LCM,GCD

飯高 茂

2017 年 4 月 21 日

初等整数論講義を最初に読んだとき LCM と GCD の箇所がゴチャゴチャしていて読むのをあきらめた思い出がある. 後でイデアル論的に扱うことになるがその方がずっと明快である.

しかし, 初回に冒頭でつまずいたのは感心しない.

反省の意味をこめてよく分かるように再構成を試みた.

1 LCM と GCD

$a|b$ を a の約数は b の意味に使う. a divides b. a 割る b と読んでも構わない.

a, b : 自然数, とし

$CD(a,b) = \{d \mid a, b \text{ の公約数 }\}$,

$CM(a,b) = \{m \mid a, b \text{ の公倍数 }\}$.

これらは集合になる. これらを用いて証明を見やすくする.

$CM(a,b)$ はイデアルに近い性質がある.

$$q > 0, m_1, m_2 \in CM(a,b) \Longrightarrow m_1 + m_2 \in CM(a,b), qm_1 \in CM(a,b)$$

$$m_1, m_2 \in CM(a,b), m_1 > m_2 \Longrightarrow m_1 - m_2 \in CM(a,b).$$

$CM(a,b)$ の最小数を $LCM(a,b)$ と書き, 最小公倍数 (Least common multiple) という.

$CD(a,b)$ の最大数を $GCD(a,b)$ と書き, 最大公約数 (Greatest common divisor) という.

$a = bq + r, r \geq 0$ なら $CD(a,b) = CD(b,r)$

(この不変性が互除法になる)

定理 1

$$m \in CM(a,b) \Longrightarrow L|m, (L = LCM(a,b))$$

Proof
m を L で割り, $m = qL + r, r < L$.
$L, m \in CM(a,b)$ により $r = m - qL \in CM(a,b)$. よって, $r = 0$.

LCM についてのこの証明は極めて容易である．しかし GCD の場合は証明が困難になる. (そこが面白い)

定理 2

$$d \in CD(a,b) \Longrightarrow d|\delta, (\delta = GCD(a,b))$$

Proof
$d \in CD(a,b), \delta = GCD(a,b)$ について, $d|\delta$ を示すのだが LCM についての結果を利用するので d, δ の LCM を利用する.
$L_0 = LCM(d,\delta)$ とおく.
定義から,$L_0 \geq \delta$.
$L_0 = \delta$ を導くために.$L_0 \leq \delta$ を以下で証明する.
$d, \delta \in CD(a,b)$ により

$$a = a'd, b = b'd, a = a''\delta, b = b''\delta.$$

$$a = a'd, a = a''\delta \Longrightarrow a \in CM(d,\delta)$$

定理 1 によれば a は $LCM(d,\delta)$ の倍数. すなわち a_0 があり, $a = a_0 L_0$
同様に b_0 があり, $b = b_0 L_0$
$a = a_0 L_0, b = b_0 L_0 \Longrightarrow L_0 \in CD(a,b)$
よって, 定義から $L_0 \leq \delta = GCD(a,b)$.
あわせて $L_0 = \delta = GCD(a,b)$. だから $d|\delta$

定理 3

$$ab = LCM(a,b) \cdot GCD(a,b)$$

$L = LCM(a,b), \delta = GCD(a,b)$ とおくとき,

$$a|L \Rightarrow L = ab', b|L \Rightarrow L = ba'.$$

$ab \in CM(a,b)$ により ab は L の倍数. よって $ab = LD$ となる D がある.
$ab = LD = ab'D, ab = ba'D \Longrightarrow b = b'D, a = a'D$

$$D \in CD(a,b).$$

定理 2 によって,D は δ の約数. $\delta = De$ となる e がある.
$b = b''\delta = Db'$, $\delta = De$ より $b''De = Db'; b''e = b'$.
$L = ab' = ab''e$, $L = a'b = ba''e$.
$L/e = L_0$ とおけば, $L_0 = a''b, L_0 = b''a$. よって $L_0 \in CM(a,b)$.
定理 1 により L_0 は L の倍数.
$L \geq L_0 = fL \geq L$ なので $L_0 = L; L = L_0, e = 1$.
$\delta = D$ によれば $ab = LD = L\delta$.

