完全数について

MATHEMATICS.PDF

平成 17 年 11 月 23 日

この文書では, 自然数は 0 を含まず, 1 から始まるものとします. また, 約数は負の整数であるものは考えず, 自然数であるもののみを考えます.

2 つの自然数 a, b の最大公約数を記号 $\gcd(a,b)$ で表します. $\gcd(a,b)=1$ であることを, a と b は互いに素であるということもあります. 自然数 a, b, c について,「c が ab の約数であり, $\gcd(b,c)=1$ ならば, c は a の約数である」という事実を随所に用いています.

1 偶数の完全数

まず, 完全数の定義を述べます.

定義 1.1 自然数 a が**完全数**であるとは, a 自身を除く a のすべての約数の和が a に等しいときにいう.

最も小さい完全数は 6 です. 実際, 6 の約数は 1, 2, 3, 6 であり,

$$1+2+3=6$$

となります. その次に小さい完全数は 28 です. 実際, 28 の約数は 1, 2, 4, 7, 14, 28 であり,

$$1+2+4+7+14=28$$

となります. その後は, 496, 8128, 33550336, 8589869056, 137438691328, ... という具合に続きます.

与えられた自然数の約数の総和をあらかじめ記号で表しておくと, 完全数について議論するときには便利です.

定義 1.2 自然数 a の約数の総和を $\sigma(a)$ で表す. つまり, a のすべての約数を d_1, d_2, ..., d_r とするとき, $\sigma(a)=d_1+d_2+\cdots+d_r$ と定義する.

自然数 $a>1$ は少なくとも 1 と a 自身を約数にもつので,

$$\sigma(a)\geq 1+a \tag{1}$$

が成り立ちます. 不等式 (1) において等号が成り立つためには a が素数であることが必要十分です. 実際, もし a が素数ならば, a の約数は 1 と a 自身しかないので, $\sigma(a)=1+a$ です. もし a が合成数[1] ならば, 1 と a 以外の約数 d_2, ..., d_{r-1} をもつので, $\sigma(a)=1+d_2+\cdots+d_{r-1}+a>1+a$ となります.

[1] 1 でも素数でもない自然数を合成数といいます.

また, 自然数 a が完全数であることと $\sigma(a) = 2a$ が成り立つこととが同値であることは, 完全数の定義からすぐにわかります.

定理 1.3 n を自然数とする. もし, $b = 2^n - 1$ が素数ならば, $a = 2^{n-1}b$ は完全数である.

証明 $\gcd(b, 2) = 1$ であり, b は素数なので, a のすべての約数は

$$\begin{aligned} &1, \quad 2, \quad \ldots, \quad 2^{n-1}, \\ &b, \quad 2b, \quad \ldots, \quad 2^{n-1}b \end{aligned}$$

である. よって, a の約数の総和 $\sigma(a)$ は

$$\begin{aligned} \sigma(a) &= 1 + 2 + \cdots + 2^{n-1} + b + 2b + \cdots + 2^{n-1}b \\ &= (1 + 2 + \cdots + 2^{n-1})(1 + b) \\ &= (2^n - 1)2^n \\ &= 2a. \end{aligned}$$

したがって a は完全数である. □

定理 1.4 n を自然数とする. もし, $2^{n-1}(2^n - 1)$ が完全数であれば, $2^n - 1$ は素数である.

証明 背理法で証明する. $2^n - 1$ が素数でないと仮定する.

$b = 2^n - 1$ とおく. b のすべての約数を d_1, d_2, ..., d_r とする. $\gcd(b, 2) = 1$ なので, a のすべての約数は

$$\begin{aligned} &d_1, \quad 2d_1, \quad \ldots, \quad 2^{n-1}d_1, \\ &d_2, \quad 2d_2, \quad \ldots, \quad 2^{n-1}d_2, \\ &\qquad \cdots\cdots, \\ &d_r, \quad 2d_r, \quad \ldots, \quad 2^{n-1}d_r \end{aligned}$$

となる. b の約数の総和 $\sigma(b)$ は

$$\sigma(b) = d_1 + d_2 + \cdots + d_r$$

なので, a の約数の総和 $\sigma(a)$ は

$$\begin{aligned} \sigma(a) &= (1 + 2 + \cdots + 2^{n-1})(d_1 + d_2 + \cdots + d_r) \\ &= (2^n - 1)\sigma(b) \end{aligned} \tag{2}$$

である.

