$\boxed{1}$ ［2000 JMO予選 問題８］

${}_{40}C_{20}$ を 41 で割った余りを求めよ。

解答 1

$$
\begin{aligned}
{}_{40}C_{20} &= \frac{40\cdot39\cdot38\cdot37\cdot36\cdot35\cdot34\cdot33\cdot32\cdot31\cdot30\cdot29\cdot28\cdot27\cdot26\cdot25\cdot24\cdot23\cdot22\cdot21}{20\cdot19\cdot18\cdot17\cdot16\cdot15\cdot14\cdot13\cdot12\cdot11\cdot10\cdot9\cdot8\cdot7\cdot6\cdot5\cdot4\cdot3\cdot2\cdot1} \\
&= 37\cdot31\cdot29\cdot23\cdot13\cdot11\cdot7\cdot5\cdot3^2\cdot2^2 \\
&= 137846528820 \\
&= 3362110459\times41+1
\end{aligned}
$$

よって，余りは１　……（答え）

解答 2

$$
\begin{aligned}
{}_{40}C_{20}\cdot20! &= 40\times39\times38\times\cdots\times21 \\
&= (41-1)\times(41-2)\times(41-3)\times\cdots\cdots\times(41-20)
\end{aligned}
$$

と変形できる。41 が素数であることに注意してこの式を展開すると，41 を素因数に含む項とそうでない項が現れるので，それらを次の形にまとめることができる。

$$ {}_{40}C_{20}\cdot20! = 41\times M + (-1)\times(-2)\times(-3)\times\cdots\cdots\times(-20) \quad (M \text{ は整数}) $$

整理して

$$ {}_{40}C_{20}\cdot20! = 41M + (-1)^{20}\times20! $$

$$ {}_{40}C_{20}\cdot20! = 41M + 20! $$

$$ ({}_{40}C_{20}-1)\times20! = 41M $$

41 と 20! は互いに素（１以外の公約数をもたない）であるから，$({}_{40}C_{20}-1)$ は 41 の倍数である。

ゆえに，

$$ {}_{40}C_{20}-1 = 41M' \quad (M' \text{ は整数}) $$

と表すことができる。すなわち

$$ {}_{40}C_{20} = 41M'+1 $$

よって，余りは１　……（答え）

解答 3

41 が素数であることを用いると

$$
\begin{aligned}
{}_{40}C_{20}\cdot20! &= 40\times39\times38\times\cdots\times21 \\
&\equiv (-1)\times(-2)\times(-3)\times\cdots\cdots\times(-20) \pmod{41} \\
&\equiv (-1)^{20}\times20! \pmod{41} \\
&\equiv 20! \pmod{41}
\end{aligned}
$$

よって，　$({}_{40}C_{20}-1)\cdot 20!\equiv 0 \pmod{41}$

41 と 20! は互いに素であるから，

$${}_{40}C_{20}-1\equiv 0 \pmod{41}$$

$${}_{40}C_{20}\equiv 1 \pmod{41}$$

よって，余りは１　……（答え）

参考　「合同式について」

整数 a，b，m に対して，$a-b$ が m で割り切れるとき a，b は m を法として合同であるといい，

$$a\equiv b \pmod{m}$$

と表す。このように記号「≡」で表された式を，合同式という。

たとえば，整数 40 と -1 について，$40-(-1)=41$ は 41 で割り切れるので，

$$40\equiv(-1) \pmod{41}$$

である。同様にして，

$$39\equiv(-2) \pmod{41},\ 38\equiv(-3) \pmod{41},\ 37\equiv(-4) \pmod{41},\ \cdots\cdots$$

などが成り立つ。

また，合同式について次のⅠ，Ⅱの性質が成り立つ。（a，b，c，d，k，m，n は整数）

Ⅰ　$a\equiv b \pmod{m}$，$c\equiv d \pmod{m}$　であるとき，

- $a+c\equiv b+d \pmod{m}$
- $a-c\equiv b-d \pmod{m}$
- $ac\equiv bd \pmod{m}$
- $a^n\equiv b^n \pmod{m}$

