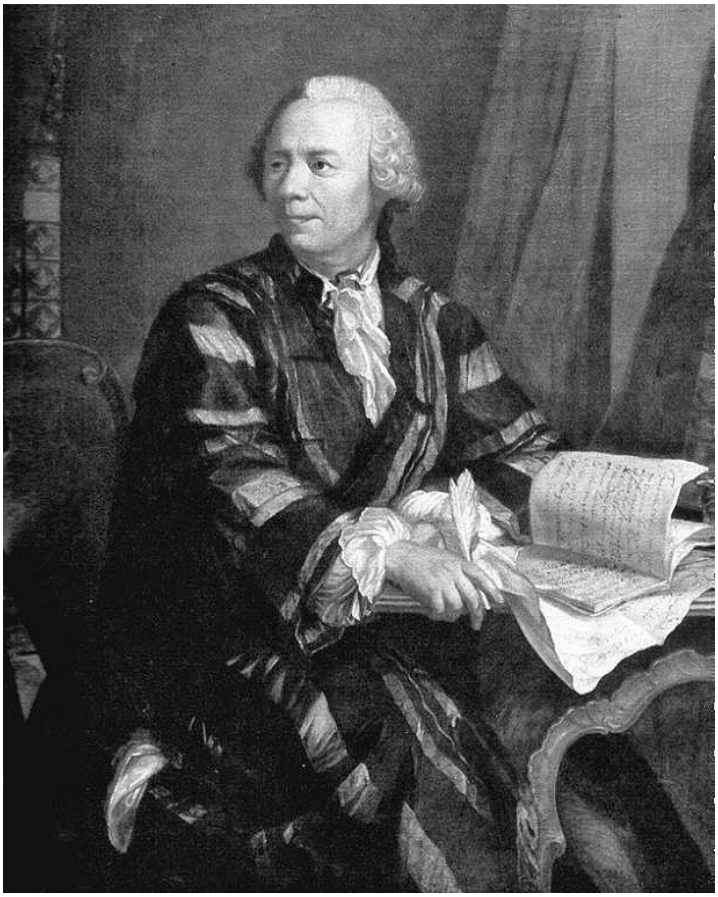
初等整数論の初歩



レオンハルト・オイラー（Leonhard Euler, 1707 年～178

以下では，断らない限り，文字は整数を表すものとする。

約数と倍数の定義

整数$a, b\,(a \neq 0)$に対して，$b=ac$ となる整数cが存在するとき，「aはbを割り切る」または「bはaで割り切れる」という。このとき，aをbの**約数**，bをaの**倍数**という。

2 つ以上の整数に共通な約数を，それらの約数の**公約数**といい，公約数のうちで最大のものを**最大公約数**という。また，2 つ以上の整数に共通な倍数を，それらの整数の**公倍数**といい，公倍数のうち正で最小なものを**最小公倍数**という。

特に，2 つの整数a, bの最大公約数を(a, b)で表すことにする。

$(a, b)=1$であるとき，aとbは**互いに素**であるという。

註　任意の整数(0 以外)は 0 の約数である。また，0 は任意の整数(0 以外)の倍数である。

例　任意の整数nに対して，nと$n+1$は互いに素であることを証明してみよう。

nと$n+1$の最大公約数をgとすると，自然数a, bを用いて

$$n=ga,\quad n+1=gb\quad (a<b)$$

と表される。これらよりnを消去すると

$$ga+1=gb\quad \text{すなわち}\quad g(b-a)=1$$

$g, b-a$はともに自然数であるから$g=1$

よって，nと$n+1$の最大公約数は 1 であるから，nと$n+1$は互いに素である。

定理 1　$a_1, a_2, \cdots\cdots, a_n$が$b$の倍数ならば，$a_1x_1+a_2x_2+\cdots\cdots+a_nx_n$は$b$の倍数である。

（bは，$a_1x_1+a_2x_2+\cdots\cdots+a_nx_n$の約数である）

証明

仮定により，

$$a_1=bk_1, a_2=bk_2, \cdots\cdots, a_n=bk_n$$

と置けるから

$$a_1x_1+a_2x_2+\cdots\cdots+a_nx_n=b(k_1x_1+k_2x_2+\cdots\cdots+k_nx_n)$$

右辺はbの倍数であるから，左辺もbの倍数である。

□

定理 2 （除法の定理）

整数aと正の整数bに対して

$$a=bq+r,\quad 0\leqq r<b$$

を満たす整数q, rがただ一通りに定まる。

証明

b の倍数の中で，a 以下で最大のものを qb （q は整数）とすると

$$qb \leqq a \quad \text{かつ} \quad a < (q+1)b$$

となるから

$$0 \leqq a - qb < b$$

よって，$a - qb = r$ とおけば，

$$a = bq + r, \quad 0 \leqq r < b$$

次に，一意性を示す。

$$a = bq_1 + r_1, \quad a = bq_2 + r_2, \quad 0 \leqq r_1 < b, \quad 0 \leqq r_2 < b$$

と 2 通りに表せたとすると

$$a = bq_1 + r_1 = bq_2 + r_2$$

であるから

$$b(q_1 - q_2) = r_2 - r_1 \quad \cdots① \quad \text{かつ} \quad -b < r_2 - r_1 < b$$

したがって

$$-b < b(q_1 - q_2) < b \quad \text{よって} \quad -1 < q_1 - q_2 < 1$$

となるから，

$$q_1 - q_2 = 0 \quad \text{すなわち} \quad q_1 = q_2$$

また，①より　$r_1 = r_2$

□

定理 2 において，q を，a を b で割ったときの**商**，r を**余り(剰余)**という。

ユークリッド(Euclid)の互除法

与えられた 2 つの正の整数の最大公約数を求めるアルゴリズムを示す。

命題　ユークリッドの互除法の原理

a, b, q を整数とするとき，$(a,b) = (a - qb, b)$

証明

m を a, b の公約数とすれば，m は $a - qb$ の約数であるから(定理 1)，m は $a - qb, b$ の公約数である。

逆に，m を $a - qb, b$ の公約数とすれば，m は $a = (a - qb) + qb$ の約数であるから(定理 1)，m は a, b の公約数である。

したがって，a, b の公約数の集合と $a - qb, b$ の公約数の集合は一致するから，その最大値も一致する。

ゆえに　$(a,b) = (a - qb, b)$

□

特に，a, b が正の整数のとき，a を b で割った剰余を c とすれば，$(a, b) = (b, c)$ である。

また，b を c で割った剰余を d とすれば，$(b, c) = (c, d)$ である。

これを繰り返していけば，$a > b > c > d \cdots\cdots \geqq 0$ であるから，剰余は 0 になる。

いま c が d で割り切れるとすれば，$(c, d) = (d, 0) = d$ すなわち $d = (a, b)$ である。

このようにして最大公約数を求めるアルゴリズムを，**ユークリッドの互除法**という。

□

例　289 と 197 の最大公約数を求める。

289＝197･1＋92　より　$(289, 197) = (197, 92)$

197＝92･2＋13　より　$(197, 92) = (92, 13)$

92＝13･7＋1　より　$(92, 13) = (13, 1)$

13＝1･13＋0　より　$(13, 1) = (1, 0) = 1$

であるから，197 と 92 の最大公約数は 1 である。

例　$7n+4$ と $4n+3$ が互いに素でないような 30 以下の自然数 n を求めてみよう。

$7n+4 = (4n+3)\cdot 1 + 3n+1$　より　$(7n+4, 4n+3) = (3n+1, 4n+3)$

$4n+3 = (3n+1)\cdot 1 + n+2$　より　$(4n+3, 3n+1) = (n+2, 3n+1)$

$3n+1 = (n+2)\cdot 3 - 5$　より　$(3n+1, n+2) = (n+2, -5)$

以上より　$(7n+4, 4n+3) = (n+2, -5) = (n+2, 5)$ であるから，$n+2$ と 5 が互いに素でなければよい。5 は素数より，$n+2$ が 5 の倍数であればよいから

$n = 3, 8, 13, 18, 23, 28$

例　[1992 一橋大学]　n を正の整数とする。n^2 と $2n+1$ が互いに素であることを示せ。

$2n^2 = (2n+1)\cdot n - n$　より　$(2n^2, 2n+1) = (-n, 2n+1) = (2n+1, n)$

$2n+1 = 2\cdot n + 1$　より　$(2n+1, n) = (1, n) = 1$

よって，$(2n^2, 2n+1) = 1$ であるから，$2n^2$ と $2n+1$ は互いに素である。

したがって，n^2 と $2n+1$ は互いに素である。

問　上記を，互除法を用いずに示せ。

拡張ユークリッドの互除法

ユークリッドの互除法を用いると，a, b の最大公約数を d として，不定方程式 $ax+by=d$ の解の 1 つを求めることができる。

例　不定方程式 $289x+197y=1$ の解の 1 つを求める。

289＝197･1＋92　より　92＝289－197･1　…①

197＝92･2＋13　より　13＝197－92･2　…②

92＝13･7＋1　より　1＝92－13･7　…③

よって

$$\begin{aligned}1&=92-(197-92\cdot2)\cdot7\\&=92\cdot15-197\cdot7\\&=(289-197\cdot1)\cdot15-197\cdot7\\&=289\cdot15+197\cdot(-22)\end{aligned}$$

すなわち，$x=15, y=-22$は解の 1 つである。

拡張ユークリッドの互除法から，次の定理が成り立つことが分かる。

定理 3　a, bの最大公約数をd とするとき，$ax+by=d$ を満たす整数x, y が存在する。

□

系　a, bの最大公約数をd とし，D をd の倍数全体の集合とするとき，

集合 $C=\{ax+by \mid x, y$ は整数$\}$ は集合D と一致する。

証明

a, bはd の倍数であるから，定理 1 により，$ax+by$はd の倍数である。よって，

$C \subset D$。

また，定理 3 により，$ax_0+by_0=d$ となる整数x_0, y_0が存在する。k を任意の整数として，この等式の両辺をk 倍すると，$a(kx_0)+b(ky_0)=kd$。よって，$C \supset D$。

ゆえに$C=D$。

□

上記の系は，次の様に書き換えられる。

命題　a, b, k を整数とするとき，1 次の不定方程式 $ax+by=k$ が整数解を持つための必要かつ十分な条件は，k がa とb の最大公約数d で割り切れることである。

□

また，特に k=1 の場合を考えると

命題　1 次の不定方程式 $ax+by=1$ が整数解を持つための必要かつ十分な条件は，a とb が互いに素であることである。

例題　a, bは 0 でない整数の定数とし，$ax+by$（x, y は整数）の形の数全体の集合を M とする。Mに属する最小の正の整数をd とするとき，次のことを示せ。

(1) Mの要素はすべてd の倍数である。

(2)　d はa, bの最大公約数である。

(3)　a, bが互いに素な整数のときは，$as+bt=1$となる整数s, t が存在する。

証明

$d = ax_0 + by_0$（x_0, y_0 は整数）とし，a, b の最大公約数を g とする。

(1) 任意の M の要素を $ax+by$ とすると，除法の定理により，

$$ax+by = qd+r \qquad q, r \text{ は整数，} 0 \leqq r < d$$

と表される。よって

$$ax+by = q(ax_0+by_0)+r \quad \text{すなわち} \quad a(x-qx_0)+b(y-qy_0) = r$$

これより，$r \in M$ であるが，$r \neq 0$ と仮定すると，$0 < r < d$ となり，d が M に属する最小の正の整数であることに反する。よって，$r = 0$。

したがって $ax+by = qd$ となるから，$ax+by$ は d の倍数である。

(2) $a = a \cdot 1 + b \cdot 0 \in M$，$b = a \cdot 0 + b \cdot 1 \in M$

であり，(1)より M の要素はすべて d の倍数であるから，a, b はともに d の倍数である。

よって，d は a, b の公約数であるから，$d \leqq g$ …①

また，$a = a'g, b = b'g$ （a', b' は整数）

と書けるから，これらを $d = ax_0 + by_0$ に代入して

$$d = a'gx_0 + b'gy_0 = (a'x_0 + b'y_0)g$$

したがって，d は g の倍数であり，$d > 0$ であるから，$d \geqq g$ …②

①，②により，$d = g$ である。

(3) $g = 1$ であるから，(2)により $d = 1$。よって，$as + bt = 1$ となる整数 s, t が存在する。

□

上記の例題により，拡張ユークリッドの互除法を用いずに，定理 3 が示された。

入試問題　[東京女子大学]

9 で割り切れる整数全体の集合を A，15 で割り切れる整数全体の集合を B とする。

$C = \{x+y \mid x \in A, y \in B\}$ とするとき，C は 3 で割り切れる整数全体と一致することを証明せよ。

命題　整数 a, b に対して，a, b の最大公約数を d，最小公倍数を l と置くとき，次が成り立つ。

(1) a, b の公約数は d の約数である。

(2) a, b の公倍数は l の倍数である。

証明

(1) 定理 3 により，

$$d = ax + by \quad \cdots①$$

となる整数 x, y が存在する。

a, b の任意の公約数 s に対して，$a = sa', b = sb'$ と置くと，①より

$$d = s(a'x + b'y)$$

となるから，s は d の約数である。

(2) a, b の任意の公倍数 t に対して，

$$t = ql + r, \qquad 0 \leqq r < l$$

とすれば，

$$r = t - ql$$

となるから，定理 1 により r は a, b の公倍数である。

$0 \leqq r < l$ であり，l は最小公倍数であったから，$r = 0$

したがって，$t = ql$ となるから，t は l の倍数である。

□

註　上記の命題は，後に示す「素因数分解の一意性」を用いても証明できる。

定理 4　a, b が互いに素で，ak が b の倍数ならば，k は b の倍数である。

証明

a, b は互いに素であるから，$1 = ax + by$ となる整数 x, y が存在する。両辺に k を掛けて

$$k = akx + bky$$

ak は b の倍数であるから，整数 m を用いて，$ak = bm$ と置ける。よって，

$$k = bmx + bky = b(mx + ky)$$

すなわち，k は b の倍数である。

□

命題　a, b が互いに素であるとき，不定方程式 $ax = by$ の解は，k を任意の整数として $x = bk, y = ak$ である。

証明　a, b は互いに素であるから，定理 4 により，x は b の倍数である。

よって，k を整数として，$x = bk$ と表される。

これを $ax = by$ に代入すると，$abk = by$　すなわち　$y = ak$

逆に，$x = bk, y = ak$ は $ax = by$ を満たす。

入試問題　[2016 センター試験]

不定方程式 $92x + 197y = 1$ を満たす整数 x の中で，x の絶対値が最小なものは $x =$ □，$y =$ □ である。

不定方程式 $92x + 197y = 10$ を満たす整数 x の中で，x の絶対値が最小なものは $x =$ □，$y =$ □ である。

例題　a, b が互いに素な自然数であるとき，b 個の自然数 $a \times k$　$(k = 1, 2, 3, \cdots\cdots, b)$ を b

で割った余りはすべて異なることを示せ。

証明

$a\times k \quad (k=1,2,3,\cdots\cdots,b)$ を b で割った商を q_k，余りを r_k とすると

$$ak=bq_k+r_k \quad (0\leqq r_k\leqq b-1)$$

よって $\quad r_k=ak-bq_k$

ここで，$r_i=r_j \quad (1\leqq i\leqq b,\ 1\leqq j\leqq b)$ と仮定すると

$$ai-bq_i=aj-bq_j \quad \text{すなわち} \qquad a(i-j)=b(q_i-q_j)$$

a と b は互いに素であるから，この等式より，$i-j$ は b の倍数である。（定理 4）

さらに，$1\leqq i\leqq b,\ 1\leqq j\leqq b$ より

$$-(b-1)\leqq i-j\leqq b-1$$

であるから，$i-j=0$ すなわち $i=j$ である。

これより，$r_i=r_j\Rightarrow i=j$ が成り立つ。

対偶をとると $\qquad i\neq j\Rightarrow r_i\neq r_j$

すなわち，b 個の自然数 $a\times k \quad (k=1,2,3,\cdots\cdots,b)$ を b で割った余りはすべて異なる。

□

例題　どのような自然数 m,n を用いても，$x=3m+5n$ と表すことができない最大の自然数 x を求めよ。

解答

（ⅰ）$n=1$ とすると，$x=3m+5=3(m+1)+2$

ここで，$m+1\geqq 2$ であるから，$x\geqq 8$

よって，x が 8 以上の 3 で割って 2 余る数(8，11，14，17，……)のときは，$x=3m+5n$ の形に表すことができる。

（ⅱ）$n=2$ とすると，$x=3m+10=3(m+3)+1$

ここで，$m+3\geqq 4$ であるから，$x\geqq 13$

よって，x が 13 以上の 3 で割って 1 余る数(13，16，19，……)のときは，$x=3m+5n$ の形に表すことができる。

（ⅲ）$n=3$ とすると，$x=3m+15=3(m+5)$

ここで，$m+5\geqq 6$ であるから，$x\geqq 18$

よって，x が 18 以上の 3 で割り切れる数(18，21，24，……)のときは，$x=3m+5n$ の形に表すことができる。

(ⅰ), (ⅱ), (ⅲ)より $x \geqq 16$ のとき， $x = 3m + 5n$ の形に表すことができる。
次に，$15 = 3m + 5n$ となる自然数 m, n が存在しないことを示す。この等式より

$$5(3-n) = 3m\ ,\quad 3(5-m) = 5n$$

であり，3 と 5 は互いに素であるから， m は 5 の倍数， n は 3 の倍数である。
さらに， m, n は自然数であるから， $m \geqq 5$ ， $n \geqq 3$
したがって， $3m + 5n \geqq 3 \cdot 5 + 5 \cdot 3 = 30$ となるが，これは，$15 = 3m + 5n$ と矛盾する。
以上より， $x = 3m + 5n$ と表すことができない最大の自然数 x は 15 である。

入試問題　[2008 奈良県立医大]
p, q を互いに素な正の整数とする。
(1) 任意の整数 x に対して， p 個の整数 $x - q, x - 2q, \cdots\cdots, x - pq$ を p で割った余りはすべて異なることを証明せよ。
(2) $x > pq$ である任意の整数 x は，適当な正の整数 a, b を用いて， $x = pa + qb$ と表されることを証明せよ。

素数
素数の節では，正の整数の範囲で考え，文字は正の整数を表すものとする。
$a > 1$ である整数 a が，1, a 以外の約数を持たないとき， a を**素数**といい，1, a 以外の約数を持つとき， a を**合成数**という。
整数がいくつかの整数の積で表されるとき，積を作る 1 つ 1 つの整数を，もとの整数の**因数**という。素数の因数を**素因数**という。

