

# $p$ 進数について (前半)

2021 年 5 月 14 日

## 1 導入

方程式の整数解, すなわち不定方程式を考察する. まずは簡単な観察であるが,  $m$  を正整数とすると,  $x, y$  に関する不定方程式

$$x^2 + y^2 = -m \quad (1.1)$$

は整数解を持たない. なぜならば, そもそも (1.1) には実数解  $x, y$ すらも存在しないためである.

さて, 次に  $m$  を整数とする. すると,  $x, y$  に関する不定方程式

$$x^2 - 3y^2 = 4m + 3 \quad (1.2)$$

は整数解を持たない. 実際, 整数解  $(x, y)$  が存在すると仮定する. このとき, (1.2) を 4 で割った余りを考えると, 以下が成立する:

$$x^2 - 3y^2 \equiv x^2 + y^2 \equiv 4m + 3 \equiv 3 \pmod{4}.$$

よって,

$$x^2 + y^2 \equiv 3 \pmod{4} \quad (1.3)$$

となる. ところが, 平方数を 4 で割った余りは 0 または 1 である.

※  $(2k)^2 = 4k^2, (2k+1)^2 = 4(k^2+k)+1$ .

したがって,  $x^2 + y^2$  を 4 で割った余りは 0, 1, 2 のどれかでなくてはならず, (1.3) は成立しない. よって矛盾が生じる. (1.2) に対する上記の観察を一般化する.  $F(X, Y) \in \mathbb{Z}[X, Y]$  に対する不定方程式  $F(x, y) = 0$  の整数解  $x, y$  が存在するための十分条件を調べる目的で, 整数で割った余りを考察

することは自然な方針である.

※ (1.2) では,  $F(X, Y) = X^2 - 3Y^2 - 4m - 3$ .  $F(x, y) = 0$  の整数解  $x, y$  が存在するための十分条件として, (議論を簡略化するために) 固定された素数  $p$  に対して  $p^n$  で割った余りを考察する. すなわち,

$$F(x, y) \equiv 0 \pmod{p^n} \quad (1.4)$$

に整数解  $(x, y)$  が存在するかどうかを考察する. 曖昧な表現ではあるが, 標語的に述べると大きい  $n$  に対して, (1.4) に解が存在すれば,  $F(x, y) = 0$  に解が存在する可能性が高い. (1.4) と関連して, 2 本のファイル (前半と後半) で  $p$  進数と呼ばれる数を紹介する.  $p$  進数は, 有理数を含む数であるが, 実数とは異なる. まず, 準備として次の章で  $\mathbb{Q}$  に対して  $p$  進距離を導入する. これは,  $\mathbb{Q}$  における通常の距離とは異なる.  $p$  進距離では, 十分大きい  $n$  に対して  $p^n$  で割りきることができる有理数は 0 に近いとみなす. この距離を導入するモチベーションの一つは方程式 (1.4) にある.  $n$  が大きいほど, 方程式 (1.4) は方程式  $F(x, y) = 0$  に近いと考えるのである.

## 2 $p$ 進ノルム

—— 文字  $p$  に関する注意 ——

このファイルでは, 本章以降  $p$  は素数を表すとする.

**定義 2.1.**  $p$  を素数とする.  $x \in \mathbb{Q}$  に対して,  $|x|_p$  を以下のように定める:

- (1)  $x = 0$  のとき,  $|0|_p = 0$  と定める.
  - (2)  $x \neq 0$  のとき,  $x = p^\ell \frac{a}{b}$  ( $\ell, a, b \in \mathbb{Z}$ , ただし,  $a, b$  は  $p$  で割り切れない.) と表す. このとき,  $|x|_p = p^{-\ell}$  と定義する.
- $|x|_p$  を  $x$  の  $p$  進ノルムと呼ぶ.

**例 2.1.**  $p = 2$  の場合を考える.

$$\left| \frac{36}{5} \right|_2 = \left| 4 \cdot \frac{9}{5} \right|_2 = \frac{1}{4}, \quad \left| \frac{27}{40} \right|_2 = \left| \frac{1}{8} \cdot \frac{27}{5} \right|_2 = 8.$$

**命題 2.1.**  $p$  を素数とする. すると, 以下が成立する:

- (1) 任意の  $x \in \mathbb{Q}$  に対して,  $|x|_p \geq 0$ .
- (2) 任意の  $x \in \mathbb{Q}$  に対して, 「 $|x|_p = 0 \Leftrightarrow x = 0$ 」.

- (3) 任意の  $x, y \in \mathbb{Q}$  に対して,  $|xy|_p = |x|_p |y|_p$ . 特に,  $|-x|_p = |x|_p$ .  
 (4) 任意の  $x, y \in \mathbb{Q}$  に対して,  $|x + y|_p \leq \max\{|x|_p, |y|_p\}$  (以下, 強三角不等式と呼ぶ).

