4097 は 1 に近いか遠いか

雪江明彦

京都大学大学院理学研究科

2012 年 6 月 1 日

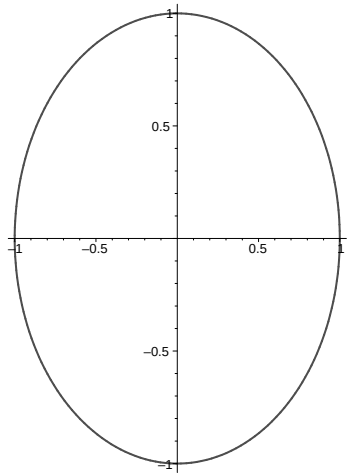
本日の予定

- 不定方定式と「遠い，近い」
- 合同式とハッセの原理
- 2 次の場合のハッセの原理
- 3 次の場合のセルマーの例

不定方定式と「遠い，近い」

整数または有理数を係数とする方程式で解を整数または有理数に限定して考えたものを**不定方程式**という．
ディオファントス方程式ともいう．

例: $x^2 + y^2 = p$ を $\mathbb{R}$ 上で考えると円 $\Rightarrow \infty$ 個の解



$x, y \in \mathbb{Z}$ なら有限個の解 (解がない場合もある)

不定方定式と「遠い，近い」

命題: 不定方定式 $x^2 + 2y^2 = -1$ には整数解がない.
証明: $x, y \in \mathbb{Z} \Rightarrow x^2, y^2 > 0$　左辺 > 0, 右辺 < 0 □
これは代数的な考察ではない.

$$x^2 + 2y^2 - (-1) = x^2 + 2y^2 + 1 \geqq 1 > 0$$

左辺は 0 から「離れている」
$4097 - 1 = 4096$ これは結構大きい数. 4097, 1 は「遠い」

不定方定式と「遠い，近い」

別の問題: $x^2 - 2y^2 = 6$

$y \in \mathbb{R} \Rightarrow x = \pm\sqrt{6 + 2y^2}$ ∞ 個の解

不定方定式としては解がないことを示す.

$x, y \in \mathbb{Q}$ とする.

1. $y = 0 \Rightarrow \sqrt{6}$ 無理数となり矛盾

$y \neq 0$. 同様に $x \neq 0$.

不定方定式と「遠い，近い」

2.

$$x = \frac{3^a x_1}{z},\ y = \frac{3^b y_1}{z},\ 3 \nmid x_1, y_1, z$$

とする.

$$x^2 - 2y^2 = 6 \Leftrightarrow 3^{2a}x_1^2 - 2 \cdot 3^{2b}y_1^2 = 6z^2$$

$b > 0$ と仮定する.

$$3^{2a}x_1^2 = 2 \cdot 3^{2b}y_1^2 + 6z^2$$

3| 右辺 $\Rightarrow a > 0 \Rightarrow$ 9| 左辺, 9 $\nmid$ 右辺 矛盾

不定方定式と「遠い，近い」

3. $b \leqq 0$ なら

$$3^{2a-2b}x_1^2 - 2 \cdot y_1^2 = 2 \cdot 3^{1-2b}z^2$$

3| 右辺, $\Rightarrow$ $a > b$ なら矛盾

よって，$a = b$

$1^2 = 1, 2^2 = 4$ を 3 で割った余りは 1

x_1^2, y_1^2 を 3 で割った余りは 1

$x_1^2 - 2y_1^2$ を 3 で割った余りは -1 矛盾

$\Rightarrow$ 有理数解はない.

不定方定式と「遠い，近い」

この証明では 3 で割り切れるかどうかの考察が重要.

割り切れる $\Rightarrow$ 0 に「近い」

割り切れない $\Rightarrow$ 0 から「遠い」

0 に近いものと遠いものが等しいことを示して矛盾を導いている.

$$4097 - 1 = 4096 = 2^{12}$$

1 と 4097 は差が 2 の高いべきで割り切れるので，ある意味では「近い」

合同式とハッセの原理

$f(x,y)$ 整数係数多項式, $n>0$
定義: $x,y\in\mathbb{Z}$, $n|f(x,y)$ なら (x,y) は n を法とする合同方程式の解といい，$f(x,y)\equiv 0 \mod n$ と書く.

$$x,y\in\mathbb{Z},\ f(x,y)=0$$

なら任意の $n>0$ に対し (x,y) は n を法とする解.
逆がいえるとき

「ハッセの原理が成り立つ」

という.