例題　p，$2p+1$，$4p+1$ がいずれも素数であるような p をすべて求めよ。(2005 一橋大学)
解
(ⅰ) $p=3$ のとき
　3 数は 3，7，13 となるので，題意を満たす。
(ⅱ) p が 3 以外の素数のとき
　p は素数であるから，3 の倍数でないので，$p=3k\pm1$ (k は自然数)と表される。
　$p=3k+1$ のとき

$$2p+1=6k+3=3(2k+1)$$

　これは，3 より大きい 3 の倍数であるから，素数でない。
　$p=3k-1$ のとき

$$4p+1=12k-3=3(4k-1)$$

　これは，3 より大きい 3 の倍数であるから，素数でない。

以上より，p が 3 以外の素数のときは，題意を満たさない。

(ⅰ)，(ⅱ)より，求める p は $p=3$

入試問題　[2004 早稲田大学]

n を自然数とする。$n, n+2, n+4$ がすべて素数であるのは $n=3$ の場合だけであることを示せ。

補題　2 つ以上の整数の積が，ある素数で割り切れるならば，因数のうち少なくとも 1 つはその素数で割り切れる。(ユークリッドの補題)

証明

ab が素数 p の倍数であるとし，a は p の倍数でないと仮定する。

p の約数は 1 と p だけであり，p は a の約数でないから，a と p の公約数は 1 のみである。よって，a と p は互いに素であるから，定理 4 により，b は p の倍数である。

ゆえに，ab が素数 p で割り切れるならば，a, b の少なくとも 1 つは p で割り切れる。

□

定理 5　素因数分解の一意性

合成数は素数の積に分解することができ，その分解は，積の順序を除いてただ 1 通りである。

証明

数学的帰納法で証明する。

(Ⅰ) 最小の合成数 $4=2\times2$ については，定理は成り立つ。

(Ⅱ) a を合成数として，a よりも小さい合成数に対して，定理が成り立つと仮定する。

a は合成数であるから，$a=bc, 1<b<a, 1<c<a$ となる b, c が存在する。このとき，b も c も素数であるか，または，帰納法の仮定により素数の積に分解されるから，a は素数の積に分解される。

次に，分解の一意性を示す。a を素因数に分解して

$$p_1\cdot p_2\cdot p_3\cdots=q_1\cdot q_2\cdot q_3\cdots$$

を得たとすれば，$q_1\cdot q_2\cdot q_3\cdots$ が素数 q_1 で割り切れるから，$p_1\cdot p_2\cdot p_3\cdots$ の中に q_1 で割り切れるものがある(ユークリッドの補題)。いま p_1 が q_1 で割り切れるとすれば，p_1 が素数であるから，$p_1=q_1$ である。したがって

$$p_2\cdot p_3\cdots=q_2\cdot q_3\cdots$$

この相等しい数を b とすれば，$b<a$ であるから，帰納法の仮定により b の両辺の分解は，積の順序を除いて一致する。

よって，a の素数の積への分解も，積の順序を除いて，ただ 1 通りしかない。

(Ⅲ) (Ⅰ), (Ⅱ)よりすべての合成数について，この定理は成り立つ。

□

b が a の倍数(a が b の約数)であるとは，ある整数 c が存在して $b=ac$ となることである。
これと，素因数分解に一意性より，次の命題が成り立つ。

命題　自然数 N を素因数分解した結果が $N=p^aq^br^c\cdots\cdots$ であるとき， N の正の約数は

$$p^iq^jr^k\cdots\cdots(0\leqq i\leqq a, 0\leqq j\leqq b, 0\leqq k\leqq c,\cdots\cdots)$$

である。

命題　a,b を素因数分解して， $a=p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots\cdots$ ， $b=p_1^{f_1}p_2^{f_2}p_3^{f_3}\cdots\cdots$ としたとき，

b が a の倍数(a が b の約数) $\Leftrightarrow$ 任意の自然数 i について $e_i\leqq f_i$

命題　N の正の約数の個数は　$(a+1)(b+1)(c+1)\cdots\cdots$

N の正の約数の総和は　$(1+p+\cdots+p^a)(1+q+\cdots+q^b)(1+r+\cdots+r^c)\cdots\cdots$

$$=\frac{p^{a+1}-1}{p-1}\cdot\frac{q^{b+1}-1}{q-1}\cdot\frac{r^{c+1}-1}{r-1}\cdots\cdots$$

命題　自然数 a,b に対して， a,b の最大公約数を d ，最小公倍数を l と置くとき，

$dl=ab$,

特に， a,b が互いに素ならば $l=ab$

証明

2 つの整数 $e,\ f$ の最小値を $\min(e,f)$ ，最大値を $\max(e,f)$ と表すことにする。

a と b の少なくとも一方の因数である素数を $p_1, p_2, p_3,\cdots\cdots$ とおく。

このとき， a と b を素因数分解すると，

$$a=p_1^{e_1}p_2^{e_2}p_3^{e_3}\cdots\cdots,\quad b=p_1^{f_1}p_2^{f_2}p_3^{f_3}\cdots\cdots$$

となる。ただし， $e_i,\ f_i$ は負でない整数である。このとき，

最大公約数 d を素因数分解したときの p_i の指数は　$\min(e_i,\ f_i)$

最小公倍数 l を素因数分解したときの p_i の指数は　$\max(e_i,\ f_i)$

したがって， dl を素因数分解したときの p_i の指数は

$$\min(e_i,\ f_i)+\max(e_i,\ f_i)=e_i+f_i$$

となり， ab を素因数分解したときの p_i の指数と等しい。よって， $dl=ab$ が示された。

□

$a=da', b=db'$ とすると， a', b' は互いに素であり， $dl=ab$ より， $dl=d^2a'b'$

よって， $l=da'b'$ が成り立つ。

例　最大公約数が 21，最小公倍数が 252 である 2 つの自然数 $a, b\ (a<b)$ の組を求めてみよう。最大公約数が 21 であるから，互いに素である自然数 $a', b'\ (a'<b')$ を用いて

$$a=21a', b=21b'$$

と表される。このとき，a, b の最小公倍数は $21a'b'$ と表されるから，

$21a'b'=252$ すなわち $a'b'=12$

$a'<b'$ かつ a', b' は互いに素であるから，

$(a', b')=(1, 12), (3, 4)$　よって　$(a, b)=(21, 252), (63, 84)$

命題　a と c が互いに素，かつ，b と c が互いに素ならば，ab と c は互いに素である。

証明　a と c が互いに素であるから，a と c に共通な素因数はない。また，b と c が互いに素であるから，b と c に共通な素因数はない。したがって，素因数分解の一意性から，ab と c に共通な素因数がないから，ab と c は互いに素である。

□

命題　n^2 が素数 p の倍数ならば，n は p の倍数である。

証明　n が素因数に p を持たないと仮定すると，素因数分解の一意性から，n^2 は素因数に p を持たない。これは n^2 が素数 p の倍数であることに矛盾する。したがって，n は p の倍数である。

□

一般に，k を自然数として，n^k が素数 p の倍数ならば，n は p の倍数である。

入試問題 [九州大学]

互いに素である自然数 a, b に対して，a^2 と b^2 は互いに素であることを証明せよ。

入試問題　[2005 東京大学]

3 以上 9999 以下の奇数 a で，a^2-a が 10000 で割り切れるものをすべて求めよ。

命題　整数 a, b が互いに素であるとき，$a+b$ と ab は互いに素である。

証明

$a+b$ と ab は互いに素でないと仮定すると，ある素数 p が存在して，$a+b=kp, ab=lp$ と表される。

このとき，$ab=lp$ より，a, b の少なくとも 1 つは p の倍数である。

a が p の倍数であると仮定すると，$b=kp-a$ より，b も p の倍数となり，a, b が互いに素であることと矛盾する。b が p の倍数であると仮定しても，同様に矛盾する。

ゆえに，$a+b$ と ab は互いに素である。

□

入試問題　[1999　一橋大学]

p, q は素数で，$p<q$ とする。

(1) $\dfrac{1}{p}+\dfrac{1}{q}=\dfrac{1}{r}$ を満たす整数 r は存在しないことを示せ。

(2) $\dfrac{1}{p}-\dfrac{1}{q}=\dfrac{1}{r}$ を満たす整数 r が存在するのは，$p=2, q=3$ のときに限ることを示せ。

例題　$\sqrt{2}$ は無理数であることを示せ。

解　$\sqrt{2}$ が有理数であると仮定する。このとき，自然数 m, n を用いて

$$\sqrt{2}=\frac{m}{n}$$

と表される。両辺を 2 乗して，

$$2=\frac{m^2}{n^2}\quad \text{よって}\quad 2n^2=m^2\cdots①$$

m, n を素因数分解して，①の両辺を素因数の積で表したとき，①の左辺は 2 で奇数回割り切れ，右辺は 2 で偶数回割り切れる。よって矛盾。したがって，$\sqrt{2}$ は無理数である。

□

命題　自然数 a が平方数でないならば $\sqrt{a}$ は無理数である。

証明

$\sqrt{a}$ が有理数であると仮定する。このとき，互いに素である自然数 m, n を用いて，

$$\sqrt{a}=\frac{m}{n}$$

と表される。ただし，a は平方数でないから，$n\neq 1$

両辺を 2 乗して，

$$a=\frac{m^2}{n^2}\quad \text{よって}\quad an^2=m^2$$

ここで，$n\neq 1$ であるから，n の素因数の一つを p とすると，この等式より，p は m^2 の素因数であるから，p は m の素因数である。これは，m, n が互いに素であることに反する。

ゆえに，$\sqrt{a}$ は無理数である。

□

命題　素数は無限に存在する

証明

素数が有限個しかないと仮定し，$2, 3, \cdots\cdots, p$ が素数のすべてであるとする。ここで，自然数 $P = 2\times 3\times\cdots\cdots\times p + 1$ を考える。$P > 1$ であるから，P は定理 5 により $2, 3, \cdots\cdots, p$ の少なくとも 1 つで割り切れる。しかし，P は $2, 3, \cdots\cdots, p$ のどれで割っても余りが 1 となり割り切れないので，矛盾する。ゆえに，素数は無限に存在する。

□

注意　$2\times 3\times 5\times 7\times 11\times 13 + 1 = 30031 = 59\times 509$ となり素数ではない。

命題　$4n-1$ の形の素数は，無限に存在する。

証明

$4n-1$ の形の素数 3, 7, 11, …… を大きさの順に並べて p が最大なものであると仮定し

$$A = 4(3\times 7\times 11\times\cdots\cdots\times p) - 1$$

と置く。すると，A は 2 および $3, 7, 11, \cdots\cdots, p$ のいずれでも割り切れないので，A を素因数分解したとき，素因数はすべて $2, 3, 7, 11, \cdots\cdots, p$ 以外の素数である。それらの素因数のすべてが $4n+1$ の形であると仮定すると，A は $4n+1$ の形になるから，矛盾する。よって，A の素因数の中に，$4n-1$ の形のもので $3, 7, 11, \cdots\cdots, p$ 以外の素数が存在するから，$4n-1$ の形の素数が $3, 7, 11, \cdots\cdots, p$ だけであるという仮定に反する。ゆえに，$4n-1$ の形の素数は，無限に存在する。

□

素数を 1 つも含まない自然数のいくらでも長い範囲が存在することは，次のように分かる。$(n+1)!+k \quad (k = 2, 3, 4, \cdots, n+1)$ を考えれば，連続する n 個の自然数がすべて素数でない。

入試問題　[千葉大学]

(1) 5 以上の素数は，ある自然数 n を用いて $6n+1$ または $6n-1$ の形で表されることを示せ。

(2) N は自然数とする。$6N-1$ は $6n-1$（n は自然数）の形で表される素数を約数にもつことを示せ。

(3) $6n-1$（n は自然数）の形で表される素数は無限に多く存在することを示せ。

双子素数

差が 2 である 2 つの素数の組を双子素数という。小さい順に

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), ……

などがある。双子素数は無限に存在するかという問題は，数学上の未解決問題である。

性質　(3，5)を除くすべての双子素数は，$(6n-1, 6n+1)$ に自然数nを代入した数である。これより，nを自然数とするとき，$n, n+2, n+4$がすべて素数であるのは$n=3$の場合だけであることが分かる。

命題　$n!$を素因数分解したときに，素因数 p の指数は，m を $p^m \leqq n < p^{m+1}$ を満たす整数として，

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots\cdots+\left[\frac{n}{p^m}\right]$$

ただし，$[x]$は，x を超えない最大の整数を表す。

証明　$n!$の因数 $1, 2, 3, \cdots\cdots, n$ のn個の中で，p の倍数がn_1個，p^2 の倍数がn_2 個，……，p^mの倍数がn_m個であるとする。このとき，求める指数は$n_1+n_2+n_3+\cdots\cdots+n_m$ であり，

$$n_1=\left[\frac{n}{p}\right], n_2=\left[\frac{n}{p^2}\right], n_3=\left[\frac{n}{p^3}\right], \cdots\cdots, n_m=\left[\frac{n}{p^m}\right]$$

である。

例題　400!を十進数で表したとき，末尾に連続して何個の 0 が並ぶか。

解　10＝2×5 であり，400!を素因数分解したときに，素因数 5 の指数は素因数 2 の指数より小さい。

よって，400!を十進数で表したとき，素因数 5 の指数だけ末尾に連続して 0 が並ぶ。

$5^3 \leqq 400 < 5^4$ であり，

$$\left[\frac{400}{5}\right]+\left[\frac{400}{5^2}\right]+\left[\frac{400}{5^3}\right]=[80]+[16]+\left[\frac{400}{125}\right]=80+16+3=99$$

したがって，末尾に連続して 99 個の 0 が並ぶ。

入試問題　[2009 京都大学]

p を素数，n を正の整数とするとき，$(p^n)!$ は p で何回割り切れるか。

整式の因数分解の利用

nが 2 以上の自然数であるとき，n^4+4 は素数にならないことを整式の因数分解を用いて示してみよう。

$$n^4+4=(n^2+2)^2-4n^2=(n^2+2n+2)(n^2-2n+2)$$

nが自然数であるとき，n^2+2n+2，n^2-2n+2 はともに整数であり，$n \geqq 2$ のとき，

$n^2+2n+2 \geqq 10$，$n^2-2n+2=(n-1)^2+1 \geqq 2$

よって，n が 2 以上の自然数であるとき，n^4+4 は素数ではない。

また，次のような因数分解が知られている。

n が 2 以上の整数のとき

$$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\cdots+a^{n-r}b^{r-1}+\cdots+b^{n-1})$$

n が 3 以上の奇数のとき

$$a^n+b^n=(a+b)\{a^{n-1}-a^{n-2}b+\cdots+(-1)^{r-1}a^{n-r}b^{r-1}+\cdots+b^{n-1}\}$$

例題　[1996 京都大学]　m, n は自然数で，$m<n$ をみたすものとする。m^n+1, n^m+1 がともに 10 の倍数となる m, n を 1 組与えよ。

解答　10 は偶数であるから，m^n+1, n^m+1 がともに 10 の倍数となるためには，m, n はともに奇数でなければならない。よって，m, n は奇数とする。このとき

$$m^n+1=(m+1)\{m^{n-1}-m^{n-2}+\cdots+(-1)^{r-1}m^{n-r}+\cdots+1\}$$

が成り立つから，$m+1$ が 10 の倍数であれば，m^n+1 は 10 の倍数になる。よって，$m=9$ とする。また，

$$n^m+1=(n+1)\{n^{m-1}-n^{m-2}+\cdots+(-1)^{r-1}n^{m-r}+\cdots+1\}$$

が成り立つから，$n+1$ が 10 の倍数であれば，n^m+1 は 10 の倍数になる。$m<n$ であるから，$n=19$ とする。

したがって，求める m, n の 1 組は $m=9, n=19$

別解　$(10-1)^{19}$ と $(20-1)^9$ を二項定理で展開することにより，$9^{19}+1$ と 19^9+1 がともに 10 の倍数となることが示される。

入試問題　[2009 一橋大学]

2 以上の整数 m, n は $m^3+1^3=n^3+10^3$ を満たす。m, n を求めよ。

合同式

整数 a, b の差 $a-b$ が m の倍数であるとき，a と b は m を法(modulus)として互いに合同であるといい，それを次のように表す。

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

合同は，次の 3 つの規律に従う。

反射律　　$a \equiv a \pmod{m}$

対称律　　$a \equiv b$ ならば $b \equiv a \pmod{m}$

推移律　　$a \equiv b,\ b \equiv c$ ならば $a \equiv c \pmod{m}$

法が同一の合同式は，加法，減法，乗法に関して，等式と同様に取り扱える。

定理 6

$a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ ならば

(1) $a+c \equiv b+d \pmod{m}$　(2) $a-c \equiv b-d \pmod{m}$　(3) $ac \equiv bd \pmod{m}$

証明

$a \equiv b \pmod{m}$ であるから　$a-b$ は m の倍数

$c \equiv d \pmod{m}$ であるから　$c-d$ は m の倍数

これより

(1) $(a+c)-(b+d)=(a-b)+(c-d)$ は m の倍数であるから

$a+c \equiv b+d \pmod{m}$

(2) $(a-c)-(b-d)=(a-b)-(c-d)$ は m の倍数であるから

$a-c \equiv b-d \pmod{m}$

(3) $ac-bd=ac-ad+ad-bd=a(c-d)+(a-b)d$ は m の倍数であるから

$ac \equiv bd \pmod{m}$

□

系　$a \equiv b \pmod{m}$ であるならば,

任意の自然数 n に対して，$a^n \equiv b^n \pmod{m}$

さらに，$f(x)$ が x の整式であるとき，$f(a) \equiv f(b) \pmod{m}$

入試問題 [1995 京都大学　文系]

自然数の関数 $f(n), g(n)$ を

$f(n)=n$ を 7 で割った余り

$$g(n)=3f\left(\sum_{k=1}^{7} k^n\right)$$

によって定める。

(1) すべての自然数 n に対して $f\left(n^7\right)=f(n)$ を示せ。

(2) あなたの好きな自然数 n を一つ決めて $g(n)$ を求めよ。

その $g(n)$ の値をこの設問(2)におけるあなたの得点とする。

入試問題　[2001 京都大学]

