初等整数論の基本定理の証明

Tomohiro Yamada（山田智宏）

概 要

本稿では、初等整数論の基本定理、つまり整数の素因数分解の一意性の証明をいくつか挙げたい。

0 はじめに

すべての正の整数は素数の積に（順序を除いて）一意的にあらわせる、すなわちどのような正の整数 n も、$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ （$p_1 < p_2 < \cdots < p_k$ は素数で $e_1, e_2, \ldots, e_k$ は正の整数、$n = 1$ のときは $k = 0$ とする）という形に一意的に表示できる、ということが初等整数論の基本定理である。

本稿では、この初等整数論の基本定理の証明をいくつか与える。ただし、これらの証明からはある整数の素因数分解が実際にどのようにあらわされるかについては何の情報も得られない。実際、素因数分解のための多項式時間のアルゴリズムが存在するとは考えにくい。ただそのことは未だ証明されていない（もし証明されれば、P$\neq$ NP であることが導かれる）。

素因数分解が可能であることは、数学的帰納法によりすぐにわかる; 2 から n までの整数がすべて素因数分解可能であるならば $n+1$ はそれ自体が素数であるか、または 2 から n までの 2 つの整数の積にあらわせるが、その 2 つの整数は先述の仮定より素因数分解可能であるため $n+1$ も素因数分解可能となるからである。

したがって、一意性の証明が問題となる。

まず、いくつかの記法を導入したい。$\gcd(a, b)$ で a と b の最大公約数を、$\mathrm{LCM}[a, b]$ で a と b の最小公倍数をあらわし、a が b を割り切ることを $a \mid b$ とかく。

1 Euclid の補題

初等整数論の基本定理の標準的な証明は Euclid が「原論」第 7 巻の命題 30 に挙げた（詳しくは最後の節を参照）Euclid の補題を用いる。

Lemma 1.1 (Euclid's lemma)**.** a, b が整数で、素数 p が ab を割り切るとき、 p は a, b の少なくとも一方を割り切る。

初等整数論の基本定理は Euclid の補題から従う。

まず、Euclid の補題は、素数 p が k 個の整数の積 $a_1a_2 \ldots a_k$ を割り切るとき、 p は a_i の少なくとも一つを割り切る、というように拡張される。実際、p が k 個の整数の積 $a_1a_2 \ldots a_k$ を割り切るとき、Euclid の補題より p は $a_1a_2 \ldots a_{k-1}$ か a_k の少なくとも一方を割り切るが、前者の場合、再び Euclid の補題より p は $a_1a_2 \ldots a_{k-2}$ か a_{k-1} の少なくとも一方を割り切る。これを繰り返し、 p は $a_1, a_2, \ldots, a_{k-1}, a_k$ のうち少なくとも一つを割り切ることがわかる。

特に p が k 個の素数の積 $q_1q_2 \ldots q_k$ を割り切るならば p は q_i のいずれかと一致する。

さて、複数の素因数分解をもつ正の整数が存在すると仮定して、 n をその中の最小の正の整数とし、そのうちの一つの素因数分解に現れる最小の素数を p とする。そうすると p は n の他の素因数分解に現れることはできない。（以下 2019/6/4 修正）というのは n/p は n より小さいから、n/p に関しては素因数分解は一意的でなければならないからである。そうなると、p が n を割り切るにもかかわらず、それにもかかわらず p は n の他の素因数分解には現れないということになり、上記の事実に矛盾する。このことから素因数分解の一意性がすべての正の整数に対して成り立つことが証明された。

（2019/6/4 追記）なお、Euclid の補題から、その双対ともいうべき、次のような事実がすぐにわかる。a, b が互に素な数で、ともに n を割り切るなら、その積 ab も n を割り切る。実際、a が n を割り切るので $n = am$ とおくと b は a と互に素な数で、 $n = am$ を割り切るから Euclid の補題より b は m を割り切らなければならない。 $m = lb$ とおくと $n = am = abl$ だから確かに ab は n を割り切る。