$b = 2^n - 1$ が素数でないという仮定から, b は 1 と b 自身以外にも約数をもつので,

$$\sigma(b) > 1 + b = 2^n.$$

これと式 (2) より

$$\sigma(a) > 2^n(2^n - 1) \tag{3}$$

が得られる.

一方, a は完全数であるから,

$$\sigma(a) = 2a = 2^n(2^n - 1).$$

これは式 (3) に反する. したがって, b は素数でなければならない.

□

実は, 偶数の完全数は $2^{n-1}(2^n-1)$ の形のものしかありません.

定理 1.5 a を自然数とする. a が偶数かつ完全数ならば, ある自然数 n が存在して $a=2^{n-1}(2^n-1)$ が成り立ち, 2^n-1 は素数である.

証明 a は偶数なので, ある自然数 n, b が存在して

$$a=2^{n-1}b, \quad \gcd(b,2)=1 \tag{4}$$

が成り立つ. b のすべての約数を d_1, d_2, ..., d_r とすると, a のすべての約数は

$$\begin{array}{llll} d_1, & 2d_1, & \ldots, & 2^{n-1}d_1, \\ d_2, & 2d_2, & \ldots, & 2^{n-1}d_2, \\ & \cdots\cdots, & & \\ d_r, & 2d_r, & \ldots, & 2^{n-1}d_r \end{array}$$

となる. b の約数の総和 $\sigma(b)$ は

$$\sigma(b)=d_1+d_2+\cdots+d_r$$

なので, a の約数の総和 $\sigma(a)$ は

$$\begin{aligned} \sigma(a) &= (1+2+\cdots+2^{n-1})(d_1+d_2+\cdots+d_r) \\ &= (2^n-1)\sigma(b) \end{aligned} \tag{5}$$

である. 一方, a が完全数であることと式 (4) より

$$\sigma(a)=2a=2^nb.$$

よって

$$(2^n-1)\sigma(b)=2^nb \tag{6}$$

が得られる. よって 2^n-1 は 2^nb を割る. ところが, $\gcd(2^n-1,2)=1$ であるから, 2^n-1 は b を割る. すなわち, ある自然数 c が存在して

$$b=(2^n-1)c \tag{7}$$

が成り立つ.

もし仮に $c>1$ なら, 式 (7) より, 少なくとも 1, 2^n-1, c, $(2^n-1)c$ の 4 つの数は b の約数である. したがって

$$\begin{aligned} \sigma(b) &\geq 1+(2^n-1)+c+(2^n-1)c \\ &= 2^n(c+1) \\ &> 2^nc. \end{aligned}$$

ところが, 式 (6), 式 (7) より,

$$\sigma(b)=\frac{2^nb}{2^n-1}=2^nc$$

となり, 矛盾が生じる. したがって $c=1$ でなければならない.

よって $b=2^n-1$ となり, $a=2^{n-1}(2^n-1)$ が得られる. 2^n-1 が素数になることは, 定理 1.4 で示されている. □

参考までに, 定理 1.3 と定理 1.5 に基づく, 偶数の完全数を見つける Maple のプログラムを掲載します[2]. 冒頭の具体例はこれで見つけました.

```
for n from 1 to 30 do
  if(isprime(2^n-1)) then
    print (2^(n-1)*(2^n-1));
  end if;
end do;
```

定理 1.5 は, 偶数の完全数が連続した自然数の和で表すことができることを意味しています. 例えば,

$$6 = 1 + 2 + 3,$$
$$28 = 1 + 2 + 3 + 4 + 5 + 6 + 7,$$
$$496 = 1 + 2 + 3 + 4 + 5 + 6 + 7 + \cdots + 31$$

です. 一般に, 任意の自然数 k に対して

$$1 + 2 + 3 + \cdots + k = \frac{1}{2}k(k+1)$$

が成り立ちます. $k = 2^n - 1$ を代入すれば, 右辺は $2^{n-1}(2^n - 1)$ になります.