任意の整数 n に対し，n^9-n^3 は 9 で割り切れることを示せ。

命題

c と p は互いに素であるとする。このとき，

$$ac \equiv bc \quad \Rightarrow \quad a \equiv b \pmod{p}$$

証明

$ac \equiv bc$ より $(a-b)c \equiv 0$ であるから，$(a-b)c$ は p の倍数である。

ここで，c と p は互いに素であるから，$a-b$ は p の倍数，すなわち

$$a-b \equiv 0 \pmod{p}$$

ゆえに $a \equiv b \pmod{p}$

□

例 $5x \equiv 5y \quad \Rightarrow \quad x \equiv y \pmod 6$ は成り立つが，$2x \equiv 2y \quad \Rightarrow \quad x \equiv y \pmod 6$ は成り立たない。実際 $2 \cdot 2 \equiv 2 \cdot 5 \pmod 6$ であるが，$2 \equiv 5 \pmod 6$ ではない。

例題 a を十進法で表して

$$a = a_n \cdot 10^n + \cdots\cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

とすれば，

(1) $a \equiv a_n + \cdots\cdots + a_2 + a_1 + a_0 \pmod 3$

(2) $a \equiv a_n + \cdots\cdots + a_2 + a_1 + a_0 \pmod 9$

(3) $a \equiv (-1)^n a_n + \cdots\cdots + a_2 - a_1 + a_0 \pmod{11}$

証明

(1) $10 \equiv 1 \pmod 3$ より $10^k \equiv 1^k = 1 \pmod 3$

(2) $10 \equiv 1 \pmod 9$ より $10^k \equiv 1^k = 1 \pmod 9$

(3) $10 \equiv -1 \pmod{11}$ より $10^k \equiv (-1)^k \pmod{11}$

である。よって，成り立つ。

□

例 $1001 = 7 \times 11 \times 13$ であるから，$1000 \equiv -1 \pmod{7, 11, 13}$

これを用いれば

$$314159265 = 314 \times 1000^2 + 159 \times 1000 + 265 \equiv 314 - 159 + 265 = 420 \equiv 0 \pmod 7$$

また，同様にして

$$314159265 \equiv 420 \equiv 4 - 2 + 0 = 2 \pmod{11}$$

$$314159265 \equiv 420 \equiv 4 \pmod{13}$$

□

定理 7　中国人剰余定理

m, n が互いに素な自然数であるとき，任意の整数 a, b に対して連立合同式

$x \equiv a \pmod{m}, \quad x \equiv b \pmod{n}$

の整数解は，mn を法としてただ一つ存在する。

証明

s, t を整数として，$x = a + ms = b + nt$ となる整数 x を求める。この等式より

$$ms - nt = b - a \quad \cdots①$$

m, n は互いに素であるから，定理 3 により

$$ms_0 - nt_0 = b - a \quad \cdots②$$

を満たす整数 s_0, t_0 が存在する。①－②より，

$$m(s - s_0) - n(t - t_0) = 0 \quad \text{すなわち} \quad m(s - s_0) = n(t - t_0)$$

m, n は互いに素であるから，u を任意の整数として

$$s - s_0 = nu \ , \ t - t_0 = mu$$

と表される。よって，$s = s_0 + nu$ であるから

$$x = a + ms = a + m(s_0 + nu) = a + ms_0 + (mn)u$$

したがって，整数解は，mn を法としてただ一つ存在する。

□

一般化すると，次のようになる。（証明は各自が試みよ。）

定理　$m_1, m_2, m_3, \cdots\cdots, m_n$ がどの 2 つも互いに素である自然数ならば，連立合同式

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \cdots\cdots, \quad x \equiv a_n \pmod{m_n}$$

の整数解は，$m_1 m_2 m_3 \cdots\cdots m_n$ を法としてただ一つ存在する。

例題　（孫子算経の「百五減算」より）

今有物不知其数　三三数之剰二　五五数之剰三　七七数之剰二　問物幾何

3 で割ると 2 余り，5 で割ると 3 余り，7 で割ると 2 余る，最小の正の整数を求めよ。

解　次の連立 1 次合同式を解けばよい。

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7}$$

3 で割れば 2 余り，5 で割れば 3 余り，7 で割ると 2 余る数を N とすると，Nは整数 k，ℓ，m を用いて

$$N = 3k + 2 = 5\ell + 3 = 7m + 2 \quad \cdots①$$

と表される。$3k + 2 = 5\ell + 3$ から

$$3k = 5\ell + 1 \quad \cdots②$$

$k = 2$，$\ell = 1$ は②の整数解の 1 つであるから

$$3 \times 2 = 5 \times 1 + 1 \quad \cdots③$$

②－③より

$3(k-2)=5(\ell-1)$

3 と 5 は互いに素であるから，整数 n を用いて $k-2=5n$，$\ell-1=3n$ と表される。

これより，$\ell=3n+1$ であるから，①より

$N=5(3n+1)+3=15n+8$　よって　$N=15n+8=7m+2$　…④

したがって

$15n=7m-6$　…⑤

拡張ユークリッドの互除法により，特殊解を求める。

$15=7\times2+1$

両辺を−6 倍して

$15\times(-6)=7\times(-12)-6$　…⑥

⑤−⑥より　　$15(n+6)=7(m+12)$

15 と 7 は互いに素であるから，整数 s を用いて $n+6=7s$，$m+12=15s$ と表される。

これより，$n=7s-6$ であるから，④より

$N=15(7s-6)+8=105s-82$

したがって，N のうち正で最小のものは $105\times1-82=23$ である。

□

入試問題　[2017 センター試験追試改作]

(1) 不定方程式 $21x+13=16y+12=96z+28$ の整数解 x, y, z を求めよ。

(2) 自然数 n は，21 で割ると 13 余り，16 で割ると 12 余り，96 で割ると 28 余るとする。このような n のうち，最小なものを求めよ。

入試問題　[1981 立教大学]

n は整数で，$0 \leqq n < 105$ とする。

n を 3 で割った余りを a，n を 5 で割った余りを b，n を 7 で割った余りを c とするとき，n は $70a+21b+15c$ を 105 で割った余りに等しいことを証明せよ。

参考　連立 1 次合同式のガウスによる解の求め方

整数 $m_1, m_2, \cdots\cdots, m_n$ がどの 2 つも互いに素であるならば，

$$M=m_1\cdot m_2\cdots\cdots m_n,\quad M=m_1M_1=m_2M_2=\cdots\cdots=m_nM_n$$

とおくと，各 m_i と M_i は互いに素であるから，$i=1, 2, 3, \cdots\cdots, n$ に対して

$$M_it_i+m_iu_i=1$$

となる t_i, u_i が存在する。したがって,

$$M_i t_i \equiv 1 \pmod{m_i}$$

となる t_i が存在する。このとき,

$$x \equiv M_1 t_1 a_1 + M_2 t_2 a_2 + \cdots\cdots + M_n t_n a_n \pmod{M}$$

は，与えられた連立 1 次合同式の解となる。

フェルマーの小定理

補題 1

x, y を整数，p を素数とするとき，　$(x+y)^p \equiv x^p + y^p \pmod{p}$

証明

$$(x+y)^p = x^p + {}_pC_1 x^{p-1}y + {}_pC_2 x^{p-2}y + \cdots + {}_pC_r x^{p-r}y^r + \cdots + {}_pC_{p-1} xy^{p-1} + y^p$$

ここで，$r = 1, 2, 3, \cdots, p-1$ のとき ${}_pC_r$ は p の倍数である。なぜなら

$${}_pC_r = \frac{p(p-1)(p-2)\cdots\cdots(p-r+1)}{r(r-1)(r-2)\cdots\cdots 1} \quad \text{より}$$

$${}_pC_r \{r(r-1)(r-2)\cdots\cdots 1\} = p(p-1)(p-2)\cdots\cdots(p-r+1)$$

であり，　$0 < r < p$ かつ p は素数より，$r, r-1, r-2, \cdots\cdots, 1$ と p は互いに素。
よって，$r(r-1)(r-2)\cdots\cdots 1$ と p は互いに素であるからである。
したがって

$${}_pC_1 x^{p-1}y + {}_pC_2 x^{p-2}y + \cdots + {}_pC_r x^{p-r}y^r + \cdots + {}_pC_{p-1} xy^{p-1} \equiv 0 \pmod{p}$$

であるから

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

□

補題 2

p を素数とし，a を自然数とするとき,

$$a^p \equiv a \pmod{p}$$

証明

a についての数学的帰納法で示す。

(Ⅰ) $a=1$は明らかに成り立つ。

(Ⅱ) $a=k$ のとき命題が成り立つと仮定すると

$$k^p \equiv k \pmod{p}$$

このとき，補題 1 により

$$(k+1)^p \equiv k^p + 1^p \equiv k+1 \pmod{p}$$

よって，$a=k+1$のときも命題は成り立つ。

(Ⅰ)，(Ⅱ)より，すべての自然数aについて，命題は成り立つ。

□

補題 3

p を素数とし，a を整数とするとき，$a^p \equiv a \pmod{p}$

証明

任意の整数aに対して，$a \equiv b \pmod{p}$となる自然数bが存在するから，

$$a^p \equiv b^p \equiv b \equiv a \pmod{p}$$

□

定理 8　フェルマーの小定理

p を素数とし，a を p の倍数でない整数とするとき，

$$a^{p-1} \equiv 1 \pmod{p}$$

証明

補題 4 より，$a \cdot a^{p-1} \equiv a \cdot 1 \pmod{p}$であり，$a$ と p は互いに素であるから

$$a^{p-1} \equiv 1 \pmod{p}$$

□

例　2^{200} を 19 で割った余りを求めてみよう。

19 は素数であり，2 と 19 は互いに素であるから，フェルマーの小定理により

$$2^{18} \equiv 1 \pmod{19}$$

ここで，200＝18×11＋2 であるから

$$2^{200} = 2^{18 \cdot 11+2} = \left(2^{18}\right)^{11} \cdot 2^2 \equiv 1^{11} \cdot 4 = 4 \pmod{19}$$

ゆえに，2^{200} を 19 で割った余りは 4 である。

□

入試問題　[2005 早稲田大学]

次の各問いに答えよ。ただし，正の整数nと整数k $(0 \leqq k \leqq n)$に対して，${}_nC_k$は正の整数であるという事実を使ってよい。

(1)　m が 2 以上の整数のとき，${}_mC_2$がmで割り切れるための必要十分条件を求めよ。

(2) p を 2 以上の素数とし，k を p より小さい正の整数とする。このとき，${}_pC_k$ は p で割り切れることを示せ。

(3) p を 2 以上の素数とする。このとき，任意の正の整数 n に対し，$(n+1)^p - n^p - 1$ は p で割り切れることを示せ。

入試問題 [1977　京都大学]

p が素数であれば，どんな自然数 n についても $n^p - n$ は p で割り切れる。このことを，n についての数学的帰納法で証明せよ。

オイラーの φ 関数

n を自然数とするとき，$m \leqq n$ で，m と n が互いに素である自然数 m の個数を $\varphi(n)$ とする。この n の関数を**オイラーの φ 関数**という。

例　p を素数とする。$m \leqq p$ で，m と p が互いに素である自然数 m は

$$1, 2, 3, \cdots, p-1$$

であるから，$\varphi(p) = p-1$ である。

命題　p, q を異なる素数とすると，$\varphi(pq) = (p-1)(q-1)$ である。

証明

p, q は異なる自然数であるから，pq と互いに素である自然数は，p の倍数でも q の倍数でもない自然数である。pq 以下の自然数で

p の倍数は	$1\cdot p, 2\cdot p, 3\cdot p, \cdots, (q-1)\cdot p, qp$	の q 個
q の倍数は	$1\cdot q, 2\cdot q, 3\cdot q, \cdots, (q-1)\cdot q, pq$	の p 個
pq の倍数は	pq	の 1 個

あるから，p の倍数，または，q の倍数であるものは，$p+q-1$ 個ある。

したがって，

$$\varphi(pq) = pq - (p+q-1) = pq - p - q + 1 = (p-1)(q-1)$$

□

命題　p は素数，k は自然数とするとき，$\varphi(p^k) = p^k - p^{k-1}$

証明

$1, 2, 3, \cdots\cdots, p^k$ の中で，p と互いに素でないものは p の倍数であるから，

$$p, 2p, 3p, \cdots\cdots, p^{k-1}\cdot p$$

の，p^{k-1} 個ある。ゆえに p と互いに素である整数の個数は $p^k - p^{k-1}$

すなわち　$\varphi(p^k) = p^k - p^{k-1}$

□

註　m と n は互いに素な自然数であるとき，$\varphi(mn) = \varphi(m)\varphi(n)$ が成り立つことが知られている。これを，定理 10 で示す。

入試問題 [2005 早稲田大学]

自然数 n に対して，n 以下の自然数で n との最大公約数が 1 となるような自然数の個数を $f(n)$ とする。例えば，$n=12$ に対しては，このような自然数は 1，5，7，11 の 4 個なので，$f(12)=4$ である。また，　$f(1)=1$ ，素数 p に対しては $f(p)=p-1$ である。

(1)　$f(77)$ を求めよ。

(2)　$f(pq)=24$ なる 2 つの素数 p, q（ただし，$p<q$ とする）の組を求めよ。

(3)　k, n を自然数とするとき，$f(2^k 3^n)$ の値を k, n の式で表せ。

平方剰余

a と m が互いに素であるとき，合同方程式 $x^2 \equiv a \pmod{m}$ が整数解を持てば，a は m を法とする**平方剰余**であるといい，整数解を持たなければ，a は m を法とする**平方非剰余**であるという。

例　$0^2 \equiv 0,\ (\pm 1)^2 \equiv 1,\ (\pm 2)^2 = 4,\ (\pm 3)^2 = 9 \equiv 1,\ 4^2 = 16 \equiv 0 \pmod 8$

より，0，1，4 は 8 を法とする平方剰余であるが，2，3，5，6，7 は 8 を法とする平方非剰余である。

□

例　$m^2 = 3n+5$ を満たす整数 m, n は存在しない。なぜなら

$0^2 \equiv 0,\ (\pm 1)^2 \equiv 1 \pmod 3$ であるから，$m^2 \equiv 0, 1 \pmod 3$

$3n+5 \equiv 5 = 3+2 \equiv 2 \pmod 3$

より，m^2 と $3n+5$ は，3 を法として合同でないからである。

□

入試問題　[2006 京都大学]

2 以上の自然数 n に対し，n と n^2+2 がともに素数となるのは，$n=3$ の場合に限ることを示せ。

平方剰余とピタゴラス数

$a^2+b^2=c^2$ を満たす自然数の組 a, b, c を，**ピタゴラス数**という。

x, y, z を整数として，$x^2+y^2=z^2$ が成り立つとき，次の補題 1，2，3 が成り立つ。

補題 1

x, y の少なくとも 1 つは偶数である。

証明

mod 4 で考える。平方剰余を求めると

$$0^2 \equiv 0, \quad (\pm 1)^2 \equiv 1, \quad 2^2 = 4 \equiv 0$$

x, y が共に奇数であると仮定する。このとき，$x \equiv \pm 1$，$y \equiv \pm 1$ であるから

$$x^2 \equiv 1, \quad y^2 \equiv 1$$

よって　$x^2+y^2 \equiv 2$

一方　　$z^2 \equiv 0, 1$

したがって，$x^2+y^2=z^2$ と矛盾するから，x, y の少なくとも 1 つは偶数である。

□

補題 2

次の条件はすべて同値である。

「x, y, z の最大公約数は 1 」，「x, y は互いに素」，「y, z は互いに素」，「z, x は互いに素」

証明

「x, y, z の最大公約数は 1 $\Leftrightarrow$ x, y は互いに素」を示す。

$\Leftarrow$　明らか

$\Rightarrow$　x, y の最大公約数が 1 でないと仮定すると，ある素数 p が存在して，x, y は共に p の倍数となる。このとき，x^2+y^2 は p の倍数となるから，$x^2+y^2=z^2$ より，z^2 は p の倍数となる。よって，z は p の倍数となるから，p は x, y, z の公約数である。これは，x, y, z の最大公約数は 1 であることと矛盾する。ゆえに，x, y の最大公約数は 1 である。

他も同様にして，同値であることが示される。

□

補題 3

x, y, z の最大公約数が 1 であるとき，x, y の一方は偶数，他方は奇数であり，z は奇数である。

証明

補題 1 より x, y の少なくとも 1 つは偶数であり，補題 2 より x, y は互いに素であるから，x, y の一方は偶数，他方は奇数である。このとき，x^2+y^2 は奇数であるから，$x^2+y^2=z^2$ より，z^2 は奇数。よって，z は奇数である。

□

命題　x, y, z を整数として，$x^2+y^2=z^2$ 満たすとき，次が成り立つ。

(1)　x, y の少なくとも 1 つは 3 の倍数である。

(2) x, y の少なくとも 1 つは 4 の倍数である。

(3) x, y, z の少なくとも 1 つは 5 の倍数である。

証明

(1) mod 3 で考える。

$$0^2 \equiv 0, \quad (\pm 1)^2 \equiv 1$$

x, y が共に 3 の倍数でないと仮定すると， $x^2 \equiv 1$， $y^2 \equiv 1$ であるから

$$x^2 + y^2 \equiv 2$$

一方　　$z^2 \equiv 0, 1$

したがって， $x^2 + y^2 = z^2$ と矛盾する。

よって， x, y の少なくとも 1 つは 3 の倍数である。

(2) x, y, z の最大公約数が 1 であるときに示せば十分である。このとき，補題 3 により，x, y の一方は偶数，他方は奇数であり， z は奇数である。

x が偶数， y が奇数であるとし，mod 8 で考える。

x が 4 の倍数でないと仮定する。すると， $x \equiv \pm 2$ であるから

$$x^2 \equiv (\pm 2)^2 \equiv 4$$

また， y は奇数であるから， $y \equiv \pm 1, \pm 3$ であり， $(\pm 1)^2 \equiv 1, \quad (\pm 3)^2 \equiv 9 \equiv 1$ より

$$y^2 \equiv 1$$

よって　$x^2 + y^2 \equiv 5$

一方， z は奇数であるから， $z \equiv \pm 1, \pm 3$ より　$z^2 \equiv 1$

したがって， $x^2 + y^2 = z^2$ と矛盾するから， x は 4 の倍数である。

(3) mod 5 で考えると

$$0^2 \equiv 0, \quad (\pm 1)^2 \equiv 1, \quad (\pm 2)^2 \equiv 4$$

x, y, z のすべてが 5 の倍数でないと仮定する。

$x^2 \equiv 1, 4$　かつ　$y^2 \equiv 1, 4$ より

$$x^2 + y^2 \equiv 0, 2, 3$$

一方　　$z^2 \equiv 1, 4$

したがって， $x^2 + y^2 = z^2$ と矛盾する。

よって， x, y, z の少なくとも 1 つは 5 の倍数である。

□

入試問題 [1990 一橋大学]