定理 4 *a, b: 互いに素, $a|bc \Longrightarrow a|c$*

Proof
仮定から $bc = ak$ となる数 $k \in \mathbb{Z}$ がある.
$GCD(a,b) = 1$ により $ab = LCM(a,b)$.
$X = bc = ak \in CM(a,b)$.
X は $ab = LCM(a,b)$ の倍数.
$X = abs, (s \in \mathbb{Z})$ がある. $X = bc = abs$ により $c = as$; $a|c$.

1.1 約数, 因数, 倍数

0 でない整数 a, b についてある整数 c により $a = bc$ と書けるとき b は a の**約数** (divisor), a は b の**倍数** (multiple) という. または b は a の因数 (あるいは因子 (factor)) という.

整数全体の集合を $\mathbb{Z}$ で表し**整数環** (ring of integers) という. 環は加法, 減法, 乗法のできる集合の意味である.

整数環 $\mathbb{Z}$ において b の倍数全体の集合を $b\mathbb{Z}$ または (b) で表しこれを b の生成する**イデアル** (ideal) という. したがって $(b) = b\mathbb{Z}$ であり b をイデアル (b) の**生成元** (generator) という. $b = 1$ のときは $(1) = \mathbb{Z}$ となる.

「a は b の倍数」をイデアルの記号で書き換えれば $a \in (b)$ となる. すなわちある数 k により, $a = bk$ と書ける. このとき記号で $b|a$ と書き,「b は a を割る」ともいう.

1.2 ユークリッドの補題

d を自然数 a, b の最大公約数とすると, $d = ax + by$ を満たす整数 x, y が存在する. これを**ユークリッドの補題**という.

たとえば $a = 11, b = 8$ に対して最大公約数 d は 1 となる.

そこで次の表により $1 = 11x+8y$ を満たす x, y を探してみよう. $y = 1, 2, 3, \cdots$ とし $1 - 8y$ が 11 で割り切れる場合[1] を調べる.

表 1: $1 = 11x + 8y$ を満たす x, y

y	1	2	3	4	5	6	7
$1 - 8y$	–7	–15	–23	–31	–39	–47	–55
11 で割った余り	4	7	10	2	5	8	0

よって, $y = 7, 11x = 1 - 8y = -55$ より, $x = -5$. したがって

$$1 = -55 + 56 = 11(-5) + 8 \cdot 7.$$

11 と 8 の加法, 減法だけで 1 をあらわすこともできる:

$$1 = -11 - 11 - 11 - 11 - 11 + 8 + 8 + 8 + 8 + 8 + 8 + 8.$$

約数, 倍数など積の概念だけから定義された最大公約数 d を a, b をそれぞれ何回か足したり引いたりして表すのが $d = ax + by$ の意味である. したがってこれは, 加法と減法の世界で最大公約数を表現していると見ることができる. これが「ユークリッドの補題」の意味であり, 積の世界と和差の世界を結ぶ懸け橋の役をしていると言えよう.

2 集合 J とイデアル

$d = ax + by$ を満たす整数 x, y を探すとき, 「 d に等しい」 という条件をはずして $ax + by$ 全体を考え, これを整数環 $\mathbb{Z}$ の部分集合とみて J とおく. すなわち

$$J = \{ax + by \mid x, y \in \mathbb{Z}\}$$

とおく. J は次の 2 性質をもつ.

1. $\alpha, \beta \in J \Rightarrow \alpha + \beta \in J$,
2. $z \in \mathbb{Z}, \alpha \in J \Rightarrow z\alpha \in J$.

[1] 整数 a, b に対して $a = bq + r, 0 \leq r < |b|$ となる自然数 r が余り.

この性質を持つ集合 J を ($\mathbb{Z}$ の) **イデアル** (ideal) という.

生成元が 1 つのイデアル (b) を**単項イデアル** (または**主イデアル** principal ideal) という. 集合 J は $\{ax+by \mid x,y \in \mathbb{Z}\}$ と書けるので a,b の生成するイデアルと呼び記号で $a\mathbb{Z}+b\mathbb{Z}$ と書く. もっと簡単に (a,b) と書くことも多い.

注意

(2) の性質から $1 \in J$ なら任意の $z \in \mathbb{Z}$ について $z \in J$. よって $J = \mathbb{Z}$.

記号 (a,b) はベクトルや開区間を表すことにも用いられるのでこれらと混同しないように注意するとよい. 数学の本を読んでいくとき前後の意味を的確に理解し (a,b) はベクトルか, 開区間か, イデアルかをよく区別して理解することが肝要である.