2 Bezout の等式

Euclid の補題の証明の方法はいくつかある。一般的なのは Bezout の等式を使う方法である。[1] ではこの方法が用いられている。

Lemma 2.1 (Bezout の等式)**.** 任意の整数 m, n に対し $am+bn = \gcd(m, n)$ となる整数 a, b が存在する。

まず次の補題（[1] の Theorem 23 にあたる）を証明する。

Lemma 2.2. l を $am + bn$ （a, b は整数）の形の最小の正の整数とする。このとき $am + bn$ （a, b は整数）の形の整数はすべて l の倍数である。

Proof. c, d を整数とし $k = cm + dn$ とする。ここで k を l で割った商を q とし余りを r とする。すなわち $k = ql + r, 0 \leq r < l$ とする。整数 a_0, b_0 を用いて $l = a_0m + b_0n$ とおくと $r = k - ql = (cm + dn) - q(a_0m + b_0n) = (c - qa_0)m + (d - qb_0)n$ となるから r も $am + bn$ （a, b は整数）の形をしている。しかし $0 \leq r < l$ であるから $r = 0$ であり $k = ql$ は l の倍数でなければならない。 □

このことから特に l は $m = 1 \times m + 0 \times n$ と $n = 0 \times m + 1 \times n$ の公約数でなければならないが m, n は $\gcd(m, n)$ の倍数であるから $l = am + bn$ も $\gcd(m, n)$ の倍数でなければならない。したがって $l = \gcd(m, n)$ であることがわかる。これにより Bezout の等式が導かれる。

さて、Euclid の補題よりも一般的な次の補題を証明する。

Lemma 2.3. m, n が整数で n が km を割り切るとき k は $n/\gcd(m, n)$ の倍数である。

Proof. Bezout の等式から $am + bn = \gcd(m, n)$ すなわち $k \gcd(m, n) = akm + bkn$ となる整数 a, b が存在するわけだが n は km を割り切るから $k \gcd(m, n) = a(km) + bkn$ は n の倍数であり、よって k は $n/\gcd(m, n)$ の倍数である。 □

特に p が素数で a が p で割り切れないとき $\gcd(a, p) = 1$ なのだから $p \mid ab$ ならば $p = p/\gcd(a, p) \mid b$ となる（2019/6/4 修正）。これにより Euclid の補題が導かれる。

Bezout の等式を用いた Euclid の補題の証明は一般の整域における素因数分解の一意性に関する一連の定理の特殊な場合である:Euclid 整域は Noether 整域でかつ Bezout 整域であり、Bezout 整域は GCD 整域であり、GCD 整域は Schreier 整域であり、原子（Noether 整域は原子整域である）Schreier 整域は PID かつ UFD である。

3 Euclid の互除法を用いた Bezout の等式の証明

Bezout の等式は Euclid の互除法を使用して証明することもできる。$a_0 = m, a_1 = n$ とおく。a_{n-2} を a_{n-1} で割った商を q_{n-1} とし余りを a_n とすることにより新たに a_n を定める。これを $a_l = 0$ となる l まで続ける。このとき $a_{l-1} = \gcd(m, n)$ となる。ところで $a_2 = m - q_1 n, a_3 = n - q_2 a_2, \ldots, a_{l-2} = a_{l-4} - q_{l-3} a_{l-3}$ となり $\gcd(m, n) = a_{l-1} = a_{l-3} - q_{l-2} a_{l-2}$ は $am + bn$ （a, b は整数）の形にあらわすことができる。

4 最小公倍数と最大公約数の理論

Euclid の補題のいくつかの証明は最小公倍数と最大公約数の理論を用いている。次の補題は [5] の定理 1.3 および [4] の定理 1.4.1 に相当する。

