『ユークリッドの互除法』を使いこなす

1　『ユークリッドの互除法』とは

手ごろな大きさの2つの数の最大公約数は，素因数分解すればすぐに分かりますが，ある程度以上の大きさになれば素因数分解が思いつかなくなり，困ってしまいます．そんなときに有効なのがユークリッドの互除法です．

フムフム

▷Point◁（☆ユークリッドの互除法☆）

2つの自然数 a，b について，a を b で割ったときの余りを r とすれば a と b の最大公約数と b と r の最大公約数は一致する．

証明

a と b の最大公約数を g とするとき，

$a=ga'$，$b=gb'$（a' と b' は互いに素）

とおける．

いま，a を b で割ったとき，商が q，余りが r になったとすると，

$$a=bq+r \quad (0\leqq r<b)$$

となる．このとき，

$$\begin{aligned} r&=a-bq\\ &=ga'-gb'q\\ &=g(a'-b'q)\end{aligned}$$

ここで，$b=gb'$ と $r=g(a'-b'q)$ の最大公約数を考える．

b' と $a'-b'q$ が互いに素であることを示す．

b' と $a'-b'q$ が互いに素でないと仮定すると，b' も $a'-b'q$ も共通の素因数 p で割り切れる．

$b'=p\alpha$，　$a'-b'q=p\beta$

このとき，$a'=p\beta+b'q=p(\beta+\alpha q)$ より，a' も p で割り切れることになり，a' と b' が互いに素であることに矛盾する．

したがって，b と r の最大公約数も g である．

つまり，a と b の最大公約数と b と r の最大公約数は一致する．

この証明の流れはとても大切なので自分で証明できるように!!

大切!!

■

一般に，a と b の最大公約数を $(a,\ b)$ と表記します．例えば $(8,\ 12)=4$，$(5,\ 7)=1$ などなど．座標と混同しないでください．

この表記方法を用いると，ユークリッドの互除法とは

$$a=bq+r \quad (0\leqq r<b)$$

$\Longrightarrow a$ と b の最大公約数と

b と r の最大公約数は同じ

$\Longrightarrow (a,\ b)=(b,\ r)$

とシンプルに表記できます．この記法は使いなれるととても便利なのでどんどん使っていきます．

具体例でやってみよう．

【例】　3059 と 2337 の最大公約数

【例】　2531 と 1709 の最大公約数

解　ユークリッドの互除法より

$$\begin{aligned}&(3059,\ 2337) && \longleftarrow 3059=2337\times1+722\\ =\ &(2337,\ 722) && \longleftarrow 2337=722\times3+171\\ =\ &(722,\ 171) && \longleftarrow 722=171\times4+38\\ =\ &(171,\ 38) && \longleftarrow 171=38\times4+19\\ =\ &(38,\ 19) && \longleftarrow 38=19\times2+0\\ =\ &(19,\ 0)\\ =\ &19\end{aligned}$$

よって，3059 と 2337 の最大公約数は 19．

どんどん割り算して余りに注目するわけね

$$\begin{aligned}&(2531,\ 1709) && \longleftarrow 2531=1709\times1+822\\ =\ &(1709,\ 822) && \longleftarrow 1709=822\times2+65\\ =\ &(822,\ 65) && \longleftarrow 822=65\times12+42\\ =\ &(65,\ 42) && \longleftarrow 65=42\times1+23\\ =\ &(42,\ 23) && \longleftarrow 42=23\times1+19\\ =\ &(23,\ 19) && \longleftarrow 23=19\times1+4\\ =\ &(19,\ 4) && \longleftarrow 19=4\times4+3\\ =\ &(4,\ 3) && \longleftarrow 4=3\times1+1\\ =\ &(3,\ 1) && \longleftarrow 3=1\times3+0\\ =\ &(1,\ 0)\\ =\ &1\end{aligned}$$

よって，2531 と 1709 の最大公約数は 1 である．

たしかに数字がどんどん小さくなって計算がラクです

■

このように，大きな2数の最大公約数を求めるのに，割り算を繰り返してどんどん数を小さくして求めていくのがユークリッドの互除法です．

ナットク

ok

➪注　2531 と 1709 と素因数分解すると

$3059 = 7 \times 19 \times 23$,　　$2337 = 3 \times 19 \times 41$

となり，確かに最大公約数が 19 であることが分かりますが，2531 と 1709 は共に素数なので素因数分解できません．よってユークリッドの互除法を利用するしかありません．

➪注　2531 と 1709 の最大公約数が 1 ということは，2531 と 1709 が互いに素であることを意味しています．

例題 1.