2.1 J の生成元

J の元である自然数 $\alpha = ax+by$ を考える. これは a,b の最大公約数 d の倍数になっていることを以下で示そう. $a = a'd, b = b'd$ と自然数 a', b' で書けるから

$$\alpha = ax+by = a'dx+b'dy = (a'x+b'y)d$$

となる. だから $\alpha = (a'x+b'y)d \geq d$. よって $J^+ = \{\alpha > 0 \mid \alpha \in J\}$ とおくと, a,b の最大公約数 d は J^+ の下界である. d は J^+ の最小数になることを次に証明しよう.

J^+ は自然数の集合なので, 最小数を持つ. それを δ とおく. α を δ で割りその商を q , 余りを r とおくと

$$\alpha = q\delta + r, \quad 0 \leq r < \delta$$

を満たす. 上の式を変形して $r = \alpha + (-q)\delta$ とおくと 前項の (2) により

$$\delta \in J \Rightarrow (-q)\delta \in J.$$

$\alpha \in J$ によれば 前項の (1) により $\alpha+(-q)\delta \in J$. したがって $r = \alpha+(-q)\delta \in J$. よって $0 \leq r \in J$. ところで δ は J^+ の最小数で $r < \delta$ を満たすから $r = 0$ になる. これより $\alpha = q\delta$. すなわち $\alpha \in (\delta)$.

$\alpha < 0$ なら $-\alpha \in J$ なので上記のことより $-\alpha \in (\delta)$. したがって $J \subset (\delta)$. ところが $\delta \in J$ なので, $(\delta) \subset J$. よって $J = (\delta)$.

$a,b \in J = (\delta)$ により δ は a,b の公約数である.

次に δ は a,b の最大公約数であることを証明しよう.

d_1 を a,b の公約数とすると $a = a_1d_1, b = b_1d_1$ と自然数 a_1, b_1 で表せる. $\delta \in J$ なので $\delta = ax_0+by_0$ と書くと

$$\delta = ax_0+by_0 = a_1d_1x_0+b_1d_1y_0 = (a_1x_0+b_1y_0)d_1$$

となるので $\delta \geq d_1$. よって δ は a, b の最大公約数 d である. したがって, $\delta = d$. かくて $J = (d)$. すなわち J の元は d の倍数になった.

以上により最大公約数 d は イデアル J の生成元であることがわかり同時に d は J^+ の最小数でもあることが示された.

x, y を求める

与えられた自然数 a, b に対してこれらの最大公約数 d と $d = ax + by$ を満たす整数 x, y を具体的に手で計算するには次の表 1.3 の図式を用いると良い.

a, b に対して 3 次ベクトルを次のように定義する.

$$v_0 = (1, 0, a), v_1 = (0, 1, b).$$

a を b で割った商を q_1, 余りを r_1 とおけば $a = bq_1 + r_1$ となる. すると $a = bq_1 + r_1 \in (b, r_1)$ なのでイデアルとして

$(a, b) \subset (b, r_1)$. $r_1 = a + (-q)b \quad \in (a, b)$ により $(b, r_1) \subset (a, b)$.

よって $(b, r_1) = (a, b)$. そこでベクトル v_2 を

$$v_2 = v_0 - q_1 v_1$$

で定めると $v_2 = (1, -q_1, r_1)$.

表 2: $d = ax + by$ のアルゴリズム

v_0		1	0	a
v_1	q_1	0	1	b
v_2		1	$-q_1$	r_1

$r_1 > 0$ なら b を r_1 で割った商を q_2, 余りを r_2 とすると $b = r_1 q_2 + r_2$ となる. ベクトル v_3 を

$$v_3 = v_1 - q_2 v_2$$

で定め, さらに続ける. $b > r_1 > \cdots$. ついには $r_{h-1} > r_h = 0$ となる $h > 0$ がある.

$v_{h-1} = (x, y, d)$ とおくと $d = r_{h-1}$ が a, b の最大公約数になることはイデアルの関係

$$(a, b) = (b, r_1) = \cdots = (r_{h-1}, r_h) = (r_{h-1})$$

から明らかであろう. その上 x, y は $ax + by = d$ を満たす.