直角三角形の 3 辺の長さがすべて整数のとき，面積は 2 の整数倍であることを示せ。

入試問題 [静岡大学]

次の問に答えよ。

(1) p を 2 と異なる素数とする。$m^2 = n^2 + p^2$ を満たす自然数の組(m, n)がただ 1 組存在することを証明せよ。
(2) $m^2 = n^2 + 12^2$ を満たす自然数の組(m, n)をすべて求めよ。

フェルマーの最終定理

「3 以上の自然数nについて，$x^n + y^n = z^n$ となる自然数 (x, y, z) の組は存在しない。」というのはフェルマーの最終定理として有名である。フェルマーは「この定理に関して，私は真に驚くべき証明を見つけたが，この余白はそれを書くには狭すぎる。」と書き残したが，多くの数学者の努力にも関わらず一般には証明されなかった。ところが，360 年後の 1995 年にアンドリュー・ワイルズによって完全に証明された。

入試問題 [1999 早稲田大学]

次の問に答えよ。
(1) $a+b \geqq a^2 - ab + b^2$ をみたす正の整数の組(a, b)をすべて求めよ。
(2) $a^3 + b^3 = p^3$ をみたす素数 p と正の整数a, bは存在しないことを示せ。

完全数とメルセンヌ素数の関係

正の整数nについて，正の約数の総和を$S(n)$とする。$S(n) = 2n$ となるとき，n を**完全数**という。

例えば，$28 = 2^2 \cdot 7$ の約数の総和は

$$(1+2+2^2)\cdot(1+7) = 56 = 2 \cdot 28$$

であるから，28 は完全数である。奇数の完全数は発見されていない。

例 p, q $(p < q)$ を素数として，$n = pq$ が完全数となるような，n の値を求めてみよう。

$$S(n) = S(pq) = pq + p + q + 1$$

であるから，$S(n) = 2n$ より

$$pq + p + q + 1 = 2pq \quad \text{すなわち} \quad pq - p - q = 1$$

変形して

$$(p-1)(q-1) = 2$$

ここで，$2 \leqq p < q$ であるから，$p-1, q-1$ は正の整数で，$p-1 < q-1$ であるから，

$$p-1 = 1, q-1 = 2 \quad \text{よって} \quad p = 2, q = 3$$

したがって $\quad n = pq = 6$

N を正の整数として，$2^N - 1$ の形の数を**メルセンヌ数**といい，素数のメルセンヌ数を**メル**

センヌ素数という。

命題　2^N-1が素数であるならば，N は素数である。（逆は成り立たない）

証明　$N=1$のときは，2^N-1は素数でないから，$N \geqq 2$ のときを考える。

N が素数でないと仮定すると，a, b を 2 以上の整数として，$N=ab$ と表される。

このとき

$$2^N-1=2^{ab}-1=(2^a)^b-1=(2^a-1)\{(2^a)^{b-1}+(2^a)^{b-2}+\cdots\cdots+1\}$$

a, b は 2 以上の整数であるから，$2^a-1>1$，$(2^a)^{b-1}+(2^a)^{b-2}+\cdots\cdots+1>1$

これは，2^N-1が素数であることと矛盾する。ゆえに，N は素数である。

□

任意の正の整数nは，$p_1, p_2, \cdots\cdots, p_r$を素数として$n=p_1^{n_1}\cdot p_2^{n_2}\cdots\cdots p_r^{n_r}$と表されるから

$$S(n)=(1+p_1+\cdots\cdots+p_1^{n_1})\cdot(1+p_2+\cdots\cdots+p_2^{n_2})\cdots\cdots(1+p_r+\cdots\cdots+p_r^{n_r})$$

これより，a, b が互いに素であるとき，$S(ab)=S(a)S(b)$ が成り立つ。

命題　2^N-1が素数であるような正の整数N に対し，$2^{N-1}(2^N-1)$ は完全数である。

証明　(1) 2^N-1は素数であるから，2^{N-1}と2^N-1は互いに素である。

$$S(2^{N-1})=1+2+2^2+\cdots\cdots+2^{N-1}=\frac{2^N-1}{2-1}=2^N-1$$

$$S(2^N-1)=1+(2^N-1)=2^N$$

よって

$$S\left(2^{N-1}(2^N-1)\right)=S(2^{N-1})S(2^N-1)=(2^N-1)\cdot 2^N=2\cdot 2^{N-1}(2^N-1)$$

したがって，$2^{N-1}(2^N-1)$ は完全数である。

□

逆に，偶数の完全数は，2^N-1が素数であるような正の整数N を用いて，$2^{N-1}(2^N-1)$ の形で表されることが知られている。（オイラーが証明した）

2^N-1が素数であるN の値は，次のものが発見されている。

2，3，5，7，13，17，19，31，61，89，107，127，521，607，1279，……，74207281

人類が発見した最大の素数は，2016 年 3 月現在で，メルセンヌ素数 $2^{74207281}-1$ である。

入試問題　[お茶の水女子大学]

正の整数nに対しnの正の約数のすべての和を$S(n)$とおく。ただし，1 とnも約数とする。

(1) 素数 p，正の整数 a に対し，$n=p^a$ とおく。$S(n)$ を p と a で表せ。
(2) 相異なる素数 p, q，正の整数 a, b に対し，$n=p^a$，$m=q^b$ とおく。このとき $S(mn)=S(n)S(m)$ が成立することを証明せよ。
(3) 正の整数 a について 2^a-1 が素数とする。このとき，$n=2^{a-1}(2^a-1)$ とおくと，$S(n)=2n$

フェルマー数

$2^{2^n}+1$（n は負でない整数）の形の整数をフェルマー数といい，これが素数であるとき，フェルマー素数という。n 番目のフェルマー数を F_n と記すことにする。このとき

$F_0=2^1+1=3$，$F_1=2^2+1=5$，$F_2=2^4+1=17$，$F_3=2^8+1=257$，

$F_4=2^{16}+1=65537$

$n=1, 2, 3, 4$ のとき，F_n は素数であることが知られている。

$$F_5=2^{32}+1=4294967297=641\times 6700417$$

と因数分解できることを，オイラーが示した。
$F_0 \sim F_4$ 以外のフェルマー素数が存在する可能性は低いと考えられている。(未解決問題)
F_n が素数であるとき，正 F_n 角形は作図可能であることが知られている。

入試問題　[千葉大学]
a, b は 2 以上の整数とする。
(1) a^b-1 が素数ならば，$a=2$ であり，b は素数であることを証明せよ。
(2) a^b+1 が素数ならば，$b=2^c$（c は整数）と表せることを証明せよ。

□

連続する整数の積

${}_nC_r=\dfrac{n(n-1)(n-2)\cdots\cdots(n-r+1)}{r!}$ が整数であることより，$n(n-1)(n-2)\cdots\cdots(n-r+1)$ は $r!$ で割り切れる。一般に，連続する r 個の整数の積は $r!$ で割り切れる。

例　n が奇数のとき，n^3-n が 24 の倍数であることを証明してみよう。
n が奇数のとき，整数 k を用いて $n=2k+1$ と表される。したがって

$$n^3-n=(2k+1)^3-(2k+1)=8k^3+12k^2+4k=4(2k^3+3k^2+k)$$

ここで,

$$2k^3+3k^2+k=2(k^3-k)+3k^2+3k=2(k-1)k(k+1)+3k(k+1)$$

$(k-1)k(k+1)$は連続する 3 個の整数の積であるから 3 の倍数，$k(k+1)$は連続する 2 個の整数の積であるから 2 の倍数である。よって，$2(k-1)k(k+1)+3k(k+1)$は 6 の倍数であるから，$2k^3+3k+4$ は 6 の倍数である。したがって，n^3-n は 24 の倍数である。

入試問題　[北海道教育大学]

整数nに対して，$2n^3-3n^2+n$ は 6 の倍数であることを示せ。

エジプト分数

分子が 1 である分数を単位分数と呼ぶ。エジプト分数とは，有理数をいくつかの異なる単位分数の和に表したもの，または，その方式をいう。ヨーロッパでは中世まで広く使われていたようである。例えば，今日では$\frac{2}{5}$と表す分数を$\frac{1}{3}+\frac{1}{15}$と表した。また，$\frac{3}{5}$は単位分数の和として $\frac{1}{5}+\frac{1}{5}+\frac{1}{5}$ と表せるが，エジプト分数では同じ単位分数を繰り返し用いることなく，$\frac{1}{2}+\frac{1}{10}$のように表す。6 個のパンを 10 人で分けるとき，1 人分は $\frac{3}{5}=\frac{1}{2}+\frac{1}{10}$ 個である。6 個のパンをそれぞれ 5 等分して 3 切れずつ取るよりも，5 個を 2 等分して 1 切れずつ取り，残りの 1 個を 10 等分する方が簡明である。

命題　任意の 1 より小さい正の有理数はエジプト分数で表される。

証明（有理数に対して，それ以下の最大の単位分数を繰り返し取る算法で，強欲算法という）

1 より小さい正の有理数$\frac{x}{y}$に対して

$$y=xq-r,\quad 0\leqq r<x$$

となる，整数q, rを求めると

$$\frac{x}{y}=\frac{xq}{yq}=\frac{y+r}{yq}=\frac{1}{q}+\frac{r}{yq}\qquad \text{これにおいて，}\ 0\leqq\frac{r}{yq}<\frac{1}{q}$$

このとき，$0\leqq r<x$であるから，$r\neq 0$の場合は，$\frac{r}{yq}$に対して上記の操作を繰り返せば，遂には$r=0$となる。

□

1 以上の正の有理数$\frac{x}{y}$は，前処理として，$\frac{x}{y}-\frac{1}{2}-\frac{1}{3}-\frac{1}{4}-\cdots\cdots$と引いていき，負になる直前

でこの処理をやめ，その後上記の命題の操作を行えば，エジプト分数で表すことができる。
また，1 つの有理数をエジプト分数で表すとき，その表し方が無数にあることは，恒等式
$\frac{1}{n}=\frac{1}{n+1}+\frac{1}{n(n+1)}$ から分かる。

例題　p を素数とする。x, y に関する方程式

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{p}$$

を満たす正の整数の組 (x, y) をすべて求めよ。[2009 お茶の水女子大学]

解

与えられた等式より

$$\frac{x+y}{xy}=\frac{1}{p}$$
$$xy-p(x+y)=0$$
$$(x-p)(y-p)=p^2$$

ここで　$\frac{1}{x}<\frac{1}{x}+\frac{1}{y}=\frac{1}{p}$　であるから，$x-p>0$，同様にして，$y-p>0$

p は素数であるから，

$$(x-p, y-p)=(1, p^2), (p^2, 1), (p, p)$$

ゆえに，

$$(x, y)=(p+1, p^2+p), (p^2+p, p+1), (2p, 2p)$$

□

入試問題　[1997 東京工業大学]

次の問いに答えよ。

(1)　$\frac{1}{x}+\frac{1}{y}=\frac{1}{2}$ を満たす自然数 x, y の組 (x, y) をすべて求めよ。

(2)　n を自然数，r を正の有理数とする。このとき $\sum_{k=1}^{n}\frac{1}{x_k}=r$ をみたす自然数 x_k の組 $(x_1, \cdots\cdots, x_n)$ の個数は有限であることを示せ。

ペル方程式

n を平方数でない自然数として，整数 x, y についての次の形の不定方程式を，ペル方程式という。

$x^2-ny^2=\pm1$

ただし，ペル自身は，この方程式とは無関係で，オイラーがこの方程式を研究したのはペルであると誤解してペル方程式と名付けたため，そう呼ばれ続けているそうである。

方程式 $x^2-ny^2=1$ だけをペル方程式ということもある。方程式 $x^2-ny^2=1$ は，自明な解 $(x=1,\ y=0)$ 以外の解を必ず持つことが知られている。

ペル方程式は，数学の色々な所で現れる。例えば，三角数にも四角数にもなる数を求めるには，$\dfrac{m(m+1)}{2}=n^2$ を解けばよいが，変形すると $(2m+1)^2-2(2n)^2=1$ となり，

$2m+1=x,\ 2n=y$ おくと，方程式 $x^2-2y^2=1$ が得られる。

例題 [1985 東京工業大学]

二つの条件

（ⅰ）$a^2-2b^2=1$ または $a^2-2b^2=-1$　　（ⅱ）$a+b\sqrt{2}>0$

をみたす任意の整数 a,b から得られる実数 $g=a+b\sqrt{2}$ 全体の集合を G とする。

1 より大きい G の元のうち最小のものを u とする。

(1) u を求めよ。

(2) 整数 n と G の元 g に対し，gu^n は G の元であることを示せ。

(3) G の任意の元 g は適当な整数 m によって，$g=u^m$ と書かれることを示せ。

解答 (1) $u=a+b\sqrt{2}$ とおく。

$a^2-2b^2=1$ または $a^2-2b^2=-1$ であるから，

$$\left|a^2-2b^2\right|=1 \quad \text{よって} \quad \left|a+b\sqrt{2}\right|\cdot\left|a-b\sqrt{2}\right|=1$$

$a+b\sqrt{2}>1$ であるから，$\left|a-b\sqrt{2}\right|<1$　すなわち　　$-1<a-b\sqrt{2}<1$

$a+b\sqrt{2}>1$，$a-b\sqrt{2}>-1$ より $a>0$

$a+b\sqrt{2}>1$，$-a+b\sqrt{2}>-1$ より $b>0$

したがって，$a>0,b>0$ であるから，$a\geqq1,b\geqq1$。よって，$u=a+b\sqrt{2}\geqq1+\sqrt{2}$

$1^2-2\cdot1^2=-1$ より，$1+\sqrt{2}\in G$ であり，u は 1 より大きい G の元のうち最小のものであるから，$a=1,b=1$ で，$u=1+\sqrt{2}$

(2) まず，G の任意の 2 元 $g_1 = a_1 + b_1\sqrt{2}$，$g_2 = a_2 + b_2\sqrt{2}$ に対して，$g_1 g_2 \in G$ を示す。

$$g_1 g_2 = (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1 a_2 + 2b_1 b_2) + (a_1 b_2 + b_1 a_2)\sqrt{2}$$

であり

$$(a_1 a_2 + 2b_1 b_2)^2 - 2(a_1 b_2 + b_1 a_2)^2 = {a_1}^2 {a_2}^2 + 4{b_1}^2 {b_2}^2 - 2{a_1}^2 {b_2}^2 - 2{b_1}^2 {a_2}^2$$

$$= ({a_1}^2 - 2{b_1}^2)({a_2}^2 - 2{b_2}^2)$$

ここで，${a_1}^2 - 2{b_1}^2 = 1$ または ${a_1}^2 - 2{b_1}^2 = -1$，${a_2}^2 - 2{b_2}^2 = 1$ または ${a_2}^2 - 2{b_2}^2 = -1$

であるから　　$({a_1}^2 - 2{b_1}^2)({a_2}^2 - 2{b_2}^2) = 1$　または　$({a_1}^2 - 2{b_1}^2)({a_2}^2 - 2{b_2}^2) = -1$

ゆえに，$g_1 g_2 \in G$ である。
これを繰り返し用いると，n が負でない整数のとき，$gu^n \in G$ が得られる。
また，$u^{-1} = \dfrac{1}{1+\sqrt{2}} = -1 + \sqrt{2}$ であり，$(-1)^2 - 2 \cdot 1^2 = -1$ であるから，$u^{-1} \in G$

したがって，n が正の整数のとき，$g\left(u^{-1}\right)^n \in G$ であるから，$gu^{-n} \in G$

以上より，任意の整数 n に対し，$gu^n \in G$

(3) $u > 1$ であるから，整数 n が増加すれば，u^n は増加し，$\lim_{n\to\infty} u^n = \infty$, $\lim_{n\to-\infty} u^n = 0$ である。

任意の $g \in G$ は $g > 0$ であるから，$u^m \leqq g < u^{m+1}$ となる整数 m が存在する。
3 辺を，u^m で割って，$1 \leqq gu^{-m} < u$
ここで，(2)より $gu^{-m} \in G$ であり，$1 < gu^{-m}$ と仮定すると u の最小性に反するから，$gu^{-m} = 1$
ゆえに，$g = u^m$

入試問題　[2015 早稲田大学]
整数 x, y が　$x^2 - 2y^2 = 1$　をみたすとき，次の問いに答えよ。

(1) 整数 a, b, u, v が $(a + b\sqrt{2})(x + y\sqrt{2}) = u + v\sqrt{2}$ をみたすとき，u, v を a, b, x, y で表せ。

さらに，$a^2 - 2b^2 = 1$ のとき，$u^2 - 2v^2$ の値を求めよ。ともに答のみでよい。

(2) $1 < x + y\sqrt{2} \leqq 3 + 2\sqrt{2}$ のとき，$x = 3, y = 2$ となることを示せ。

(3) 自然数nに対して，$\left(3+2\sqrt{2}\right)^{n-1} < x+y\sqrt{2} \leqq \left(3+2\sqrt{2}\right)^{n}$ のとき，$x+y\sqrt{2} = \left(3+2\sqrt{2}\right)^{n}$ を示せ。

註　例えば，$\left(3+2\sqrt{2}\right)^{2} = 17+12\sqrt{2} = (2\cdot 8+1)+2\cdot 6\sqrt{2}$ より，$m=8, n=6$ は方程式 $\dfrac{m(m+1)}{2} = n^{2}$ の整数解である。

入試総合問題

[2018　京都大学]

n^3-7n+9 が素数となるような整数 n をすべて求めよ。

[2018　東京工業大学]

(1) $35x+91y+65z=3$ を満たす整数の組$(x,\ y,\ z)$を 1 組求めよ。

(2) $35x+91y+65z=3$ を満たす整数の組$(x,\ y,\ z)$の中で x^2+y^2 の値が最小となるもの，およびその最小値を求めよ。

[2018　一橋大学]

