

## 離散対数問題 (Discrete Logarithm Problem)

---

$p$  : 素数

$g \in \mathbb{Z}$  を 1 つ取って固定

問題 :  $x$  を与えたとき、

$g^a \equiv x \pmod{p}$  を満たす  $a$  を見出せ。

→

$G = (\mathbb{Z}/p\mathbb{Z})^\times$

$g \in G$  を 1 つ取って固定

問題 :  $x \in G$  を与えたとき、

$g^a = x$  を満たす  $a$  を見出せ。

群  $G = (\mathbb{Z}/p\mathbb{Z})^\times$  に於ける離散対数問題

## 離散対数問題の一般化

以前扱った離散対数問題は、

有限アーベル群  $G = (\mathbb{Z}/p\mathbb{Z})^\times$  に於ける  
離散対数問題であると言える

実は、有限アーベル群があれば、

離散対数問題が定式化できる

問題：

$G$ ：有限アーベル群

$g \in G$  を 1 つ取って固定

このとき、 $x \in G$  に対し、

$$g^a = x$$

を満たす  $a$  を見出せ。

## 離散対数問題の一般化

### 離散対数問題が

- 解くのは困難
- 作るのは (冪の計算は) 高速  
である (暗号に使える) 有限アーベル群の例
- 有限体上の楕円曲線の有理点の群  
(楕円曲線暗号)
- 有限体上の超楕円曲線の **Jacobian** の有理点の群  
(超楕円曲線暗号)
- 代数体の **ideal** 類群

## 楕円曲線暗号

「有限体上の楕円曲線の有理点の成す群」  
に於ける離散対数問題を用いた暗号

楕円曲線：

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

の形の方程式で定義される代数曲線  
(で然るべき条件を満たすもの)

## 楕円曲線暗号

「有限体上の楕円曲線の有理点の成す群」  
に於ける離散対数問題を用いた暗号

楕円曲線：

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

の形の方程式で定義される代数曲線  
(で然るべき条件を満たすもの)

## 楕円曲線

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- 標数  $\neq 2$  なら  $y$  について平方完成して

