$2\sigma(a)-3a=-1$ かつ $s(a)=3$ を満たす自然数 a の素因数分解について

山上 敦士　　鈴木 大輔
創価大学 理工学部 情報システム工学科
2020 年 2 月 13 日

命題 自然数 a は $2\sigma(a)-3a=-1$ かつ $s(a)=3$ を満たすとし, a の素因数分解を $a=p^iq^jr^k$ とする. ただし, $p<q<r$ は相異なる素数であり, i,j,k は自然数である. このとき, 次が成り立つ：

(1) $p=3$ または $p=5$ である.
　とくに, $p=5$ のとき, $q=7$ かつ $11\le r\le 31$ である.

(2) $p=3$ のとき,
　(i) $q\equiv r\equiv 2 \pmod 3$ ならば, $j\equiv k\equiv 0 \pmod 2$ である.
　(ii) $q\equiv r\equiv 1 \pmod 3$ ならば,

$$j\equiv k\equiv 0 \pmod 3 \quad \text{or} \quad j\equiv k\equiv 1 \pmod 3$$

である.
　(iii) $q\equiv 1 \pmod 3$, $r\equiv 2 \pmod 3$ ならば,

$$j\equiv 0 \pmod 3, \quad k\equiv 0 \pmod 2$$

である.
　(iv) $q\equiv 2 \pmod 3$, $r\equiv 1 \pmod 3$ ならば,

$$j\equiv 0 \pmod 2, \quad k\equiv 0 \pmod 3$$

である.

(3) $p=5$, $q=7$, $11\le r\le 31$ のとき,

$$i\equiv 0 \pmod 2, \quad j\equiv 0,1,4,6,9,10 \pmod{12}$$

であり,

$$r=11,31 \Rightarrow k\not\equiv 5 \pmod 6,$$
$$r=29 \Rightarrow k\not\equiv 3 \pmod 4,$$
$$r=13,17,19,23 \Rightarrow k\not\equiv 3,5,7,11 \pmod{12}$$

が成り立つ.

証明 (1)　$2\sigma(a)-3a=-1$ より, a は奇数であるので, $p\ge 3$ である. また, a の素因数分解を $a=p^iq^jr^k$ とおいていることから,

$$\begin{aligned}\sigma(a)&=\sigma(p^i)\sigma(q^j)\sigma(r^k)\\&=\frac{(p^{i+1}-1)(q^{j+1}-1)(r^{k+1}-1)}{(p-1)(q-1)(r-1)}\end{aligned}$$

であるので,

$$\frac{2(p^{i+1}-1)(q^{j+1}-1)(r^{k+1}-1)}{(p-1)(q-1)(r-1)}=3p^iq^jr^k-1$$

となる. よって,

$$\begin{aligned}&2(p^{i+1}-1)(q^{j+1}-1)(r^{k+1}-1)\\&\quad=3p^iq^jr^k(p-1)(q-1)(r-1)-(p-1)(q-1)(r-1)\end{aligned}$$

となり, この等式の左辺の式を展開すると,

$$2p^{i+1}q^{j+1}r^{k+1}+2(-p^{i+1}q^{j+1}-q^{j+1}r^{k+1}-r^{k+1}p^{i+1}+p^{i+1}+q^{j+1}+r^{k+1}-1)$$

となるので, 等式

$$\begin{aligned}2p^{i+1}q^{j+1}r^{k+1} &- 3p^iq^jr^k(p-1)(q-1)(r-1)\\ &= 2(p^{i+1}q^{j+1}+q^{j+1}r^{k+1}+r^{k+1}p^{i+1}-p^{i+1}-q^{j+1}-r^{k+1}+1)\\ &\quad -(p-1)(q-1)(r-1) \qquad \cdots(*)\end{aligned}$$

が得られる.

等式 $(*)$ の左辺の式を変形すると,

$$p^iq^jr^k(2pqr-3(p-1)(q-1)(r-1)) \qquad \cdots(**)$$

となり, 等式 $(*)$ の右辺の式を変形すると,

$$\begin{aligned}&2(p^{i+1}q^{j+1}+q^{j+1}r^{k+1}+r^{k+1}p^{i+1}-p^{i+1}-q^{j+1}-r^{k+1}+1)\\ &-(pqr-pq-qr-rp+p+q+r-1)\\ =\ &2(p^{i+1}q^{j+1}+q^{j+1}r^{k+1}+r^{k+1}p^{i+1}-p^{i+1}-q^{j+1}-r^{k+1}+1)\\ &-pqr+pq+qr+rp-p-q-r+1\\ =\ &r(2q^{j+1}r^k+2r^kp^{i+1}-2r^k-pq+p+q-1)\\ &+2p^{i+1}q^{j+1}-2p^{i+1}-2q^{j+1}+pq-p-q+2+1\\ =\ &r(p(2r^kp^i-q+1)+2r^k(q^{j+1}-1)+q-1)\\ &+2(p^{i+1}-1)(q^{j+1}-1)+(p-1)(q-1)\end{aligned}$$