正の整数 n の各位の数の和を $S(n)$ で表す。たとえば

$$S(3)=3,\ S(10)=1+0=1,\ S(516)=5+1+6=12$$

である。

(1)　$n \geqq 10000$ のとき，$n>30S(n)+2018$ を示せ。

(2)　$n=30S(n)+2018$ を満たす n を求めよ。

[2018　東京大学　理系]

数列 $a_1, a_2, \cdots\cdots$ を $a_n=\dfrac{{}_{2n+1}C_n}{n!}$ $(n=1, 2, \cdots\cdots)$ で定める。

(1)　$n \geqq 2$ とする。$\dfrac{a_n}{a_{n-1}}$ を既約分数 $\dfrac{q_n}{p_n}$ として表したときの分母 $p_n \geqq 1$ と分子 q_n を求めよ。

(2)　a_n が整数となる $n \geqq 1$ をすべて求めよ。

[センター試験試作問題]

和が 600，最小公倍数が 5772 である 2 つの自然数 $a, b\ (a>b)$ がある。

a, b の最大公約数を G とし，$a=a'G, b=b'G$ とすると，a', b' の最大公約数は［　　］である。

また，$a'G+b'G=600, a'b'G=5772$ である。ここで，600，5772 を素因数分解すると

$$600=2^3\cdot 3\cdot 5^2$$

$$5772=2^{\square}\cdot\overline{\square}\cdot 13\cdot 37$$

であるから $G=$［　　］である。したがって，$a=$［　　］，$b=$［　　］である。

このとき，$G=ma+nb$ を満たす整数 m, n の組のうち，m が正で最小であるものは，

$m=$□，$n=$□である。

[2016 東京工業大学]

nを2以上の自然数とする。

(1) nが素数または4のとき，$(n-1)!$はnで割り切れないことを示せ。

(2) nが素数でなくかつ4でもないとき，$(n-1)!$はnで割り切れることを示せ。

[2016 京都大学]

素数p, qを用いてp^q+q^pと表される素数をすべて求めよ。

[2014 一橋大学]

$a-b-8$と$b-c-8$が素数となるような素数の組(a, b, c)をすべて求めよ。

[2015 東京大学]

mを2015以下の正の整数とする。${}_{2015}C_m$が偶数となる最小のmを求めよ。

[2007 大阪府立大学]

nは2以上の自然数とする。n桁の自然数mを

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

と表す。ただし，a_k $(k=1, 2, \cdots\cdots, n-1)$は0以上9以下の整数であり，$a_n$は1以上9以下の自然数とする。次の各問いに答えよ。

(1) $\dfrac{1}{11}\displaystyle\sum_{k=1}^{n}(-1)^{k-1}a_k$が整数であることはmが11で割り切れるための必要十分条件であることを証明せよ。

(2) 自然数 $\ell=9876543210123456789$ は11で割り切れるかどうか(1)を利用して判定せよ。

(3) $n=19$とする。自然数mは

$$a_{19}=a_1=9,\qquad a_{18}=a_2=8,\qquad a_{17}=a_3=7,\qquad a_{10}=0$$

かつ

$$a_{20-k}=a_k\ (\mathrm{k}=4,\ 5,\ 6,\ 7,\ 8,\ 9)$$

で表されているとする。ただし，$a_4, a_5, a_6, a_7, a_8, a_9$は相違なる1以上6以下の自然数である。このとき，自然数mのうちで11で割り切れるものはいくつあるか答えよ。

[2012　東京大学]

n を 2 以上の整数とする。自然数（1 以上の整数）の n 乗になる数を n 乗数と呼ぶことにする。以下の問いに答えよ。

（1）連続する 2 個の自然数の積は n 乗数ではないことを示せ。

（2）連続する n 個の自然数の積は n 乗数ではないことを示せ。

[2016 慶應義塾大学]

i を虚数単位とする。次の事実がある。

事実 F

a, b を互いに素な正の整数とする。このとき，

$$\left(\cos\frac{2a}{b}\pi+i\sin\frac{2a}{b}\pi\right)^k=\cos\frac{2}{b}\pi+i\sin\frac{2}{b}\pi$$

となる整数 k が存在する。

(1) 等式

$$\left(\cos\frac{4}{5}\pi+i\sin\frac{4}{5}\pi\right)^k=\cos\frac{2}{5}\pi+i\sin\frac{2}{5}\pi$$

を満たす最小の正の整数 k は［　　］である。

(2) a, b を互いに素な正の整数とし，集合 P を

$$P=\left\{z\ \middle|\ z\text{は整数}k\text{を用いて}\left(\cos\frac{2a}{b}\pi+i\sin\frac{2a}{b}\pi\right)^k\text{と表される複素数}\right\}$$

で定める。事実 F を考慮すると，集合 P の要素の個数 $n(P)$ は［　　］である。

(3) 事実 F を証明しなさい。

(4) a_1, b_1 を互いに素な正の整数とし，a_2, b_2 も互いに素な正の整数としする。集合 Q_1, Q_2 を，

$$Q_1=\left\{z\ \middle|\ z\text{は整数}k\text{を用いて}\left(\cos\frac{2a_1}{b_1}\pi+i\sin\frac{2a_1}{b_1}\pi\right)^k\text{と表される複素数}\right\}$$

$$Q_2=\left\{z\ \middle|\ z\text{は整数}k\text{を用いて}\left(\cos\frac{2a_2}{b_2}\pi+i\sin\frac{2a_2}{b_2}\pi\right)^k\text{と表される複素数}\right\}$$

で定め，集合 R を

R＝{z | z は集合Q_1の要素と集合Q_2の要素の積で表される複素数}

で定める。b_1とb_2が互いに素ならば，集合 R の要素の個数$n(R)$は［　　］である。

b_1とb_2が互いに素でないとき，それらの最大公約数をdとすれば，集合 R の要素の個数$n(R)$は［　　］である。

研究　フェルマーの小定理の別証

補題

p を素数とし，aをpの倍数でない整数とするとき，

集合$\{a, 2a, 3a, \cdots, (p-1)a\}$は，全体として集合$\{1, 2, 3, \cdots, p-1\}$と$p$を法として合同である。

証明

i, jを$1 \leqq i \leqq p-1$，$1 \leqq j \leqq p-1$を満たす整数として

$$ia \equiv ja \pmod{p}$$

が成り立つとする。すると，aとpは互いに素であるから，

$$i \equiv j \pmod{p}$$

$1 \leqq i \leqq p-1$，$1 \leqq j \leqq p-1$であるから

$$i = j$$

対偶を考えると，$i \neq j$ならば，iaとjaは，pを法として合同でない。

よって，$p-1$個の整数 $a, 2a, 3a, \cdots, (p-1)a$から取り出したどの 2 つも，$p$を法として合同ではない。また，$a, 2a, 3a, \cdots, (p-1)a$はどれも 0 と合同でない。

ゆえに，集合$\{a, 2a, 3a, \cdots, (p-1)a\}$は，全体として集合$\{1, 2, 3, \cdots, p-1\}$と$p$を法として合同である。

□

フェルマーの小定理

pを素数とし，aをpの倍数でない整数(aとpは互いに素)とするとき，

$$a^{p-1} \equiv 1 \pmod{p}$$

証明

補題により，集合$\{a, 2a, 3a, \cdots, (p-1)a\}$は，全体として集合$\{1, 2, 3, \cdots, p-1\}$と$p$を法として合同であるから

$$a \cdot 2a \cdot 3a \cdots\cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots\cdots (p-1) \pmod{p}$$

よって

$$(p-1)! \times a^{p-1} \equiv (p-1)! \times 1 \pmod{p}$$

ここで，pは素数であるから，$1, 2, 3, \cdots, p-1$とpは互いに素である。よって，$(p-1)!$とpは互いに素であるから，

$$a^{p-1} \equiv 1 \pmod{p}$$

□

フェルマーの小定理は，$a^{p-1} \equiv 1$ の両辺に a を掛けて

$$a^{p} \equiv a \pmod{p}$$

と表すこともある。この形では，a が p の倍数のときも成り立つ。

研究　オイラーの定理 （フェルマーの小定理の拡張）

補題　a と n は互いに素な整数であるとし，$m \leqq n$ で，n と互いに素である自然数 m の集合を $M=\{m_1, m_2, m_3, \cdots, m_N\}$ とする。このとき，集合 $A=\{m_1a, m_2a, m_3a, \cdots, m_Na\}$ は，全体として集合 M と n を法として合同である。

証明

m_i と n は互いに素であり，a と n は互いに素であるから，m_ia と n は互いに素である。

よって，m_ia は M の要素のいずれかと n を法として合同である。…①

また，i, j を $1 \leqq i \leqq N, 1 \leqq j \leqq N$ を満たす整数として

$$m_ia \equiv m_ja \pmod{n}$$

が成り立つとする。すると，a と n は互いに素であるから，

$$m_i \equiv m_j \pmod{n}$$

ここで　$0 < m_i < n$，$0 < m_j < n$ であるから，$m_i = m_j$ すなわち $i = j$

対偶を考えると，$i \neq j$ ならば，m_ia と m_ja は，n を法として合同でない。…②

①，②より，集合 A は，全体として集合 M と n を法として合同である。

□

定理 9 （オイラーの定理）

n を自然数，a を整数とし，a と n は互いに素であるとするとき，

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

証明

$N=\varphi(n)$ とすると，補題により，集合 $\{m_1, m_2, m_3, \cdots, m_N\}$ は，全体として集合 $\{m_1a, m_2a, m_3a, \cdots, m_Na\}$ と n を法として合同であるから

$$m_1a \cdot m_2a \cdot m_3a \cdots\cdots m_Na \equiv m_1 \cdot m_2 \cdot m_3 \cdots\cdots m_N \pmod{n}$$

よって

$$m_1 \cdot m_2 \cdot m_3 \cdots\cdots m_N \cdot a^N \equiv m_1 \cdot m_2 \cdot m_3 \cdots\cdots m_N \cdot 1 \pmod{n}$$

ここで，$m_1, m_2, m_3, \cdots, m_N$ はそれぞれ n と互いに素であるから，$m_1 \cdot m_2 \cdot m_3 \cdots\cdots m_N$ と n は互いに素である。よって

$$a^N \equiv 1 \pmod{n} \quad \text{すなわち} \quad a^{\varphi(n)} \equiv 1 \pmod{n}$$

□

定理 10　オイラーの φ 関数の乗法性

$(m, n) = 1$ ならば $\varphi(mn) = \varphi(m)\varphi(n)$

証明

$$r = \varphi(m),\ s = \varphi(n),\ t = \varphi(mn)$$

として，

$u_1, u_2, \cdots\cdots, u_r$ を $1, 2, \cdots\cdots, m$ の中で m と互いに素な整数

$v_1, v_2, \cdots\cdots, v_s$ を $1, 2, \cdots\cdots, n$ の中で n と互いに素な整数

$w_1, w_2, \cdots\cdots, w_t$ を $1, 2, \cdots\cdots, mn$ の中で mn と互いに素な整数

とする。ここで，$(w_k, mn) = 1$ であるから，$(w_k, m) = 1$ かつ $(w_k, n) = 1$

よって，　$w_k \equiv u_i \pmod{m}$，　$w_k \equiv v_j \pmod{n}$

となる u_i と v_j が，それぞれ，ただ一つずつ存在する。

w_k の個数は t で，組 (u_i, v_j) の個数は $r \cdot s$ であるから

$$t \leqq r \cdot s \quad \cdots①$$

逆に，組 (u_i, v_j) に対して，中国人剰余定理から

$$x \equiv u_i \pmod{m}, \quad x \equiv v_j \pmod{n}$$

となる x が mn を法としてただ一つ存在する。ここで，u_i と v_j は，それぞれ，m と n と互いに素であるから，x は m とも n とも互いに素である。よって x は mn と互いに素である。したがって，$x = w_k$ となる k がただ 1 つ存在するから

$$t \geqq r \cdot s \quad \cdots②$$

①，②より

$$t = r \cdot s \quad \text{すなわち} \quad \varphi(mn) = \varphi(m)\varphi(n)$$

□

これまでのことから，次が成り立つ。

自然数nを素因数分解し $n = p_1^{e_1} \cdot p_2^{e_2} \cdots\cdots p_r^{e_r}$ とする。このとき，

$$\varphi(n) = \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2}) \cdots\cdots \varphi(p_r^{e_r})$$

$$= (p_1^{e_1} - p_1^{e_1-1}) \cdot (p_2^{e_2} - p_2^{e_2-1}) \cdots\cdots (p_r^{e_r} - p_r^{e_r-1})$$

$$= p_1^{e_1} \cdot p_2^{e_2} \cdots\cdots p_r^{e_r} \cdot \left(1-\frac{1}{p_1}\right) \cdot \left(1-\frac{1}{p_2}\right) \cdots\cdots \left(1-\frac{1}{p_r}\right)$$

$$= n \cdot \left(1-\frac{1}{p_1}\right) \cdot \left(1-\frac{1}{p_2}\right) \cdots\cdots \left(1-\frac{1}{p_r}\right)$$

□

オイラーの定理とφ関数の乗法性から，次の公式が得られる。

公式　p, qを異なる素数とし，aをpqと互いに素な整数とするとき，

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$$

例題　3^{100}を35で割った余りを求めよ。

解　$35 = 5 \times 7$ より，$\varphi(35) = (5-1) \times (7-1) = 24$ であるから，$3^{24} \equiv 1 \pmod{35}$

よって，$3^{100} = 3^{24 \times 4 + 4} = \left(3^{24}\right)^4 \times 3^4 \equiv 1^4 \times 81 = 35 \times 2 + 11 \equiv 11 \pmod{35}$

初等整数論の初歩　解答

[1992 一橋大学]

n^2 と $2n+1$ の最大公約数を d とすると，整数 k, l を用いて，次のように表される。

$$n^2 = kd \quad \cdots① \qquad 2n+1 = ld \quad \cdots②$$

①より，$(2n)^2 = 4kd \quad \cdots③$

②より，$2n = ld - 1 \quad \cdots④$

④を③に代入して，$(ld-1)^2 = 4kd$

よって $(4k - l^2 d + 2l)d = 1$

$4k - l^2 d + 2l$ は整数，d は自然数であるから，$d = 1$

したがって，n^2 と $2n+1$ は互いに素である。

別解　n と $n+1$ は互いに素であるから，素因数分解の一意性により n^2 と $(n+1)^2$ は互いに素。

したがって，n^2 と $(n+1)^2 - n^2$ は互いに素である。

[東京女子大学]

3 で割り切れる整数全体の集合を D とする。

$z \in C$ ならば,

$$z = x + y,\ x = 9l,\ y = 15m \quad (l, m \text{ は整数})$$

と表されるから,

$$z = 9l + 15m = 3(3l + 5m)$$

よって，$z \in D$ であるから，$C \subset D$

また，$z \in D$ ならば，$z = 3k$ （k は整数）と表される。ここで

$$9 \times 2 + 15 \times (-1) = 3$$

であるから，両辺を k 倍すると

$$9 \times 2k + 15 \times (-k) = 3k$$

よって，$x = 9 \times 2k,\ y = 15 \times (-k)$ とおくと，$x \in A,\ y \in B$ であり，$z = x + y$ となる。

したがって，$z \in C$ であるから，$D \subset C$

ゆえに，$C = D$

[2016 センター試験]

(1) 92 と 197 にユークリッドの互除法の計算を行うと

$$197 = 92 \cdot 2 + 13 \quad \cdots①$$

$$92 = 13 \cdot 7 + 1 \quad \cdots②$$

$$13 = 1 \cdot 13 + 0$$

よって，92 と 197 の最大公約数は 1 である。

また，②より　　$1=92-13\cdot 7$　　…③

①より　　$13=197-92\cdot 2$　…④

④を③の右辺に代入して

$$1=92-(197-92\cdot 2)\cdot 7$$

すなわち

$$92\cdot 15+197\cdot(-7)=1 \qquad \cdots⑤$$

よって，$x=15,\ y=-7$ は不定方程式

$$92x+197y=1 \qquad \cdots⑥$$

の整数解の 1 つである。⑥－⑤より

$$92(x-15)+197(y+7)=0$$

したがって

$$92(x-15)=197(-y-7)$$

92 と 197 は互いに素であるから，k を整数として

$$x-15=197k,\quad -y-7=92k$$

すなわち

$$x=197k+15,\quad y=-92k-7$$

と表される。

よって，x の絶対値は $k=0$ のとき最小値 $x=15$ をとる。このとき，$y=-7$ である。

次に⑤の両辺を 10 倍して

$$92\cdot 150+197\cdot(-70)=10 \qquad \cdots⑦$$

よって，$x=150,\ y=-70$ は不定方程式

$$92x+197y=10 \qquad \cdots⑧$$

の整数解の 1 つである。（特殊解）

⑧－⑦より

$$92(x-150)+197(y+70)=0$$

したがって

$$92(x-150)=197(-y-70) \qquad \cdots⑨$$

92 と 197 は互いに素であるから，ℓ を整数として

$$x-150=197\ell,\quad -y-70=92\ell$$

すなわち，

$$x=197\ell+150,\quad y=-92\ell-70$$

と表される。

よって，x の絶対値は，$\ell=-1$ のとき最小値 $x=-47$ をとる。このとき，$y=22$ である。

[2008 奈良県立医大]

(1) $x-q, x-2q, \cdots\cdots, x-pq$ を p で割った余りの中に，等しいものがあると仮定する。
すなわち，i, j を $1 \leqq i < j \leqq p$ を満たす整数とし，$x-iq$ と $x-jq$ を p で割った商をそれぞれ k_i, k_j 余りを共に r とする。すると

$$x-iq = pk_i + r \cdots①, \quad x-jq = pk_j + r \cdots②$$

と表されるから，①－②より

$$(j-i)q = p(q_i - q_j) \quad \cdots③$$

p, q は互いに素であるから，③より $j-i$ は p の倍数である。
ところが，$1 \leqq i < j \leqq p$ より $1 \leqq j-i \leqq p-1$ であるから，$j-i$ は p の倍数とは成らない。
よって，矛盾する。
ゆえに，$x-q, x-2q, \cdots\cdots, x-pq$ を p で割った余りは全て異なる。
(2) (1)より p 個の異なる数 $x-q, x-2q, \cdots\cdots, x-pq$ を p で割った余りは全て異なり，余りは 0 から $p-1$ までの p 種類しかないから，$x-q, x-2q, \cdots\cdots, x-pq$ を p で割った余りの中に 0 となるものがある。それを $x-bq$ $(1 \leqq b \leqq p)$ とすると，a を整数として，

$$x-bq = ap \quad \text{よって} \quad x = ap+bq$$

ここで，$1 \leqq b \leqq p$ より $ap = x-bq \geqq x-pq > 0$ であるから，$a > 0$
すなわち，正の整数 a, b を用いて，$x = ap+bq$ と表される。