$$y^2 = x^3 + b_2x^2 + b_4x + b_6$$

の形に変数変換できる

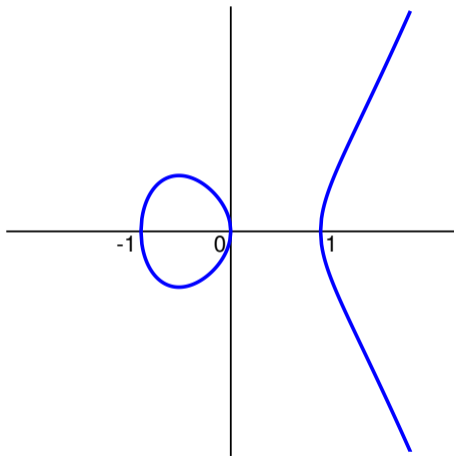
- さらに標数  $\neq 3$  なら  $x$  について立方完成して

$$y^2 = x^3 + c_4x + c_6$$

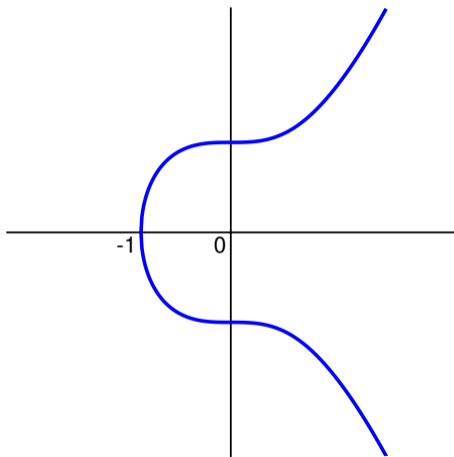
の形に変数変換できる

$y^2 = (x \text{ の } 3 \text{ 次式})$  の形の代数曲線

例： $y^2 = x^3 - x$

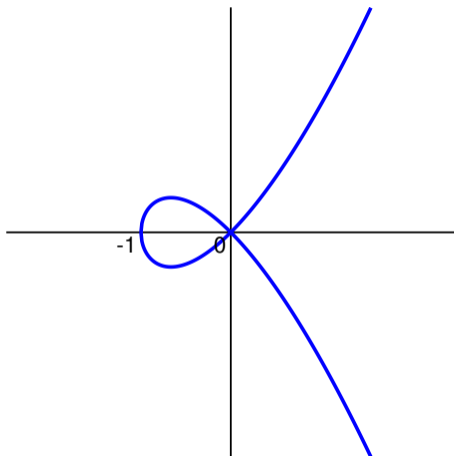


例： $y^2 = x^3 + 1$

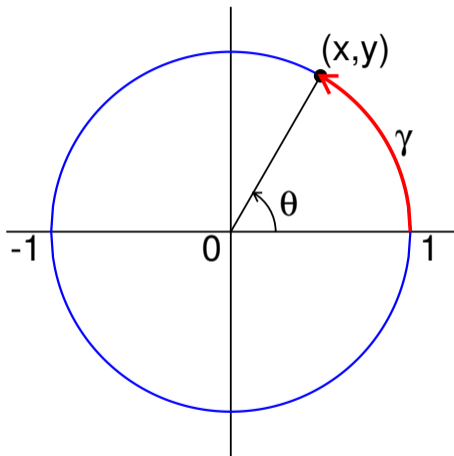




例：  $y^2 = x^3 + x^2 = x^2(x + 1)$  : 楕円曲線でない



円周の群構造 :  $y^2 = 1 - x^2$



## 射影空間

$K$  : 体

$V = K^{n+1}$  :  $K$  上の  $(n+1)$  次元ベクトル空間

$x = (x_0, x_1, \dots, x_n), y = (y_0, y_1, \dots, y_n) \in V \setminus \{0\}$   
に対し、

$$x \sim y \iff (\exists t \in K^\times : y = tx)$$

とすると  $\sim$  は同値関係

$\mathbb{P}^n(K) := (V \setminus \{0\})/\sim$  :  $K$  上の  $n$  次元射影空間

$(x_0, x_1, \dots, x_n)$  の属する同値類を

$[x_0 : x_1 : \dots : x_n]$  などと書く

## 射影空間

$[x_0 : x_1 : \cdots : x_n] \in \mathbb{P}^n(\mathbb{K})$  で、 $x_0 \neq 0$  ならば、

$$[x_0 : x_1 : \cdots : x_n] = \left[ 1 : \frac{x_1}{x_0} : \cdots : \frac{x_n}{x_0} \right]$$

$$\mathbb{K}^n \hookrightarrow \mathbb{P}^n(\mathbb{K})$$

$$(x_1, \dots, x_n) \longmapsto [1 : x_1 : \cdots : x_n]$$

$$\mathbb{P}^n(\mathbb{K}) \setminus \mathbb{K}^n \simeq \mathbb{P}^{n-1}(\mathbb{K})$$

## 楕円曲線の射影化

$y^2 = x^3 + ax + b$  を  $\mathbb{P}^2(K)$  内で考える

$$K^2 \hookrightarrow \mathbb{P}^2(K)$$

$$(x, y) \longmapsto [x : y : 1] = [X : Y : Z]$$

$x = \frac{X}{Z}, y = \frac{Y}{Z}$  とおいて、

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

## 楕円曲線の射影化

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

$$E(K) = \{[X : Y : Z] \in \mathbb{P}^2(K) \mid Y^2Z = X^3 + aXZ^2 + bZ^3\}$$

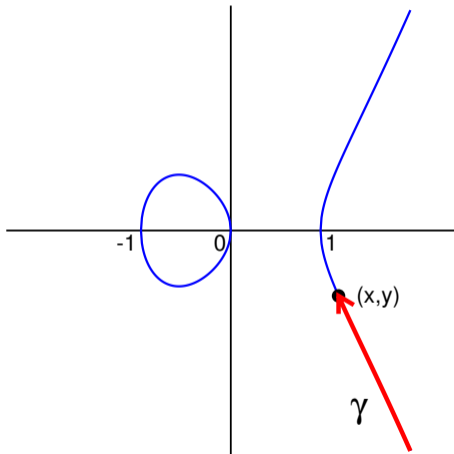
:  $E$  の  $K$ -有理点の成す集合

$$E(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + ax + b\} \sqcup \{[0 : 1 : 0]\}$$

