整数の性質

更新日 2023 年 3 月 21 日

定義

整数 a , b , k の間に $a=bk$ の関係がある時、 a を b の**倍数**、 b を a の**約数**という。

整数 a,b,c,k_1,k_2 , $a=bk_1$ かつ $b=ck_2$ ならば $a=c(k_1k_2)$ だから、次の推移律が成立する。
[推移律] a が b の倍数(約数)かつ b が c の倍数(約数)ならば a は c の倍数(約数)である。

整数 $a_1,a_2,\cdots,a_n$ に共通の倍数を**公倍数**、共通の約数を**公約数**という。
正の公倍数の中で最小のものを**最小公倍数**という。 $LCM(a_1,a_2,\cdots,a_n)$ と書く。
正の公約数の中で最大のものを**最大公約数**という。 $GCD(a_1,a_2,\cdots,a_n)$ と書く。

証明のためのツールとして、整数 $a_1,a_2,\cdots,a_n$ に対する集合を次のように決める。

$M(a)=\{x;x\text{は}a\text{の倍数}\}$, $M(a_1,a_2,\cdots,a_n)=\{x;x\text{は}a_1,a_2,\cdots,a_n\text{の公倍数}\}$

$D(a)=\{x;x\text{は}a\text{の約数}\}$, $D(a_1,a_2,\cdots,a_n)=\{x;x\text{は}a_1,a_2,\cdots,a_n\text{の公約数}\}$

定義から

$M(a_1,a_2,\cdots,a_n)=M(a_1)\cap M(a_2)\cap\cdots\cap M(a_n)$

$D(a_1,a_2,\cdots,a_n)=D(a_1)\cap D(a_2)\cap\cdots\cap D(a_n)$

§A 整数の割り算

[A1 わり算における商と余り]

任意の整数 m ,自然数 n に対して、(A1)を満たす整数 Q [商], 自然数 r [余り]がただ一つ存在する。

$m=Qn+r$ かつ $0\leq r<n$ (A1)

[存在の証明] $q\leq\dfrac{m}{n}$ となる整数 q の中で最大のものを Q とする。

$Q\leq\dfrac{m}{n}<Q+1 \Rightarrow Qn\leq m<Qn+n \Rightarrow 0\leq m-Qn<n \Rightarrow r=m-Qn$ とおくと $0\leq r<n$

[一意性の証明] (A1)を満たす (Q,r) と (Q',r') があるとする。

$m=Qn+r$ $0\leq r<n$ かつ $m=Q'n+r'$ $0\leq r'<n \Rightarrow (Q'-Q)n=r-r'$ かつ $-n<r-r'<n$

$\Rightarrow -n<(Q'-Q)n<n \Rightarrow -1<Q'-Q<1 \Rightarrow Q'=Q \Rightarrow r=r'$

(証明終わり)

[A2 ユークリッドの互除法] (A1) において $D(m,n)=D(n,r)$ (m,n の公約数は n,r の公約数)

証明

$x\in D(m,n) \Rightarrow m=n_1x, n=n_2x \Rightarrow r=m-Qn=(n_1-Qn_2)x \Rightarrow x\in D(n,r) \Rightarrow D(m,n)\subseteq D(n,r)$

$x\in D(n,r) \Rightarrow n=n_3x, r=n_4x \Rightarrow m=Qn+r=(Qn_3+n_4)x \Rightarrow x\in D(m,n) \Rightarrow D(n,r)\subseteq D(m,n)$

[A3 最大公約数を求めるアルゴリズム] 最大公約数を求める2つの自然数を a,b とする。

数列 a_n を次のように定義する。 $a_1=a$, $a_2=b$

a_n,a_{n+1} に対して [A1]より $a_n=Qa_{n+1}+r$, $0\leq r<a_{n+1}$ となる r がだた一つ存在する。

$r>0$ の時, $a_{n+2}=r$

$r=0$ の時, a_{n+1} が求める最大公約数である。

証明

$GCD(a_n,a_{n+1})=GCD(a_{n+1},a_{n+2}) \Rightarrow GCD(a_1,a_2)=GCD(a_n,a_{n+1}) \Rightarrow r=0$ で $GCD(a_n,a_{n+1})=a_{n+1}$