[2004 早稲田大学]

$n = 1, 4$ は素数でない。
$n = 2$ のとき，3 数は 2，4，6 となるので，すべてが素数とはならない。
よって，$n \geqq 5$ とし，n が素数であると仮定する。
n が素数となるのは，3 の倍数でないときであるから，2 以上の自然数 k を用いて $n = 3k-1$ または $n = 3k+1$ と表される。
$n = 3k-1$ のとき
$n+4 = 3k+3 = 3(k+1)$ であり，$k \geqq 2$ であるから，$3(k+1) \geqq 9$
よって，$n+4$ は素数ではない。
$n = 3k+1$ のとき
$n+2 = 3k+3 = 3(k+1)$ であり，$k \geqq 2$ であるから，$3(k+1) \geqq 9$
よって，$n+2$ は素数ではない。
以上より，$n, n+2, n+4$ がすべて素数であるのは $n = 3$ の場合の 3，5，7 だけである。

[九州大学]

a^2 と b^2 が互いに素でないと仮定すると，a^2 と b^2 は共通な素因数 p を持つ。このとき，

a^2 は p の倍数であるから，a は p の倍数である。

b^2 は p の倍数であるから，b は p の倍数である。

これは，a と b が互いに素であることに矛盾する。

ゆえに，a^2 と b^2 は互いに素である。

[2005 東京大学]

$a^2-a=a(a-1)$ ，$10000=2^4\times5^4=16\times625$

$a(a-1)$ は 10000 の倍数であり，a と $a-1$ は互いに素で，a は奇数，$a-1$ は偶数で，

$3\leqq a\leqq9999$ であるから，奇数 k と整数 l を用いて，

$$a=625k,\ a-1=16l$$

と表される。よって

$$625k-16l=1 \quad \cdots①$$

ここで，$625=16\times39+1$ であるから，（ユークリッドの互除法）

$$625\cdot1-16\cdot(-39)=1 \quad \cdots②$$

①－②より

$$625(k-1)-16(l+39)=0 \quad \text{すなわち} \quad 625(k-1)=16(l+39)$$

625 と 16 は互いに素であるから，整数 m を用いて $k-1=16m$ と表される。

よって，$k=16m+1$ であるから，

$$a=625(16m+1)=10000m+625$$

$3\leqq a\leqq9999$ であるから，$m=0$ であり，$a=625$

[1999　一橋大学]

(1) $\dfrac{1}{p}+\dfrac{1}{q}=\dfrac{1}{r}$　より　$\dfrac{q+p}{pq}=\dfrac{1}{r}$　よって　$pq=(p+q)r$ …①

ここで，整数 a, b の最大公約数を (a, b) で表すことにして，互除法の原理を用いる。すると

p, q は異なる素数であるから

$$(p+q,\ p)=(p+q-p,\ p)=(q,\ p)=1$$

$$(p+q,\ q)=(p+q-q,\ q)=(p,\ q)=1$$

よって，①より r は p の倍数かつ q の倍数である。

したがって，r は pq の倍数であるから k を整数として，$r=kpq$ と置ける。

これを①に代入して

$$pq=(p+q)kpq$$

よって

$$1=(p+q)k$$

p, q は素数で，$p<q$ であるから，$p+q \geqq 2+3=5$。したがって，この式は矛盾する。

ゆえに，$\dfrac{1}{p}+\dfrac{1}{q}=\dfrac{1}{r}$ を満たす整数 r は存在しない。

(2) $\dfrac{1}{p}-\dfrac{1}{q}=\dfrac{1}{r}$ より $\dfrac{q-p}{pq}=\dfrac{1}{r}$ よって $pq=(q-p)r$ …②

p, q は異なる素数であるから

$$(q-p,\ p)=(q-p+p,\ p)=(q,\ p)=1$$
$$(q-p,\ q)=(q-p-q,\ q)=(-p,\ q)=1$$

よって，②より r は p の倍数かつ q の倍数である。

したがって，r は pq の倍数であるから k を整数として，$r=kpq$ …③と置ける。

これを②に代入して

$$pq=(q-p)kpq \quad \text{よって} \quad 1=(q-p)k$$

ここで，$q-p$ は正の整数，k は整数であるから，$q-p=1$

したがって，$q=p+1$

これより，p, q の 1 つは偶数である。

ここで，q, p は素数であり，$q>p$ であるから，$p=2, q=3$

このとき，②より $r=6$ である。

したがって，$\dfrac{1}{p}-\dfrac{1}{q}=\dfrac{1}{r}$ を満たす整数 r が存在するのは，$p=2, q=3$ のときに限る。

[千葉大学]

(1) 5 以上の自然数は，自然数 n を用いて

$$6n-1,\ 6n,\ 6n+1,\ 6n+2,\ 6n+3,\ 6n+4$$

のいずれかの形に表される。ここで

$$6n=2\cdot 3n \qquad (3n \geqq 3)$$
$$6n+2=2(3n+1) \quad (3n+1 \geqq 4)$$
$$6n+3=3(2n+1) \quad (2n+1 \geqq 3)$$
$$6n+4=2(3n+2) \quad (2n+1 \geqq 3)$$

であるから，これらは素数でない。

ゆえに，5 以上の素数は，ある自然数 n を用いて $6n+1$ または $6n-1$ の形に表される。

(2) $6N-1$ は奇数であるから，2 を素因数にもたない。

また，$6N-1$ は 3 で割り切れないから，3 を素因数にもたない。

したがって，$6N-1$の素因数は5以上であるから，$6N-1$の素因数はすべて，自然数nを用いて$6n+1$または$6n-1$の形に表される。

ここで，$6N-1$の素因数のすべてが$6n+1$の形であると仮定し，素因数を$6n_k+1 \quad (k=1,2,3,\cdots,m)$

とすると

$$6N-1=(6n_1+1)(6n_2+1)\cdots\cdots(6n_m+1)$$

このとき，左辺は6で割ると5余り，右辺は6で割ると1余るから矛盾する。

ゆえに，$6N-1$の素因数の少なくとも1つは$6n-1$の形であるから，$6N-1$は$6n-1$の形で表される素数を約数にもつ。

(3) $6n-1$の形の素数が有限個だけしか存在しないと仮定し，それらを小さい順に$5,11,\cdots,p$とする。

このとき，

$$M=6(5\times11\times\cdots\times p)-1$$

とおくと，Mは$6N-1$の形に表されるから，(2)より$6n-1$の形の素数qを約数にもつ。

ところが，Mは，5，11，…，pのいずれでも割り切れないから，qは5，11，…，pのいずれとも異なる。これは，$6n-1$の形の素数が5，11，…，pだけであるという仮定と矛盾する。

ゆえに，$6n-1$の形の素数は無限に多く存在する。

[2009 京都大学]

1からp^nまでの自然数のうち，p^k（$k=1,2,3,\cdots\cdots,n$）で割り切れるものは

$$1\cdot p^k,2\cdot p^k,\cdots\cdots,p^{n-k}\cdot p^k$$

のp^{n-k}個ある。よって，$(p^n)!$はpで$\sum_{k=1}^{n}p^{n-k}$回割り切れる。ここで

$$\sum_{k=1}^{n}p^{n-k}=\sum_{k=1}^{n}p^{k-1}=\frac{p^n-1}{p-1}$$

であるから，$(p^n)!$はpで$\dfrac{p^n-1}{p-1}$回割り切れる。

[2009 一橋大学]

$m^3+1^3=n^3+10^3$ より $m^3-n^3=999$

よって $(m-n)(m^2+mn+n^2)=3^3\cdot37$

これより，$m-n>0$である。ここで$m-n=a$とおくと，aは自然数であり

$$m^2+mn+n^2=(a+n)^2+(a+n)n+n^2=3n^2+3an+a^2$$

a が 3 の倍数のとき，$3n^2+3an+a^2$ は 3 の倍数であり，a が 3 の倍数でないとき，$3n^2+3an+a^2$ は 3 の倍数でない。

$$a(3n^2+3an+a^2)=3^3\cdot 37$$

であるから $a, 3n^2+3an+a^2$ はともに 3 の倍数である。

よって，

$$(a, 3n^2+3an+a^2)=(3, 3^2\cdot 37), (3^2, 3\cdot 37)$$

$a=3$ のとき

$$3n^2+3an+a^2=333$$
$$n^2+3n-108=0$$
$$(n+12)(n-9)=0$$

$n \geqq 2$ より　$n=9$

$m-n=3$ より，$m=12$

$a=9$ のとき

$$3n^2+3an+a^2=111$$
$$n^2+9n-10=0$$
$$(n-1)(n+10)=0$$

$n \geqq 2$ より，解はない。

以上より，$m=12$，$n=9$

[1995 京都大学]

7 を法とする合同(mod 7)で考える。

(1) n^7 が n と合同であることを示せばよい。

以下，複合同順とする。

自然数 n は 0，± 1，± 2，± 3 のいずれかと合同である。

$n \equiv 0$　のとき，$n^7 \equiv 0^7 \equiv 0 \equiv 0$

$n \equiv \pm 1$　のとき，$n^7 \equiv (\pm 1)^7 \equiv \pm 1 \equiv n$

$n \equiv \pm 2$　のとき，$n^7 \equiv (\pm 2)^7 \equiv \pm\left\{(2)^3\right\}^2 \cdot 2 \equiv \pm 8^2 \cdot 2 \equiv \pm 1^2 \cdot 2 \equiv \pm 2 \equiv n$

$n \equiv \pm 3$　のとき，$n^7 \equiv (\pm 3)^7 \equiv \pm\left\{(3)^2\right\}^3 \cdot 3 \equiv \pm 9^3 \cdot 3 \equiv \pm 2^3 \cdot 3 \equiv \pm 8 \cdot 3 \equiv \pm 1 \cdot 3 \equiv \pm 3 \equiv n$

したがって，$f\left(n^7\right) \equiv n$

別解　$n^7-n=n(n^6-1)=n(n^3+1)(n^3-1)=n(n+1)(n-1)(n^2-n+1)(n^2+n+1)$

この式の因数のうちの 1 つが 7 の倍数となることを示せばよい。

(2) $4\equiv -3, 5\equiv -2, 6\equiv -1$ であるから,

$$\sum_{k=1}^{7} k^n \equiv 1^n+2^n+3^n+4^n+5^n+6^n \equiv 1^n+2^n+3^n+(-3)^n+(-2)^n+(-1)^n$$

n が奇数のとき

$$1^n+2^n+3^n+(-3)^n+(-2)^n+(-1)^n \equiv 1^n+2^n+3^n-3^n-2^n-1^n=0$$

n が偶数のとき

$$1^n+2^n+3^n+(-3)^n+(-2)^n+(-1)^n \equiv 1^n+2^n+3^n+3^n+2^n+1^n=2(1^n+2^n+3^n)$$

$n=2$ のとき

$$2(1^n+2^n+3^n)=2(1^2+2^2+3^2)=2\cdot 14\equiv 2\cdot 0=0$$

$n=4$ のとき

$$2(1^n+2^n+3^n)=2(1^4+2^4+3^4)=2\cdot 98=2^2\cdot 7\cdot 7\equiv 0$$

$n=6$ のとき

$$2(1^n+2^n+3^n)=2(1^6+2^6+3^6)=2\cdot(1+8^2+9^3)\equiv 2\cdot(1+1^2+2^3)=20\equiv 6$$

よって, $n=6$ のとき

$$\sum_{k=1}^{7} k^n \equiv 6 \quad \text{であるから} \quad g(n)=3f\left(\sum_{k=1}^{7} k^n\right)=3\times 6=18$$

好きな自然数 n を 6 と決めますので 18 点下さい。

なお, (1)より $k^{n+6}=k^{n-1}k^7\equiv k^{n-1}k=k^n \quad (k=1, 2, \cdots\cdots, 7)$ であるから, $g(n+6)=g(n)$ が成り立ち, $g(n)$ の値は周期 6 で繰り返されるため, $n\geqq 8$ を考慮する必要はない。

[2001 京都大学]

$\mod 9$ で考える。

$n^9-n^3=n^3(n^6-1)=n^3(n^3+1)(n^3-1)$

$n\equiv 0$ のとき $n^3\equiv 0^3=0$

$n\equiv 1$ のとき $n^3-1\equiv 1^3-1=0$

$n\equiv 2$ のとき $n^3+1\equiv 8+1=9\equiv 0$

$n\equiv 3$ のとき $n^3\equiv 27=9\times 3\equiv 0$

$n\equiv 4$ のとき $n^3-1\equiv 64-1=63=9\times 7\equiv 0$

よって, $n=0, 1, 2, 3, 4$ のときは, $n^3(n^3+1)(n^3-1)\equiv 0$ となるから, $n^9-n^3\equiv 0$ である。

次に, $f(n)=n^9-n^3$ とおくと, $f(-n)=-f(n)$ が成り立つ。

$n\equiv 1, 2, 3, 4$ のとき, $f(n)\equiv 0$ であるから, $f(-n)=-f(n)\equiv 0$

したがって, $n\equiv -1, -2, -3, -4$ のとき, $f(n)\equiv 0$ となる。

任意の整数は $n=-4, -3, -2, -1, 0, 1, 2, 3, 4$ のいずれかと 9 を法として合同であるから,

任意の整数nに対し，n^9-n^3は9で割り切れる。

註　n^9-n^3は504で割り切れる。

[2017　センター試験追試改作]

(1) 不定方程式

$$21x+13=16y+12=96z+28$$

の整数解x, y, zを求めるには，2つの不定方程式

$$21x+13=16y+12 \qquad \cdots\cdots①$$

$$16y+12=96z+28 \qquad \cdots\cdots②$$

の共通の整数解を求めればよい。

①より，$-21x+16y=1$　…③

21と16にユークリッドの互除法の計算を行うと

$$21=16\cdot1+5 \qquad \cdots④$$

$$16=5\cdot3+1 \qquad \cdots⑤$$

よって，21と16の最大公約数は1である。

④より　$5=21-16\cdot1$

これを⑤に代入して

$$16=(21-16\cdot1)\cdot3+1$$

すなわち

$$-21\cdot3+16\cdot4=1 \quad \cdots⑥$$

③－⑥より

$$-21(x-3)+16(y-4)=0$$

$$21(x-3)=16(y-4)$$

21と16は互いに素であるから，③すなわち①のすべての解はsを整数として

$$x=3+16s,\ y=4+21s$$

と表される。次にこれらのうち，②を満たすものを求める。

②に$y=4+21s$を代入すると，

$$2z-7s=1 \qquad \cdots\cdots⑦$$

となる。

$7=2\cdot3+1$であるから，⑦の整数解z, sのうちの1組は，$z=-3, s=-1$であり，⑦は

$$2(z+3)=7(s+1) \quad \cdots\cdots⑧$$

と変形できる。2と7は互いに素であるから，⑧すなわち⑦のすべての解はtを実数として

$$z=-3+7t,\quad s=-1+2t$$

と表される。よって，①，②の共通解は

$$x=-13+32t,\quad y=-17+42t,\quad z=-3+7t$$

である。

(2) 自然数nは，21 で割ると 13 余り，16 で割ると 12 余り，96 で割ると 28 余るから，x, y, z をそれぞれの商とすると，

$$n=21x+13=16y+12=96z+28$$

を満たす。よって，(1)より

$$n=96z+28=96(-3+7t)+28=672t-260$$

であるから，このようなnのうち最小のものは$672-260=412$である。

[1981 立教大学]

$70a+21b+15c$を 105 で割った商をq余りをrとすると

$$r=70a+21b+15c-105q$$

と表される。

$70a+21b+15c=(3\times23+1)a+3\times7b+3\times5c=3(23a+7b+5c)+a$

$70a+21b+15c=5\times14a+(5\times4+1)b+5\times3c=5(14a+4b+3c)+b$

$70a+21b+15c=7\times10a+7\times3b+(7\times2+1)5c=7(10a+3b+2c)+c$

また，$105q=3\cdot5\cdot7q$であるから，rを 3 で割った余りはa，rを 5 で割った余りはb，rを 7 で割った余りはcである。

よって，$n-r$は 3，5，7 のいずれでも割り切れる。

ここで，3，5，7 はどの 2 つも互いに素であるから，$n-r$は 3･5･7＝105 で割り切れる。

また，0≦n＜105 かつ 0≦r＜105 であるから，－105＜$n-r$＜105

したがって，$n-r=0$すなわち$n=r$

ゆえに，nは$70a+21b+15c$を 105 で割った余りに等しい。

入試問題　[2005 早稲田大学]

(1) ${}_mC_2=\dfrac{m(m-1)}{2}$より，$\dfrac{{}_mC_2}{m}=\dfrac{m-1}{2}$

これが整数である必要十分条件は$m-1$が偶数，すなわち，mが奇数であることである。

(2) ${}_pC_k=\dfrac{p(p-1)(p-2)\cdots\cdots(p-k+1)}{k(k-1)(k-2)\cdots\cdots1}$

より

$${}_pC_k\{k(k-1)(k-2)\cdots\cdots1\}=p(p-1)(p-2)\cdots\cdots(p-k+1)\quad\cdots①$$

ここで，$k<p$であり，pは素数であるから $k, k-1, k-2, \cdots\cdots, 1$と$p$は互いに素である。

よって，$k(k-1)(k-2)\cdots\cdots 1$ と p は互いに素であるから①より ${}_pC_k$ は p で割り切れる。

別解　$k \geqq 1$ より ${}_pC_k = \dfrac{p!}{k!(p-k)!} = \dfrac{p}{k} \times \dfrac{(p-1)!}{(k-1)!\{(p-1)-(k-1)\}!} = \dfrac{p}{k} \times {}_{p-1}C_{k-1}$

であるから

$$k \times {}_pC_k = p \times {}_{p-1}C_{k-1}$$

ここで，$k < p$ であり，p は素数であるから，p と k は互いに素である。

よって，${}_pC_k$ は p で割り切れる。

(3)　$(n+1)^p = \displaystyle\sum_{k=0}^{p} {}_pC_k n^{p-k} = n^p + \sum_{k=1}^{p-1} {}_pC_k n^{p-k} + 1$