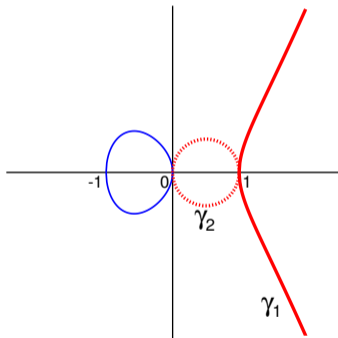
$[0 : 1 : 0]$  :  $E$  上にある “無限遠点”

( $\infty, 0$  などと書く)

# 楕円曲線の有理点の群構造 (解析的)



## 楕円曲線の有理点の群構造 (解析的)



$$\omega_1 := \int_{\gamma_1} \frac{dx}{y}$$
$$\omega_2 := \int_{\gamma_2} \frac{dx}{y}$$
$$\Gamma := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

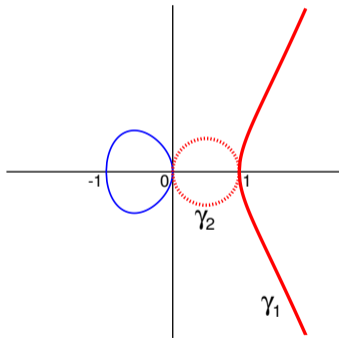
$(x, y) \in E(\mathbb{C})$   
に対して、

$$z := \int_{\gamma} \frac{dx}{y} \text{ は、}$$

mod  $\Gamma$  で定まる



## 楕円曲線の有理点の群構造 (解析的)



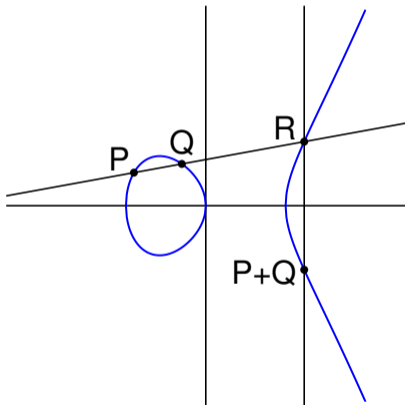
$$E(\mathbb{C}) \simeq \mathbb{C}/\Gamma$$

$$(x, y) \mapsto z = \int_{\gamma} \frac{dx}{y}$$

$\mathbb{C}/\Gamma$  の  
加法群構造から  
 $E(\mathbb{C})$  にも  
群構造が入る  
 $O = [0 : 1 : 0]$   
が単位元

## 楕円曲線の有理点の群構造 (代数的)

$P, Q, R$  が共線 (同一直線上)  $\iff P + Q + R = O$



## 楕円曲線の有理点の群構造 (代数的)

$E(\mathbb{C})$  の群構造は、座標  $(x, y)$  で代数的に書ける

$$E : y^2 = x^3 + ax + b$$

$$l : y = sx + t$$

$P(x_1, y_1), Q(x_2, y_2)$  で交わるとすると、

$$s = \frac{y_2 - y_1}{x_2 - x_1}, \quad t = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

もう一つの交点  $R(x_3, -y_3)$  は、

$$x_3 = s^2 - (x_1 + x_2), \quad -y_3 = sx_3 + t$$

## 楕円曲線の有理点の群構造 (代数的)

$$E : y^2 = x^3 + ax + b$$

$P(x_1, y_1), Q(x_2, y_2)$  に対し、  
 $P + Q$  の座標  $(x_3, y_3)$  は次で求められる

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

$$y_3 = -\frac{y_2 - y_1}{x_2 - x_1} x_3 - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

## 有限体上の楕円曲線

$p$  : 素数 (ここでは簡単のため  $p \neq 2, 3$ )