§B 最小公倍数と最大公約数

整数 a,b に関して

[B1 最小公倍数の性質] $M(a,b)=M(LCM(a,b))$ （ a,b の公倍数は a,b の最小公倍数の倍数。）

[B2 最大公約数の性質] $D(a,b)=D(GCD(a,b))$ （ a,b の公約数は a,b の最大公約数の約数。）

[B3] $a\times b=LCM(a,b)\times GCD(a,b)$

[B4] $LCM(ca,cb)=|c|LCM(a,b)$, $GCD(ca,cb)=|c|GCD(a,b)$

[B1 の証明]

a,b の公倍数を m , a,b の最小公倍数を m_0 とする。

a,b は共に m,m_0 の公約数(b1)でもある。

割り算の性質より $m=Q\,m_0+r\,,0\le r<m_0$ (b2) となる整数 Q ,自然数 r がただ一組存在する。

(b1)とユークリッドの互除法より a,b は共に r の約数であり、 r は a,b の公倍数となる。

もし $r>0$ と仮定すると m_0 の最小性から $r\ge m_0$ となり(b2)に矛盾する。

よって $r=0$ であり $m=Q\,m_0$ $\Rightarrow$ $M(a,b)\subseteq M(m_0)$

これと、推移律から $M(m_0)\subseteq M(a,b)$ よって $M(a,b)=M(m_0)$

（証明終わり）

[B2 と B3 の証明]

a,b の最小公倍数を m_0 とする。

ab は a,b の公倍数であるから、最小公倍数の性質より ab は m_0 の倍数である。

よって、自然数 d_0 により $ab=d_0m_0$ (b3) $\Rightarrow$ $d_0=GCD(a,b)$ を示せば[B3]が成立する。

m_0 は a,b の公倍数だから、整数 k_a,k_b により、 $m_0=k_a a=k_b b$ (b4)

(b4)を(b3)に代入すると $ab=d_0k_a a=d_0k_b b$ $\Rightarrow$ $a=d_0k_b$, $b=d_0k_a$

$\Rightarrow$ d_0 は a,b の公約数である。

d が a,b の公約数とすると、整数 n_a,n_b により $a=n_a d$, $b=n_b d$ (b5)

$m=\dfrac{ab}{d}$ とおくと(b5)より $m=n_a b=a\,n_b$

$\Rightarrow$ m は a,b の公倍数である。

最小公倍数の性質から、整数 k により $m=k\,m_0$ $\Rightarrow$ $\dfrac{ab}{d}=k\dfrac{ab}{d_0}$ $\Rightarrow$ $d_0=k\,d$

d_0 は a,b の公約数であり、すべての正の公約数を約数にもつので、公約数の中で最大になる。

（証明終わり）

[B4 の証明]

$x\in M(ca,cb)$ $\Leftrightarrow$整数 i_1,i_2 により $x=i_1(ca)=i_2(cb)=c(i_1a)=c(i_2b)$ $\Leftrightarrow$ $x\in c\,M(a,b)$

$M(ca,cb)=c\,M(a,b)$ $\Rightarrow$両辺の正の最小値は一致するから $LCM(ca,cb)=|c|LCM(a,b)$

[B3]より $LCM(ca,cb)GCD(ca,cb)$ = $ca\times cb$ = $c^2LCM(a,b)GCD(a,b)$

= $|c|^2LCM(a,b)GCD(a,b)$ = $|c|LCM(ca,cb)GCD(a,b)$

$\Rightarrow$ $|c|GCD(a,b)=GCD(ca,cb)$

（証明終わり）

[最小公倍数および最大公約数の性質その2]
整数 $a_1, a_2, \cdots, a_n, \cdots$ に関して
[B5] 漸化式 $m_1 = a_1$, $m_{n+1} = LCM(m_n, a_{n+1})$ と定義する⇒[B5-1] $M(a_1, a_2, \cdots, a_n) = M(m_n)$
[B5-2] $m_n = LCM(a_1, a_2, \cdots, a_n)$ ($a_1, a_2, \cdots, a_n$ の公倍数は $a_1, a_2, \cdots, a_n$ の最小公倍数の倍数。)

[B6] 漸化式 $d_1 = a_1$, $d_{n+1} = GCD(d_n, a_{n+1})$ と定義する⇒[B6-1] $D(a_1, a_2, \cdots, a_n) = D(d_n)$
[B6-2] $d_n = GCD(a_1, a_2, \cdots, a_n)$ ($a_1, a_2, \cdots, a_n$ の公約数は $a_1, a_2, \cdots, a_n$ の最大公約数の約数。)

[B7] $LCM(ca_1, ca_2, \cdots, ca_n) = |c| LCM(a_1, a_2, \cdots, a_n)$
[B8] $GCD(ca_1, ca_2, \cdots, ca_n) = |c| GCD(a_1, a_2, \cdots, a_n)$

