

数学 A 整数 No.1

1 約数と倍数

整数 a が整数 b で割り切れるとき、すなわち、 $a = bc$ (c は整数) と表されるとき、 a を b の **倍数**、 b を a の **約数** という。

2 つ以上の整数に共通する倍数を **公倍数** といい、正の公倍数の中で最も小さいものを **最小公倍数** (LCM) という。

2 つ以上の整数の共通する約数を **公約数** といい、公約数の中で最も大きいものを **最大公約数** (GCD) という。

とくに、2 つの整数 a, b の最大公約数が 1 のとき、 a と b は **互いに素** であるという。

例 10 と 21 は互いに素である。

——最小公倍数、最大公約数の性質——

2 つの整数 A, B の最大公約数を G 、最小公倍数を L とするとき、 $A = aG$ 、 $B = bG$ を満たす互いに素な整数 a, b が存在して、次の式が成り立つ。

$$(1) L = abG = aB = Ab$$

$$(2) AB = LG$$

——素数と合成数——

1 とそれ自身のほかに約数を持たない正の整数を **素数** という。ただし、1 は素数ではないとする。1 より大きい整数のうち、素数でないものを **合成数** という。

例 60 より小さい素数は 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59 の 17 個である。

合成数は (積の順序の入れ替えを除いて) ただ 1 通りの方法で、素数の積の形で表すことができる。これを **素因数分解** という。

例 3600 を素因数分解すると、 $2^4 \times 3^2 \times 5^2$ である。

——約数の数とその和——

自然数 N が $N = a^p \times b^q \times \cdots \times c^r$ と素因数分解されるとき、1 および N を含めたその約数の数は

$$(p+1) \times (q+1) \times \cdots \times (r+1)$$

個であり、それらすべての和は

$$(1 + a + a^2 + \cdots + a^p) \times (1 + b + b^2 + \cdots + b^q) \times \cdots \times (1 + c + c^2 + \cdots + c^r).$$

例 3600 の約数の数は、1 および 3600 を含めて $(4+1) \times (2+1) \times (2+1) = 45$ 個であり、それらすべての和は

$$(1 + 2 + 4 + 8) \times (1 + 3 + 9) \times (1 + 5 + 25) = 15 \times 13 \times 31 = 6045.$$

2 不定方程式

一般に、未知数の数と方程式の数が同じであれば、その方程式の解が一意的に定まる。一方、未知数の数よりも有効な方程式の数が少ない方程式を **不定方程式** という。

例 不定方程式 $12x + 5y = 1$ の整数解は $(x, y) = (3, -7), (-2, 5)$ など無数に存在する。

例 不定方程式 $12x + 6y = 1$ の整数解は存在しない。

例 不定方程式 $x^2 - 2x + y^2 - 2y + 2 = 0$ の整数解は $(x, y) = (1, 1)$ のみである。

3 Euclid の互除法

不定方程式の解を求めることは一般には難しいが、 a, b, c を整数とすると、 x, y についての不定方程式

$$ax + by = c$$

の整数解は、 a, b が互いに素な整数であれば、ある「効率的」な手続き^{*1} で求められることが知られている。ここではその方法を学ぼう。

A, B を整数とする。 A を B で割った商を Q 、余りを R とするとき

$$A = BQ + R \quad (\diamond)$$

が成り立つ。ただし、 $0 \leq R < B$ である。 A と B の最大公約数を G 、 B と R の最大公約数を g とする。GCD の性質より、

$$A = aG, \quad B = bG \quad (a \text{ と } b \text{ は互いに素})$$

となる a, b が存在する。 $(\diamond)$ より $R = A - BQ = G(a - bQ)$ であるから、 R もまた G の倍数である。ゆえに、 G は B と R の公約数である。 B と R の最大公約数は g であったから

$$G \leq g \quad (\clubsuit)$$

が成り立つ。一方、GCD の性質より

$$B = b'g, \quad R = rg \quad (b' \text{ と } r \text{ は互いに素})$$

となる整数 b', r が存在する。 $(\diamond)$ より $A = BQ + R = g(b'Q + r)$ であるから、 A もまた g の倍数である。ゆえに g は A と B の公約数である。 A と B の最大公約数は G であったから

$$g \leq G \quad (\heartsuit)$$

である。 $(\clubsuit)$ 、 $(\heartsuit)$ より、 $G = g$ である。この手続きをまとめると、次のことが言える。

Euclid の互除法

整数 A, B に対し、 A を B で割った余りを R とする。 A と B の最大公約数は、 B と R の最大公約数と等しい。

例 133 と 299 の最大公約数を求める。

$$299 = 133 \times 2 + 33, \quad 133 = 33 \times 4 + 1, \quad 33 = 1 \times 33 + 0$$

より、最大公約数は 1 である。

これにより 2 つの整数 a, b の最大公約数を機械的に求めることができる。この手続きを逆からたどると、次の結果を得る。

$$2 \text{ つの整数 } a, b \text{ の最大公約数を } d \text{ とするとき, } ax + by = d \text{ を満たす整数 } x, y \text{ が存在する。}$$

実際、上の例では例えば $299 \times 2 + 133 \times (-3) = 1$ が成り立つから、 $(x, y) = (2, -3)$ である。また、互いに素な 2 つの整数の最大公約数は 1 であるから、次が成り立つことが判る。

a と b が互いに素であるとき、 $ax + by = 1$ を満たす整数 x, y が存在する。

これを踏まえて、実際に不定方程式の解を Euclid の互除法を用いて求める例を示す。

^{*1} ここでいう「効率」とは、コンピュータによる計算時間という意味での「効率」である。慣れている人であれば、この手続きに頼らなくても、パッとみて答えが閃いてしまうこともあるだろう。

例 不定方程式 $44x + 13y = 7$ の整数解を 1 組求める. 44 と 13 は互いに素であるから, $44X + 13Y = 1$ を満たす整数 X, Y が存在する. まずはこの X, Y を 1 組求める. Euclid の互除法を, 余りが 1 になるまで繰り返すと

$$\begin{aligned}44 &= 13 \times 3 + 5 &\iff 5 &= 44 - 13 \times 3 \\13 &= 5 \times 2 + 3 &\iff 3 &= 13 - 5 \times 2 \\5 &= 3 \times 1 + 2 &\iff 2 &= 5 - 3 \\3 &= 2 \times 1 + 1 &\iff 1 &= 3 - 2\end{aligned}$$

である. これを下の式から順次代入していくと

$$\begin{aligned}1 &= 3 - 2 \\&= 3 - (5 - 3) \\&= 3 \times 2 - 5 \\&= (13 - 5 \times 2) \times 2 - 5 \\&= 13 \times 2 - 5 \times 5 \\&= 13 \times 2 - (44 - 13 \times 3) \times 5 \\&= 13 \times 17 - 44 \times 5\end{aligned}$$

であるから, $44 \times (-5) + 13 \times 17 = 1$ が成り立つ. 両辺を 7 倍すれば $44 \times (-35) + 13 \times 119 = 7$ が成り立つことが判るから,

$$(x, y) = (-35, 119)$$

が 1 つの解である.