Ⅱ　$ka\equiv kb \pmod{m}$ で，k と m が互いに素であるとき，$a\equiv b \pmod{m}$

ここでは証明を行わないが，各自で確かめてほしい。

2　自然数 n のすべての正の約数の和は 60 であるという。
このような 自然数 n をすべて求めなさい。

解答

自然数 n が $n=a^p\times b^q\times c^r\times\cdots$ の形に素因数分解できるとき，n の正の約数の和は，

$(1+a^1+a^2+\cdots+a^p)(1+b^1+b^2+\cdots+b^q)(1+c^1+c^2+\cdots+c^r)\cdot\cdots$

となる。すなわち，正の約数の和は必ず

$1+p+p^2+\cdots+p^n$（p は素数）… ①

の形の数の積となるので，60 が①の形の数のみの積として表される場合を調べればよい。

60 の正の約数は 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60 であるから，この中で①の形をしているものを調べると，

3（$=1+2$），4（$=1+3$），6（$=1+5$），12（$=1+11$），15（$=1+2^1+2^2+2^3$），
20（$=1+19$）30（$=1+29$），60（$=1+59$）

に限られる。これらの数のうちどれを用いるかによって場合分けをする。

(i) 3 を用いるとき

(a) $60=3\times20=(1+2)\times(1+19)$　とすれば適する。このとき，$n=2\times19=38$

(b) $60=3\times4\times5=(1+2)(1+3)\times5$　とすると，①の形でないので適さない。

(ii) 4 を用いるとき

$60=4\times15=(1+3)(1+2+2^2+2^3)$　とすれば適する。このとき，$n=3\times2^3=24$

(iii) 6 を用いるとき

$60=6\times10=(1+5)\times2\times5$　となり，①の形でないの適さない。

(iv) 12 を用いるとき

$60=12\times5=(1+11)\times5$ となり，①の形でないので適さない。

(v) 15 を用いるとき

$60=15\times4=(1+2^1+2^2+2^3)(1+3)$　とすれば適する。これは(ii)の結果に等しい。

(vi) 20 を用いるとき

$60=20\times3=(1+19)\times(1+2)$　とすれば適する。これは(i)(a)の結果に等しい。

(vii) 30 を用いるとき

$60=30\times2=(1+29)\times2$となり，①の形でないので適さない。

(viii) 60 を用いるとき

$60=60\times1=(1+59)\times1$　とすれば適する。このとき，$n=59\times1=59$

以上より，求める自然数 n は　24, 38, 59 の 3個である。　……（答え）

※実際に確かめると，

24の正の約数の和 … $1+2+3+4+6+8+12+24=60$

38の正の約数の和 … $1+2+19+38=60$

59の正の約数の和… $1+59=60$　　となり，すべて適する。

$\boxed{3}$ (1) $a^2+b^2=1999$ となる整数 a，b の組が存在しないことを示せ。

(2) $a^3+b^3=1999$となる整数 a，b の組が存在しないことを示せ。

(1)

[証明] 1

$a^2=(-a)^2$ なので a，b は正の数と考えてよい。さらに $a \geqq b$ としても一般性は失われない。

$45^2=2025>1999$　，$31^2=961<\dfrac{1999}{2}$

であるから，$32 \leqq a \leqq 44$

与えられた式から $b=\sqrt{1999-a^2}$　.....　①

①に $a=32$ を代入すると $b=\sqrt{975}=\sqrt{3\times5^2\times13}$ となり，これは整数ではない。

①に $a=33$ を代入すると $b=\sqrt{910}=\sqrt{2\times5\times7\times13}$ となり，これは整数ではない。

①に $a=34$ を代入すると $b=\sqrt{843}=\sqrt{3\times281}$ となり，これは整数ではない。

（紙面の関係で途中を省略します。）

①に $a=44$ を代入すると $b=\sqrt{63}=\sqrt{3^2\times7}$ となり，これは整数ではない。

いずれの場合も b は整数とはならないので，条件を満たす整数 a，b の組は存在しない。[終]

[証明] 2

整数 n は $n=2k$，$n=2k+1$（kは整数）のいずれかの形で表すことができる。

$n=2k$ のとき，　$n^2=(2k)^2=4k^2$　となるので，

n^2 を 4 で割った余りは 0

$n=2k+1$ のとき，$n^2=(2k+1)^2=4k^2+4k+1=4(k^2+k)+1$　となるので，

n^2 を 4 で割った余りは 1

したがって，整数の 2 乗を 4 で割った余りは 0，1 のいずれかになる。

与えられた等式の左辺は，整数の 2 乗の和の形であるから，4 で割った余りは 0，1，2 のいずれかである。

与えられた等式の右辺を 4 で割ると余りは 3 になる。

ゆえに，条件を満たす整数 a，b の組は存在しない。[終]

