

「ユークリッドの互除法」

公約数

2つの自然数の共通の約数をその2つの自然数の公約数という。

最大公約数 (Greatest Common Divisor)

2つの自然数の公約数のうち最大のものをその2つの自然数の最大公約数という。
自然数 m と n の最大公約数を $\text{GCD}(m, n)$ 、またはより簡単に (m, n) とかく。

例. $(6, 4) = 2$ 、 $(180, 336) = 12$

2つの数の素因数分解が分かれば、最大公約数は簡単にわかる。

例. $(2^2 \cdot 3^2 \cdot 5, 2^4 \cdot 3 \cdot 7) = 2^2 \cdot 3$

大きな数の素因数分解は難しい!

互いに素

2つの自然数が1以外の公約数をもたないとき、互いに素という。

例. $(13, 5) = 1$ 、 $(14, 9) = 1$

ユークリッドの互除法

ユークリッド (BC 330? ~ BC 275) の有名な著作「原論」第7巻命題1から命題3に書かれている最大公約数を計算する方法。「原論」は当時知られていた数学をまとめたものといわれており、このアルゴリズムはピタゴラスの時代に既に知られていたらしい。「最古のアルゴリズム」といわれる。

具体的には、「自然数 m と n の最大公約数は、 m を n で割った余り r と n の最大公約数に等しい」という原理を繰り返し使って、最大公約数をもとめる方法。

例. $336 = 180 \cdot 1 + 156$ $13 = 5 \cdot 2 + 3$ $28829 = 14351 \cdot 2 + 127$

$180 = 156 \cdot 1 + 24$ $5 = 3 \cdot 1 + 2$ $14351 = 127 \cdot 113$

$156 = 24 \cdot 6 + 12$ $3 = 2 \cdot 1 + 1$

$24 = 12 \cdot 2$ $2 = 1 \cdot 2$

$(336, 180) = (180, 156) = (156, 24) = (24, 12) = 12$

$(13, 5) = (5, 3) = (3, 2) = (2, 1) = 1$

$(28829, 14351) = (14351, 127) = 127$

$mx + ny = (m, n)$ の解法 (x, y は整数)

例. $m = 13, n = 5$ のとき: $13x + 5y = 1$

$$1 = 3 - 2 \cdot 1$$

$$= 3 - (5 - 3 \cdot 1) \cdot 1 = 5 \cdot (-1) + 3 \cdot 2$$

$$= 5 \cdot (-1) + (13 - 5 \cdot 2) \cdot 2 = 13 \cdot 2 + 5 \cdot (-5)$$

Brent の改良型アルゴリズム (コンピュータでの計算に適す)

1. m, n が共に偶数なら、それを 2 で割れるだけ割って、2 のべきをくくりだし、どちらかが奇数の場合に帰着させる。
2. 一方のみが偶数なら、2 は公約数ではないので、その偶数を 2 で割れるだけ割り、両方が奇数になったら、 m, n をそのうちの小さい方と 2 数の差に置き換え、同様なことを最初に戻って、差が 0 になるまで繰り返す。
3. 差が 0 になったら、そのときの数と 2 のべきの積が最大公約数。

ラメの定理

L 桁以下の 2 つの自然数の最大公約数は、ユークリッドの互除法を用いると、必要な割り算の回数は実数

$$4.785 \cdot L - 0.327$$

を越えない。特に桁数の 5 倍未満の回数となる。

例. $L = 1, 2, \dots, 10$ のとき, 回数はそれぞれ 4, 9, 14, 18, 23, 28, 33, 37, 42, 47 回以下 (それぞれこれは最良) .

フィボナッチ数列

自然数を並べたもので、以下の 2 つの性質で定まるもの。

- ・先頭の 2 つは共に 1
- ・ 3 番目以降の数は、その直前と 2 つ前の数の和に等しい。

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946, 17711, 28657, 46368, 75025, 121393, 196418, 317811, 514229, 832040, 1346269, 2178309, 3524578, 5702887 9227465, 14930352, 24157817, ...

100 番目: 354224848179261915075

200 番目: 280571172992510140037611932413038677189525

300 番目: 222232244629420445529739893461909967206666939096499764990979600

- ・フィボナッチ数列の並んだ 2 つの自然数は互いに素である。
- ・このなかに素数が無数に現れるかどうかは、分かっていない。

$$13 = 8 \cdot 1 + 5$$

$$8 = 5 \cdot 1 + 3$$

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1$$

$$2 = 1 \cdot 2$$

フィボナッチ数列の n 番目の数は

$$\frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$