[B5の証明]
$n=2$ の時 $m_2 = LCM(m_1, a_2) = LCM(a_1, a_2)$ [B1]より $M(a_1, a_2) = M(m_2)$ [B5-1]が成立。
$n=k$ の時、[B5-1]が成立と仮定する。 $M(a_1, a_2, \cdots, a_k) = M(m_k)$
$M(a_1, a_2, \cdots, a_k, a_{k+1}) = M(a_1, a_2, \cdots, a_k) \cap M(a_{k+1}) = M(m_k) \cap M(a_{k+1}) = M(m_k, a_{k+1})$
$= M(LCM(m_k, a_{k+1})) = M(m_{k+1}) \Rightarrow n=k+1$ の時にも[B5-1]が成立

m_n は $a_1, a_2, \cdots, a_n$ の公倍数であり $a_1, a_2, \cdots, a_n$ の公倍数は m_n の倍数である。
したがって m_n は $a_1, a_2, \cdots, a_n$ の正の公倍数の中で最小であり、[B5-2]が成立。

[B6の証明]
$n=2$ の時、 $d_2 = GCD(d_1, a_2) = GCD(a_1, a_2)$ [B2]より $D(d_1, a_2) = D(d_2)$ [B6-1]が成立。
$n=k$ の時、[B6-1]が成立と仮定する。 $D(a_1, a_2, \cdots, a_k) = D(d_k)$
$D(a_1, a_2, \cdots, a_k, a_{k+1}) = D(a_1, a_2, \cdots, a_k) \cap D(a_{k+1}) = D(d_k) \cap D(a_{k+1}) = D(d_k, a_{k+1})$
$= D(GCD(d_k, a_{k+1})) = D(d_{k+1}) \Rightarrow n=k+1$ の時にも[B6-1]が成立

d_n は $a_1, a_2, \cdots, a_n$ の公約数であり $a_1, a_2, \cdots, a_n$ の公約数は d_n の約数である。
したがって d_n は $a_1, a_2, \cdots, a_n$ の正の公約数の中で最大であり、[B6-2]が成立

[B7の証明]
$x \in M(ca_1, ca_2, \cdots, ca_n)$
⇔整数 $i_1, i_2, \cdots, i_n$ により $x = i_1(ca_1) = i_2(ca_2) = \cdots = i_n(ca_n) = c(i_1 a_1) = c(i_2 a_2) = \cdots = c(i_n a_n)$
⇔ $x \in cM(a_1, a_2, \cdots, a_n)$
∴ $M(ca_1, ca_2, \cdots, ca_n) = cM(a_1, a_2, \cdots, a_n)$
⇒両辺の正の最小値は一致するから $LCM(ca_1, ca_2, \cdots, ca_n) = |c| M(a_1, a_2, \cdots, a_n)$

(証明終わり)

[B8の証明] $c>0$ の場合に数学的帰納法で証明する。
$n=2$ の時[B4]より[B8]は成立。
$n=k$ の時[B8]が成立と仮定する。漸化式より
$GCD(ca_1, ca_2, \cdots, ca_k, ca_{k+1}) = GCD(GCD(ca_1, ca_2, \cdots, ca_k), ca_{k+1})$
$= GCD(c\,GCD(a_1, a_2, \cdots, a_k), ca_{k+1}) = c\,GCD(GCD(a_1, a_2, \cdots, a_k), a_{k+1}) = c\,GCD(a_1, a_2, \cdots, a_k, a_{k+1})$
$n=k+1$ の時にも[B8]が成立する。
$c \leq 0$ の時、定義から $GCD(ca_1, ca_2, \cdots, ca_n) = GCD(|c|a_1, |c|a_2, \cdots, |c|a_n) = |c| GCD(a_1, a_2, \cdots, a_n)$

(証明終わり)

§C 演算による最小公倍数および最大公約数の計算

自然数 a,b,c について演算 $a\vee b=LCM(a,b)$, $a\wedge b=GCD(a,b)$ と定義する。

単位元 $a\vee 1=a$ [C1-1]

零元 $a\wedge 1=1$ [C2-1]

交換法則 $a\vee b=b\vee a$ [C1-2]

交換法則 $a\wedge b=b\wedge a$ (C2-2)

結合法則 $(a\vee b)\vee c=a\vee(b\vee c)$ [C1-3]

結合法則 $(a\wedge b)\wedge c=a\wedge(b\wedge c)$ (C2-3)

積との分配法則 $(a\,c)\vee(b\,c)=(a\vee b)c$ [C1-4]

積との分配法則 $(a\,c)\wedge(b\,c)=(a\wedge b)c$ [C2-4]

モジュラー律 $(a\vee b)\wedge a=a$, $(a\wedge b)\vee a=a$ [C3]

簡約律 $a\,b\vee a=a\,b$, $a\,b\wedge a=a$ [C4]

[C1-2 の証明] $a\vee b=LCM(a,b)=LCM(b,a)=b\vee a$

[C2-2 の証明] $a\wedge b=GCD(a,b)=GCD(b,a)=b\wedge a$

[C1-3 の証明] $M((a\vee b)\vee c)=M(a\vee b,c)=M(a\vee b)\cap M(c)=M(a,b)\cap M(c)=M(a,b,c)$