Lemma 4.1. a, b の公倍数は常に $\mathrm{LCM}[a, b]$ の倍数である。

Proof. n を a, b の任意の公倍数とし n を $\mathrm{LCM}[a, b]$ で割った商を q とし、余りを r とする。つまり $n = q\,\mathrm{LCM}(a, b) + r, 0 \leq r < \mathrm{LCM}(a, b)$ となるように q, r をとる。すると $r = n - q\,\mathrm{LCM}[a, b]$ もまた a, b の公倍数であるが $0 \leq r < \mathrm{LCM}[a, b]$ であるから $r = 0$ であるよりない。つまり n は $\mathrm{LCM}[a, b]$ の倍数である。 □

双対的に次の補題が成り立つ。これは、通常の最大公約数は、一般の可換環における最大公約数の概念に当てはまる（可換環 R において a, b の最大公約数とは a, b の公約数のうち、いかなる a, b の公約数でも割り切れるものをいう)、すなわち（有理）整数環が GCD 整域であることを意味する。

Lemma 4.2. a, b の公約数は常に $\gcd(a, b)$ の約数である。

Proof. n を a,b の任意の公約数とする。a,b は n と $\gcd(a,b)$ の公倍数であるから先ほどの補題より a,b は共に $l = \mathrm{LCM}[n, \gcd(a,b)]$ の倍数である。よって l は a,b の公約数である。したがって $\gcd(a,b) \leq l \leq \gcd(a,b)$ であるから $l = \gcd(a,b)$ である。しかしこれは n の倍数であるから n は $\gcd(a,b)$ の約数である。 □

[5] では次の補題を用いる。

Lemma 4.3. m,n が正の整数のとき $L = \mathrm{LCM}[m,n], d = \gcd(m,n)$ とおくと $mn = dL$ である。

Proof. $mn/d = m(n/d) = n(m/d)$ は m,n の公倍数だから補題 4.1 より mn/d は L の倍数である。つまり $dL \mid mn$ である。一方 $mn/L = m/(L/n) = n/(L/m)$ は m,n の公約数だから補題 4.2より mn/L は d の約数である。つまり $mn \mid dL$ である。

それで $mn \mid dL \mid mn$ となり $mn = dL$ を得る。 □

実際 Euclid の補題を証明するには、次の補題で足りる。

Lemma 4.4. p が素数で a が p で割り切れない正の整数なら $\mathrm{LCM}[a,p] = ap$ である。

Proof. a は $\mathrm{LCM}[a,p]$ の約数で補題 4.1より $\mathrm{LCM}[a,p]$ は ap の約数だから $\mathrm{LCM}[a,p] = a$ または $\mathrm{LCM}[a,p] = ap$ である。しかし a は p の倍数ではないので $\mathrm{LCM}[a,p] = ap$ でなければならない。 □

さて Euclid の補題を証明する。 p が ab を割り切るが a を割り切らないとき上の補題より $\mathrm{LCM}[a,p] = ap$ である。 ab は a,p の公倍数なので補題 4.1より ab は $\mathrm{LCM}[a,p] = ap$ の倍数である。つまり b は p の倍数であり、Euclid の補題が正しいことがわかる。

[4] の定理 1.4.3 はこれと類似しているが、最大公約数について、やや異なる議論をしている。

Lemma 4.5. a が bc の約数で $\gcd(a,b) = 1$ のとき a は c を割り切る。

Proof. a が bc を割り切るので $a = \gcd(a,bc)$ である。$\gcd(a,b) = 1$ なので $c = \gcd(a,b)c$ であるから $\gcd(a,c) = \gcd(a, \gcd(a,b)c)$ となる。それ

で $\gcd(a, bc) = \gcd(a, \gcd(a, b)c)$ を示すことができれば $a = \gcd(a, bc) = \gcd(a, \gcd(a, b)c) = \gcd(a, c)$ となり補題にある通り $a \mid c$ であることが確かめられる。

