# 数学入門公開講座

平成6年8月8日（月）から8月12日（金）まで

京都大学数理解析研究所

# 講師及び内容

## 1．代数曲線の幾何（6時間15分）

京都大学数理解析研究所・教授　森　　重　文

代数幾何は代数的に定義された図形（代数多様体）を研究する学問である。19世紀に始まり、現在までに目覚ましい発展を遂げている。図形には次元という概念があり、現在は1次元（曲線）、2次元（曲面）そして3次元までが大まかに分類されてきている。

ここでは、曲線について、その形そして分類などを中心に入門的な話をする。

## 2．プログラミング言語の数理モデル（6時間15分）

京都大学数理解析研究所・助教授　大　堀　　淳

プログラミング言語は、単なる計算の手順を記述する手段であるばかりでなく、複雑なプログラムを構築する上で必要な抽象化の概念と構造化の機構を提供するものです。ここでは、プログラミング言語の持つべき種々の望ましい性質の分析や新しいプログラミング言語の設計などを行なう基礎となる数学的モデルの概略を解説した後、プログラミング言語研究における最近の話題を幾つか紹介します。

## 3．楕円曲線と整数論（6時間15分）

京都大学数理解析研究所・助手　玉　川　安騎男

楕円曲線は、代数幾何学的には、（有理点を1つ与えられた）種数1の代数曲線として特徴づけられる比較的易しい代数多様体であるが、整数論的には、多くの重要な問題（しかもその多くは現在もなお未解決）と関連した、たいへん豊かな対象である。この講義では、予備知識の解説を含む楕円曲線についての入門的な話と並行して、いくつかのより進んだ「夢のある」話も折り込んでいく予定である。

# 時　間　割

| 日 / 時間 | 8月8日(月) | 9日(火) | 10日(水) | 11日(木) | 12日(金) |
|---|---|---|---|---|---|
| 10：30～11：45 | 森 | 森 | 森 | 森 | 森 |
| 11：45～13：00 | 休　憩 | | | | |
| 13：00～14：15 | 大堀 | 大堀 | 大堀 | 大堀 | 大堀 |
| 14：15～14：45 | 休　憩 | | | | |
| 14：45～16：00 | 玉川 | 玉川 | 玉川 | 玉川 | 玉川 |

平成6年度(第16回)数学入門公開講座テキスト(京都大学数理解析研究所, 平成6年8月8日～8月12日開催)

# 楕円曲線と整数論

京都大学数理解析研究所・助　手　玉川安騎男

1994, AUGUST 8, 9, 10, 11, 12,　　14:45 ~ 16:00

# 楕円曲線と整数論

玉川安騎男

毎回、最初の１時間は（５日連続の）講義形式の話、最後の１５分間は日替わりの「夢のある」話をする予定です。以下のテキストは最初の１時間（× ５）の分です。

## §1. はじめに（Diophantus 方程式について）

記法：

$$\begin{aligned}
&\mathbb{Z} = \{\text{整数全体}\} = \{0, \pm 1, \pm 2, \dots\},\\
&\mathbb{Q} = \{\text{有理数全体}\} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\},\\
&\mathbb{R} = \{\text{実数全体}\},\\
&\mathbb{C} = \{\text{複素数全体}\} = \{a + b\sqrt{-1} \mid a, b \in \mathbb{R}\}.
\end{aligned}$$

Diophantus 方程式（＝不定方程式）とは、$\mathbb{Z}$ に係数を持つ有限個の（多変数）方程式で、変数も $\mathbb{Z}$（あるいは $\mathbb{Q}$）に制限して考えたものをいいます。より具体的には、$f_1, \dots, f_m$ を $m$ 個の $\mathbb{Z}$ - 係数 $n$ 変数多項式とした時、連立方程式

$$\begin{aligned}
&f_1(x_1, \dots, x_n) = 0\\
&\cdots\\
&f_m(x_1, \dots, x_n) = 0
\end{aligned}$$