2　メルセンヌ素数について

$2^n - 1$ の形の素数を**メルセンヌ素数**といいます. つまり, 自然数 a がメルセンヌ素数であるとは, ある自然数 n が存在して $a = 2^n - 1$ が成り立ち, かつ a が素数であるときにいいます.

定理 1.3 と定理 1.5 より, メルセンヌ素数がすべて求められれば, 偶数の完全数もすべて求められることがわかります.

$2^n - 1$ がメルセンヌ素数になるためには, 少なくとも n が素数でなければなりません.

定理 2.1 n を自然数とする. もし $2^n - 1$ が素数ならば, n は素数である.

証明 対偶を示す.

まず, $n = 1$ のとき, $2^n - 1 = 1$ なので, $2^n - 1 = 1$ は素数ではない.

$n \geq 2$ のとき, もし n が合成数ならば, ある自然数 u, v が存在して

$$n = uv, \quad u > 1, \quad v > 1$$

と書ける. このとき

$$2^n - 1 = 2^{uv} - 1 = (2^u - 1)(2^{u(v-1)} + 2^{u(v-2)} + \cdots + 2^u + 1)$$

となる. $u > 1$, $v > 1$ より,

$$2^u - 1 > 1,$$
$$2^{u(v-1)} + 2^{u(v-2)} + \cdots + 2^u + 1 > 1$$

である. したがって $2^n - 1$ は合成数である. □

[2]Maple 9.5 で動作確認. ちなみに, Maple では, 改行を入力するときは Shift+Enter, プログラムを実行するときは Enter です. 念のため.

2^n-1 がメルセンヌ素数になるような自然数 n は完全には決定できていません. また, メルセンヌ素数が無数に存在するかどうかということも未解決です.

自然数 n を具体的に与えたとき, 2^n-1 が素数かどうかを判定するときに有効な方法として, ルカスの判定法が知られています.

定理 2.2（ルカスの判定法） 数列 (a_n) を

$$a_{n+1}=a_n^2-2, \quad a_1=4$$

により定義する. このとき,

$$M_n=2^n-1$$

が素数であるための必要十分条件は, a_{n-1} が M_n で割り切れることである.

ルカスの判定法の証明は省略します.

例として, $p=7$ のとき, $M_7=2^7-1=127$ が素数であることを, ルカスの判定法で判定してみます.

$$\begin{aligned}
&a_1=4,\\
&a_2=2^2-2=14,\\
&a_3=14^2-2\equiv 67 \pmod{127},\\
&a_4=67^2-2\equiv 42 \pmod{127},\\
&a_5=42^2-2\equiv 111 \pmod{127},\\
&a_6=111^2-2\equiv 0 \pmod{127}.
\end{aligned}$$

割り切れるかどうかが分かればよいので, $\bmod M_7$ で計算すればよいことに注意してください. a_6 は M_7 で割り切れるので, M_7 は素数です.

3　約数の総和について

この節では, 次の定理を証明することを目標とします.

定理 3.1 a, b を自然数とし, $\gcd(a,b)=1$ であるとする. このとき,

$$\sigma(ab)=\sigma(a)\sigma(b)$$

が成り立つ.

定理 3.1 を証明するために, いくつかの補助的な定理を証明します.

定理 3.2 a, b, d を自然数とする. もし

$$\gcd(a,d)=\gcd(b,d)=1$$

ならば

$$\gcd(ab,d)=1$$

が成り立つ.

証明 $g = \gcd(ab, d)$, $g' = \gcd(a, g)$ とおく.

g' は a の約数である. 一方, g' は g の約数, したがって d の約数である. ゆえに, g' は a と d の公約数である. $\gcd(a, d) = 1$ より, $g' = 1$ が得られる.

g は ab の約数であり, $g' = \gcd(a, g) = 1$ なので, g は b を割る. 一方, g は d の約数である. ゆえに, g は b と d の公約数である. $\gcd(b, d) = 1$ より, $g = 1$ が得られる. □

定理 3.3 a, b を自然数とし, $\gcd(a, b) = 1$ であるとする. このとき, 積 ab の任意の約数 d に対して, a の約数 u と b の約数 v が存在して $d = uv$ と書ける.