であるから

$$(n+1)^p - n^p - 1 = \sum_{k=1}^{p-1} {}_pC_k n^{p-k}$$

ここで，(2)より ${}_pC_k$　$(k = 1, 2, 3, \cdots\cdots, p-1)$ は p の倍数であるから $(n+1)^p - n^p - 1$ は p で割り切れる。

[1977　京都大学]

(Ⅰ)　$n = 1$ のとき，$n^p - n = 0$ であるから命題は成り立つ。

(Ⅱ)　$n = k$ のとき命題が成り立つと仮定すると，$k^p - k$ は p で割り切れる。

このとき，

$$(k+1)^p - (k+1) \equiv \sum_{i=0}^{p} {}_pC_i k^{p-i} - (k+1)$$

$$= k^p + \sum_{i=1}^{p-1} {}_pC_i k^{p-i} + 1 - (k+1)$$

$$= \sum_{i=1}^{p-1} {}_pC_i k^{p-i} + k^p - k$$

ここで，早稲田大学の問題の(2)により，${}_pC_i$ は p で割り切れるから，$\displaystyle\sum_{i=1}^{p-1} {}_pC_i k^{p-i}$ は p で割り切れ，また，仮定により $k^p - k$ は p で割り切れる。

よって，$\sum_{i=1}^{p-1} {}_pC_i k^{p-i} + k^p - k$ は p で割り切れるから，$(k+1)^p - (k+1)$ は p で割り切れる。

したがって，$n = k+1$のときも命題は成り立つ。

(Ⅰ)，(Ⅱ)より，すべての自然数nについて，命題は成り立つ。

[2005 早稲田大学]

(1) 77＝7×11　であり，7，11 は素数であるから，77 以下の自然数で 7 の倍数の集合を A，11 の倍数の集合を B とすると，77 との最大公約数が 1 でない自然数の個数は

$$n(A)+n(B)-n(A\cap B)$$

である。

$$n(A)=\frac{77}{7}=11,\ n(B)=\frac{77}{11}=7,\ n(A\cap B)=1$$

であるから，

$$n(A)+n(B)-n(A\cap B)=11+7-1=17$$

よって，$f(77)=77-\{n(A)+n(B)-n(A\cap B)\}=77-17=60$

(2) pq以下の自然数で p の倍数の集合を A，q の倍数の集合を Bとすると，pqとの最大公約数が 1 でない自然数の個数は

$$n(A)+n(B)-n(A\cap B)=p+q-1$$

よって，

$$f(pq)=pq-(p+q-1)=pq-p-q+1=(p-1)(q-1)$$

$f(pq)=24$であるから

$$(p-1)(q-1)=24$$

$0<p<q$より

$$(p-1,\ q-1)=(1,\ 24),\ (2,\ 12),\ (3,\ 8),\ (4,\ 6)$$

よって

$$(p,\ q)=(2,\ 25),\ (3,\ 13),\ (4,\ 9),\ (5,\ 7)$$

$p,\ q$は素数であるから

$$(p,\ q)=(3,\ 13),\ (5,\ 7)$$

(3) 2^k3^n 以下の自然数で 2 の倍数の集合を A，3 の倍数の集合を Bとすると，2^k3^n との最大公約数が 1 でない自然数の個数は

$$n(A)+n(B)-n(A\cap B)=\frac{2^k3^n}{2}+\frac{2^k3^n}{3}-\frac{2^k3^n}{2\cdot3}$$

よって

$$f\left(2^k3^n\right)=2^k3^n-\left(\frac{2^k3^n}{2}+\frac{2^k3^n}{3}-\frac{2^k3^n}{2\cdot3}\right)=2^k3^n\left(1-\frac{1}{2}-\frac{1}{3}+\frac{1}{6}\right)=2^k3^n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=2^k3^{n-1}$$

[2006 京都大学]

$\mathrm{mod}\,3$で考える。

$n\equiv1$であるとき，$n^2+2\equiv1^2+2=3\equiv0$

$n\equiv2$であるとき，$n^2+2\equiv2^2+2=3\cdot2\equiv0$

よって，nが3の倍数でないとき，n^2+2は3の倍数であり，$n^2+2\geqq6$であるから，

n^2+2は素数でない。

nが3の倍数のとき，

$n\geqq4$のとき，nは素数ではない。

$n=3$のとき，$n^2+2=11$となるから，nとn^2+2はともに素数である。

以上より，nとn^2+2がともに素数となるのは，$n=3$の場合に限る。

別解

$n(n^2+2)=n^3+2n=n^3-n+3n=(n-1)n(n+1)+3n$

ここで，$(n-1)n(n+1)$が連続する3整数の積であるから3の倍数である。よって，

$(n-1)n(n+1)+3n$は3の倍数であるから，$n(n^2+2)$は3の倍数である。

したがって，n, n^2+2の少なくとも1つは3の倍数であるから，$n\geqq4$のときは，

n, n^2+2の少なくとも1つは素数でない。

$n=3$のとき，$n^2+2=11$となるから，nとn^2+2はともに素数である。

以上より，nとn^2+2がともに素数となるのは，$n=3$の場合に限る。

[1990 一橋大学]

直角三角形の3辺の長さをa, b, c（cは斜辺の長さ）とし，面積をSとすると，$S=\frac{1}{2}ab$であるから，abが4の倍数であることを示せばよい。

また，三平方の定理により，$a^2+b^2=c^2$が成り立つ。

（ⅰ）a, bがともに偶数のとき，abは4の倍数である。

（ⅱ）a, bがともに奇数のとき，$a=2k+1, b=2l+1$（k, lは整数）と置けて，

$$c^2=a^2+b^2=(2k+1)^2+(2l+1)^2=4(k^2+k+l^2+l)+2 \quad \cdots①$$

よって，c^2は偶数であるから，cは偶数。ところが，cが偶数であるときc^2は4の倍数となるが，これは①と矛盾する。ゆえに，a, bがともに奇数となることはない。

（ⅲ）a, bの一方が偶数，他方がともに奇数のとき

a が偶数，b が奇数としても一般性は失われない。

このとき，a^2+b^2 は奇数であるから，$a^2+b^2=c^2$ より，c は奇数。

よって，$a=2k, b=2l+1, c=2m+1$（k, l, m は整数）と置けて，$a^2+b^2=c^2$ より

$$(2k)^2+(2l+1)^2=(2m+1)^2$$

変形して

$$k^2=m(m+1)-l(l+1)$$

ここで，$m(m+1), l(l+1)$ は連続した 2 つの整数の積であるから，偶数である。

よって，k^2 は偶数であるから，k は偶数である。

したがって，$a\ (=2k)$ は 4 の倍数であるから，ab は 4 の倍数である。

以上より，S は 2 の整数倍である。

[静岡大学]

(1) $m^2=n^2+p^2$ より $m^2-n^2=p^2$ であるから

$$(m+n)(m-n)=p^2 \quad \cdots①$$

m, n は自然数であるから，$m+n>m-n$

p は素数であるから，①より

$$m+n=p^2, m-n=1$$

したがって

$$m=\frac{p^2+1}{2}, n=\frac{p^2-1}{2}$$

p は 2 と異なる素数であるから，p は奇数である。

よって，p^2+1, p^2-1 は共に偶数であるから，$\frac{p^2+1}{2}, \frac{p^2-1}{2}$ は共に自然数である。

したがって，$m^2=n^2+p^2$ を満たす自然数の組 (m, n) はただ 1 組存在する。

(2) $m^2=n^2+12^2$ より $m^2-n^2=12^2$ であるから

$$(m+n)(m-n)=2^4\cdot 3^2 \quad \cdots②$$

また，$(m+n)-(m-n)=2n$ は偶数であるから，$m+n, m-n$ の偶奇は一致する。

さらに，②より $(m+n)(m-n)$ は偶数であるから，$m+n, m-n$ は共に偶数である。

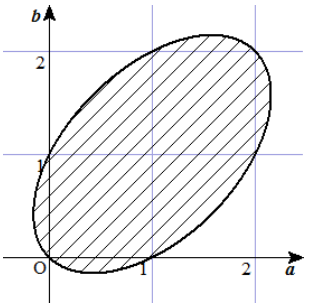
m, n は自然数であるから，$m+n>m-n$。よって②より，

$$(m+n, m-n)=(72, 2), (36, 4), (18, 8), (24, 6)$$

したがって

$$(m, n)=(37, 35), (20, 16), (13, 5), (15, 9)$$

[1999 早稲田大学]



(1)　　$a+b \geqq a^2-ab+b^2$　…①

より

$$a^2-(b+1)a+b^2-b \leqq 0$$

$$\left(a-\frac{b+1}{2}\right)^2+\frac{3b^2-6b-1}{4} \leqq 0$$

$$0 \leqq \left(a-\frac{b+1}{2}\right)^2 \leqq -\frac{3b^2-6b-1}{4}$$

よって

$$3b^2-6b-1 \leqq 0$$

したがって

$$\frac{3-2\sqrt{3}}{3} \leqq b \leqq \frac{3+2\sqrt{3}}{3}$$

$\sqrt{3}<2$ であるから

$$\frac{3-4}{3}<\frac{3-2\sqrt{3}}{3} \leqq b \leqq \frac{3+2\sqrt{3}}{3}<\frac{3+4}{3}$$　すなわち　$-\frac{1}{3}<b<\frac{7}{3}$

b は正の整数であるから　$b=1, 2$

不等式①は a, b について対称であるから，同様にして　$a=1, 2$

よって

$$(a, b)=(1, 1), (1, 2), (2, 1), (2, 2)$$

これらはすべて①を満たすので，これらが求めるものである。

(2)　$a^3+b^3=p^3$ より

$$(a+b)(a^2-ab+b^2)=p^3$$

(ⅰ) $a+b<a^2-ab+b^2$ のとき

$a+b \geqq 2$ であり，p は素数であるから

$$a+b=p, a^2-ab+b^2=p^2$$

よって

$$a^2-ab+b^2=(a+b)^2$$

したがって

$$ab=0$$

これは，a, b が正であることに反するから，与えられた条件を満たす a, b は存在しない。

(ⅱ) $a+b \geqq a^2-ab+b^2$ のとき

(1)より $(a, b) = (1, 1), (1, 2), (2, 1), (2, 2)$

これらを

$$a^3 + b^3 = p^3$$

に代入すると

$$p^3 = 2, 9, 16$$

これを満たす素数 p は存在しないから，与えられた条件を満たす a, b は存在しない。

[お茶の水女子大学]

(1) $n = p^a$ の正の約数は,

$$1,\ p, p^2, \cdots\cdots,\ p^a$$

よって

$$S(n) = 1 + p + p^2 + \cdots\cdots + p^a = \frac{p^{a+1} - 1}{p - 1}$$

(2) $mn = p^a q^b$ の正の約数は,

$$1,\ p,\ p^2, \cdots\cdots, p^a$$
$$q,\ pq,\ p^2 q, \cdots\cdots, p^a q$$
$$q^2,\ pq^2,\ p^2 q^2, \cdots\cdots, p^a q^2$$
$$\cdots\cdots$$
$$q^b,\ pq^b,\ p^2 q^b, \cdots\cdots, p^a q^b$$

よって

$$\begin{aligned} S(mn) = {} & 1 + p + p^2 + \cdots\cdots + p^a \\ & + q + pq + p^2 q + \cdots\cdots + p^a q \\ & + q^2 + pq^2 + p^2 q^2 + \cdots\cdots + p^a q^2 \\ & \qquad\qquad \cdots\cdots \\ & + q^b + pq^b + p^2 q^b + \cdots\cdots + p^a q^b \\ = {} & (1 + p + p^2 + \cdots\cdots + p^a)(1 + q + q^2 + \cdots\cdots + q^b) \\ = {} & \frac{p^{a+1} - 1}{p - 1} \cdot \frac{q^{b+1} - 1}{q - 1} = S(n)S(m) \end{aligned}$$

(3) 2 は素数であり，$2^a - 1$ は奇数の素数であるから，$2^a - 1 \neq 2$

したがって，(2)により，

$$S(n) = S(2^{a-1}(2^a - 1)) = S(2^{a-1})S(2^a - 1)$$

ここで，(1)より

$$S(2^{a-1}) = \frac{2^{(a-1)+1} - 1}{2 - 1} = 2^a - 1$$

また，2^a-1は素数であるから

$$S(2^a-1)=1+(2^a-1)=2^a$$

したがって

$$S(n)=2^a(2^a-1)=2\cdot 2^{a-1}(2^a-1)=2n$$

[千葉大学]

(1)　$a^b-1=(a-1)(a^{b-1}+a^{b-2}+\cdots\cdots+a+1)$　…①

$a\geqq 3$と仮定する。このとき，$a-1\geqq 2$

また，$b\geqq 2$であるから，

$$a^{b-1}+a^{b-2}+\cdots\cdots+a+1\geqq a+1\geqq 4$$

よって，①より，a^b-1は素数でない。

したがって，a^b-1が素数ならば，$a=2$である。

このとき，$a^b-1=2^b-1$

次に，bが素数でないと仮定する。すると，2以上の整数c, dを用いて，$b=cd$と置けるから

$$2^b-1=2^{cd}-1=\left(2^c\right)^d-1=(2^c-1)\left\{\left(2^c\right)^{d-1}+\left(2^c\right)^{d-2}+\cdots\cdots+2^c+1\right\}$$　…②

$c\geqq 2$であるから，$2^c-1\geqq 3$

$d\geqq 2$であるから，$\left(2^c\right)^{d-1}+\left(2^c\right)^{d-2}+\cdots\cdots+2^c+1\geqq 2^c+1\geqq 5$

したがって，②は素数でないから矛盾。よって，bは素数である。

(2)　cを負でない整数，dを1以上の奇数として$b=2^c d$と表す。

このとき，$2^c=e$とおくと$b=ed$

$d\geqq 3$と仮定する。dは奇数であるから

$$a^b+1=a^{ed}+1=\left(a^e\right)^d+1=(a^e+1)\left\{\left(a^e\right)^{d-1}-\left(a^e\right)^{d-2}+\cdots\cdots+\left(a^e\right)^2-a^e+1\right\}$$　…③

ここで，$a\geqq 2, e\geqq 1$であるから

$$a^e+1\geqq a+1\geqq 3$$

であり，$a^e\geqq 2$となるから

$$\left(a^e\right)^{d-1}-\left(a^e\right)^{d-2}>0,\ \left(a^e\right)^{d-3}-\left(a^e\right)^{d-4}>0,\ \cdots\cdots,\ \left(a^e\right)^2-a^e>0$$

さらに，$d\geqq 3$であるから

$$\left(a^e\right)^{d-1}-\left(a^e\right)^{d-2}+\cdots\cdots+a^{2e}-a^e+1\geqq(a^{2e}-a^e)+1\geqq 2$$

したがって，③は素数でないから矛盾。よって，$d=1$であるから，$b=2^c$（cは整数）と表せる。

[北海道教育大学]

$2n^3-3n^2+n=2(n^3-n)+3n^2+3n=2(n-1)n(n+1)+3n(n+1)$　…①

$n-1, n, n+1$は連続する3整数であるから，$n-1, n, n+1$のどれか1つは3の倍数である。

したがって，$(n-1)n(n+1)$は3の倍数であるから，$2(n-1)n(n+1)$は6の倍数である。

また，$n, n+1$は連続する2整数であるから，$n, n+1$の1つは2の倍数である。

したがって，$n(n+1)$は2の倍数であるから，$3n(n+1)$は6の倍数である。

ゆえに，①は6の倍数である。

[1997 東京工業大学]

(1) 与えられた等式より

$$\frac{x+y}{xy}=\frac{1}{2}$$

$$xy-2(x+y)=0$$

$$(x-2)(y-2)=2^2$$

ここで　$\frac{1}{x}<\frac{1}{x}+\frac{1}{y}=\frac{1}{2}$　であるから，$x-2>0$，同様にして，$y-2>0$

よって

$$(x-2, y-2)=(1, 2^2), (2^2, 1), (2, 2)$$

ゆえに，

$$(x, y)=(3, 6), (6, 3), (4, 4)$$

別解

$x \leqq y$とすると$\frac{1}{x} \geqq \frac{1}{y}$であり，

$$\frac{1}{2}=\frac{1}{x}+\frac{1}{y} \leqq \frac{1}{x}+\frac{1}{x}=\frac{2}{x}$$

よって　$x \leqq 4$

また，$\frac{1}{x}<\frac{1}{x}+\frac{1}{y}=\frac{1}{2}$　であるから，

$$x>2$$

したがって，$x=3, 4$

これらを，与えられた方程式に代入して

$x=3$のとき，$y=6$

$x=4$のとき，$y=4$

$x>y$の場合も考えて

$$(x, y)=(3, 6), (6, 3), (4, 4)$$

(2) 数学的帰納法により示す。

(Ⅰ) n $=1$のとき

$\dfrac{1}{x_1}=r$より，これを満たす自然数x_1は多くて1 個であるから，命題は成り立つ。

(Ⅱ) $n=m$のとき，命題が成り立つと仮定すると，任意の有理数rについて，$\displaystyle\sum_{k=1}^{m}\frac{1}{x_k}=r$をみたす自然数$x_k$の組$(x_1,\cdots\cdots,x_m)$の個数は有限である。

ここで，rを任意の有理数として，

$$\sum_{k=1}^{m+1}\frac{1}{x_k}=r \quad \cdots①$$

をみたす自然数x_kの組$(x_1,\cdots\cdots,x_{m+1})$の個数が有限であることを示す。このとき，$x_1 \geqq x_2 \geqq \cdots\cdots \geqq x_{m+1}$の場合に示せば十分である。

$$\frac{1}{x_1} \leqq \frac{1}{x_2} \leqq \cdots\cdots \leqq \frac{1}{x_{m+1}} \quad \text{であるから} \quad \sum_{k=1}^{m+1}\frac{1}{x_k} \leqq \frac{m+1}{x_{m+1}}$$

