in \mathbb{E}$, $P_2 = (x_2,\, y_2) \in \mathbb{E}$ について，(a) $x_1 \neq x_2$，または，(b) $x_1 = x_2,\ y_1 = y_2 \neq 0$ が成り立つものとする．そのとき，

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \big(\text{ (a) の場合 }\big) \\ \dfrac{3x_1^2 + a}{2y_1} & \big(\text{ (b) の場合 }\big) \end{cases} \tag{5}$$

$$x_3 = \lambda^2 - x_1 - x_2,\ \ y_3 = \lambda(x_1 - x_3) - y_1 \tag{6}$$

で定まる点 $P_3 = (x_3,\, y_3)$ は $\mathbb{E}$ の要素となる．

例（楕円曲線 $E(5;\, 1,\, 1)$ 上の点の加法）$\mathbb{F}_5$ の 2 乗と逆数は，

x	0	1	2	3	4
x^2	0	1	4	4	1

x	1	2	3	4
$1/x$	1	3	2	4

のようになる．$P = (0,\, 1) \in E(5;\, 1,\, 1)$ について，$2P = P + P$ を計算する．$x_1 = 0,\ y_1 = 1$ として，公式 (5) の (b) の場合と公式 (6) を用いると，

$$\lambda = \frac{3x_1^2 + 1}{2y_1} = \frac{3 \cdot 0^2 + 1}{2 \cdot 1} = \frac{1}{2} = 3$$

$$x_3 = \lambda^2 - 2x_1 = 3^2 - 2 \cdot 0 = 4$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 3 \cdot (0 - 4) - 1 = 2$$

となる．したがって，$2P = (4,\, 2)$ である．さらに，$3P = P + 2P$ を計算する．$x_1 = 0,\ y_1 = 1,\ x_2 = 4,\ y_2 = 2$ として，公式 (5) の (a) の場合と公式 (6) を用いると，

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{2 - 1}{4 - 0} = \frac{1}{4} = 4$$

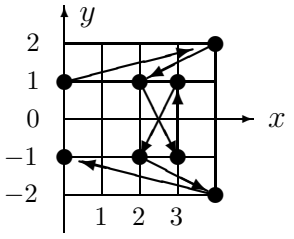
$$x_3 = \lambda^2 - x_1 - x_2 = 4^2 - 0 - 4 = 1 - 4 = 2$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = 4 \cdot (0 - 2) - 1 = 1$$

となる．したがって，$3P = (2, 1)$ である．以下，同様に

$$4P = P + 3P = (3, 4),\ 5P = P + 4P = (3, 1),$$
$$6P = P + 5P = (2, 4),\ 7P = P + 6P = (4, 3),$$
$$8P = P + 7P = (1, 4)$$

のように計算される．$4 = -1$ より，$8P = (1, 4)$ は $-P$ である．したがって，$9P = P + 8P = \mathcal{O}$ となる．

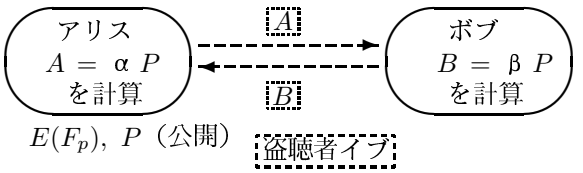


4 楕円曲線を利用したエルガマル暗号

$E(\mathbb{F}_p) = E(p; a, b)$ を $\mathbb{F}_p$ 上の楕円曲線とし，非常に大きな自然数 n で，はじめて $nP = \mathcal{O}$ となる $P \in E(\mathbb{F}_p)$ を選ぶ．この P をベースポイントと呼ぶ．アリスは自分の秘密鍵 α を，ボブは自分の秘密鍵 β を，それぞれ，$\Sigma_n = \{0, 1, ..., n-1\}$ から選び，アリスは $A = \alpha P$ を，ボブは $B = \beta P$ を計算して，相手に送信する．アリスが，αB を，ボブが，βA を計算すると，