(2)

[証明] 1

$a^3+b^3=(a+b)(a^2-ab+b^2)$ と因数分解する。

$a^2-ab+b^2=\left(a-\dfrac{b}{2}\right)^2+\dfrac{3}{4}b^2 \geqq 0$ であり，等号成立は $a=b=0$ のときに限るが，$a=b=0$ は与えられた等式を満たさないので，$a^2-ab+b^2>0$ としてよい。したがって，1999 が素数であることに注意すると，次の (i)，(ii) のいずれかが成り立つ。

（ｉ）$a+b=1$，$a^2-ab+b^2=1999$

（ii）$a+b=1999$，$a^2-ab+b^2=1$

（ｉ）の場合，両式から b を消去して整理すると　$3a^2-3a-1998=0$　……　①

この判別式を D_1 とすると $D_1=(-3)^2-4\times3\times(-1998)=23985=3^2\times5\times13\times41$ となり，これは平方数ではないので①は整数の解をもたない。すなわち，a は整数ではない。

（ii）の場合，両式から b を消去して整理すると　$3a^2-5997a+3996000=0$　……　①

この判別式を D_2 とすると $D_2=(-5997)^2-4\times3\times(3996000)=-11987991$　となり，これは負の数であるから①は整数の解をもたない。すなわち，a は整数ではない。

以上より，条件を満たす整数 a，b の組は存在しない。㊫

証明 2

整数 n を７で割った余り r を，$n=7k+r$（kは整数，$r=-3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3$）を満たす値と定義する。このとき，整数 n は $n=7k$，$n=7k\pm1$，$n=7k\pm2$，$n=7k\pm3$ のいずれかの形で表すことができる。以下，複号同順とする。

$n=7k$ のとき，　$n^3=(7k)^3=7(49k^3)$　となるので，n^3 を７で割った余りは０

$n=7k\pm1$ のとき，$n^3=(7k\pm1)^3$

$=(7k)^3\mp3(7k)^2\cdot1\pm3(7k)\cdot1^2\mp1^3$

$=(7k)^3\mp3(7k)^2\cdot1\pm3(7k)\cdot1^2\mp1$

となるが，最初の３項は７で割り切れるので，

n^3 を７で割った余りは１または-1である。

$n=7k\pm2$ のとき，$n^3=(7k\pm2)^3$

$=(7k)^3\mp3(7k)^2\cdot2\pm3(7k)\cdot2\mp2^3$

$=(7k)^3\mp3(7k)^2\cdot2\pm3(7k)\cdot2\mp7\mp1$

となるが，最初の４項は７で割り切れるので，

n^3 を７で割った余りは１または-1である。

$n=7k\pm3$ のとき，$n^3=(7k\pm3)^3$

$=(7k)^3\mp3(7k)^2\cdot3\pm3(7k)\cdot3\mp3^3$

$=(7k)^3\mp3(7k)^2\cdot2\pm3(7k)\cdot2\mp28\pm1$

となるが，最初の４項は７で割り切れるので，

n^3 を７で割った余りは１または-1である。

したがって，整数の３乗を７で割った余りは０，１，-1　のいずれかになる。

与えられた等式の左辺は，整数の３乗の和の形であるから，７で割った余りは０，１，-1，２，-2 のいずれかである。

与えられた等式の右辺を７で割ると余りは -3 になる。

ゆえに，条件を満たす整数 a，b の組は存在しない。㊫

【参考】整数で割った余りを使うテクニック

本問の$\boxed{\text{証明}}$２において，整数をある数で割った余りを用いる解法を示した。この手法はとても強力ではあるが、割る数の決め方が難しい。そこで、割る数の決め方のテクニックを紹介する。併せて，その理論的背景の概要を述べる。