※  $a, b$  が  $p$  で割りきれない整数のとき,  $\left| p^\ell \frac{a}{b} \right|_p = p^{-\ell}$  (再掲).

※ (4) 任意の  $x, y \in \mathbb{Q}$  に対して,  $|x + y|_p \leq \max\{|x|_p, |y|_p\}$  (以下, 強三角不等式と呼ぶ) (再掲).

証明. (1), (2), (3) は  $p$  進ノルムの定義により従う. (4) のみを示す.  $x = 0$  または  $y = 0$  の場合は明らかであるので,  $x \neq 0$  かつ  $y \neq 0$  であると仮定する. また,  $x + y = 0$  の場合も明らかなので,  $x + y \neq 0$  であると仮定する.

$$x = p^{\ell_1} \frac{a_1}{b_1}, \quad y = p^{\ell_2} \frac{a_2}{b_2}$$

と置く ( $\ell_1, \ell_2, a_1, a_2, b_1, b_2 \in \mathbb{Z}$ .  $a_1, a_2, b_1, b_2$  は  $p$  で割り切れない).  
 $\ell_1 \leq \ell_2$  としても一般性を失わない. このとき,  $\max\{|x|_p, |y|_p\} = p^{-\ell_1}$  である. よって,

$$x + y = p^{\ell_1} \cdot \frac{a_1 b_2 + p^{\ell_2 - \ell_1} a_2 b_1}{b_1 b_2}.$$

$b_1 b_2$  は  $p$  で割り切れないので,  $|x + y|_p \leq p^{-\ell_1} = \max\{|x|_p, |y|_p\}$ . □

命題 2.1 より, 以下の系が従う:

**系 2.1.**  $p$  を素数とする.  $x, y \in \mathbb{Q}$  に対して,  $d_p(x, y) = |x - y|_p$  とおく. すると, この  $d_p$  は距離関数の公理を満たす. つまり,

1. 任意の  $x, y \in \mathbb{Q}$  に対して,  $d_p(x, y) \geq 0$ .
2. 任意の  $x, y \in \mathbb{Q}$  に対して,  $d_p(x, y) = 0$  となる必要十分条件は,  $x = y$ .
3. 任意の  $x, y \in \mathbb{Q}$  に対して,  $d_p(x, y) = d_p(y, x)$ .
4. 任意の  $x, y, z \in \mathbb{Q}$  に対して,  $d_p(x, z) \leq d_p(x, y) + d_p(y, z)$ .

なお, 最後の性質に関しては, より強い次の性質が成立する:

$$\text{任意の } x, y, z \in \mathbb{Q} \text{ に対して, } d_p(x, z) \leq \max\{d_p(x, y), d_p(y, z)\}. \quad (2.1)$$

(2.1) が成り立つ距離を非アルキメデス距離と呼び,  $d_p$  を  $p$  進距離と呼ぶ.

通常の距離と  $p$  進距離の違いを強調するために、 $\mathbb{Q}$  における収束列の例を紹介する。

**例 2.2.** (1) 通常の距離で  $9 + 9 \cdot 10^{-1} + 9 \cdot 10^{-2} + \cdots = \sum_{n=0}^{\infty} 9 \cdot (10^{-1})^n$  は、 $\mathbb{Q}$  において  $9/9 = 1$  に収束する。

(2)  $p$  進距離に関して、 $p - 1 + (p - 1)p + (p - 1)p^2 + \cdots = \sum_{n=0}^{\infty} (p - 1)p^n$  は、 $(\mathbb{Q} \text{ において }) -1$  に収束する!

実際に、 $a_N = \sum_{n=0}^N (p - 1)p^n$  とおく。  $\sum_{n=0}^{\infty} (p - 1)p^n = -1$  を示すためには、 $1 + a_N$  が  $0$  に収束することを示せばよい。  $1 + a_N = p^{N+1}$  より、 $|1 + a_N|_p = p^{-1-N}$  である。 よって、 $1 + a_N$  は  $0$  に収束する。

通常の距離にて、 $\mathbb{Q}$  のコーシー列は必ずしも収束するとは限らない。

※有理数の列  $(a_n)_{n \geq 0}$  が通常の距離に関するコーシー列であるとは、任意の  $\varepsilon > 0$  に対して、 $N > 0$  が存在して、以下を満たすことである：

$n, m$  が  $n \geq N$  かつ  $m \geq N$  を満たすならば、 $|a_n - a_m| < \varepsilon$ 。

$\mathbb{Q}$  のコーシー列すべてに収束先を与えたものが  $\mathbb{R}$  である (完備化)。 おおまかなイメージでは、 $\sum_{n=-\infty}^R a_n \cdot 10^n (\forall n, 0 \leq a_n \leq 9)$  という形の数をも  $\mathbb{Q}$  に補ったものが  $\mathbb{R}$  である。