$$\alpha B = \beta A = \alpha \beta P \tag{7}$$

となって，秘密の共有鍵 $K = \alpha \beta P$ が得られる．



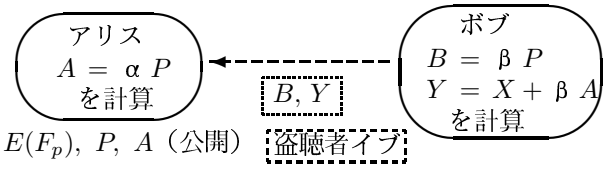
こうして秘密鍵の交換が可能になれば，対応するエルガマル暗号を考えることは容易である．送信者ボブが，平文 $X \in \mathbb{E}$ を暗号化してアリスに送りたいとする．ボブは，アリスの公開鍵 P, A と自分の秘密鍵 β を使って，

$$B = \beta P,\ Y = X + \beta A \tag{8}$$

を計算し，アリスに送信する．受け取ったアリスは

$$X = Y + (-\alpha B) \tag{9}$$

で復号化する．



5 数値実験

楕円曲線 $(31; 2, 17)$ 上の点を考える．有限体 $\mathbb{F}_{31}$ において，$f(x) = x^3 + 2x + 17$ のとき，楕円曲線 $E(31; 2, 17)$ の要素数は $\sharp E(31; 2, 17) = 41$ になる．$P = (10, 13)$ であり，$P, 2P, ..., 40P$ まで打ち出してグラフにすると以下のようになる．

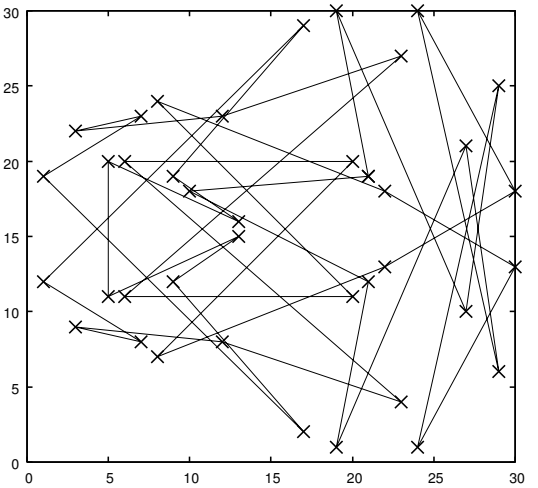


図 1 数値計算結果

ここで実際にアリスとボブのようなやり取りをしてみた．アリスは自分の秘密鍵を 24 とし，ボブは自分の秘密鍵を 29 とした．アリスは $A = 24P = (17, 29)$ を，ボブは $B = 29P = (23, 4)$ を計算して相互に送信しあう．アリスが $24B$ をボブが $29A$ を計算して，

$$24\,B = 29\,A = (10, 18) \tag{10}$$

となって，秘密の共有鍵 $K = (10, 18)$ が得られる．ここで対応するエルガマル暗号を考える．ボブが平文 $X = (30, 13) \in \mathbb{E}$ を暗号化してアリスに送る．ボブは P, A , β を使って，

$$B = \beta P,\ Y = X + \beta A = (30, 13) + (10, 18) \tag{11}$$

を計算し，アリスに送信する．受け取ったアリスは

$$X = Y + (-\alpha B) = (24, 1) + (10, -18) \tag{12}$$

で復号化でき，$X = (30, 13)$ を求めることができる．

6 おわりに

楕円曲線の鍵交換の原理について学び，実際に鍵交換をし，暗号化して，復号化することができた．今回はエルガマル暗号について着目したが，その他の暗号も現代では重要であり，どのように活用されているのかも学んでいきたいと感じた．

参考文献

[1] 辻井重男，笠原正雄 編，有田正剛，境隆一，只木孝太郎，趙晋輝，松尾和人：『暗号理論と楕円曲線』，森北出版，東京，2008.