証明 $u = \gcd(a, d)$, $g = \gcd(u, b)$ とする.

g は u の約数, したがって a の約数である. 一方, g は b の約数である. ゆえに g は a と b の公約数である. $\gcd(a, b) = 1$ より, $g = 1$ が得られる.

u は d の約数なので, ある自然数 v が存在して

$$d = uv$$

と書ける. v が b の約数であることをこれから証明する.

$u' = \gcd(a, v)$ とおく. u' は v の約数なので, ある v' が存在して $v = u'v'$ と書ける. よって

$$d = uu'v'$$

となる. uu' は d の約数, したがって ab の約数である. また, $g = \gcd(u, b) = 1$ であり, u のときと同様にして u' についても $\gcd(u', b) = 1$ であることがいえる. 定理 3.2 より $\gcd(uu', b) = 1$ である. ゆえに uu' は a の約数である. したがって uu' は d と a の公約数である. ところが, $u = \gcd(a, d)$ なので, uu' は u の約数である. よって $u' = 1$ でなければならない.

v は d の約数, したがって ab の約数であり, $u' = \gcd(a, v) = 1$ なので, v は b の約数でなければならない. 以上で証明は完了した. □

定理 3.4 a, b を自然数とし, $\gcd(a, b) = 1$ であるとする. a のすべての約数を u_1, u_2, …, u_r とし, b のすべての約数を v_1, v_2, …, v_s とするとき, ab のすべての約数は

$$u_i v_j, \quad 1 \leq i \leq r, \quad 1 \leq v \leq s \tag{8}$$

である.

証明 ab の約数が式 (8) のいずれかに一致することは定理 3.3 ですでに示した. よって, 式 (8) に重複がないこと, すなわち

$$u_{i_1} v_{j_1} = u_{i_2} v_{j_2} \Longrightarrow u_{i_1} = u_{i_2},\ v_{j_1} = v_{j_2}$$

を示せばよい. いま,

$$u_{i_1} v_{j_1} = u_{i_2} v_{j_2} \tag{9}$$

と仮定する.

$g = \gcd(u_{i_1}, v_{j_2})$ とおく. g は u_{i_1} の約数なので a の約数である. 一方, g は v_{i_2} の約数なので b の約数である. ゆえに, g は a と b の公約数である. $\gcd(a, b) = 1$ より, $g = 1$ が得られる.

式 (9) より u_{i_1} は $u_{i_2} v_{j_2}$ を割るので, $g = \gcd(u_{i_1}, v_{j_2}) = 1$ と合わせると, u_{i_1} が u_{i_2} を割らなければならないことがいえる. 同様にして u_{i_2} が u_{i_1} を割ることもいえる. したがって $u_{i_1} = u_{i_2}$ が得られる. これと式 (9) より $v_{j_1} = v_{j_2}$ も得られる. □

定理 3.3 と定理 3.4 について補足しておきます. a, b, ab の約数の全体からなる集合をそれぞれ D_a, D_b, D_{ab} とおき, 写像

$$D_a \times D_b \to D_{ab}, \quad (u, v) \mapsto uv$$

を考えます. $\gcd(a, b) = 1$ であるとき, 定理 3.3 の証明では上の写像が全射であることを示し, 定理 3.4 の証明では上の写像が単射であることを示したことになります.

準備が整ったので, いよいよ定理 3.1 を証明します.