の $\mathbb{Z}$（あるいは $\mathbb{Q}$）における解を求めよ、という問題です。

以下では、主に $m = 1, n = 2$ の場合を考えます。

例１：（Fermat の問題。） $x^n + y^n = 1$ の $\mathbb{Q}$ における解は、$n \geqq 3$ の時、

$$(x, y) = \begin{cases} (1,0), (0,1), & n：\text{奇数} \\ (\pm 1, 0), (0, \pm 1), & n：\text{偶数} \end{cases}$$

に限るか？

このような問題は一般にはたいへん難しいことが多く、ある意味で一般的な解法が存在しないことさえ知られています（Hilbert の第１０問題）。

さて、与えられた Diophantus 方程式 $f(x, y) = 0$ を解くという問題を考える時、この問題をいくつかの段階に分けることができます。

問題Ａ：$f(x, y) = 0$ に解があるかないか？

問題Ｂ：$f(x, y) = 0$ の解は（たかだか）有限個か？

問題Ｃ１：解が有限個の場合は、すべて書き上げよ。

問題Ｃ２：解が無限個の場合は、なんとかして（！）記述せよ。

もちろん、これらの問題が $\mathbb{Z}$ と $\mathbb{Q}$ に対してそれぞれ考えられるわけです。

これらの問題について現在どのようなことがわかっているかを述べる前に、$\mathbb{R}$ と $\mathbb{C}$ における方程式 $f(x,y)=0$ の解について見てみましょう。

$\mathbb{R}$ における $f(x,y)=0$ の解全体 $\{(x,y)\in\mathbb{R}^2 \mid f(x,y)=0\}$ は、平面 $\mathbb{R}^2$ 上のグラフによって表すことができます。（$x^2+y^2+1=0$ のように、空集合になってしまうこともあります。）

一方、$\mathbb{C}$ における $f(x,y)=0$ の解全体 $\{(x,y)\in\mathbb{C}^2 \mid f(x,y)=0\}$ は、$\mathbb{C}^2$ が実4次元の空間なので目に見えるグラフを作ることはできませんが、解全体のなす図形だけを取り出せば、（伸ばしたり縮めたりして）3次元空間 $\mathbb{R}^3$ に埋め込むことができます。$f$ が $\mathbb{C}$ 上の多項式として既約で、「特異点を持たない」図形を定める時には、$\mathbb{C}$ における $f(x,y)=0$ の解全体のなす図形は、$n$ 個の点でパンクした $g$ 人乗りの浮き袋のような形をしていることが知られています。ここで、$g\geqq 0$ と $n\geqq 1$ は $f$ から決まるある整数です。（$g$ を種数といいます。$n$ は「無限遠点」の個数です。）

しかし、これらのグラフや図形をいくらながめていても、$\mathbb{Z}$ あるいは $\mathbb{Q}$ に座標をもつ点がどこにあるのかさっぱりわかりません。

ところが、たいへん不思議なことに、Diophantus 問題（＝ Diophantus 方程式を解く問題）は、その方程式の $\mathbb{C}$ における解全体の定める図形の「形」に大きく依存していることがわかってきています。　例えば、$\mathbb{Q}$ における問題Ａについては

$g=0$：判定法あり（Hasse 原理）。
$g\geqq 1$：一般には Hasse 原理は成立しない。

問題Ｂについては

$g=0$：解は0個または無限個。
$g=1$：解は有限個のことも無限個のこともある。
$g\geqq 2$：解はいつでも有限個。

となっています。最後の結果は Mordell 予想と呼ばれていたもので、１０年ほど前に Faltings によって証明されました：

定理（Faltings）：$g\geqq 2$ の時、$f(x,y)=0$ の $\mathbb{Q}$ における解は有限個。

なお、$\mathbb{Z}$ における解についても、同様の結果があります。

定理（Siegel）：$g=0, n\geqq 3$ または $g\geqq 1$ の時、$f(x,y)=0$ の $\mathbb{Z}$ における解は有限個。