この完備化という操作を、 $p$  進距離でおこなったものが  $\mathbb{Q}_p$  である。 次回のファイルで詳細を述べるが、 $\sum_{n=-R}^{\infty} a_n \cdot p^n (\forall n, 0 \leq a_n \leq p - 1)$  という形の数をも  $\mathbb{Q}$  に補ったものが  $\mathbb{Q}_p$  である。 次の章に移る前に、 $p$  進距離特有の命題を一つ述べる：

**命題 2.2.**  $a, b \in \mathbb{Q}$  とする。  $|a|_p < |b|_p$  と仮定する。 すると、 $|a - b|_p = |b|_p$ 。

※さらに、同じ仮定のもとで、 $|-b|_p = |b|_p < |a|_p$  から

$|a + b|_p = |a - (-b)|_p = |b|_p$  も導ける。

**補足 2.1.**  $a, b \in \mathbb{Q}$  に対して、 $0, a, b$  を頂点とする三角形  $A$  を考える。 命題 2.2 により、 $p$  進距離に関して常に二等辺三角形である! 実際、 $|a|_p = |b|_p$  のときはもちろん三角形  $A$  は二等辺三角形。  $|a|_p \neq |b|_p$  のときは、 $|a|_p < |b|_p$  としても一般性を失わない。 このとき、命題 2.2 により  $|a - b|_p = |b|_p$  であり、やはり三角形  $A$  は二等辺三角形。

平行移動を考えると、 $x, y, z \in \mathbb{Q}$  を頂点とする三角形は  $p$  進距離に関して常に二等辺三角形!

命題 2.2 の証明。 まず、強三角不等式より、 $|a - b|_p \leq |-b|_p = |b|_p$  である。 以下、 $|b|_p \leq |a - b|_p$  を示せばよい。 再び強三角不等式より、

$$|b|_p = |a - (a - b)|_p \leq \max\{|a|_p, |a - b|_p\}$$

しかし、仮定より  $|b|_p \leq |a|_p$  はあり得ない。 よって、 $|b|_p \leq |a - b|_p$ 。  $\square$

### 3 $p$ 進数

$\mathbb{Q}$  の  $p$  進距離に関する完備化  $\mathbb{Q}_p$  を紹介する. 以下の方法は, 一般の距離空間の完備化について, 特殊な場合を  $p$  進ノルムを用いて述べたもの.

有理数の列  $\mathbf{a} = (a_n)_{n \geq 0}$  が  $p$  進距離に関するコーシー列であるとは, 任意の  $\varepsilon > 0$  に対して,  $N > 0$  が存在して, 以下を満たすことである:  $n, m$  が  $n \geq N$  かつ  $m \geq N$  を満たすならば,  $|a_n - a_m|_p < \varepsilon$ .

$\mathbf{a} = (a_n)_{n \geq 0}$ ,  $\mathbf{a}' = (a'_n)_{n \geq 0}$  をともに有理数からなる  $p$  進距離に関するコーシー列とする. 同値関係  $\mathbf{a} \sim \mathbf{a}'$  を以下で定義:  $\lim_{n \rightarrow \infty} |a_n - a'_n|_p = 0$ .

例:  $a_n = \sum_{j=0}^n (p-1)p^j$ ,  $a'_n = \sum_{j=0}^{2n} (p-1)p^j$  を用いて

$\mathbf{a} = (a_n)_{n \geq 0}$ ,  $\mathbf{a}' = (a'_n)_{n \geq 0}$  を定める. すると,  $\mathbf{a} \sim \mathbf{a}'$  である.

$\sim$  における  $\mathbf{a}$  の同値類を  $\bar{\mathbf{a}}$  と定める. すなわち,

$\bar{\mathbf{a}} = \{\mathbf{a}' \mid \mathbf{a}' \text{ は有理数からなる } p \text{ 進距離に関するコーシー列, } \mathbf{a} \sim \mathbf{a}'\}$ .

$\mathbb{Q}_p := \{\bar{\mathbf{a}} \mid \mathbf{a} \text{ は有理数からなる } p \text{ 進距離に関するコーシー列}\}$  (同値類全体の集合) と定める.  $\mathbb{Q}_p$  の元を  $p$  進数と呼ぶ.  $a, b \in \mathbb{Q}$  に対して, 数列  $\mathbf{a} = (a_n)_{n \geq 0}$ ,  $\mathbf{b} = (b_n)_{n \geq 0}$  を  $(\forall n \geq 0) a_n = a, b_n = b$  で定める. このとき,  $\mathbf{a} \sim \mathbf{b}$  と  $a = b$  は同値である.  $a \in \mathbb{Q}$ , および定数の列  $(a)_{n \geq 0} \in \mathbb{Q}_p$  を同一視することで,  $\mathbb{Q} \subset \mathbb{Q}_p$  とみなす. 定数の列  $(a)_{n \geq 0} \in \mathbb{Q}_p$  も  $a$  と書く.