証明 $\gcd(a, b) = 1$ なので, 定理 3.4 より, a のすべての約数を u_1, u_2, …, u_r とし, b のすべての約数を v_1, v_2, …, v_s とするとき, ab のすべての約数は

$$\begin{array}{llll} u_1v_1, & u_2v_1, & \ldots, & u_rv_1, \\ u_1v_2, & u_2v_2, & \ldots, & u_rv_2, \\ & \cdots\cdots, & & \\ u_1v_s, & u_2v_s, & \ldots, & u_rv_s \end{array}$$

となる. よって

$$\begin{aligned} \sigma(ab) &= u_1v_1 + u_2v_1 + \cdots + u_rv_s \\ &= (u_1 + u_2 + \cdots + u_r)(v_1 + v_2 + \cdots + v_s) \\ &= \sigma(a)\sigma(b) \end{aligned}$$

が成り立つ. □

定理 3.1 は, 2 つずつ互いに素な 3 つ以上の自然数に対しても成立します. 例えば, 3 つの自然数 a, b, c に対しては, 定理 3.2 より

$$\gcd(a, c) = \gcd(b, c) = 1 \Longrightarrow \gcd(ab, c) = 1$$

なので, 定理 3.1 を繰り返し適用すれば,

$$\sigma(abc) = \sigma(ab)\sigma(c) = \sigma(a)\sigma(b)\sigma(c)$$

となります.

自然数 $a > 1$ は

$$a = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}, \quad e_i \geq 1, \quad 1 \leq i \leq r$$

のように素因子分解することができます. 定理 3.1 より

$$\sigma(a) = \sigma(p_1^{e_1})\sigma(p_2^{e_2})\cdots\sigma(p_r^{e_r})$$

が成り立ちます. したがって, 各素因子のベキの約数の総和 $\sigma(p_1^{e_1})$ の計算結果を利用して, a の約数の総和 $\sigma(a)$ を計算することができます.

e を自然数とするとき, 素数 p のベキ p^e のすべての約数は

$$1, \quad p, \quad p^2, \quad \ldots, \quad p^e$$

なので,

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}$$

となります.

例えば, $60 = 2^2 \cdot 3 \cdot 5$ の約数の総和 $\sigma(60)$ は

$$\sigma(60) = \sigma(2^2)\sigma(3)\sigma(5) = 7 \cdot 4 \cdot 6 = 168$$

となります.

4 奇数の完全数について

奇数の完全数の例は 1 つも見つかっていません. 奇数の完全数は存在しないであろうと予想されていますが, 未解決です.

1 の 1 自身を除く約数の和は 0 なので, 1 は完全数ではありません.

奇素数[3] p が完全数でないことはすぐにわかります. 実際,

$$\sigma(p) = 1 + p \neq 2p$$

となります[4].

定理 4.1 自然数 e に対して, 奇素数 p のベキ p^e は完全数ではない.

証明

$$\begin{aligned} 2p^e - \sigma(p^e) &= 2p^e - \frac{p^{e+1} - 1}{p - 1} \\ &= \frac{1}{p-1}(p^{e+1} - 2p^e + 1) \\ &= \frac{1}{p-1}\big(p^e(p-2) + 1\big) \\ &> 0. \end{aligned}$$

ゆえに

$$\sigma(p^e) < 2p^e$$

であるから, p^e は完全数ではない.

□

定理 4.2 もし奇数 $a > 1$ が完全数ならば, a は相異なる素因子を 3 つ以上もつ.

証明 a が素因子を 1 つしかもたないとき, すなわち a が素数のベキで表されるとき, a が完全数でないことは定理 4.1 ですでに示されている.

そこで, a が相異なる素因子をちょうど 2 つもつ場合を考える. すると,

$$a = p_1^{e_1} p_2^{e_2}$$

と素因子分解でき,

$$\sigma(a) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \tag{10}$$

[3]奇数であるような素数を奇素数といいます. 偶数は 2 の倍数なので, 2 以外の偶数はすべて素数ではありません. ゆえに, 2 を除く素数はすべて奇素数です.

[4]自然数 a が完全数であることと $\sigma(a) = 2a$ が成り立つこととが同値であることを思い出してください.