問題Ｃ１は、問題Ｂの答えが Yes であっても（つまり、解の個数が有限個であることがわかっても）、簡単ではありません。順番に代入していく方法では、いつになった

ら終わってよいのかわかりません。例えば、例1の $x^n + y^n = 1$ の場合、$\mathbb{C}$ における解全体のなす図形の種数 $g$ は $\frac{1}{2}(n-1)(n-2)$ となり、したがって、Faltings の定理によって $n \geqq 4$ ならば $\mathbb{Q}$ における解の個数が有限個であることがわかります（実は、$n = 3$ の時も有限個になることが示せます）。しかし、その有限個の解全部を書き上げることは、また別の問題です。

最後に問題C 2についてですが、無限個の解を記述する方法としては、パラメータを使って表示する方法（例2）、いくつかの基本解からある（いくつかの）操作によって帰納的に与えていく方法（例3）、などが考えられます。

例2： $x^2 = 3y^2 + 1$ の $\mathbb{Q}$ における解全体は、

$$\{(\frac{3t^2+1}{3t^2-1}, \frac{-2t}{3t^2-1}) \mid t \in \mathbb{Q}\} \cup \{(1,0)\}$$

で与えられる。（$(1,0)$ は、$t$ に $\infty$ を代入したものと考えることもできる。）

例3： $x^2 = 3y^2 + 1$ の $\mathbb{Z}$ における解全体は、次のように表される。$P = (x,y)$ に対し、$\tau(P) = (2x+3y, x+2y), \iota(P) = (x,-y)$ とおく。この時、解全体は、

$$\{(\pm 1, 0)\} \cup \{\tau^n((\pm 1,0)) \mid n = 1,2,\dots\} \cup \{\iota(\tau^n((\pm 1,0))) \mid n = 1,2,\dots\}$$

で与えられる。ここで、

$$\tau^n(P) = \underbrace{\tau(\tau(\dots(\tau}_{n\text{回}}(P))\dots)).$$

なお、問題C 2は、Faltings の定理と Siegel の定理によって、$\mathbb{Q}$ における解ならば $g = 0, 1$、$\mathbb{Z}$ における解ならば $g = 0, n = 1, 2$ の場合だけが問題になります。例2、例3は、$g = 0, n = 2$ の場合です。$g = 1$ の場合に $\mathbb{Q}$ における解全体を記述する方法を考えるのが、この講義の1つの大きなテーマです。

## §2. 群についての準備

この§では、群に関する知識を用語集的にまとめておきます。講義では、必要に応じて、例を出して解説を加える予定です。

群： 集合 $G$ の上に演算 $G \times G \to G$, $(x,y) \mapsto x \circ y$ が与えられているとする。この時、次の公理1、2、3が満たされれば、$G$ は（正確には、$(G, \circ)$ は）群であるという。

1、任意の $x, y, z \in G$ に対し、$(x \circ y) \circ z = x \circ (y \circ z)$
2、$e \in G$ があって、任意の $x \in G$ に対し、$x \circ e = e \circ x = x$
3、任意の $x \in G$ に対して、$\iota(x) \in G$ があって、$x \circ \iota(x) = \iota(x) \circ x = e$

2を満たす$e$はただ一つ定まる。$e$を$G$の単位元という。各$x$に対し、3を満たす$\iota(x)$はただ一つ定まる。$\iota(x)$を$x$の逆元という。

アーベル群： 群$G$が、さらに

4、任意の$x, y \in G$に対し、$x \circ y = y \circ x$

を満たす時、$G$をアーベル群（または、可換群）という。

（注意）普通、群の演算は積で表し、$x \circ y$を$xy$と書く。この時は、単位元$e$を1、$x$の逆元$\iota(x)$を$x^{-1}$と書く。アーベル群については、演算を和で表し$x \circ y$を$x+y$と書くこともあり、この時は、単位元$e$を0、$x$の逆元$\iota(x)$を$-x$と書く。

$n$乗（または$n$倍）： 群の元$x$と整数$n$に対して、

$$x^n = \begin{cases} \underbrace{x \circ \cdots \circ x}_{n}, & n > 0 \\ e, & n = 0 \\ \iota(x)^{-n}, & n < 0 \end{cases}$$