> ※テクニック
> 割る整数は，主に奇素数（３以上の素数）または２のベキ乗（2^n の形の数）である。

(1)　奇素数 p で割ると効果的な場合

このとき，p で割った余りを考える利点は，フェルマーの小定理

「a が p で割りきれないとき，$a^{p-1}\equiv 1 \pmod p$ が成り立つ」

を使うことができる点にある。

特に，「$a^n+\cdots$」という問題において，$p=n+1$ が素数である場合には，

$a^n\equiv 0,\ 1\ (\bmod\ p=n+1)$

となるので，これを用いて問題を解くことができる場合がある。

また，フェルマーの小定理から次のことが導かれる。（証明が必要であるが，ここでは触れない）

「p を奇素数とし $n=\dfrac{p-1}{2}$ とする。a が p で割り切れないとき，$a^n\equiv\pm1 \pmod p$」

特に，「$a^n+\cdots$」という問題において，$p=2n+1$ が素数である場合には，

$a^n\equiv 0,\ 1,\ -1\ (\bmod\ p=2n+1)$

となるので，これを用いて問題を解くことができる場合がある。

例えば、「$a^3+\cdots$」なら７で割る，「$a^5+\cdots$」なら11で割る，といった感じである。

(2)　２のベキ乗で割ると効果的な場合

「$a^n+\cdots$」という問題において，n が２のベキ乗である（$n=2^r$ の形）場合，２のベキ乗で割るという手法が効果的である。これは，次の事実が理由である。

「$n=2^r$ とする。a が奇数のとき，$a^n\equiv 1\ (\bmod\ 4n=2^{r+2})$ が成り立つ。」

（この事実は大学２回生で習う、難しい事実である。）

特に、$r\geqq 2$ のとき，$2^n\equiv 0 \pmod{4n}$ であるから，$a^n\equiv 0,\ 1\ (\bmod\ 4n=2^{r+2})$

となるので，これを用いて問題を解くことができる場合がある。

［例題］ $a^4+b^4+c^4+d^4+e^4=2013$ を満たす整数 $a,\ b,\ c,\ d,\ e$ の組が存在しないことを示せ。

［解説］ ４乗なので５で割ればよいと考えられるが，変数が５個あるのでこの手法では解けない。実は，16で割ることにより，左辺は余りが0，1，2，3，4，5のいずれかであることがわかり，右辺は余りが13であるから，非存在性が言える。

4 [2001 JMO本選 問題 2]

10進法表記で，自然数 n が $a_m a_{m-1} \cdots a_1$ と表されていたとする。つまり，0 以上 9 以下の整数 a_m，a_{m-1}，…，a_1（ただし $a_m \neq 0$）を用いて，

$$n = 10^{m-1}a_m + 10^{m-2}a_{m-1} + \cdots\cdots\cdots + 10a_2 + a_1$$

と表される。このとき，

$$n = (a_m+1)(a_{m-1}+1)\cdots\cdots\cdots(a_2+1)(a_1+1)$$

を満たす n をすべて求めよ。

解答

$m=1$ のときは明らかに条件を満たさないので，$m \geqq 2$ である。

$m=2$ のとき，

$$n = 10a_2 + a_1 = (a_2+1)(a_1+1)，ゆえに，a_2\{10-(a_1+1)\} = 1$$

よって，$a_2=1$ かつ $10-(a_1+1)=1$ より，$a_1=8$, $a_2=1$，ゆえに　$n=18$

一般の m ($\geqq 2$) について，$m=2$ のときと同様に考える。

$$n = 10^{m-1}a_m + 10^{m-2}a_{m-1} + \cdots + a_1 = (a_m+1)(a_{m-1}+1)\cdot\cdots\cdot(a_1+1)$$

より

$$10^{m-1}a_m + 10^{m-2}a_{m-1} + \cdots + a_1 = (a_m+1)(a_{m-1}+1)\cdot\cdots\cdot(a_1+1) \quad \cdots\cdots ①$$

①の右辺について，

$$\begin{aligned}
(①の右辺) &= a_m(a_{m-1}+1)\cdot\cdots\cdot(a_2+1)(a_1+1) + (a_{m-1}+1)\cdot\cdots\cdot(a_2+1)(a_1+1) \\
&= a_m(a_{m-1}+1)\cdot\cdots\cdot(a_2+1)(a_1+1) + a_{m-1}(a_{m-2}+1)\cdot\cdots\cdot(a_2+1)(a_1+1) \\
&\qquad + (a_{m-2}+1)\cdot\cdots\cdot(a_2+1)(a_1+1) \\
&= \cdots\cdots\cdots \\
&= a_m(a_{m-1}+1)\cdots\cdots(a_2+1)(a_1+1) + a_{m-1}(a_{m-2}+1)\cdot\cdots\cdot(a_2+1)(a_1+1) \\
&\qquad + a_{m-2}(a_{m-3}+1)\cdots\cdots(a_2+1)(a_1+1) \\
&\qquad + \cdots\cdots\cdots \\
&\qquad + a_2(a_1+1) + (a_1+1)
\end{aligned}$$