**命題 3.1.**  $\bar{\mathbf{a}} = \overline{(a_n)_{n \geq 0}} \in \mathbb{Q}_p$  とする.

- (1)  $\bar{\mathbf{a}} = 0$  となる必要十分条件は,  $\lim_{n \rightarrow \infty} |a_n|_p = 0$  である.
- (2)  $\bar{\mathbf{a}} \neq 0$  ならば,  $(\exists N) (\forall n \geq N) |a_n|_p = |a_N|_p =: c(\mathbf{a}) > 0$  である.
- (3) (2) において,  $c(\mathbf{a})$  の値は  $\bar{\mathbf{a}}$  の代表元  $(a_n)_{n \geq 0}$  の選び方に依らない.

**証明.** (1) は  $\sim$  の定義より従う. (2) を示す. まず (1) より  $\lim_{n \rightarrow \infty} |a_n|_p = 0$  ではない. よって, ある  $\varepsilon > 0$  と非負整数から成る単調増加列  $(j(\ell))_{\ell \geq 0}$  が存在して, 以下が成立する: 任意の  $\ell \geq 0$  に対して  $|a_{j(\ell)}|_p > \varepsilon$ . さて,  $(a_n)_{n \geq 0}$  は  $p$  進距離に関してコーシー列なので, ある  $N \geq 0$  が存在して, 以下が成立:  $n, m \geq N$  ならば  $|a_n - a_m|_p < \varepsilon$ . さて,  $n$  を  $N$  以上の任意の整数とする.  $m$  として,  $j(M) \geq N$  を満たす  $j(M)$  を採用する. すると,  $|a_n - a_{j(M)}|_p < \varepsilon$  である. さて,  $|a_{j(M)}|_p > \varepsilon$  と命題 2.2 より, 以下が成立:

$$|a_n|_p = |(a_n - a_{j(M)}) + a_{j(M)}|_p = |a_{j(M)}|_p (> 0). \quad \text{※ } n \text{ に依存しない正定数.}$$

(3) の証明:  $(a_n)_{n \geq 0} \sim (a'_n)_{n \geq 0}$  と仮定する. 十分に大きい任意の  $n$  に対して,  $|a'_n - a_n|_p < c(\mathbf{a}) = |a_n|_p$  である. よって, 再び命題 2.2 より

$$|a'_n|_p = |(a'_n - a_n) + a_n|_p = |a_n|_p$$

□

命題 3.1 より,  $\bar{a} = \overline{(a_n)_{n \geq 0}} \in \mathbb{Q}_p$  に対して,  $|\bar{a}|_p := \lim_{n \rightarrow \infty} |a_n|_p$  は代表元  $(a_n)_{n \geq 0}$  の取り方に依らない. これを  $\bar{a} \in \mathbb{Q}_p$  の  $p$  進ノルムと呼ぶ.  
 さて,  $\bar{a} = \overline{(a_n)_{n \geq 0}}, \bar{b} = \overline{(b_n)_{n \geq 0}} \in \mathbb{Q}_p$  に対して, 和および積を以下のように定義する:

$$\bar{a} + \bar{b} := \overline{(a_n + b_n)_{n \geq 0}}, \quad \bar{a} \cdot \bar{b} := \overline{(a_n \cdot b_n)_{n \geq 0}}.$$

これらの演算が, 代表元  $(a_n)_{n \geq 0}, (b_n)_{n \geq 0}$  の選び方に依らないことは後半のファイルで証明する. また,  $\bar{a}, \bar{b} \in \mathbb{Q}_p$  に対して,  $d_p(\bar{a}, \bar{b}) = |\bar{a} - \bar{b}|_p$  を  $\bar{a}, \bar{b}$  の  $p$  進距離と呼ぶ. 命題 2.1, 系 2.1, 命題 2.2 については,  $\mathbb{Q}$  を  $\mathbb{Q}_p$  に置き換えても成立する. 実際, 例えば  $\mathbb{Q}_p$  に対する命題 2.1(3) は,  $|a_n b_n|_p = |a_n|_p |b_n|_p$  の極限を取れば確認できる.  $\mathbb{Q}_p$  に対する系 2.1 は,  $\mathbb{Q}_p$  に対する命題 2.1 から導ける. なお, 命題 2.2 は強三角不等式を用いることで,  $\mathbb{Q}$  の場合と同様に証明可能.

※  $\mathbb{Q}_p$  が  $p$  進距離に関する完備性は, 後半のファイルで証明する.