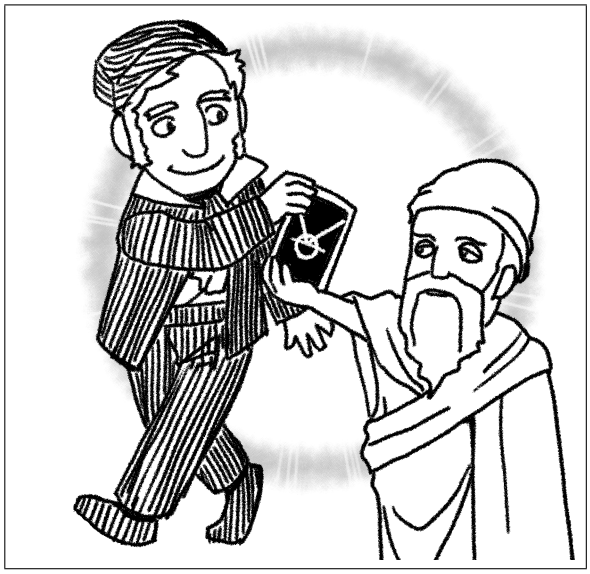
『数学セミナー』2019年10月号 「高校数学ではじめる整数論」



連載●第 7 回

素因数分解の一意性　付録

谷口 隆◎神戸大学大学院理学研究科

※ 式番号は本誌 2019 年 10 月号の連載と通しで振っています.

◎——1　互除法

互除法とは，正の整数 a, b が与えられたときに，その最大公約数 d を求めるアルゴリズムのことです．またそのアルゴリズムからは，$ax + by = d$ となるような整数 x, y を求めることができます.

互除法のアルゴリズムはきわめて平易で，互除法の名の通り,「交互に割る」だけです．一例として，$a = 1343$ と $b = 323$ の最大公約数を求めてみましょう．忘れたなぁという人も，この式を見れば思い出せるのではないでしょうか.

$$1343 = 323 \times 4 + 51, \tag{2}$$

$$323 = 51 \times 6 + 17, \tag{3}$$

$$51 = 17 \times 3 + 0 \tag{4}$$

まず 1323 を 323 で割ります．すると，商は 4 で余りが 51 です．これが (2) です．今度は 323 をこの余り 51 で割ります．すると商が 6 で余りが 17 です．これが (3) です．そして 51 を 17 で割ると割り切れます．これが (4) です．このときの 17 が最大公約数になる，というものです.

一般の手順は

『割り算を行い，割った数と余りを用いて次の割り算を行い，余りが 0 になるまで繰り返し続ける』

です．今の $(1343, 323)$ の場合，順々に行った割り算を，割られる数と割る数を組にして表すとこのようになります.

$$(1343, 323) \longrightarrow (323, 51) \longrightarrow (51, 17) \longrightarrow (17, 0)$$

割り切れて余りが 0 になると，0 で割ることはできないので，ここで手順が止まります．このときの 17 がちょうど最大公約数になるのです.

互除法では，手順ごとに割る数が小さくなるので，有限回の割り算の後，必ず手順が止まります．どうしてこの手順で最大公約数が求められるでしょうか？　アルゴリズムを見ていると，要はこんな命題が成り立つからだということになるでしょう．命題 6 を繰り返し用いれば，互除法で最大公約数が求められることが分かります．

命題 6　a と b は正の整数とし，その最大公約数を d とする．a を b で割ったときの余りを r とすると，b と r の最大公約数も d である．　□

注　余り r が 0 のときは，0 はどんな整数の約数でもあるので，$b\,(>0)$ と r の最大公約数は b です．

命題 6 の証明はとても単純です．

証明　a を b で割ったときの商を q とすると，$a = qb + r$ である．$a = da_1$, $b = db_1$ とすると $r = a - qb = d(a_1 - qb_1)$ だから，d は r の約数である．よって d は b と r の公約数である．したがって，b と r の最大公約数を d' とすると，$d \leqq d'$ である．一方，$a = qb + r$ から，同様にして d' は a の約数であることが分かる．よって d' は a と b の公約数だから，$d' \leqq d$ でもある．$d \leqq d'$ と $d' \leqq d$ から $d = d'$ である．　■