が成り立つ. さらに,

$$\begin{aligned}\sigma(p_1^{e_1})\sigma(p_2^{e_2}) &= \frac{p_1^{e_1+1}-1}{p_1-1}\cdot\frac{p_2^{e_2+1}-1}{p_2-1}\\ &< \frac{p_1^{e_1+1}}{p_1-1}\cdot\frac{p_2^{e_2+1}}{p_2-1}\\ &= \frac{p_1}{p_1-1}\cdot\frac{p_2}{p_2-1}\cdot a \end{aligned} \tag{11}$$

である.

p_1, p_2 は奇素数であり, $p_1 < p_2$ と仮定しても一般性を失わないので, $p_1 \geq 3$, $p_2 \geq 5$ と考えてよい. このとき,

$$\frac{p_1}{p_1-1}\cdot\frac{p_2}{p_2-1} \leq \frac{3}{2}\cdot\frac{5}{4} = \frac{15}{8} < 2. \tag{12}$$

ここで, 2 つの自然数 $u \geq 2$, $v \geq 2$ に対して,

$$\begin{aligned} u < v &\Longleftrightarrow -v < -u \Longleftrightarrow uv - v < uv - u\\ &\Longleftrightarrow v(u-1) < u(v-1)\\ &\Longleftrightarrow \frac{v}{v-1} < \frac{u}{u-1} \end{aligned}$$

が成り立つことに注意する.

式 (10), 式 (11), 式 (12) より

$$\sigma(a) < 2a$$

が得られる. したがって, 相異なる素因子を 2 つしかもたないとき, a は完全数ではない. □

他にも, 与えられた奇数が完全数でないことが簡単に示せる場合があります.

定理 4.3 奇数 $a > 1$ に対して, a^2 は完全数ではない.

証明

$$a = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$$

と素因子分解すると, 各々の素因子 p_i は奇数である. このとき,

$$a^2 = p_1^{2e_1}p_2^{2e_2}\cdots p_r^{2e_r}$$

であり,

$$\sigma(a^2) = \sigma(p_1^{2e_1})\sigma(p_2^{2e_2})\cdots\sigma(p_r^{2e_r})$$

となる. もし仮に a^2 が完全数ならば, $\sigma(a^2) = 2a^2$ なので,

$$2a^2 = \sigma(p_1^{2e_1})\sigma(p_2^{2e_2})\cdots\sigma(p_r^{2e_r}) \tag{13}$$

が成り立つ. このとき, 例えば $\sigma(p_1^{2e_1})$ について,

$$\begin{aligned}\sigma(p_1^{2e_1}) &= 1 + p_1 + p_1^2 + \cdots + p_1^{2e_1}\\ &\equiv \overbrace{1+1+\cdots+1}^{2e_1+1}\\ &\equiv 1 \pmod 2\end{aligned}$$

である. $\sigma(p_2^{2e_2})$, …, $\sigma(p_r^{2e_r})$ についても同様である. よって, 式 (13) の右辺は $\bmod 2$ で 1 と合同である. ところが, 式 (13) の左辺は $\bmod 2$ で 0 と合同なので, 矛盾である. したがって a^2 は完全数ではない. □

定理 4.4 奇数 $a > 1$ の素因子 p がすべて $p \equiv 3 \pmod 4$ を満たすならば, a は完全数ではない.

証明

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

と素因子分解する. このとき,

$$\sigma(a) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r})$$

となる. もし仮に a が完全数ならば, $\sigma(a) = 2a$ なので,

$$2a = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r}) \tag{14}$$

が成り立つ. このとき, 例えば $\sigma(p_1^{e_1})$ について, 仮定より $p_1 \equiv 3 \pmod 4$ なので,

$$\begin{aligned} \sigma(p_1^{e_1}) &= 1 + p_1 + p_1^2 + \cdots + p_1^{e_1} \\ &\equiv \begin{cases} 1 \pmod 4, & e_1 \text{ が偶数のとき} \\ 0 \pmod 4, & e_1 \text{ が奇数のとき} \end{cases} \end{aligned}$$

である. $\sigma(p_2^{e_2})$, ..., $\sigma(p_r^{e_r})$ についても同様である. よって, 式 (14) の右辺は $\bmod 4$ で 0 か 1 と合同である. ところが, 式 (14) の左辺は $\bmod 4$ で 2 と合同なので, 矛盾である. したがって a は完全数ではない. □

定理 4.5 奇数 $a > 1$ が平方因子をもたなければ[5], a は完全数ではない.