と変形できるので，①は，

$$\begin{aligned}
&a_m\{10^{m-1} - (a_{m-1}+1)\cdots\cdots(a_2+1)(a_1+1)\} + a_{m-1}\{10^{m-2} - (a_{m-2}+1)\cdots\cdots(a_2+1)(a_1+1)\} \\
&\qquad + \cdots\cdots\cdots \\
&\qquad + a_2\{10-(a_1+1)\} = 1 \quad \cdots\cdots ②
\end{aligned}$$

と変形できる。

ここで，自然数 k について，$0 \leqq a_k \leqq 9$ であるから，$1 \leqq a_k+1 \leqq 10$ となり，

$$10^k - (a_k+1)\cdots\cdots(a_2+1)(a_1+1) \geqq 0$$

が成り立つ。そして，等号は $a_1=a_2=\cdots\cdots=a_k=9$ のときに成り立つ。しかしこのとき，②の左辺は 0 となり，条件を満たさない。

よって，

$a_i \neq 9\ (1 \leqq i \leqq m)$

となる自然数 i が少なくとも１つ存在することになる。

このことと，$a_m \neq 0$ より，

$a_m\{10^{m-1}-(a_{m-1}+1)\cdot\cdots\cdot(a_2+1)(a_1+1)\}>0$

つまり，

②の左辺の第１項は自然数　……③

である。

また，②の左辺の残りの項はすべて０以上の整数となるが，これらのうち１つでも自然数となってしまうと，③の条件より，②の等式は成立しない。

したがって，残りの項はすべて０であり，

$a_m\{10^{m-1}-(a_{m-1}+1)\cdot\cdots\cdot(a_2+1)(a_1+1)\}=1$

でなければならない。よって，

$$\begin{cases} a_m=1 \\ 10^{m-1}-(a_{m-1}+1)\cdot\cdots\cdot(a_2+1)(a_1+1)=1 \end{cases}$$

となるが，これを満たすのは $m=2$, $a_1=8$ に限る。

このとき，$a_2=1$ であるから $n=18$ である。

以上から，$n=18$　……（答え）

5 ［2004 JMO予選 問題5］

2004個の正の整数 $a_1, a_2, \ldots\ldots, a_{2004}$ が，次の条件を満たしているとする。

- $a_1 < a_2 < \cdots\cdots\cdots < a_{2004}$
- 2004以下の互いに異なる正の整数 $i,\ j,\ k$ について，常に $a_i \times a_j \neq a_k$ が成立する.

a_{2004} としてありうる値のうち，最小のものを求めよ。

解答

まず,

$$(a_1, a_2, a_3, \ldots\ldots, a_{2004}) = (1, 45, 46, \ldots\ldots, 2047)$$

は条件を満たす。なぜなら，$a_1 \times a_j = a_j\,(2 \leqq j \leqq 2004)$ であり，また,

$$a_2 \times a_3 = 45 \times 46 = 2070\ (>2047)$$

であるから，a_1 以外の 異なる正の整数 $a_i,\ a_j$ のどれを掛けても2047より大きくなるため，上記の2004個の正の整数は2つ目の条件を満たす。

では次に，この $a_{2004} = 2047$ が条件を満たす最小の値であることを示す。

題意を満たす $a_1, a_2, \ldots\ldots, a_{2004}$ であって，$a_{2004} \leqq 2046$ となるものが存在すると仮定すると，1つ目の条件より，$a_1, a_2, \ldots\ldots, a_{2004}$ はすべて2046以下である。

また，2つ目の条件より，2046以下の3つの正の整数

$$44,\ 45,\ 44 \times 45\ (=1980 < 2046)$$

のうち，$a_1, a_2, \ldots\ldots, a_{2004}$ の中に現れないものが少なくとも1つは存在する。

同様に,

$$43,\ 46,\ 43 \times 46\ (=1978 < 2046)$$
$$42,\ 47,\ 42 \times 47\ (=1974 < 2046)$$
$$\vdots$$
$$2,\ 87,\ 2 \times 87\ (=174 < 2046)$$