表 3: $a = 11, b = 8$ の例

	1	0	$a = 11$
1	0	1	$b = 8$
2	1	-1	3
1	-2	3	2
	$x = 3$	$y = -4$	$d = 1$

数値例

$a = 11, b = 8$ のとき次のような図式を書いて計算する. $v_0, v_1, \cdots$ は書かなくてよいが, 左の列に商を書くとよい.

これより $x = 3, y = -4, d = 1$. 実際に, $11 \times 3 + 8 \times (-4) = 1$.

内積を使った証明

$d = ax + by$ となることは内積を使うと簡単に証明できる.
ベクトル w を $w = (a, b, -1)$ で定義する.

$$v_0 \cdot w = (1, 0, a) \cdot (a, b, -1) = 1 \cdot a - a = 0, v_1 \cdot w = 1 \cdot b - b = 0$$

なので

$$v_2 \cdot w = v_0 \cdot w - q_1 v_1 \cdot w = 0,$$

$$v_3 \cdot w = v_1 \cdot w - q_2 v_2 \cdot w = 0,$$

と続けるとついに $v_{h-1} \cdot w = 0$.
一方 $v_{h-1} = (x, y, d)$ なので $v_{h-1} \cdot w = ax + by - d$. したがって $d = ax + by$.

3 因数 a, b, c の補題

自然数 a, b の最大公約数 d が 1 のとき a と b は**互いに素** (relatively prime) という. このときユークリッドの補題により a と b の生成するイデアル (a, b) は 1 を含むので $(a, b) = \mathbb{Z}$ となる.

a, b が整数でもその絶対値 $|a|, |b|$ が互いに素なら, やはり a, b を互いに素という. このときも $1 = ax + by$ と整数 x, y で表せる.

a, b が互いに素というとき, a, b は 0 でないことを仮定している.

つぎの結果を因数 a, b, c の補題という.

補題 1 a, b, c を整数とし a, b は互いに素とする. a が bc の因数なら a は c の因数である.

Proof
a が bc の因数なので $ak = bc$ と整数 k で書ける. a, b は互いに素なので $1 = ax + by$ と整数 x, y を用いて表される. そこで c を掛けて

$$c = acx + bcy = acx + aky = a(cx + ky).$$

$f = cx + ky$ とおくと $c = af$. よって a は c の因数.

a, b が互いに素なら $(a, b) = (1)$（イデアルとして） を満たす. 補題を記号的に書けば次のようになる.

$(a, b) = (1)$ を満たすとき, $bc \in (a) \Rightarrow c \in (a)$.

4　素因数分解の定理

自然数の世界で素因数分解の一意性定理が成り立つことはユークリッドらのすでに知ることであるが１８世紀の終わりごろガウスがこの定理の証明が不完全であることを嘆いて次の結果を D.A.(ガウス 整数論, 高瀬訳) で証明している.

補題
p が素数で a, b : 自然数のとき $ab \equiv 0 \mod p$ なら $a \equiv 0$ または $b \equiv 0 \mod p$.

背理法で示すため $ab \equiv 0 \mod p$ のとき $a \not\equiv 0$ かつ $b \not\equiv 0 \mod p$ を仮定する.

ここで, a, p を固定して考える. 上記を満たす b の中で最小に選ぶ. p を b で割るときその商とあまりを 自然数 Q と r で示すと $p = bQ + r, r < b$.

$ab = pm$ と書いてから $p = bQ + r$ を a 倍すると

$ap = abQ + ar = pmQ + ar$.

$p(a - mQ) = ar$ なので $m' = a - mQ$ とおくとき $ar = pm', 0 \leq r < b$.

b は最小値なので $r = 0$.

ゆえに $p = bQ$. p は素数なので $Q = 1; p = b$. 仮定:$b \not\equiv 0 \mod p$ に反する.

伝統的な証明法は素数 p に対し、イデアル $J = pZ$ が極大イデアルになることを示す. そのとき互除法の結果を用いる.

a が $J = pZ$ に属さないとき p で割れない. a と p の最大公約数は 1 なので $1 = am + pn$ を満たす整数 n, m がある.

これは a と J の生成するイデアルが全体になることを意味する. したがって, J は極大イデアルになりその結果, 素イデアルになる.

ガウスの証明は直ちに素イデアルを導く.

5　究極の完全数とその平行移動

オイラー 完全数を導入する前に究極の完全数の定義を述べる.