$=M(a)\cap M(b,c)=M(a)\cap M(b\vee c)=M(a,b\vee c)=M(a\vee(b\vee c))$

$\therefore\ M((a\vee b)\vee c)=M(a,b,c)=M(a\vee(b\vee c))$ より各集合の正の最小要素は一致する。

[C2-3 の証明] $D((a\wedge b)\wedge c)=D(a\wedge b,c)=D(a\wedge b)\cap D(c)=D(a,b)\cap D(c)=D(a,b,c)$

$=D(a)\cap D(b,c)=D(a)\cap D(b\vee c)=D(a,b\vee c)=D(a\vee(b\vee c))$

$\therefore\ D((a\vee b)\vee c)=D(a,b,c)=D(a\vee(b\vee c))$ より各集合の正の最小要素は一致する。

[C1-4 の証明] [B4]より $(a\,c)\vee(b\,c)=LCM(a\,c,b\,c)=LCM(a,b)c=(a\vee b)c$

[C2-4 の証明] [B4]より $(a\,c)\wedge(b\,c)=GCD(a\,c,b\,c)=GCD(a,b)c=(a\wedge b)c$

[C3 の証明]

$a\vee b=LCM(a,b)$ は a の倍数だから $a\vee b=k\,a$

$(a\vee b)\wedge a=(k\,a)\wedge a=(k\wedge 1)a=1\times a=a$

$a\wedge b=GCD(a,b)$ は a の約数だから $a=k(a\wedge b)$

$(a\wedge b)\vee a=(a\wedge b)\vee(k(a\wedge b))=(1\vee k)(a\wedge b)=k\times(a\wedge b)=a$

[C4 の証明] $a\,b\vee a=a(b\vee 1)=a\,b$, $a\,b\wedge a=a(b\wedge 1)=a\times 1=a$

証明終わり

§D 互いに素な整数

[定義] 自然数 a,b の最大公約数が 1 の時, a,b を**互いに素**という。

[互いに素な自然数の性質] 自然数 a,b について以下のように成立する。

[D1] a,b が互いに素であり、 a' が a の約数、 b' が b の約数ならば a',b' も互いに素である。

[D2] a,b が互いに素ならば a,b の最小公倍数は $a\,b$ である。

[D3] 自然数 a,b に対して、互いに素な自然数 a',b' が存在して

$a=a'\times GCD(a,b)$, $b=b'\times GCD(a,b)$, $LCM(a,b)=a'\times GCD(a,b)\times b'$

[D4] a,b は互いに素とする。 a が $b\,c$ の約数ならば a は c の約数である。

[D5] a,b が互いに素ならば任意の自然数 c について $GCD(a\,b,c)=GCD(a,c)GCD(b,c)$

[D6] a,b,c のどの 2 つも互いに素ならば $a\,b,c$ も互いに素である。

[D6 -系] $a_1,a_2,\cdots,a_n$ のどの 2 つも互いに素ならば $a_1,a_2,\cdots,a_n$ の最小公倍数は $a_1a_2\cdots a_n$

$GCD(a_1a_2\cdots a_n,b)=GCD(a_1,b)GCD(a_2,b)\cdots GCD(a_n,b)$

証明

[D1の証明] $d=GCD(a',b')$ とすると推移律より d は互いに素な a,b の公約数。よって $d=1$

[D2の証明] a,b は互いに素だから $GCD(a,b)=1 \Rightarrow ab=LCM(a,b)\times GCD(a,b)=LCM(a,b)$

[D3の証明] $d_0=GCD(a,b)$, $m_0=LCM(a,b)$ とおくと、 $a=a'd_0$, $b=b'd_0$

$d_0=GCD(a,b)=GCD(a'd_0,b'd_0)=GCD(a',b')d_0 \Rightarrow GCD(a',b')=1 \Rightarrow a',b'$ は互いに素。

[D2]より $m_0=LCM(a,b)=LCM(a'd_0,b'd_0)=LCM(a',b')d_0=a'b'd_0$

[D4の証明] a,b は互いに素だから[D2]より $LCM(a,b)=ab$

a が bc の約数⇒ bc は a,b の公倍数⇒整数 k により $bc=k\times LCM(a,b)=kab \Rightarrow c=ka$

[D5の証明] $c_a=GCD(a,c)$, $c_b=GCD(b,c)$ とおく。

(1) c が ab の約数の場合。自然数 k により $ab=kc$ (d1)

a,c について[D3]より、互いに素な a',c' が存在して $a=a'c_a$, $c=c'c_a$

$\Rightarrow \dfrac{a}{c}=\dfrac{a'}{c'} \Rightarrow a'=\dfrac{ac'}{c}$ ⇒(d1)より $a'b=\dfrac{abc'}{c}=\dfrac{kcc'}{c}=kc'$