のそれぞれについても言える。これら 3×43 個の正の整数はすべて相異なるので，これらの相異なる（2046以下の）正の整数のうち，$a_1, a_2, \ldots\ldots, a_{2004}$ に現れないものが少なくとも43個あることになる。

しかし，$2046-43=2003$ となるため，2046以下の正の整数で2004個の正の整数 $a_1, a_2, \ldots\ldots, a_{2004}$ を表現できないため，矛盾が生じる。

したがって，題意を満たす $a_1, a_2, \ldots\ldots, a_{2004}$ であって，$a_{2004} \leqq 2046$ となるものが存在しない。

以上より，a_{2004} としてありうる値のうち，最小のものは，$a_{2004} = 2047$ ……（答え）

別解

まず,

$$(a_1, a_2, a_3, \ldots\ldots, a_{2004})=(1, 2, 3, \ldots\ldots, 2004)$$

として考える。明らかに $a_2 \times a_3=6\ (=a_6)$ となり，条件を満たさない。

そこで，$a_1=1$ を固定し，a_2 から a_{2004} までの値を n ずつ増やして考えたとき,

$$(a_2+n)(a_3+n) \geqq 2004+n \quad \cdots\cdots \quad ①$$

を満たす自然数 n のうち最小のものを求めればよい。

なぜなら,

$$(a_2+n)(a_3+n)<2004+n$$

を満たすとき，数列 a_2+n，a_3+n，a_4+n，……，$a_{2004}+n$ の中に $(a_2+n)(a_3+n)$ と等しい数が存在するからである。

①より,

$$n^2+4n-1998<0$$

$n>0$ より，$0<n<-2+\sqrt{2002}$

$44<\sqrt{2002}<45$ であるから，$0<n<43$

したがって，①を満たす最小の自然数は $n=43$

ゆえに，a_{2004} としてありうる値のうち，最小のものは，$2004+43=2047$　……（答え）

[6] 自然数 n に対して，n の正の約数の和を $f(n)$ で表す。n を奇数とするとき，$f(n)$ が奇数となることと，n が平方数になることは同値であることを示せ。

[証明] 1

$n=p_1^{e_1}\cdot p_2^{e_2}\cdot\cdots\cdot p_k^{e_k}$ ($p_1, p_2, \cdots, p_k$ は素数，$e_1, e_2, \cdots, e_k$ は自然数) を n の素因数分解とすると，

$$f(n)=\prod_{i=1}^{k}\left(1+p_i+p_i^2+\cdots+p_i^{e_i}\right)$$

である。n が奇数なら，上記の積に現れる各素数 p_i は 2 ではないから

$1+p_i+p_i^2+\cdots+p_i^{e_i}$ が奇数 $\Leftrightarrow$ e_i が偶数

よって，n が奇数のとき

$f(n)$ が奇数 $\Leftrightarrow$ n が平方数 [終]

[参考]

記号 Π は，i に 1 から k までの自然数を順に代入して得られる値の積を表す。

$$\prod_{i=1}^{k} x_i = x_1\times x_2\times x_3\times\cdots\cdots\times x_k$$

[証明] 2

n の約数を $d_1<d_2<\cdots<d_r$ ($d_1=1$, $d_r=n$) とすると，n が奇数なので $d_1, d_2, \cdots, d_r$ はすべて奇数となる.。したがって，$f(n)$ が奇数であることと r が奇数であることは同値である.。

また，$\dfrac{n}{d_r}$, $\dfrac{n}{d_{r-1}}$, $\dfrac{n}{d_{r-2}}$, $\cdots$, $\dfrac{n}{d_1}$ も n の約数になるが，大小関係から

$$\frac{n}{d_r}=d_1\ ,\ \frac{n}{d_{r-1}}=d_2\ ,\ \cdots\cdots$$

であり，一般に $n=d_i d_{r+1-i}$ $(1\leqq i\leqq r)$ が成立する。しかもこれは n を 2 つの自然数の積に表す方法を尽くしている。r が偶数のとき，これは互いに異なる自然数の積にしかならないが，r が奇数のときは，$n=\left(d_{\frac{r+1}{2}}\right)^2$ という積表示が存在する。したがって，r が奇数のときかつそのときに限って n は平方数になる。[終]