合同式とハッセの原理

合同方程式は素数べきの法に帰着する.

例えば，$n = 2^2 \cdot 3^2 = 36$.

$$f(x, y) \equiv 0 \mod 36$$
$$\Rightarrow f(x, y) \equiv 0 \mod 4, 9$$

逆に

$$f(x_1, y_1) \equiv 0 \mod 4,$$
$$f(x_2, y_2) \equiv 0 \mod 9$$

なら，

合同式とハッセの原理

中国式剰余定理により $x, y \in \mathbb{Z}$ を

$$x \equiv x_1 \mod 4,\ x \equiv x_2 \mod 9,$$
$$y \equiv y_1 \mod 4,\ y \equiv y_2 \mod 9$$

とすれば，

$$f(x, y) \equiv 0 \mod 36.$$

よって，合同方程式は素数べきの法の場合に帰着する.

合同式とハッセの原理

例: $f(x) = x^2 + 14 \equiv 0 \mod 5^n$ の解を求める

$$f(1) = 15 \equiv 0 \mod 5$$

$$\begin{aligned} f(1+5t) &= (1+5t)^2 + 14 \\ &= 15 + 10t + 25t^2 \\ &\equiv 5(2t+3) \mod 25 \end{aligned}$$

$t = 1$ にとれば $f(6) \equiv 0 \mod 25$

合同式とハッセの原理

$$f(t) \equiv 0 \mod 5^n,\ t \equiv 1 \mod 5$$

となったとする. $f(t) = 5^n a$ なら,

$$\begin{aligned} f(t + 5^n x) &= f(t) + 5^n f'(t)x + 5^{2n} * \\ &\equiv 5^n(2tx + a) \mod 5^{n+1}. \end{aligned}$$

$t \equiv 1 \mod 5$ なので, $2tx + a \equiv 0 \mod 5$ となる $x \in \mathbb{Z}$ がある. 赤の部分はテイラー展開.
5^n を法とする解は n が大きくなるにつれ, ある意味, 解に近いとみなせる.

合同式とハッセの原理

実数 $3.141592\cdots$ とは

$$3+\frac{1}{10}+\frac{4}{10^2}+\frac{1}{10^3}+\cdots$$

を数学的対象と認めたもの.
$a_0, a_1, a_2, \ldots \in \mathbb{Z}$ とし，

$$a_0+5a_1+5^2a_2+\cdots$$

を数学的対象と認めたものを 5 進数という.
素数 p に対し，p 進整数環 $\mathbb{Z}_p$ を定義できる.

$$\sqrt{-14} \in \mathbb{Z}_5.$$

ヘンゼルの補題

定理: (ヘンゼルの補題) $f(x)$ 整数係数多項式，

$$
\begin{aligned}
& f(t) \equiv 0 \mod p, \\
& f'(t) \not\equiv 0 \mod p \\
\Rightarrow & {}^{\exists} x \in \mathbb{Z}_p, f(x) = 0, \ x \equiv t \mod p.
\end{aligned}
$$

例: $f(x) = x^5 - x - 3$ なら，

$$
\begin{aligned}
& f(2) = 27 \equiv 0 \mod 3, \\
& f'(2) = 79 \not\equiv 0 \mod 3
\end{aligned}
$$

したがって，$f(x) = 0$ となる $x \in \mathbb{Z}_3$ がある.

2次の場合のハッセの原理

$\mathbb{Z} \subset \mathbb{Z}_p$ なので，

$f(x) = 0$ が整数解 $\Rightarrow$ $f(x) = 0$ が p 進整数解

$\Leftrightarrow {}^{\forall} n, f(x) \equiv 0$ が n を法とする解

多変数でも同様

定理: (2次形式のハッセの原理) $a, b, c \in \mathbb{Z}$

$$f(x, y) = ax^2 + bxy + cy^2 = 0$$

がすべての $\mathbb{Z}_p$ と $\mathbb{R}$ で自明でない解を持てば，自明でない整数解がある. (n 変数でも成り立つ.)

2次の場合のハッセの原理

証明: $D = b^2 - 4ac$ とおく.

$$f(x,y) = 0 \Leftrightarrow (2ax + by)^2 + (4ac - b^2)y^2 = 0,$$
$$\Leftrightarrow (2ax + by)^2 = Dy^2.$$

D が平方数であることを証明したい.

$$\mathbb{R} \text{ で解} \Rightarrow D > 0.$$

D が平方数でなければ,

$$D = p_1 \cdots p_t D_1^2$$

($p_1, \ldots, p_t$ は異なる素数).

