ユークリッドの互除法と不定方程式

ユークリッドの互除法

自然数（または整式）の最大公約数を求める方法の一つ。

「a を b で割った余りを r とすると，a と b の最大公約数は b と r の最大公約数に等しい」

このことを利用して，次に b を r で割った余りを r_1 とすると，

「b と r の最大公約数は r と r_1 の最大公約数と等しい」

「a と b の最大公約数は b と r の最大公約数に等しい」から，

「a と b の最大公約数は r と r_1 の最大公約数と等しい」

さらに，r を r_1 で割った余りを r_2 とすると，・・・と次々とこの操作を行っていくと，

やがて，余りが 0 となる割り算に至る。

このときの割り算の割る数（除数）を r_k とすると，

「0 と任意の整数 n の最大公約数は n」だから，r_k と余り 0 の最大公約数は r_k である。

ゆえに，a と b の最大公約数は r_k となる。

補足

「0 と任意の整数 n の最大公約数は n」

n を任意の整数とすると，n を 0 倍した数は 0 だから，0 は n の倍数である。

あるいは，0 を n で割った余りは 0，すなわち 0 は n で割り切れる。

よって，n は 0 の約数，すなわち 0 の約数はすべての整数である。

一方，n の約数の最大値は n である。

ゆえに，0 と任意の整数 n の最大公約数は n である。

「a を b で割った余りを r とすると，a と b の最大公約数は b と r の最大公約数に等しい」の証明

a を b で割った商を q，余りを r とすると，$a = bq + r$　・・・①

a と b の最大公約数を G，b と r の最大公約数を G' とすると，

$a = a'G, b = b'G$（a' と b' は互いに素）　・・・②

$b = b''G', r = r'G'$（b'' と r' は互いに素）　・・・③

②を①に代入すると，$a'G = b'G + r$　$\therefore r = G(a' - b')$

よって，r は G を約数にもつ。

b も G を約数にもつから，G は b と r の公約数である。

これと b と r の最大公約数が G' であることから，$G' \geq G$　・・・④　が成り立つ。

③を①に代入すると，$a = b''G'q + r'G'$　$\therefore a = G'(b''q + r')$

よって，a は G' を約数にもつ。

b も G' を約数にもつから，G' は a と b の公約数である。

これと a と b の最大公約数が G であることから，$G \geq G'$　・・・⑤　が成り立つ。

④かつ⑤より，$G = G'$

よって，a と b の最大公約数は b と r の最大公約数に等しい。

例題 1

不定方程式$95x+28y=3$の一般解を求めよ。

略解

不定方程式$95x+28y=3$の特殊解を求める。

$95=28\cdot 3+11$，$28=11\cdot 2+6$，$11=6\cdot 2-1$より，

$$
\begin{aligned}
1&=\cdot 6\cdot 2-11\\
&=(28-11\cdot 2)\cdot 2-11\\
&=28\cdot 2-11\cdot 5\\
&=28\cdot 2-(95-28\cdot 3)\cdot 5\\
&=95\cdot(-5)+28\cdot 17
\end{aligned}
$$

よって，$\{95\cdot(-5)+28\cdot 17\}\times 3=1\times 3$　$\therefore 95\cdot(-15)+28\cdot 51=3$

これと$95x+28y=3$より，$95(x+15)+28(y-51)=0$

$\therefore 95(x+15)=-28(y-51)$

95 と 28 は互いに素だから，$x+15=28k$（kは整数）とおくと，$y-51=-95k$

よって，$(x,y)=(28k-15,-95k+51)$

例題 2

3 で割ると 1 余り，7 で割ると 3 余るような自然数のうち，

3 桁で最大のものと最小のものを求めよ。

略解

このような自然数は，自然数m,nを用いて$3m-2$または$7n-4$と表せるから，

$3m-2=7n-4$より，$7n-3m=2$　・・・①

また，$7=3\cdot 2+1$より，$7\cdot 2-3\cdot 4=2$　・・・②

①と②より，$7(n-2)-3(m-4)=0$　$\therefore 7(n-2)=3(m-4)$

7 と 3 は互いに素だから，$n-2=3k$（kは整数）　$\therefore n=3k+2$

これを$7n-4$に代入することにより，

条件を満たす自然数は整数kを用いて，$21k+10$と表せる。

これと$100\leq 21k+10\leq 999$より，$5\leq k\leq 47$

よって，3 桁で最大のものと最小のものは，それぞれ 997，115

例題 3

n^2+n+1と$n+1$は互いに素であることを証明せよ。

略解

$n^2+n+1=n(n+1)+1$より，

n^2+n+1と$n+1$の最大公約数は$n+1$と 1 の最大公約数と等しい。

これと$n+1$と 1 の最大公約数は 1 であることから，n^2+n+1と$n+1$は互いに素である。

例題 4

$5n+1$ と $6n+4$ の最大公約数が 7 になるような 100 以下の自然数 n をすべて求めよ。

略解

$6n+4=(5n+1)\cdot 1+n+3$ より，

$6n+4$ と $5n+1$ の最大公約数は $5n+1$ と $n+3$ の最大公約数は等しい。

$5n+1=(n+3)\cdot 5-14$ より，

$5n+1$ と $n+3$ の最大公約数は $n+3$ と -14 の最大公約数と等しい。

よって， $6n+4$ と $5n+1$ の最大公約数は $n+3$ と -14 の最大公約数と等しい。

$6n+4$ と $5n+1$ の最大公約数は 7 だから， $n+3$ と -14 の最大公約数も 7 であり，

$-14=7\cdot(-2)$ より， $n+3$ と -14 の最大公約数が 7 であるためには，

$n+3$ が 2 を約数にもたなければよい。

よって， $n+3$ は 7 の奇数倍である。

したがって， $n+3$ は自然数 k を用いて， $n+3=7\cdot(2k-1)$ と表せる。 $\therefore n=14k-10$

これと n が 100 以下の自然数であることから， $n=4,18,32,46,60,74,88$

例題 5

n を自然数とする。 n^2+n+6 と $n+5$ の最大公約数として考えられる数をすべて求めよ。

略解

$n^2+n+6=(n+5)(n-4)+26$ より，

n^2+n+6 と $n+5$ の最大公約数は $n+5$ と 26 の最大公約数と等しい。

$26=2\cdot 13$ より，26 の約数は 1,2,13,26 だから，

$n+5$ と 26 の最大公約数として考えられる数は，1,2,13,26 である。

よって， n^2+n+6 と $n+5$ の最大公約数として考えられる数も 1,2,13,26 である。