$\Rightarrow c'$ は $a'b$ の約数である。 c',a' は互いに素だから、[D4]より c' は b の約数。

$\Rightarrow c'$ は b,c の公約数となる。最大公約数の性質より c' は c_b の約数。(d2)

a,b は互いに素であり、 c_a は a の約数、 c_b は b の約数⇒[D1]より c_a,c_b も互いに素。

これと c_b は $c=c'c_a$ の約数だから c_b は c' の約数。(d3)

(d2) (d3)より $c_b=c'$

(2) c が一般の自然数の場合。 $c'=GCD(ab,c)$ は ab の約数⇒ $c'=GCD(a,c')GCD(b,c')$

結合律と簡約律より $GCD(a,c') = a\wedge c' = a\wedge(ab\wedge c)=(a\wedge ab)\wedge c=a\wedge c = GCD(a,c)$

$GCD(b,c') = b\wedge c' = b\wedge(ab\wedge c) = (b\wedge ab)\wedge c=b\wedge c = GCD(b,c)$ よって[D5]が成立。

[D6の証明] $d=GCD(ab,c)$ とおくと[D1]より

a,c が互いに素⇒ a,d が互いに素

b,c が互いに素⇒ b,d が互いに素

[D5]より a,b が互いに素⇒ $d=GCD(a,d)\times GCD(b,d)=1\times 1=1$

[D6-系の証明] 漸化式 $m_1=a_1$, $m_{n+1}=LCM(m_n,a_{n+1})$ において

命題 P $m_n,a_{n+1},a_{n+2},\cdots$ のどの2つも互いに素を帰納法で示す。

$n=1$ の時 $m_1,a_2,a_3,\cdots=a_1,a_2,a_3,\cdots$ のどの2つも互いに素だから成立

$n=k$ の時、成立と仮定すると $m_k,a_{k+1},a_{k+2},\cdots$ のどの2つも互いに素

$\Rightarrow m_{k+1}=LCM(m_k,a_{k+1})=m_k a_{k+1}$ (d4) かつ [D5]より $m_k a_{k+1},a_{k+2},\cdots$ のどの2つも互いに素

$\Rightarrow n=k+1$ の時にも成立。

(d4) $m_{k+1}=m_k a_{k+1}$ より $m_k=m_{k-1}a_k=m_{k-2}a_{k-1}a_k=\cdots=m_1 a_2 a_3\cdots a_k = a_1 a_2 a_3\cdots a_k$ (d5)

$\therefore LCM(a_1,a_2,\cdots,a_n)=m_n=a_1 a_2\cdots a_n$

(d5)より、命題 P を $n\to k$ で書き換えると

命題 P $(a_1 a_2\cdots a_k),a_{k+1},a_{k+2},\cdots,a_n$ のどの2つも互いに素

[D5]より $GCD(a_1 a_2\cdots a_{n-1}a_n,b) = GCD(a_1 a_2\cdots a_{n-1},b)GCD(a_n,b)$

$= GCD(a_1 a_2\cdots a_{n-2},b)GCD(a_{n-1},b)GCD(a_n,b)$

$=\cdots= GCD(a_1 a_2,b)\cdots GCD(a_{n-1},b)GCD(a_n,b)$

$= GCD(a_1,b)GCD(a_2,b)\cdots GCD(a_{n-1},b)GCD(a_n,b)$

(証明終わり)

§E 素因数

[定義]

2 以上の自然数で、1 とそれ自身以外に約数を持たない自然数を**素数**という。

2 以上の自然数で、素数でない自然数を**合成数**という。

自然数 n の約数 p が素数である時、 p を n の**素因数**という。

[E1 合成数の性質] 合成数を n に対して $n=ab$, $1<a,b<n$ となるような自然数 a,b が存在する。

[E2 ユークリッドの補題]

自然数 a,b とする。素数 p が ab の約数ならば p は a の約数、または b の約数

[E3 素因数の性質 1] すべての自然数は素因数を持つ

[E4 素因数の性質2]

自然数 a,b に共通の素因数が存在するための必要十分条件は $GCD(a,b)>1$ である。

（対偶）自然数 a,b に共通の素因数が存在しないためのの必要十分条件は a,b が互いに素である。

[E1 の証明]

合成数 n は $a\neq 1$ かつ $a\neq n$ であるような約数 a を持つから、自然数 b により $n=ab$

$1\leq b \Rightarrow a\leq ab=n \Rightarrow a\neq n$ だから $a<n$

$1<a<n$ かつ $a=\frac{n}{b}$ だから $1<\frac{n}{b}<n \Rightarrow 1<b<n$

証明終わり

[E2 の証明]

p が a の約数でないとすれば p,a の公約数は 1 のみで互いに素[C4]より p は b の約数

[E3 の証明]