証明 a は平方因子をもたないので,

$$a = p_1 p_2 \cdots p_r$$

と素因子分解できる. $r = 1$ のとき, すなわち a が素数のとき, a が完全数でないことはすでに示した. よって $r \geq 2$ と仮定する. このとき,

$$\sigma(a) = \sigma(p_1)\sigma(p_2) \cdots \sigma(p_r)$$

となる. もし仮に a が完全数ならば, $\sigma(a) = 2a$ なので,

$$2a = \sigma(p_1)\sigma(p_2) \cdots \sigma(p_r) \tag{15}$$

が成り立つ. このとき, 例えば $\sigma(p_1)$ について, p_1 は奇数なので,

$$\sigma(p_1) = 1 + p_1 \equiv 0 \pmod 2$$

である. $\sigma(p_2^{e_2})$, ..., $\sigma(p_r^{e_r})$ についても同様である. $r \geq 2$ なので, 式 (15) の右辺は $\bmod 4$ で 0 と合同である. ところが, 式 (15) の左辺は $\bmod 4$ で 2 と合同なので, 矛盾である. したがって a は完全数ではない. □

次の定理は, オイラーが証明したと伝えられている有名な結果です.

[5] 自然数 a が平方因子をもたないとは, どのような自然数 $d > 1$ に対しても a が d^2 で割り切れないことをいいます.

定理 4.6（オイラー）奇数 $a > 1$ が完全数であるための必要条件は, a を

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

と素因子分解したとき,

$$p_1 \equiv e_1 \equiv 1 \pmod 4, \tag{16}$$
$$e_2 \equiv e_3 \equiv \cdots \equiv e_r \equiv 0 \pmod 2 \tag{17}$$

が成り立つことである.

証明

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

と素因子分解する. このとき,

$$\sigma(a) = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r})$$

となる.

a が完全数であると仮定すると, $\sigma(a) = 2a$ なので,

$$2a = \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r})$$

が成り立つ. a は奇数なので,

$$2a \equiv 2 \pmod 4$$

となる. ゆえに,

$$2 \equiv \sigma(p_1^{e_1})\sigma(p_2^{e_2}) \cdots \sigma(p_r^{e_r}) \pmod 4.$$

したがって,

$$\sigma(p_1^{e_1}) \equiv 2 \pmod 4,$$
$$\sigma(p_i^{e_i}) \equiv 1 \pmod 2, \quad 2 \leq i \leq r$$

のようになっていなければならない.

e を自然数, p を奇素数とすると,

$$\sigma(p^e) = 1 + p + p^2 + p^3 + \cdots + p^e$$

が成り立つ. このとき,

$$\sigma(p^e) \equiv 2 \pmod 4 \Longleftrightarrow p \equiv e \equiv 1 \pmod 4,$$
$$\sigma(p^e) \equiv 1 \pmod 2 \Longleftrightarrow e \equiv 0 \pmod 2$$

である. ゆえに, 式 (16), 式 (17) が成り立つ. □

5　過剰数と不足数

自然数 a が完全数であるための必要十分条件は, $\sigma(a) = 2a$ が成り立つことです. 完全数ではない自然数 a のうち, $\sigma(a) > 2a$ を満たすものを**過剰数**といいます. また, 過剰数でも完全数でもないもの, すなわち $\sigma(a) < 2a$ を満たすものを**不足数**といいます.

例えば, 任意の自然数 e と任意の素数 p に対して, p^e は不足数です. 実際,

$$2p^e - \sigma(p^e) = 2p^e - \frac{p^{e+1}}{p-1} = \frac{1}{p-1}\big(p^e(p-2)+1\big) > 0$$

となります.

また, 例えば, $945 = 3^3 \cdot 5 \cdot 7$ は過剰数です. 実際,

$$\begin{aligned}\sigma(945) &= \sigma(3^3)\cdot\sigma(5)\sigma(7) = 40\cdot 6\cdot 8 = 1920,\\ 2\cdot 945 &= 1890\end{aligned}$$

となります. ちなみに, 945 は奇数の過剰数のうちで最小のものです.