それで、これより $\gcd(a, bc) = \gcd(a, \gcd(a, b)c)$ を示すことにする。

l が $a, \gcd(a, b)c$ の公約数であるとき $l \mid \gcd(a, b)c \mid bc$ であるから l は a, bc の公約数である。よって $\gcd(a, \gcd(a, b)c) \leq \gcd(a, bc)$ となることがわかる。

$d = \gcd(a, bc)$ とおくと $d \mid a \mid ac$ なので d は ac, bc の公約数である。ac と bc は c, d の公倍数なので c, d と同様 $\mathrm{LCM}[c, d]$ は ac, bc の公倍数である。$\mathrm{LCM}[c, d] = ck$ とおくと k は a, b の公約数だから補題 4.2より k は $\gcd(a, b)$ を割り切る。したがって $\mathrm{LCM}[c, d] = ck$ は $\gcd(a, b)c$ を割り切るから、 d も $\gcd(a, b)c$ を割り切る。したがって d は $a, \gcd(a, b)c$ の公約数である。しかし上記のように $d = \gcd(a, bc) \geq \gcd(a, \gcd(a, b)c)$ であるから $d = gcd(a, \gcd(a, b)c)$ が示された。 □

5 その他の Euclid の補題の証明

[2] による簡明な Euclid の補題の証明を挙げる。

Lemma 5.1. a, b を整数とし k_0 を $k_0 a$ が b の倍数となる最小の正の整数とする。ka が b の倍数ならば、 k は k_0 の倍数である。

Proof. k を k_0 で割った商を q とし余りを r とする。このとき $ra = (k - qk_0)a = ka - qk_0 a$ も b の倍数だが $0 \leq r < k_0$ なので $r = 0$ すなわち k は k_0 の倍数となるほかない。 □

これを用いて補題 2.3を証明でき、Euclid の補題が得られる。

Lemma 5.2. $k_0 = b/\gcd(a, b)$ である。

Proof. まず ba は明らかに b の倍数だから先の補題において常に $k = b$ ととることができる。したがって k_0 は b の約数である。

そこで $b = d_0 k_0, k_0 a = n_0 b$ とおく。このとき $a = n_0 d_0$ であるから d_0 は a, b の公約数である。d が a, b の公約数ならば $(b/d)a = ab/d = a(b/d)$ は

a の倍数であるから b/d は k_0 の倍数、すなわち d は $b/k_0 = d_0$ の約数である。よって $d_0 = \gcd(a,b)$ つまり $k_0 = b/\gcd(a,b)$ である。 □

（2019/6/4 追記）こうして、Bezout の等式を使わずに Euclid の補題を証明することができたが、補題 5.2 から Bezout の等式を証明することもできる。

$u_k(k = 0, 1, \ldots)$ を ka を b で割った余りとする。すると $u_k(0 \leq k \leq k_0 - 1)$ はそれぞれ異なる値を取る。というのは、$u_k = u_l(0 \leq k \leq l \leq k_0 - 1)$ ならば $(l-k)a$ は b の倍数だから補題 5.2 から $k - l$ は b の倍数でないといけないが $0 \leq l - k \leq k_0 - 1$ だから、結局 $k = l$ でなければならない。

それで $u_k(0 \leq k \leq k_0 - 1)$ は k_0 個の異なる値を取る。一方、 $ka - lb$ は $\gcd(a,b)$ の倍数だから $u_k(0 \leq k \leq k_0 - 1)$ は $k_0 = b/\gcd(a,b)$ 個の数 $0, \gcd(a,b), \ldots, (k_0 - 1)\gcd(a,b)$ のうちから値を取らなければならない。つまり $u_k(0 \leq k \leq k_0 - 1)$ は これらの k_0 個の値を一度ずつ取る。特に $u_k = \gcd(a,b)$ となる k が存在する。つまり $ka - lb = \gcd(a,b)$ となる整数 k, l が取れるので Bezout の等式が導かれる。