$7n+3$ と $2n+3$ の最大公約数が 5 になるような 50 以下の自然数 n をすべて求めよ．

考え方　$7n+3$ も $2n+3$ も素因数分解の様子が全く分からないので，ユークリッドの互除法を利用するしかありません．

文字式の場合にも利用できるのが「ユークリッドの互除法」のスゴイところ

解

$7n+3 = (2n+3) \times 3 + (n-6)$

$2n+3 = (n-6) \times 2 + 15$

ヤッホーイ

したがって，ユークリッドの互除法より，$7n+3$ と $2n+3$ の最大公約数は，$n-6$ と 15 の最大公約数に等しい．$15 = 3 \times 5$ なので，$n-6$ が「5 の倍数であるが 3 の倍数でない数」になればよいので，$1 \leqq n \leqq 50$ に注意して，

これはスゴイオモロイ

$n-6 = -5,\ 5,\ 10,\ 20,\ 25,\ 35,\ 40.$

$\therefore\ n = 1,\ 11,\ 16,\ 26,\ 31,\ 41,\ 46.$

■

➪注　(　　,　　) で表記すれば

$$(7n+3,\ 2n+3) = (2n+3,\ n-6) = (n-6,\ 15)$$

となります．とてもシンプルで見やすいですね．

そうだネ

2　互いに素 (Part.3)

これまで，互いに素であることの証明は，すべて「互いに素でないと仮定して矛盾」という方法で証明してきました．これはこれで基本かつ重要な方法なのですが，ユークリッドの互除法を用いれば，否定せずに直接的に証明することもできます．

互いに素？マジっすか

スゴっ

そもそもユークリッドの互除法とは，2 つの数の最大公約数を求める方法のことなので，最大公約数を実際に計算して，1 になれば互いに素，1 にならなければ互いに素ではない，のです．

▷Point◁

2 つの自然数 a, b について，ユークリッドの互除法を繰り返し行い，

$$(a,\ b) = (b,\ c) = (c,\ d) = \cdots = \cdots$$

最終的に 1 になれば a と b は互いに素である．

実際に，ユークリッドの互除法を繰り返して最大公約数を直接求めようというわけです．

フムフム

例題 2.

n が自然数のとき，n^2+n+1 と $n+1$ が互いに素であることを証明せよ．

考え方　従来通り，互いに素でないと仮定して矛盾を示すことも可能ですが・・・

解　$n^2+n+1 = (n+1) \times n + 1$

したがって，ユークリッドの互除法より，n^2+n+1 と $n+1$ の最大公約数は，$n+1$ と 1 の最大公約数に等しい．

あっという間に終わった

スゲ～

$n+1$ と 1 の最大公約数は 1 なので，n^2+n+1 と $n+1$ は互いに素である．

■

➪注　(　　,　　) で表記すれば

$$(n^2+n+1,\ n+1) = (n+1,\ 1) = 1$$

となります．とてもシンプルで見やすいですね．

➪注　従来通りの方法でやるなら，

$n^2+n+1 = p\alpha$, $n+1 = p\beta$ とし，

$n^2 = p(\beta-\alpha)$ なので，n も p で割り切れることになり，連続する 2 整数が互いに素であることに矛盾する，とします．これはこれで大切な証明です．

ちょっとメンドイ

う～

例題 3.

x と y を互いに素な自然数とするとき，$\dfrac{4x+9y}{3x+7y}$ は既約分数であることを証明せよ．

↳ これ以上 約分できない分数のこと。つまり…

考え方　$4x+9y$ と $3x+7y$ が互いに素であることを証明すればよいです．