自然数 n の 1 以外の約数で 最小のものを p $(1<p\leq n)$ とする。

自然数 k により $n=pk$ (d1)

p が合成数と仮定すると $p=ab$, $1<a<p$, $1<b<p$ (d2)

(d2)を(d1)に代入すると、 $n=abk$, $1<a<p$

a は n の 1 以外の約数であり、かつ p より小さい。これは p の最小性に矛盾する。

従って p は素数であり、 n の素因数である。

[E4 の証明]

[十分性]

a,b の共通の素因数を p とすると a,b の公約数だから

最大公約数の性質より p は $GCD(a,b)$ の約数である。$\Rightarrow$ $gcd(a,b)\geq p>1$

[必要性]

素因数の性質1より $GCD(a,b)$ の素因数 p は a,b の共通の素因数である。

[E5 素因数分解の一意性定理] 自然数はただ一通りに素因数分解できる。

[素因数分解の可能性の証明]
自然数 m の素因数の集合を A とすると素因数の性質1より $A \neq \emptyset$
$A = \{p_1, p_2, \cdots, p_n\}$ とおく。

p_j^k が m の約数となるような自然数 k の中で最大のものを $k(j)$ とする。
この決め方により $p_j^{k(j)}$ は m の約数かつ $p_j^{k(j)+1}$ は m の約数ではない。(d1)
m は $p_1^{k(1)}, p_2^{k(2)}, \cdots, p_n^{k(n)}$ の公倍数である。

$p_1^{k(1)}, p_2^{k(2)}, \cdots, p_n^{k(n)}$ のどの2つも互いに素だから[D6-系]より
$p_1^{k(1)}, p_2^{k(2)}, \cdots, p_n^{k(n)}$ の最小公倍数は $a = p_1^{k(1)} p_2^{k(2)} \cdots p_n^{k(n)}$ である。
最小公倍数の性質より m は $a = p_1^{e(1)} p_2^{e(2)} \cdots p_n^{e(n)}$ の倍数である。

$m = k a$ とおける。
$k > 1$ と仮定すると、素因数の性質1より k は素因数 q を持つ。 $k = k' q$
$q \in A$ となるので、 $q = p_j$ となる j が存在し、 $k = k' p_j$ となるので
$m = k' p_j a = k' p_1^{k(1)} p_2^{k(2)} \cdots p_j^{k(j)+1} \cdots p_n^{k(n)} \Rightarrow p_j^{k(j)+1}$ は m の約数
これは(d1)に矛盾する。よって $k = 1$ であり、 $m = p_1^{k(1)} p_2^{k(2)} \cdots p_j^{k(j)+1} \cdots p_n^{k(n)}$

[素因数分解の一意性の証明]
どの２つも異なる素数 $q_1, q_2, \cdots, q_N$ によって $m = q_1^{c(1)} q_2^{c(2)} \cdots q_N^{c(N)}$ となるとき
$B = \{q_1, q_2, \cdots, q_N\}$ とおく。
すべての j について q_j は m の素因数だから $B \subseteq A$ (d2)
もし $p_i \notin B$ となる $p_i \in A$ があれば
素因数の性質2より p_i と $m = q_1^{c(1)} q_2^{c(2)} \cdots q_N^{c(N)}$ は共通の素因数がなく $GCD(p_i, m) = 1$
これは p_i が m の素因数であることに矛盾する。
したがって $p_i (i = 1, 2, \cdots, n) \in B \Rightarrow A \subseteq B$ (d3)
(d2), (d3)より $A = B$ ここで必要なら添え字を付け替えて $p_j = q_j (j = 1, 2, \cdots, , n)$ とできる。
$k(j) (j = 1, 2, \cdots, n)$ の最大性より $k(j) \geq c(j) (j = 1, 2, \cdots, n)$
もし $k(j) > c(j)$ となる j があると仮定すれば
$m = p_1^{k(1)} p_2^{k(2)} \cdots p_n^{k(n)} > p_1^{c(1)} p_2^{c(2)} \cdots p_n^{c(n)} = m$ となり矛盾⇒すべての j で $k(j) = c(j)$

[E6 約数の素因数分解]

自然数 a, b について、素因数分解 $a = p_1^{e(1)} p_2^{e(2)} \cdots p_n^{e(n)}$ の時、(１)は(２)の必要十分条件である。

(１) b が a の約数

(２) b の素因数分解は $b = p_1^{c(1)} p_2^{c(2)} \cdots p_n^{c(n)}$, $0 \le c(i) \le e(i)$, $i = 1, 2, \cdots, n$

[十分性の証明] b の素因数 q は a の素因数でもあるから、ある j があって $q = p_j$ と一致する。
したがって b の素因数分解は $b = p_1^{c(1)} p_2^{c(2)} \cdots p_n^{c(n)}$, $c(i) \ge 0$, $i = 1, 2, \cdots, n$ となる。