$a, b \in \mathbb{F}_p$

$E : y^2 = x^3 + ax + b$  :  $\mathbb{F}_p$  上の楕円曲線  
( $\Delta = -4a^3 - 27b^2 \neq 0$ )

$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p^2 \mid y^2 = x^3 + ax + b\} \sqcup \{O\}$   
: 有限アーベル群を成す  
( $O = [0 : 1 : 0]$  : 単位元)

## 有限体上の楕円曲線の有理点

Hasse の限界 :

$p$  : 素数

$E : \mathbb{F}_p$  上の楕円曲線 に対し、

$$|\#E(\mathbb{F}_p) - (p + 1)| \leq 2\sqrt{p}$$

即ち、

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}$$

## 楕円曲線暗号

$p$  : 素数

$E$  : 有限体  $\mathbb{F}_p$  上の楕円曲線

$E(\mathbb{F}_p)$  :  $E$  の  $\mathbb{F}_p$ -有理点全体  
→ 有限アーベル群を成す

$G = E(\mathbb{F}_p)$  に於ける離散対数問題を用いた暗号  
... 楕円曲線暗号

## 楕円曲線の離散対数問題 (ECDLP)

$p$  : 素数

$E$  : 有限体  $\mathbb{F}_p$  上の楕円曲線

$E(\mathbb{F}_p)$  :  $E$  の  $\mathbb{F}_p$ -有理点全体の成す有限アーベル群

$P \in E(\mathbb{F}_p)$  を一つ取って固定

$n \in \mathbb{Z}$  に対し、 $nP \in E(\mathbb{F}_p)$  は充分高速に計算できる

問題 :

$Q \in E(\mathbb{F}_p)$  に対し、 $Q = nP$  となる  $n \in \mathbb{Z}$  を見出せ



## 楕円曲線を用いた Diffie-Hellman 鍵共有

楕円離散対数問題 (ECDLP) の困難さを利用して、  
公開通信路で秘密裡に鍵共有を行なう方式

$p$  : 素数,  $E$  :  $\mathbb{F}_p$  上の楕円曲線 (公開)

$E$  の  $\mathbb{F}_p$ -有理点の一つ  $Q \in E(\mathbb{F}_p)$  を  
公開通信路で秘密裡に共有したい

## 楕円曲線を用いた Diffie-Hellman 鍵共有

$p$  : 素数,  $E$  :  $\mathbb{F}_p$  上の楕円曲線 (公開)

$E$  の  $\mathbb{F}_p$ -有理点の一つ  $P \in E(\mathbb{F}_p)$  を1つ取る (公開)  
(位数が充分大きいように選んでおく)

- $A, B$  両者が ランダム かつ 秘密裡に  
それぞれ  $a, b$  を選ぶ
- $A$  は  $aP$  を計算し、 $B$  に送る  
 $B$  は  $bP$  を計算し、 $A$  に送る
- $A$  は  $a(bP)$  を計算、 $B$  は  $b(aP)$  を計算

→  $Q := a(bP) = b(aP)$  を秘密裡に共有出来た !!

## 楕円曲線暗号の利点

- $(\mathbb{Z}/p\mathbb{Z})^\times$  は素数  $p$  で決まってしまう  
→ 群を変えるには  $p$  を大きくする必要あり
- 一方、1つの素数  $p$  に対して、  
楕円曲線  $E$  を変えれば  $E(\mathbb{F}_p)$  は色々出来る  
→  $p$  を大きくしなくても適切なものを選べる
- $(\mathbb{Z}/p\mathbb{Z})^\times$  に関する離散対数問題より、  
 $E(\mathbb{F}_p)$  に関する離散対数問題の方が難しいようだ
- 現状で同程度の安全性を求めると、  
楕円曲線暗号の方が小さな  $p$  で済む (効率的)

このように、

現代の情報化社会では、

深い数理現象に基づいた様々な数理技術によって、

安全性・確実性・効率性が支えられている

(ので、数学にしっかり取り組みましょう)

おしまい