では，互除法から，方程式 $ax + by = d$ の整数解をどう求められるでしょうか．再び $a = 1343$, $b = 323$ の場合を考えましょう．$d = 17$ が出てきた (3) の式から始め，次のようにして (2) を代入します．

$$\begin{aligned} 17 &= 323 - 51 \times 6 \\ &= 323 - (1343 - 323 \times 4) \times 6 \\ &= 1343 \times (-6) + 323 \times 25 \end{aligned}$$

これで，17 を $1343x + 323y$ の形で表すことができました．

一般の場合も同様です．互除法の手順が

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

となり，r_{n-1} が r_n で割り切れたとしましょう．このとき r_n が最大公約数 d になります．最後からひとつ手前の式から始め

$$d = r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = \cdots$$

として，順に手前の式を代入して r_i の添え字 i を小さくしていくと，最後は $r_1 = a - qb_1$ を代入して r_i はすべてなくなり，$ax + by$ の形になります．このときの x, y は整数で，$d = ax + by$ とすることができました．

◎——2　素因数分解の一意性を使う問題集

もう一つの付録として，素因数分解の一意性を使う問題を，いくつか集めておきます．解答は簡単なものにとどめます．考えてみてください．以下一般に，正の整数の素因数分解を $p_1^{e_1} \cdots p_k^{e_k}$ と書いたときは，$p_1, \cdots, p_k$ は相異なる素数とします．

2.1　問題

問 1　正の整数 n の素因数分解を $n = p_1^{e_1} \cdots p_k^{e_k}$ とする．n の約数は $p_1^{f_1} \cdots p_k^{f_k}$ であって各 i で $0 \leqq f_i \leqq e_i$ となるものですべてであり，この中に重複はない．特に n の約数の個数は $(e_1 + 1) \cdots (e_k + 1)$ である．

問 2　正の整数 n の約数の和は，その素因数分解を $n = p_1^{e_1} \cdots p_k^{e_k}$ として，$\dfrac{p_1^{e_1+1} - 1}{p_1 - 1} \cdots\cdots \dfrac{p_k^{e_k+1} - 1}{p_k - 1}$ である．

問 3　正の整数 m, n の最大公約数を d，最小公倍数を ℓ とする．m, n の素因数分解をそれぞれ $m = p_1^{e_1} \cdots p_k^{e_k}$，$n = p_1^{f_1} \cdots p_k^{f_k}$ とする．ただし指数は 0 の場合もあるとし，たとえば，p_i が m のみの素因数で n の素因数でなければ，$f_i = 0$ であるとする．このとき，$d = p_1^{\min\{e_1, f_1\}} \cdots p_k^{\min\{e_k, f_k\}}$，$\ell = p_1^{\max\{e_1, f_1\}} \cdots p_k^{\max\{e_k, f_k\}}$ である．

問 4　正の整数 m, n の最小公倍数を ℓ とする．m の約数 m_1 と n の約数 n_1 であって，m_1 と n_1 の最大公約数は 1 であり，かつ $m_1 n_1 = \ell$ となるものが存在する．

問 5　p を素数とする．二項係数 $\binom{p}{k}$ は，$0 < k < p$ で p の倍数である．より一般に，$\binom{p^e}{k}$ は，$0 < k < p^e$ で p の倍数であり，k がちょうど p の f 乗で割り切れるならば，p^{e-f} の倍数である．

問 6　整数 n が平方数でないとき，$\sqrt{n}$ は無理数である．

問 7　$P(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d$ を整数係数の多項式とする．$P(x) = 0$ が有理数解をもつとき，その解を既約分数で $\dfrac{k}{\ell}$ と表せば，k は a_d の約数であり，ℓ は a_0 の約数である．