2次の場合のハッセの原理

$2ax + by = z$ とおくと，

$$z^2 = Dy^2.$$

左辺 p_1 で偶数回割れる，
右辺 p_1 で奇数数回割れる
$\Rightarrow$ 矛盾.

$D = D_1^2$ とすると，

$$z^2 = (D_1 y)^2$$

は整数解がある.
(チェボタレフの密度定理 $\Rightarrow$ 2変数3次形式でもOK.)

3 次の場合のセルマーの例

3 変数 3 次形式の場合にはハッセの原理は成り立たない.

定理: (セルマー 1951) $f(x,y,z) = 3x^3 + 4y^3 + 5z^3$
(1) $f(x,y,z) = 0$ は $\mathbb{Z}_p$, $\mathbb{R}$ で自明でない解を持つ.
(2) $f(x,y,z) = 0$ は $\mathbb{Q}$ で自明でない解を持たない.

以下，この定理の証明の概略

3次の場合のセルマーの例

1. $p \geqq 7$ 素数の場合

$$a, b \in \mathbb{Z},\ p \nmid a, b,\ 3a^3 \equiv 4b^3$$
$$\Rightarrow 3a^3 + 4(-b)^3 + 5 \cdot 0^3 \equiv 0 \mod p$$
$$\Rightarrow \text{ヘンゼルの補題より } \mathbb{Z}_p \text{ に解}$$

$3a^3 \equiv 5b^3$ といった場合も同様.
$3a^3, 4b^3, 5c^3$ を p で割った余りはすべて異なるとしてよい.

3次の場合のセルマーの例

次の定理は認める

定理: $a \in \mathbb{Z}$ があり，$p \nmid n$ なら $n \equiv a^t \mod p$.

上の定理は「$\mathbb{F}_p^\times$ は巡回群」と解釈できる.

$$3 \equiv a^t,\ 4 \equiv a^s,\ 5 \equiv a^u \mod p$$

とする. $t = 3c + s$ なら

$$3 \equiv a^{3c+s} \equiv 4(a^c)^3 \mod p$$

矛盾. よって，t, s, u を 3 で割った余りは異なる.
$t, s, u \equiv 0, 1, 2 \mod 3$.

3次の場合のセルマーの例

$3 \cdot 4 \cdot 5 = 60 \equiv a^{0+1+2+3c} = (a^{c+1})^3 \mod p.$
$b = a^{c+1}$ とおくと，

$$
\begin{aligned}
& 3 \cdot 4^3 + 4 \cdot 3^3 - 5 \cdot b^3 \\
& \equiv 3 \cdot 4 \cdot (3^2 + 4^2) - 5 \cdot 60 \\
& \equiv 0 \mod p
\end{aligned}
$$

となるので，$f(x, y, z) \equiv 0 \mod p$ は解がある．
ヘンゼルの補題より $\mathbb{Z}_p$ で解．

3次の場合のセルマーの例

2. $p = 2$ の場合

$F(x) = x^3 - 3$, $G(x) = x^3 - 5$ とおくと，

$$F(1) \equiv G(1) \equiv 0 \mod 2,$$
$$F'(1) \equiv G'(1) = 3 \not\equiv 0 \mod 2.$$

よって，$a, b \in \mathbb{Z}_2$ があり，

$$3 = a^3,\ 5 = b^3$$

$$\Rightarrow 3b^3 + 4 \cdot 0^3 + 5(-a)^3 = 0.$$

3次の場合のセルマーの例

3. $p = 5$ の場合

$F(x) = x^3 - 3$, $G(x) = x^3 - 4$ とおく，

$$F(2) \equiv G(4) \equiv 0 \mod 5,$$
$$F'(2) = 12, G'(4) = 48 \not\equiv 0 \mod 5.$$

よって，$a, b \in \mathbb{Z}_5$ があり，

$$3 = a^3,\ 4 = b^3$$

$$\Rightarrow 3b^3 + 4(-a)^3 + 5 \cdot 0^3 = 0.$$

3次の場合のセルマーの例

4. $p = 3$ の場合

$F(x) = x^3 - 10$ とおく.

$$3^3 | F(4) = 54,$$
$$F'(4) = 3 \cdot 4^2.$$

ヘンゼルの補題を少し拡張すると，$10 = a^3$ となる $a \in \mathbb{Z}_3$ がある.

$$3 \cdot 0^3 + 4a^3 + 5(-2)^3 = 0.$$

3次の場合のセルマーの例

5. $F(x,y,z)=0$ は自明でない整数解を持たない.