となる. これは正の値であり, 式 $(**)$ において, $p^iq^jr^k>0$ であるので, 不等式

$$2pqr-3(p-1)(q-1)(r-1)>0$$

が得られる. この不等式の左辺の式を変形すると,

$$\begin{aligned}&2pqr-3(p-1)(q-1)(r-1)\\ =\ &2pqr-3pqr+3pq+3qr+3rp-3p-3q-3r+3\\ =\ &-pqr+3pq+3qr+3rp-3p-3q-3r+3\\ =\ &-p(qr-3q-3r+3)+3(qr-q-r+1)\\ =\ &-p((q-3)(r-3)-6)+3((q-3)(r-3)+2q+2r-8)\\ =\ &-p(q-3)(r-3)+6p+3(q-3)(r-3)+6q+6r-24\\ =\ &-(p-3)(q-3)(r-3)+6(p+q+r-4)\end{aligned}$$

となるので, 不等式

$$6(p+q+r-4)>(p-3)(q-3)(r-3) \qquad \cdots(***)$$

が得られる.

ここで, $p\geq 7$ と仮定し, 素数の組 (p,q,r) を $(p+s,q+t,r+u)$ $(s,t,u\geq 0)$ に取り替えたときの $(***)$ の左辺と右辺それぞれの増加量を比較してみる. ただし, s,t,u のうち少なくとも 1 つは 0 ではないとする. 左辺の増加量は,

$$6(p+s+q+t+r+u-4)-6(p+q+r-4)=6(s+t+u)$$

である. 一方で, 右辺の増加量は, $p\geq 7$, $q\geq 11$ であることに注意して,

$$\begin{aligned}&(p+s-3)(q+t-3)(r+u-3)-(p-3)(q-3)(r-3)\\ =\ &stu+st(r-3)+tu(p-3)+us(q-3)\\ &\quad +s(q-3)(r-3)+t(p-3)(r-3)+u(p-3)(q-3)\\ \geq\ &(s+t+u)(p-3)(q-3)\\ \geq\ &32(s+t+u)\end{aligned}$$

となる. よって, 左辺の増大量は右辺の増大量よりも真に小さい.

さらに, $p\geq 7$ の場合における最小の素因数の組 $(p,q,r)=(7,11,13)$ に対し, 不等式 $(***)$ の左辺の値

$$6(7+11+13-4)=162$$

は, 右辺の値

$$(7-3)(11-3)(13-3)=320$$

よりも小さい. よって, $p\geq 7$ と仮定すると, 不等式 $(***)$ は成立しないことが示された. したがって, $p=3$ または $p=5$ であることが示された.

とくに, $p=5$ のとき, 不等式 $(***)$ は,

$$6(q+r+1)>2(q-3)(r-3) \qquad \cdots (***)'$$

となり, $q\geq 11$ と仮定したときの最小の素数の組 $(q,r)=(11,13)$ に対し, 不等式 $(***)'$ の左辺の値

$$6(11+13+1)=150$$

は, 右辺の値

$$2(11-3)(13-3)=160$$

よりも小さいので, 先ほどと同様の議論により, 不等式 $(***)'$ は成立しないことがわかる. よって, $q=7$ であり, 不等式 $(***)$ より,

$$6(r+8)>8(r-3),$$

つまり,

$$r<36$$

となる. よって,

$$11\leq r\leq 31$$

であることが示された.

(2) $p=3$ のとき, 関係式

$$\frac{2(p^{i+1}-1)(q^{j+1}-1)(r^{k+1}-1)}{(p-1)(q-1)(r-1)}=3p^iq^jr^k-1$$

は,

$$\frac{(3^{i+1}-1)(q^{j+1}-1)(r^{k+1}-1)}{(q-1)(r-1)}=3^{i+1}q^jr^k-1$$

となる.

(i) $q\equiv r\equiv 2 \pmod 3$ のとき,

$$((-1)^{j+1}-1)((-1)^{k+1}-1)\equiv 1 \pmod 3$$

であるので,

$$j\equiv k\equiv 0 \pmod 2$$

となる.