2.2　略解・方針

答 1　この形の整数が n の約数であることは明らかである．重複がないことは定理 2 からしたがう．d が n の約数であるとすれば，$n = dc$ となる整数 c が存在する．d, c の素因数分解を考えると，d が上記の形になることは，再び定理 2 からしたがう．

注　n の約数のうちの 1 は，$p_1^{f_1}\cdots p_k^{f_k}$ で $f_1=\cdots=f_k=0$ としたものに対応する．つまり

$$1=p_1^0\cdots p_k^0 \tag{5}$$

である．一般に $p_1^{f_1}\cdots p_k^{f_k}$ は $f_1+\cdots+f_k$ 個の素数の積だから，(5) の右辺は 0 個の素数の積と見なされる．「1 を形式的に 0 個の素数の積とみなしたものが 1 の素因数分解」としておくと，整除の問題をこのように素因数分解によって論ずるときに統一的に扱えて便利である．

答 2　$(1+p_1+\cdots+p_1^{e_1})(1+p_2+\cdots+p_2^{e_2})\cdots\cdots(1+p_k+\cdots+p_k^{e_k})$ を展開すれば，問 1 から，これが n の約数すべての和であることが分かる．

答 3　d,ℓ の素因数分解を考えればよい．

答 4　問 3 よりしたがう．ℓ の素因数分解の各素数冪 $p_i^{\max\{e_i,f_i\}}$ は，$p_i^{e_i}$ または $p_i^{f_i}$ だから，m,n のどちらかの素因数分解に含まれる．m に含まれるそれらの素数冪の積を m_1，n に含まれるそれらの素数冪の積を n_1 とすればよい．ただし $e_i=f_i$ のときは任意に m_1,n_1 のどちらかに入れる．

答 5　$k\binom{p^e}{k}=p^e\binom{p^e-1}{k-1}$ に注意して，両辺を素因数分解したときの p の指数を見較べる．

答 6　n の素因数分解を $n=p_1^{e_1}\cdots p_k^{e_k}$ とすると，n は平方数でないので，ある e_i は奇数である．$\sqrt{n}$ が有理数であるとし，$\sqrt{n}=\dfrac{k}{\ell}$ とすると，$\ell^2n=k^2$ である．k,ℓ の素因数分解に p_i がそれぞれ a,b 個現れるとすると，定理 2 より $2a+e_i=2b$ となり，e_i が奇数であることと矛盾する．

注　同様に考えて一般に，n が k 乗数でなければ，$\sqrt[k]{n}$ は無理数であることが示される．

答 7　記号が煩雑になるのを避けるため，$d=3$ として示す．一般の d でもまったく同様である．$P\left(\dfrac{k}{\ell}\right)=0$ より，分母を払うと $a_0k^3+a_1k^2\ell+a_2k\ell^2+a_3\ell^3=0$ である．よって $k(a_0k^2+a_1k\ell+a_2\ell^2)=-a_3\ell^3$ である．両辺の素因数分解を考えると，k,ℓ に共通の素因数はないから，k の素因数分解は a_3 の素因数分解の一部である．よって k は a_3 の約数である．同様に，ℓ の素因数分解は a_0 の素因数分解の一部だから，ℓ は a_0 の約数である．

注　これは問 6 をより一般化な形で解決している．$P(x)=x^2-n$ は整数係数の多項式で，$\sqrt{n}$ は $P(x)=0$ の解である．$P(x)$ の解が有理数であれば，問 7 よりそれは整数である．つまり，$\sqrt{n}$ が有理数ならばそれは整数で，$\sqrt{n}=m$ と書ける．$m^2=n$ なので n は平方数である．(n が k 乗数でないときに $\sqrt[k]{n}$ が無理数であることも同様にしたがう．)

[たにぐち たかし]
[絵／森脇かみん]