「数」の概念を広げて考える必要がある.

$$\mathbb{Q}(\sqrt[3]{6}) = \{a + b\sqrt[3]{6} + c\sqrt[3]{36} \mid a,b,c \in \mathbb{Q}\},$$
$$\mathbb{Z}[\sqrt[3]{6}] = \{a + b\sqrt[3]{6} + c\sqrt[3]{36} \mid a,b,c \in \mathbb{Z}\}.$$

$\mathbb{Z}[\sqrt[3]{6}]$ では足し算，引き算，掛け算ができる.
$\mathbb{Q}(\sqrt[3]{6})$ ではそれにくわえて，0 でない数でも割れる.

定理: $\mathbb{Z}[\sqrt[3]{6}]$ では「素因数分解」ができ一意的である.

3次の場合のセルマーの例

$F(x,y,z)=0,\ (x,y,z)\neq(0,0,0)$ として矛盾を導く.
$\gcd(x,y,z)=1$ としてよい.

$$\gcd(x,y)=d>1$$
$$\Rightarrow d^3|(3x^3+4y^3)$$
$$\Rightarrow d^3|5z^3$$
$$\Rightarrow p \text{ が } d \text{ の素因子なら } p|z$$

矛盾. よって $\gcd(x,y)=1$
同様に $\gcd(x,z)=1,\ \gcd(y,z)=1$.

3次の場合のセルマーの例

以下，$\alpha = \sqrt[3]{6}$ とおく.

$$-10z^3 = (2y)^3 + 6x^3 = (2y + \alpha x)(4y^2 - 2\alpha xy + \alpha^2 x^2)$$

左辺はほとんど3乗
$2y + \alpha x$ と $4y^2 - 2\alpha xy + \alpha^2 x^2$ が「互いに素」なら，両方とも3乗になる.

$$(2 - \alpha)^3 = 8 - 12\alpha + 6\alpha^2 - 6 = 2(1 - 6\alpha + 3\alpha^2),$$
$$(1 - 6\alpha + 3\alpha^2)(109 + 60\alpha + 33\alpha^2) = 1.$$

だから 2 は $(2 - \alpha)^3$ とほとんど同じ.

3次の場合のセルマーの例

$\mathbb{Z}[\alpha]^\times$: $\mathbb{Z}[\alpha]$ で割り算できる数の集合
$\epsilon = 1 - 6\alpha + 3\alpha^2 \in \mathbb{Z}[\alpha]^\times$
$2y + \alpha x$ は完全には3乗にはならないが，

$$2y + \alpha x = (2 - \alpha)(1 - \alpha)\epsilon^j \xi^3$$

$(\xi \in \mathbb{Z}[\alpha])$.
$\epsilon_0 = (2 - \alpha)^3/2$ とおくと ϵ は ϵ_0 のべき. $j = 0, 1, 2$ があり

$$2y + \alpha x = (2 - \alpha)(1 - \alpha)\epsilon_0^j \xi_0^3.$$

$\xi_1 = \xi_0(2 - \alpha)$ とおくと，

$$2^j(2y + \alpha x) = (2 - \alpha)(1 - \alpha)\xi_1^3.$$

3次の場合のセルマーの例

$\xi_1 = a + b\alpha + c\alpha^2$ として右辺を展開し，α^2 の項

$$\begin{aligned} 0 = {} & a^3 + 6b^3 + 36c^3 + 36abc \\ & + 6ab^2 + 6a^2c + 36bc^2 \\ & - 9a^2b - 54ac^2 - 54b^2c. \end{aligned}$$

すると，

$$\begin{aligned} a^3 \text{ 以外は } 3 \text{ で割れる} &\Rightarrow 3|a, \\ 6b^3 \text{ 以外は } 9 \text{ で割れる} &\Rightarrow 3|b, \\ 36c^3 \text{ 以外は } 27 \text{ で割れる} &\Rightarrow 3|c. \end{aligned}$$

よって，$3|2y + \alpha x$ である．$3|y$, $3x^3 + 4y^3 + 5z^3 = 0$ なので，$3|z$. 矛盾.