定理 5.1　自然数 a が過剰数ならば, a の倍数もまた過剰数である.

定理 5.2　自然数 a が不足数ならば, a の約数もまた不足数である.

定理 5.1, 定理 5.2 を証明するために, 補助的な定理を証明します.

定理 5.3　e, u を自然数とし, p を素数とする. このとき,

$$p^u\sigma(p^e) < \sigma(p^{e+u}) \tag{18}$$

が成り立つ.

証明

$$\begin{aligned}p^u\sigma(p^e) &= p^u(1+p+\cdots+p^e)\\ &= p^u + p^{1+u} + \cdots + p^{e+u}\\ &< 1 + p + p^2 + \cdots + p^u + p^{1+u} + \cdots + p^{e+u}\\ &= \sigma(p^{e+u}).\end{aligned}$$

ゆえに, 式 (18) が成り立つ. □

定理 5.4　a, b を自然数とする. b が a の約数で $b < a$ ならば,

$$\frac{a}{b} < \frac{\sigma(a)}{\sigma(b)} \tag{19}$$

が成り立つ.

証明

$$b = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$$

と素因子分解すると, 負でない整数 u_1, u_2, …, u_r と, p_1, p_2, …, p_r と互いに素な自然数 c が存在して

$$a = p_1^{e_1+u_1}p_2^{e_2+u_2}\cdots p_r^{e_r+u_r}c$$

と表せる. $b < a$ という仮定から, $c > 1$ であるか, または u_1, u_2, …, u_r のうち少なくとも 1 つは 0 より大きいことに注意せよ. また, このとき

$$\frac{b}{a} = p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r} c$$

である.

任意の自然数 e, u と任意の素数 p に対して, 定理 5.3 より $\sigma(p^{e+u}) > p^u \sigma(p^e)$ である[6]. ゆえに,

$$\begin{aligned}
\sigma(a) &= \sigma(p_1^{e_1+u_1})\sigma(p_2^{e_2+u_2}) \cdots \sigma(p_r^{e_r+u_r})\sigma(c) \\
&> p_1^{u_1}\sigma(p_1^{e_1}) p_2^{u_2}\sigma(p_2^{e_2}) \cdots p_r^{u_r}\sigma(p_r^{e_r})c \\
&= p_1^{u_1} p_2^{u_2} \cdots p_r^{u_r} c\, \sigma(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) \\
&= \frac{a}{b}\sigma(b).
\end{aligned}$$

したがって, 式 (19) が成り立つ. □

定理 5.1 の証明 定理 5.4 より, a の任意の倍数 a' に対して

$$\sigma(a') \geq \frac{a'}{a}\sigma(a)$$

が成り立つ. また, a は過剰数なので, $\sigma(a) > 2a$ が成り立つ. ゆえに

$$\sigma(a') > \frac{a'}{a} \cdot 2a = 2a'.$$

したがって a' も過剰数である. □

定理 5.2 の証明 定理 5.4 より, a の任意の約数 b に対して

$$\sigma(b) \leq \frac{b}{a}\sigma(a)$$

が成り立つ. また, a は不足数なので, $\sigma(a) < 2a$ が成り立つ. ゆえに

$$\sigma(b) < \frac{b}{a} \cdot 2a = 2b.$$

したがって b も不足数である. □

a を完全数とします. a' を a の倍数とし, $a' > a$ であるとすると, 定理 5.4 より,

$$\sigma(a') > \frac{a'}{a}\sigma(a) = \frac{a'}{a} \cdot 2a = 2a'.$$

したがって a' は過剰数になります. すなわち, 完全数の自分自身を除く倍数は過剰数になります. また, b を a の倍数とし, $b < a$ であるとすると, 定理 5.4 より,

$$\sigma(b) < \frac{b}{a}\sigma(a) = \frac{b}{a} \cdot 2a = 2b.$$

したがって b は不足数になります. すなわち, 完全数の自分自身を除く約数は不足数になります.

[6] $u = 0$ のときは自明な等式 $\sigma(p^e) = \sigma(p^e)$ が成り立ちます.