$\sigma(a)$ を自然数 a の約数の和とし, $\sigma(a)$ を関数と見て ユークリッド関数という.

P を素数とし, 整数 m に関して $\sigma(P^e) + m$ が素数 q のとき $a = P^e q$ を m だけ平行移動した底が P の (狭義の) 究極の完全数と呼ぶ.

これは次式を満たす.

$$\overline{P}\sigma(a) - Pa = (P - 2)\mathrm{Maxp}(a) - m(P - 1). \tag{1}$$

$\mathrm{Maxp}(a)$ は a の最大素因子を指している.

この式を満たす a を m だけ平行移動した底が P の (広義) の究極の完全数と呼ぶ.

6　φ 完全数

究極の完全数の定義を参考にユークリッド関数の代わりにオイラー関数 $\varphi(a)$ を使って完全数と類似した概念を定義しよう.

しかしながら $\varphi(P^e), (e > 1)$ は合成数なので完全数の定義をそのままは使えない. そこで, 1 を加えて $\varphi(P^e) + 1$ が素数 q になるとき $a = P^e q$ をもって P を底とする狭義のオイラー φ **完全数**と定義する.

さて最も簡単な　$P = 2$ の場合を定義に沿ってパソコンで計算してみる.

表 4: $P = 2$ を底とする φ 完全数

e	a	素因数分解	$\varphi(a)$
2	12	$2^2 * 3$	4
3	40	$2^3 * 5$	16
5	544	$2^5 * 17$	256
9	131584	$2^9 * 257$	65536
17	8590065664	$2^{17} * 65537$	4294967296

計算の結果,a の素数部分には 3,5,17,257,65537 のようにフェルマ素数が並んでいるではないか.

しかし, 定義に戻ると, $P = 2$ のとき $q = \varphi(P^e) + 1 = 2^{e-1} + 1$ が素数という条件になるので $e - 1 = 2^m$ と書けて q がフェルマ素数になるのは当然である.

7　底 P, 平行移動 m の劣完全数

$q = P^{e+1} - 1 + m$ が素数のとき $a = P^e q$ を底 P, 平行移動 m の狭義のサブ完全数, 劣完全数 (subperfect number) といい, このときの q をサブ素数 (subprime number) という. サブ素数は素数である.

ここで劣完全数の方程式の導入を行う.

劣完全数 $a = P^e q$ について

$$\overline{P}\sigma(a) = \overline{P}\sigma(P^e q) = (P^{e+1} - 1)(q + 1) = Pa - (q + 1 - P^e)$$

$q = P^{e+1} - 1 + m$ によれば $q + 1 - P^e = m$ なので

$$\overline{P}\sigma(a) = Pa - m.$$

究極の完全数の場合と比べて簡明な式になった.

この方程式の解を底 P, 平行移動 m の広義の劣完全数 (subperfect number with translation parameter m) というのである.

広義の劣完全数を簡単に劣完全数という.

$P > 2$ なら, $m = 0$ のとき $P^{e+1} - 1 + m$　は素数にならない. これを克服するために $\sigma(P^e)$ を使うことになり $q = \sigma(P^e) - 1 + m$ が素数のとき $a = P^e q$ を究極の完全数が定義された.

しかし, m によっては $P^{e+1} - 1 + m$ は素数なのでこのように完全数を定義しても一向構わない.

7.1　正規形の劣完全数

$a = P^f Q(Q : \text{素数})$ と書ける解を正規形の劣完全数という.

このとき $\overline{P}\sigma(a) = (P^{f+1} - 1)(Q + 1) = Pa + P^{f+1} - (Q + 1)$ になり

$$-m = \overline{P}\sigma(a) - Pa = P^{f+1} - (Q + 1).$$

これより $Q = P^{f+1} + m - 1$.

これは底 P, 平行移動 m の狭義の劣完全数のときの劣素数である.

7.2　$P = 3$, 平行移動 $m = 3$ の劣完全数

狭義の劣完全数の場合には $P = 3$ のとき $Q = 3^{e+1} - 1 + m$ が素数となる. だから m は奇数になる. しかし $m = 1, 7, 10$ の場合 Q は素数にならない.

そこで 広義の劣完全数の場合 $m = 3$ について調べる.

5 を除くと, $5 * 7 * 11$ の他は, 正規形と第 2 正規形 の解ばかりである. おとなしい解があるだけだ.