を$x$の$n$乗という。演算を和で表す時には、$x$の$n$倍といい、$nx$で表す。すなわち、

$$nx = \begin{cases} \underbrace{x + \cdots + x}_{n}, & n > 0 \\ 0, & n = 0 \\ (-n)(-x), & n < 0 \end{cases}$$

部分群： 群$G$の部分集合$H$が

(i) $x, y \in H \Longrightarrow x \circ y \in H$
(ii) $e \in H$
(iii) $x \in H \Longrightarrow \iota(x) \in H$

を満たす時、$H$を$G$の部分群という。この時$H$は、$G$の演算$\circ$を制限することによって群となる。アーベル群の部分群はアーベル群になる。

正規部分群： 群$G$の部分群$H$が、

$y \in H, x \in G \Longrightarrow x \circ y \circ \iota(x) \in H$

を満たす時、$H$を$G$の正規部分群という。アーベル群のすべての部分群は正規部分群である。

商群： $G$を群とし、$H$をその部分群とする。この時、$x, y \in G$に対し、$\iota(x) \circ y \in H$であることを$x \sim y$で表すと、$\sim$は$G$の上の同値関係になる。すなわち、

(i) $x \sim x$ （反射律）
(ii) $x \sim y \Longrightarrow y \sim x$ （対称律）
(iii) $x \sim y, y \sim z \Longrightarrow x \sim z$ （推移律）。

さらに、$H$ が $G$ の正規部分群の時、

(iv) $x \sim y, z \sim w \Longrightarrow x \circ z \sim y \circ w$

も満たされ、この時、同値関係 $\sim$ による $G$ の商集合は、$G$ の演算から誘導される演算によって群となる。この群を $G/H$ で表し、$G$ の $H$ による商群と呼ぶ。

直積： $(G, \circ), (G', \circ')$ を 2 つの群とする。この時、$G$ と $G'$ の直積集合 $G \times G'$ の上に

$$(x, x') \cdot (y, y') = (x \circ y, x' \circ y')$$

によって演算 $\cdot$ を定義すると、$(G \times G', \cdot)$ は群となる。これを $G$ と $G'$ の直積（群）という。3 つ以上の群の直積も同様に定義される。

準同型と同型： $(G, \circ), (G', \circ')$ を 2 つの群とする。$G$ から $G'$ への写像 $f$ が、任意の $x, y \in G$ に対して

$$f(x \circ y) = f(x) \circ' f(y)$$

を満たす時、$f$ を $G$ から $G'$ への準同型（写像）という。この時、

$$f(e) = e', \ f(\iota(x)) = \iota'(f(x))$$

となる。（$e'$ は $G'$ の単位元、$\iota'(x')$ は $x' \in G'$ の逆元を表す。）

さらに $f$ が全単射の時、$f$ を $G$ から $G'$ への同型（写像）という。この時、$f$ の逆写像 $f^{-1}$ は $G'$ から $G$ への同型写像となる。

2 つの群 $G, G'$ の間に同型写像が（一つでも）ある時、$G$ と $G'$ は（互いに）同型であるといい、$G \simeq G'$ と表す。

像と核： $f$ を群 $G$ から群 $G'$ への準同型写像とする。この時、$f$ の像

$$\mathrm{Im}(f) = \{f(x) \mid x \in G\}$$

は $G'$ の部分群となる。また、$f$ の核

$$\mathrm{Ker}(f) = \{x \in G \mid f(x) = e'\}$$

は $G$ の正規部分群となる。

準同型定理： $f$ を $G$ から $G'$ への準同型写像とする時、

$$G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)。$$

有限生成アーベル群の基本定理： $(G, +)$ をアーベル群とする。もし、有限個の $G$ の元 $x_1, \ldots, x_N$ があって、すべての $G$ の元 $x$ が

$$x = n_1 x_1 + \cdots + n_N x_N, \ n_1, \ldots, n_N \in \mathbb{Z}$$

という形に表されるならば、$G$ は有限生成であるという。