6 直接証明

素因数分解の一意性の直接的な証明が [1] の 2.11 節に記載されている。

n を複数の方法で素因数分解できる最小の数とし、p を「一方の素因数分解」に現れる最小の素数とし、 q を「もう一方の素因数分解」に現れる最小の素数とする。p は「もう一方の素因数分解」には現れない。というのは p が「もう一方の素因数分解」に現れれば p を双方の素因数分解から除くことで n/p も複数の素因数分解を持ってしまうことになり、 n の最小性に反するからである。特に $p \neq q$ である。

素数自身は明らかに一通りの素因数分解しか持っていないので n は合成数である。したがって $p^2, q^2 \leq n$ である。 $p \neq q$ であるから $pq < n$ である。

$N = n - pq$ とする。このとき $0 < N < n$ であるから N は一通りの素因数分解しか持たない。p, q は共に $N = n - pq$ を割り切るから p, q は共に N の素因数分解に現れる。したがって N は pq で割り切れなければならず $n = N + pq$ も pq で割り切れなければならない。よって n/q は p で割り切れなければならないが、 $n/q < n$ は一通りの素因数分解しか持たないから

p は n/q の素因数分解に現れなければならず、よって n の「もう一方の素因数分解」にも現れなければならない。しかしこれは上記の、p が「もう一方の素因数分解」には現れないということに反する。

これより複数の方法で素因数分解できる数など存在しないことがわかり、整数の素因数分解の一意性が証明された。

7 Euclid の証明

Euclid 自身は第 7 巻の最初に Euclid の互除法を挙げているにもかかわらず補題の証明には互除法を用いていない一方、Euclid 自身の補題の証明には誤りがあることが知られている。しかしこのことはそれほど単純ではない。詳しくは [3] を参照されたい。

Euclid の証明は $a : b = c : d$ と $ad = bc$ が同値であること（命題 7.19）と (a, b) が比 $a : b$ を持つ最小の正の整数の対であるとき $a : b = c : d$ なら $c = an, d = bn$ となる整数 n が存在すること（命題 7.20）を用いる。

Euclid の命題 7.20 の証明は $a = c(m/n), b = d(m/n)$ となる整数 m, n を $m \geq 2$ で n が c の約数となるようにとれば、$(a/m) : (b/m) = (c/n) : (d/n) = c : d$ となり a, b の最小性に反することを用いる。

ここで n が d の約数であることを確かめていないとすぐに指摘できそうだが、Euclid は第 7 巻では比が等しいことを $(a, b, c, d) = (mx, nx, my, ny)$ となる整数 m, n, x, y が存在することと定義している（第 5 巻では通常の定義を用いている）ことに注意しなければならない。

だが、この定義のもとで命題 7.19 の証明を検討すると、Euclid は $a : b = c : d$ を $ad : bd = a : b$ と $bc : bd = c : d$ から導き出しているが、この定義のもとでは $a : b = e : f, e : f = c : d$ のとき $a : b = c : d$ となることは自明ではないのである。

参考文献

[1] G. H. Hardy and E. M. Wright, D. R. Heath-Brown, J. Silverman, A. Wiles, *An Introduction to the Theory of Numbers*, the 6th edition, Oxford University Press, 2008.

[2] Trygve Nagell, *Introduction to Number Theory*, AMS Chelsea Publishing, 2001.

[3] David Pengelley and Fred Richman, Did Euclid Need the Euclidean Algorithm to Prove Unique Factorization? *Amer. Math. Monthly* **113** (2006), 196–205, `https://www.math.nmsu.edu/~davidp/euclid.pdf` で入手可能。

[4] Harold N. Shapiro, *Introduction to the Theory of Numbers*, Dover, 2008 (old edition, John Wiley and Sons, 1983).

[5] 高木貞治, 初等整数論講義, 第 2 版, 共立出版, 1971.