$d = \dfrac{a}{b}$ も a の約数であり、同様に $d = p_1^{d(1)} p_2^{d(2)} \cdots p_n^{d(n)}$, $d(i) \ge 0$, $i = 1, 2, \cdots, n$

$a = b\,d = p_1^{c(1)+d(1)} p_2^{c(2)+d(2)} \cdots p_n^{c(n)+d(n)}$

⇒素因数分解の一意性より $e(i) = c(i) + d(i) \ge c(i)$, $i = 1, 2, \cdots, n$

[必要性の証明] $0 \le c(i) \le e(i)$ より $d(i) = e(i) - c(i)$ とおくと $0 \le d(i) \le e(i)$, $i = 1, 2, \cdots, n$
$d = p_1^{d(1)} p_2^{d(2)} \cdots p_n^{d(n)}$ とおくと $b\,d = p_1^{c(1)+d(1)} p_2^{c(2)+d(2)} \cdots p_n^{c(n)+d(n)} = p_1^{e(1)} p_2^{e(2)} \cdots p_n^{e(n)} = a$

[E6-系 約数の個数]

n の素因数分解が $n = p_1^{e(1)} p_2^{e(2)} \cdots p_n^{e(n)}$ とする。

n の約数の個数は $(e(1)+1)(e(2)+1) \cdots (e(n)+1)$

n の約数の和は $\dfrac{p_1^{e(1)+1}-1}{p_1-1} \dfrac{p_2^{e(2)+1}-1}{p_2-1} \cdots \dfrac{p_n^{e(n)+1}-1}{p_n-1}$

証明

$$\sum_{k(1)=0}^{e(1)} \sum_{k(2)=0}^{e(2)} \cdots \sum_{k(n)=0}^{e(n)} p_1^{k(1)} p_2^{k(2)} \cdots p_n^{k(n)} = \sum_{k(1)=0}^{e(1)} p_1^{k(1)} \sum_{k(2)=0}^{e(2)} p_2^{k(2)} \cdots \sum_{k(n)=0}^{e(n)} p_n^{k(n)} = \frac{p_1^{e(1)+1}-1}{p_1-1} \frac{p_2^{e(2)+1}-1}{p_2-1} \cdots \frac{p_n^{e(n)+1}-1}{p_n-1}$$

[E7 最大公約数,最小公倍数の素因数分解]

$a \vee b$ の素因数分解を $a \vee b = p_1^{e(1)} p_2^{e(2)} \cdots p_n^{e(n)}$ とする。

a, b および $a \wedge b$ は $a \vee b$ の約数だから、約数の素因数分解より

$a = p_1^{a(1)} p_2^{a(2)} \cdots p_n^{a(n)}$, $0 \le a(i) \le e(i)$, $i = 1, 2, \cdots, n$

$b = p_1^{b(1)} p_2^{b(2)} \cdots p_n^{b(n)}$, $0 \le b(i) \le e(i)$, $i = 1, 2, \cdots, n$

$a \wedge b = p_1^{d(1)} p_2^{d(2)} \cdots p_n^{d(n)}$, $0 \le d(i) \le e(i)$, $i = 1, 2, \cdots, n$

この時 $e(i) = max(a(i), b(i))$, $d(i) = min(a(i), b(i))$, $i = 1, 2, \cdots, n$ が成立する。

証明

$c(i) = min(a(i), b(i))$, $(i = 1, 2, \cdots, n)$, $c = p_1^{c(1)} p_2^{c(2)} \cdots p_n^{c(n)}$ とおく。

[E6]より $a \wedge b$ は a, b の約数だから $0 \le d(i) \le a(i), b(i)$ ⇒ $d(i) \le min(a(i), b(i))$, $i = 1, 2, \cdots, n$

[E6]より c は a, b の公約数であるから $a \wedge b$ の約数⇒ $c(i) \le d(i)$, $i = 1, 2, \cdots, n$

∴ $d(i) = min(a(i), b(i))$, $i = 1, 2, \cdots, n$ (e1)

$a\,b = (a \wedge b)(a \vee b)$ に素因数分解を代入⇒ $p_1^{a(1)+b(1)} p_2^{a(2)+b(2)} \cdots p_n^{a(n)+b(n)} = p_1^{d(1)+e(1)} p_2^{d(2)+e(2)} \cdots p_n^{d(n)+e(n)}$

⇒素因数分解の一意性より $a(i) + b(i) = d(i) + e(i)$, $i = 1, 2, \cdots, n$ (e2)

一般に $a(i) + b(i) = max(a(i), b(i)) + min(a(i), b(i))$, $i = 1, 2, \cdots, n$ (e3)