(ii) $\dfrac{q^{j+1}-1}{q-1}=q^j+\cdots+q+1$, $\dfrac{r^{k+1}-1}{r-1}=r^k+\cdots+r+1$ であるので, $q\equiv r\equiv 2 \pmod 3$ のとき,

$$\overbrace{(1+\cdots+1)}^{j+1}\overbrace{(1+\cdots+1)}^{k+1}\equiv 1 \pmod 3,$$

つまり,

$$(j+1)(k+1)\equiv 1 \pmod 3$$

となる. よって,

$$j\equiv k\equiv 0 \pmod 3 \quad \text{or} \quad j\equiv k\equiv 1 \pmod 3$$

である.

(iii) $q\equiv 1 \pmod 3$, $r\equiv 2 \pmod 3$ のとき,

$$(j+1)((-1)^{k+1}-1)\equiv 1 \pmod 3$$

となる. よって,

$$j\equiv 0 \pmod 3, \quad k\equiv 0 \pmod 2$$

である.

(iv) $q \equiv 2 \pmod 3,\ r \equiv 1 \pmod 3$ のとき,

$$((-1)^{j+1} - 1)(k+1) \equiv 1 \pmod 3$$

となる. よって,

$$j \equiv 0 \pmod 2, \quad k \equiv 0 \pmod 3$$

である.

(3) $p = 5,\ q = 7$ のとき, 関係式

$$\frac{2(p^{i+1}-1)(q^{j+1}-1)(r^{k+1}-1)}{(p-1)(q-1)(r-1)} = 3p^i q^j r^k - 1$$

を変形して,

$$\frac{(5^{i+1}-1)(7^{j+1}-1)(r^{k+1}-1)}{6(r-1)} = 2(3 \cdot 5^i \cdot 7^j \cdot r^k - 1) \qquad \cdots (\sharp)$$

となる.

$7 \equiv 1 \pmod 3$ であるから, 等式 $(\sharp)$ の両辺を mod 3 でみることで,

$$((-1)^{i+1} - 1)(j+1)(r^k + \cdots + r + 1) \equiv 1 \pmod 3$$

となる. よって,

$$i \equiv 0 \pmod 2, \quad j \not\equiv 2 \pmod 3$$

である. また, 等式 $(\sharp)$ の両辺を mod 5 でみると,

$$(2^{j+1} - 1)(r^k + \cdots + r + 1) \equiv 2 \pmod 5$$

となり, mod 5 での既約剰余類群 $(\mathbb{Z}/5\mathbb{Z})^\times$ における $2 \pmod 5$ の位数は 4 であるから, $j + 1 \not\equiv 0 \pmod 4$, つまり,

$$j \not\equiv 3 \pmod 4$$

である. $j \not\equiv 2 \pmod 3$ であることと合わせると,

$$j \equiv 0, 1, 4, 6, 9, 10 \pmod{12}$$

となる. このとき,

$$r^{k+1} \equiv 2(2^{j+1} - 1)^{-1}(r-1) + 1 \pmod 5$$

となるので,

$$r \not\equiv 1 \pmod 5 \ \Rightarrow\ k \not\equiv 3 \pmod 4$$

が成り立つ. さらに, 等式 $(\sharp)$ の両辺を mod 7 でみると,

$$((-2)^{i+1} - 1)(r^k + \cdots + r + 1) \equiv -2 \pmod 7$$

となる. mod 7 での既約剰余類群 $(\mathbb{Z}/7\mathbb{Z})^\times$ における $-2 \pmod 7$ の位数は 6 であり, $i \equiv 0 \pmod 2$ であるから, $(-2)^{i+1} - 1 \not\equiv 0 \pmod 7$ となる. よって,

$$r^{k+1} \equiv 2((-2)^{i+1} - 1)^{-1}(r-1) + 1 \pmod 7$$

となり,

$$r \not\equiv 1 \pmod 7 \ \Rightarrow\ k \not\equiv 5 \pmod 6$$

が成り立つ. よって, $11 \le r \le 31$ であることに注意して,

$$r = 11, 31 \Rightarrow k \not\equiv 5 \pmod 6,$$

$$r = 29 \Rightarrow k \not\equiv 3 \pmod 4,$$

$$r = 13, 17, 19, 23 \Rightarrow k \not\equiv 3, 5, 7, 11 \pmod{12}$$

が成り立つ.

(証明終)