$A = 750946651497972490400980615625696 1$

$B = 3^{35} * 150094635296999123$

表 5: $[P=3, m=3]$ 狭義の劣完全数, 正規形

e	a	素因数分解
1	33	$3*11$
2	261	3^2*29
3	2241	3^3*83
7	14353281	3^7*6563
9	1162300833	$3^9*59051$
13	7625600673633	$3^{13}*4782971$
14	68630386930821	$3^{14}*14348909$
23	26588814359145789645441	$3^{23}*282429536483$
25	21536939630772523435296 33	$3^{25}*2541865828331$
35	A	B

7.3 第２種正規形の劣完全数

$a = P^f rq(r < q$: 素数) と書ける解を第２種正規形の劣完全数という.
このとき $\overline{P}\sigma(a) = (P^{f+1}-1)(r+1)(q+1), Pa - m = P^{f+1}rq - m$ になる.
$N = P^{f+1}-1, A = (r+1)(q+1), B = rq, \Delta = r+q$ とおくとき

$$NA = (P^{f+1}-1)(r+1)(q+1), Pa - m = P^{f+1}rq - m = (N+1)B - m.$$

$A = B + \Delta + 1$ を代入して

$$NB + N(\Delta+1) = P^{f+1}rq - m = (N+1)B - m.$$

これより

$$N(\Delta+1) = B - m.$$

$q_0 = q - N, r_0 = r - N, B_0 = q_0 r_0$ とおくと
$B_0 = B - N\Delta + N^2$. これを代入し

$$N(\Delta+1) = B - m = B_0 + N\Delta - N^2.$$

$D = N(N+1) + m$ とおけば, $B_0 = D$.

ここで話を逆転する. 与えられた f と m に対して $N = P^{f+1}-1, D = N(N+1)+m$ として D を求めそれを因数分解して, $B_0 = D$ から　$q = q_0 + N, r = r_0 + N$ がともに素数となるものを探す. すると, $a = P^f rq$ が解になる.

8 $P=3$, 平行移動 $m=0$ の劣完全数

$m=0$ のとき定義に戻れば $q=3^{e+1}-1+m$ は素数にならないので狭義の劣完全数にならない. しかし広義の劣完全数は定義できて $2\sigma(a)=3a$ となる. 実はこの場合は解がないことが証明できる. そこで一般の場合にして考える.

9 P:奇数, 平行移動 $m=0$ の劣完全数

広義の劣完全数を与える方程式は $\overline{P}\sigma(a)=Pa$ になる. $P=2$ のときは元祖完全数になるので特段の興味があるが, ここでは $P\geq$, $m=0$ のとき解がないことを示す.

命題 1 $P=3, a=2$ 以外なら P:奇素数, 平行移動 $m=0$ の広義の劣完全数は存在しない.

Proof.

素因数分解の一意性から, $\sigma(a)$ は P で割れるので,$\sigma(a)=P^{\varepsilon}L(L$ は P で割れない) とかける.

$$\overline{P}\sigma(a)=\overline{P}P^{\varepsilon}L=Pa.$$

これより, $a=P^{\varepsilon-1}L\overline{P}$. $N=P^{\varepsilon}-1, M=\overline{P}L$ とおけば $a=P^{\varepsilon-1}M, Pa=(N+1)M$. M は P で割れないから,

$$\sigma(a)=\sigma(M)\sigma(P^{\varepsilon-1}).$$

$$\overline{P}\sigma(a)=\sigma(M)\overline{P}\sigma(P^{\varepsilon}-1)=N\sigma(M).$$

$\overline{P}\sigma(a)=Pa$ によって,

$$N\sigma(M)=(N+1)M.$$

これより

$$\frac{N}{N+1}=\frac{M}{\sigma(M)}.$$

$\dfrac{N}{N+1}$ は既約分数なので, $M=kN, \sigma(M)=k(N+1)$ を満たす整数 k が存在する. 2 つの式を引いて,

$$\sigma(M)-M=k.$$

$M=kN$ により, k も M の約数なので, $\sigma(M)=M+k$ から M : 素数,$k=1$ が出る.

M : 素数なら, $P = 3, L = 1, a = 4$. これ以外なら $M = \overline{P}L$ は素数ではないので矛盾.

(この証明は オイラーが偶数完全数はユークリッドの完全数なる証明と類似している)