(e1)(e2)(e3)より $d(i) + e(i) = max(a(i), b(i)) + d(i)$ ⇒ $e(i) = max(a(i), b(i))$

[E7-系]
分配法則　$(a\vee b)\wedge c=(a\wedge c)\vee(b\wedge c)$　,　$(a\wedge b)\vee c=(a\vee c)\wedge(b\vee c)$

証明
見やすくするため、演算子　$a\uparrow b = max(a,b)$　,　$a\downarrow b = min(a,b)$　を定義する。
$a\geq b$　の時　$a\uparrow b = a$　,　$a\downarrow b = b$
$-a\leq -b$　だから　$-a\uparrow -b = -b = -(a\downarrow b)$　,　$-a\downarrow -b = -a = -(a\uparrow b)$
$\therefore$　$-(a\downarrow b) = -a\uparrow -b$　,　$-(a\uparrow b) = -a\downarrow -b$　(e4)

a,b,c　の大小関係は6通りある。
$a\geq b\geq c$　の時　$(a\uparrow b)\downarrow c=a\downarrow c=c$　,　$(a\downarrow c)\uparrow(b\downarrow c)=c\uparrow c=c$
$a\geq c\geq b$　の時　$(a\uparrow b)\downarrow c=a\downarrow c=c$　,　$(a\downarrow c)\uparrow(b\downarrow c)=c\uparrow b=c$
$b\geq a\geq c$　の時　$(a\uparrow b)\downarrow c=b\downarrow c=c$　,　$(a\downarrow c)\uparrow(b\downarrow c)=c\uparrow c=c$
$b\geq c\geq a$　の時　$(a\uparrow b)\downarrow c=b\downarrow c=c$　,　$(a\downarrow c)\uparrow(b\downarrow c)=a\uparrow c=c$
$c\geq a\geq b$　の時　$(a\uparrow b)\downarrow c=a\downarrow c=a$　,　$(a\downarrow c)\uparrow(b\downarrow c)=a\uparrow b=a$
$c\geq b\geq a$　の時　$(a\uparrow b)\downarrow c=b\downarrow c=b$　,　$(a\downarrow c)\uparrow(b\downarrow c)=a\uparrow b=b$
いずれも　$(a\uparrow b)\downarrow c = (a\downarrow c)\uparrow(b\downarrow c)$　(e5)が成立する。

(e5)を　$-a,-b,-c$　に使うと　$(-a\uparrow -b)\downarrow -c = (-a\downarrow -c)\uparrow(-b\downarrow -c)$
$(-a\uparrow -b)\downarrow -c = -(a\downarrow b)\downarrow -c = -\{(a\downarrow b)\uparrow c\}$
$(-a\downarrow -b)\uparrow(-b\downarrow -c) = -(a\uparrow b)\uparrow -(b\uparrow c) = -\{(a\uparrow b)\downarrow(b\uparrow c)\}$
$\therefore$　$(a\downarrow b)\uparrow c = (a\uparrow b)\downarrow(b\uparrow c)$　(e6)

$a\vee b\vee c$　の素因数分解を　$a\vee b\vee c = p_1^{e(1)}p_2^{e(2)}\cdots p_n^{e(n)}$　とする。
a,b,c　は　$a\vee b\vee c$　の約数だから約数の素因数分解より
$a = p_1^{a(1)}p_2^{a(2)}\cdots p_n^{a(n)}$　,　$0\leq a(j)\leq e(j)$
$b = p_1^{b(1)}p_2^{b(2)}\cdots p_n^{b(n)}$　,　$0\leq b(j)\leq e(j)$
$c = p_1^{c(1)}p_2^{c(2)}\cdots p_n^{c(n)}$　,　$0\leq c(j)\leq e(j)$

素因数分解を　$(a\vee b)\wedge c=p_1^{s(1)}p_2^{s(2)}\cdots p_n^{s(n)}$　,　$(a\wedge c)\vee(b\wedge c)=p_1^{t(1)}p_2^{t(2)}\cdots p_n^{t(n)}$　とする。
[E7]より　$s(i)=(a(i)\uparrow b(i))\downarrow c(i)=(a(i)\downarrow c(i))\uparrow(b(i)\downarrow c(i))=t(i)$
$(a\vee b)\wedge c=(a\wedge c)\vee(b\wedge c)$

素因数分解を　$(a\wedge b)\vee c=p_1^{s(1)}p_2^{s(2)}\cdots p_n^{s(n)}$　,　$(a\vee c)\wedge(b\vee c)=p_1^{t(1)}p_2^{t(2)}\cdots p_n^{t(n)}$
[E7]より　$s(i)=(a(i)\downarrow b(i))\uparrow c(i)=(a(i)\uparrow c(i))\downarrow(b(i)\uparrow c(i))=t(i)$
$(a\wedge b)\vee c=(a\vee c)\wedge(b\vee c)$

(証明終わり)