よって

$$r \leqq \frac{m+1}{x_{m+1}} \quad \text{であるから} \quad x_{m+1} \leqq \frac{m+1}{r} \quad \cdots②$$

x_{m+1}は自然数であるから，②を満たすx_{m+1}の個数は有限である。①を

$$\sum_{k=1}^{m}\frac{1}{x_k}=r-\frac{1}{x_{m+1}} \quad \cdots③$$

と変形する。右辺は有理数であるから，③を満たす自然数x_kの組$(x_1,\cdots\cdots,x_m)$の個数は有限である。

以上より，①をみたす自然数x_kの組$(x_1,\cdots\cdots,x_{m+1})$の個数は有限であるから，$n=m+1$のときも命題は成り立つ。

(Ⅰ)，(Ⅱ)により，すべての自然数nについて命題は成り立つ。

[2015 早稲田大学] (1) $(a+b\sqrt{2})(x+y\sqrt{2})=u+v\sqrt{2}$より

$$(ax+2by)+(ay+bx)\sqrt{2}=u+v\sqrt{2}$$

a, b, x, y, u, v が有理数で，$\sqrt{2}$ が無理数であるから，

$$u = ax + 2by\ ,\quad v = ay + bx$$

また，

$$\begin{aligned} u^2 + 2v^2 &= (ax+2by)^2 - 2(ay+bx)^2 \\ &= a^2x^2 + 4b^2y^2 - 2a^2y^2 - 2b^2x^2 \\ &= \left(a^2 - 2b^2\right)\left(x^2 - 2y^2\right) \\ &= 1\cdot 1 = 1 \end{aligned}$$

(2) $x^2 - 2y^2 = 1$ …① $1 < x + y\sqrt{2} \leqq 3 + 2\sqrt{2}$ …②

①より $(x+y\sqrt{2})(x-y\sqrt{2}) = 1$ よって $x - \sqrt{2}y = \dfrac{1}{x+y\sqrt{2}}$

したがって，②より $\dfrac{1}{3+2\sqrt{2}} \leqq x - y\sqrt{2} < 1$

すなわち $3 - 2\sqrt{2} \leqq x - y\sqrt{2} < 1$ …③

$\dfrac{②+③}{2}$ より $2 - \sqrt{2} < x < 2 + \sqrt{2}$

x は整数であるから，$x = 1, 2, 3$

$x = 1$ のとき ①より $y = 0$ で，このとき②を満たさない。

$x = 2$ のとき ①より $y^2 = \dfrac{3}{2}$ で，このとき y は整数ではない。

$x = 3$ のとき ①より $y^2 = 4$ で，②より，$y = 2$。

以上より，$x = 3, y = 2$

(3) $\left(3+2\sqrt{2}\right)^{n-1} < x + y\sqrt{2} \leqq \left(3+2\sqrt{2}\right)^{n}$ より $1 < \dfrac{x+y\sqrt{2}}{\left(3+2\sqrt{2}\right)^{n-1}} \leqq 3 + 2\sqrt{2}$ …④

$\dfrac{1}{3+2\sqrt{2}} = 3 + (-2)\sqrt{2}$ であるから $\dfrac{x+y\sqrt{2}}{\left(3+2\sqrt{2}\right)^{n-1}} = \left\{3+(-2)\sqrt{2}\right\}^{n-1}(x+y\sqrt{2})$

ここで，$3^2 - 2(-2)^2 = 1$，$x^2 - 2y^2 = 1$ であるから，(1)を繰り返し用いることにより，u, v を $u^2 - 2v^2 = 1$ を満たす整数として，

$$\left\{3+(-2)\sqrt{2}\right\}^{n-1}(x+y\sqrt{2}) = u + v\sqrt{2}$$

と置ける。これより

$$\frac{x+y\sqrt{2}}{\left(3+2\sqrt{2}\right)^{n-1}}=u+v\sqrt{2}$$

これと④より，$1<u+v\sqrt{2}\leqq 3+2\sqrt{2}$
ここで，(2)の結果を用いると　$u=3, v=2$

したがって，$\dfrac{x+y\sqrt{2}}{\left(3+2\sqrt{2}\right)^{n-1}}=3+2\sqrt{2}$　ゆえに　$x+y\sqrt{2}=\left(3+2\sqrt{2}\right)^{n}$

[2018　京都大学]

まず，任意の整数nについてn^3-7n+9が 3 の倍数であることを示す。
任意の整数nは，3 を法として 0，1，－1 のいずれかと合同である。

$n\equiv 0 \pmod 3$ のとき　$n^3-7n+9\equiv 0^3-7\cdot 0+9=9\equiv 0 \pmod 3$

$n\equiv 1 \pmod 3$ のとき　$n^3-7n+9\equiv 1^3-7\cdot 1+9=3\equiv 0 \pmod 3$

$n\equiv -1 \pmod 3$ のとき　$n^3-7n+9\equiv (-1)^3-7\cdot(-1)+9=15=3\cdot 5\equiv 0 \pmod 3$

よって，任意の自然数nについて，$n^3-7n+9\equiv 0 \pmod 3$ であるからn^3-7n+9は 3 の倍数である。

3 の倍数で素数である数は 3 だけである。したがって，n^3-7n+9が素数であるとき

$$n^3-7n+9=3$$

これより

$$n^3-7n+6=0$$
$$(n-1)(n-2)(n+3)=0$$

ゆえに，$n=1, 2, -3$

別解　$n^3-7n+9=(n^3-n)-6n+9=(n-1)n(n+1)+3(-2n+3)$

連続する 3 個の整数の積は 3 の倍数であるから，$(n-1)n(n+1)$は 3 の倍数であり，$-2n+3$は整数であるから$3(-2n+3)$は 3 の倍数である。

よって，n^3-7n+9は 3 の倍数である。

[2018　東京工業大学]

$35x+91y+65z=3$　…①　より

$5\cdot 7x+7\cdot 13y+5\cdot 13z=3$

$5\cdot 7x+13(7y+5z)=3$

7 と 5 は互いに素であるから，y，z が任意の整数値をとるとき，$7y+5z$ は任意の整数値をとる。

よって，$7y+5z=w$ とおき，

$$35x+13w=3$$

を満たす整数 x，w を求めれば y，z も求まる。

35 と 13 は互いに素であるから，

$$35x+13w=1$$

を満たす x，w が存在する。これを 1 組求める。

$$35=13\times3-4 \quad \text{より} \quad 4=-35+13\times3 \quad \cdots②$$

$$13=4\times3+1 \quad \text{より} \quad 13-4\times3=1 \quad \cdots③$$

②を③に代入して

$$13-(-35+13\times3)\times3=1$$

よって

$$35\times3+13\times(-8)=1$$

両辺を 3 倍して

$$35\times9+13\times(-24)=3 \quad \cdots④$$

次に，$w=-24$，すなわち $7y+5z=-24$ を満たす y，z を 1 組求めると，次のようになる。

$$7\times(-2)+5\times(-2)=-24 \quad \cdots⑤$$

⑤を④に代入して

$$35\times9+13\times\{7\times(-2)+5\times(-2)\}=3$$

よって　$35\times9+91\times(-2)+65\times(-2)=3$　…⑥

したがって，①を満たす整数の組(x, y, z)の 1 組は$(9, -2, -2)$

(2) ①－⑥より

$$35(x-9)+91(y+2)+65(z+2)=0$$

$$35(x-9)=13\{-7(y+2)-5(z+2)\}$$

35 と 13 は互いに素であるから，整数 k を用いて，

$$x-9=13\mathrm{k}, \quad -7(y+2)-5(z+2)=35k \quad \cdots⑦$$

と表される。⑦より

$$-7(y+2)=5(z+2+7k)$$

7 と 5 は互いに素であるから，整数 ℓ を用いて

$$y+2=5\ell, \quad z+2+7k=-7\ell$$

と表される。以上より

$$x=13k+9, \quad y=5\ell-2, \quad z=-7k\ -7\ell-2$$

このとき，

$x^2+y^2=(13k+9)^2+(5\ell-2)^2$

k，ℓ は任意の整数であるから，x^2+y^2 が最小となるのは，x^2 と y^2 のそれぞれがともに最小となるときで，$k=-1$，$\ell=0$ のときである。このとき，$(x,\ y,\ z)=(-4,\ -2,\ 5)$であり，$x^2+y^2$ の最小値は 20 である。

[2018　一橋大学]

(1)　n を m 桁の整数とすると，$n \geqq 10^{m-1}$ かつ $9m \geqq S(n)$

よって　$n \geqq 10^{m-1}$ かつ $270m+2018 \geqq 30S(n)+2018$

したがって，$m \geqq 5$ のとき

$$10^{m-1} > 270m+2018 \quad \cdots①$$

が成り立つことを示せばよい。①を数学的帰納法によって示す。

[1]　$m=5$ のとき

左辺 $=10^4=10000$，右辺 $=270\times5+2018=3368$

よって，左辺＞右辺であるから，①は成り立つ。

[2]　$k \geqq 5$ として，$m=k$ のとき①が成り立つと仮定すると，

$$10^{k-1} > 270k+2018$$

これを用いると

$$\begin{aligned} 10^{(k+1)-1}-\{270(k+1)+2018\} &= 10\cdot10^{k-1}-(270k+2288) \\ &> 10\cdot(270k+2018)-(270k+2288) \\ &= 2430k+17892>0 \end{aligned}$$

よって　$10^{(k+1)-1} > 270(k+1)+2018$

したがって，$m=k+1$ のときも①は成り立つ。

[1]，[2]から，$m \geqq 5$ であるすべての自然数 m について，①は成り立つ。

したがって，$n \geqq 10000$ のとき，$n > 30S(n)+2018$

(2)　(1)より，

$$n = 30S(n)+2018 \quad \cdots②$$

を満たす n があるとすれば，$n<10000$

また，②の右辺の一の位の数は 8 であるから，a, b, c を 0 から 9 までの整数として

$$n=1000a+100b+10c+8$$

と表される。よって，②より

$$1000a+100b+10c+8=30(a+b+c+8)+2018$$

整理して

$$970a+70b-20c=2250$$

$$97a+7b-2c=225$$

$7b-2c=225-97a$　…③

ここで，$0 \leqq b \leqq 9, 0 \leqq c \leqq 9$ であるから $-18 \leqq 7b-2c \leqq 63$

よって，③より　$-18 \leqq 225-97a \leqq 63$

すなわち　$162 \leqq 97a \leqq 243$

したがって，$1.6\cdots \leqq a \leqq 2.5\cdots$ であるから，$a=2$

これを③に代入して

$7b-2c=31$

よって　$7b=2c+31$　…④

ここで，$0 \leqq c \leqq 9$ であるから $31 \leqq 2c+31 \leqq 49$

よって，④より　$31 \leqq 7b \leqq 49$

したがって　$4.4\cdots \leqq b \leqq 7$

④の右辺は奇数であるから，$7b$ は奇数。よって，b は奇数である。

したがって　$b=5, 7$

これを④に代入して　$(b, c)=(5, 2), (7, 9)$

ゆえに　$n=2528, 2798$

[2018　東京大学　理系]

(1)　$a_n={}_{2n+1}C_n \times \frac{1}{n!}=\frac{(2n+1)!}{n!\{(2n+1)-n\}!}\times\frac{1}{n!}=\frac{(2n+1)!}{(n!)^2(n+1)!}$ であるから

$$\frac{a_n}{a_{n-1}}=\frac{(2n+1)!}{(n!)^2(n+1)!}\times\frac{\{(n-1)!\}^2 n!}{(2n-1)!}=\frac{(2n+1)!}{(2n-1)!}\times\frac{(n-1)!}{n!}\times\frac{(n-1)!}{(n+1)!}$$

$$=\{2n\cdot(2n+1)\}\times\frac{1}{n}\times\frac{1}{n(n+1)}=\frac{2(2n+1)}{n(n+1)}=\frac{2n+1}{\frac{n(n+1)}{2}}$$

ここで，$n(n+1)$ は連続する 2 つの整数の積であるから偶数より，$\frac{n(n+1)}{2}$ は整数である。

また，2 つの整数 a, b の最大公約数を (a, b) で表すと，ユークリッドの互除法の原理により

$(2n+1, n)=(2n+1-2n, n)=(1, n)=1$

$(2n+1, n+1)=(2n+1-2(n+1), n)=(-1, n)=1$

よって，$2n+1$ と n，$2n+1$ と $n+1$ はそれぞれ互いに素であるから，$2n+1$ と $\frac{n(n+1)}{2}$ は互いに素である。

ゆえに，$\dfrac{2n+1}{\dfrac{n(n+1)}{2}}$ は既約分数であるから，$p_n=\dfrac{n(n+1)}{2}, q_n=2n+1$ である。

(2) $a_1=\dfrac{{}_3C_1}{1!}=3$，$a_2=\dfrac{{}_5C_2}{2!}=\dfrac{10}{2}=5$，$a_3=\dfrac{{}_7C_3}{3!}=\dfrac{35}{6}=\dfrac{5\cdot 7}{2\cdot 3}$

よって，a_3 は整数でなく，a_3 を既約分数で表したとき，分母の素因数に 2 が含まれる。

ここで，(1)より

$$a_n=\frac{2n+1}{\dfrac{n(n+1)}{2}}\times a_{n-1}$$

であり，$\dfrac{2n+1}{\dfrac{n(n+1)}{2}}$ は既約分数で，分子 $2n+1$ は奇数である。

よって，a_{n-1} が整数でなく，a_{n-1} を既約分数で表したとき，分母の素因数に 2 が含まれるならば，a_n は整数でなく，a_n を既約分数で表したとき，分母の素因数に 2 が含まれる。

したがって，数学的帰納法により，3 以上のすべての自然数 n について，a_n は整数でない。

ゆえに，a_n が整数となる自然数 n は $n=1, 2$

補足　文系では，次のように出題されている。各自，問題文の誘導に従って解答せよ。

数列 $a_1, a_2, \cdots\cdots$ を $a_n=\dfrac{{}_{2n+1}C_n}{n!}$ $(n=1, 2, \cdots\cdots)$ で定める。

(1) a_7 と 1 の大小を調べよ。

(2) $n\geqq 2$ とする。$\dfrac{a_n}{a_{n-1}}<1$ を満たす n の値の範囲を求めよ。

(3) a_n が整数となる $n\geqq 1$ をすべて求めよ。

答え　(1) $a_7<1$　(2) $n\geqq 4$　(3) $n=1, 2$

[センター試験試作問題]

和が 600，最小公倍数が 5772 である 2 つの自然数 $a, b\ (a>b)$ がある。

a, b の最大公約数を G とし，$a=a'G, b=b'G$ とすると，a', b' の最大公約数は $\boxed{1}$ である。

また，$a'G+b'G=600, a'b'G=5772$ である。ここで，600，5772 を素因数分解すると

$$600=2^3\cdot 3\cdot 5^2$$

$$5772=2^{\boxed{2}}\cdot\underline{\boxed{3}}\cdot 13\cdot 37$$

$(a'+b')G=600, (a'b')G=5772$ であり，$a'+b'$ と $a'b'$ は互いに素であるから，600 と 5772 の最大公約数が G である。よって，$G=\boxed{12}$

したがって，

$$a'+b'=2\cdot 5^2, a'b'=13\cdot 37$$

これより，$a'=37, b'=13$ であるから，$a=\boxed{444}$，$b=\boxed{156}$ である。

このとき，$G=ma+nb$ より $G=ma'G+nb'G$ であるから

$$37m+13n=1$$

これを満たす整数 m, n の組のうち，m が正で最小であるものを，ユークリッドの互除法により求める。

37＝13×2＋11　より　37－13×2＝11　…①

13＝11×1＋2　より　13－11×1＝2　…②

11＝2×5＋1　より　11－2×5＝1　…③

②，③より

11－(13－11×1)×5＝1

よって　11×6－13×5＝1

①を用いて

(37－13×2)×6－13×5＝1

よって　37×6＋13×(－17)＝1

したがって，$m=\boxed{6}$，$n=\boxed{-17}$ である。

[2016 東京工業大学]

(1) n が素数のとき，

$1, 2, 3, \cdots\cdots, n-1$ と n は互いに素であるから，$(n-1)!=1\cdot 2\cdot 3\cdots\cdots(n-1)$ と n は互いに素である。

よって，$(n-1)!$ は n で割り切れない。

$n=4$ のとき，

$(n-1)!=3!=6$ であるから，4 で割り切れない。

以上より，n が素数または 4 のとき，$(n-1)!$ は n で割り切れない。

(2) n が素数でなくかつ 4 でもないとき，$n \geqq 6$ である。

このとき，n が素数でないから，a, b を整数として，$n = ab \quad (2 \leqq a, b \leqq n-1)$ と表される。

$a \neq b$ のとき

a, b は $2, 3, \cdots\cdots, n-1$ の中の 2 つの異なる数であるから，$(n-1)!$ は $n = ab$ で割り切れる。

$a = b$ のとき

$n = a^2$ であるから $a = \sqrt{n}$ であり，$n \geqq 6$ であるから，

$$(n-1)^2 - (2\sqrt{n})^2 = n^2 - 6n + 1 = n(n-6) + 1 > 0$$

ここで $n-1 > 0, 2\sqrt{n} > 0$ であるから

$$n - 1 > 2\sqrt{n} = 2a$$

したがって，$a, 2a$ は，$2, 3, \cdots\cdots, n-1$ の中の 2 つの異なる数であるから，$(n-1)!$ は $n = a^2$ で割り切れる。

以上より，n が素数でなくかつ 4 でもないとき，$(n-1)!$ は n で割り切れる。

［2016 京都大学］

$p^q + q^p$ が素数であると仮定し，その素数を r とする。

$p \geqq 2, q \geqq 2$ より，$p^q + q^p \geqq 8$ であるから r は奇数の素数である。

p, q が共に奇数であるとすると，p^q, q^p は共に奇数であるから，r は偶数となり矛盾する。

$p = q = 2$ とすると，p^q, q^p は共に偶数であるから，r は偶数となり矛盾する。

したがって，p, q の一方が 2 で，他方が奇数の素数である。

$p^q + q^p$ は p, q について対称であるから，$p = 2$ で q が奇数の素数の場合を調べればよい。

(1) $q = 3$ のとき，

$$2^q + q^2 = 2^3 + 3^2 = 17$$

であり，17 は素数である。

次に，$q \geqq 5$ であるときを調べる。5 以上の素数を 6 で割った余りは，1 または 5 である。

(2) q を 6 で割った余りが 1 であるとき

k を正の整数として $q = 6k + 1$ と表される。$2^6 = 64 \equiv 1 \pmod 3$ であるから

$$2^q + q^2 = 2 \cdot \left(2^6\right)^k + (6k+1)^2 \equiv 2 \cdot 1^k + 1 = 3 \equiv 0 \pmod 3$$

(3) q を 6 で割った余りが 5 であるとき

k を負でない整数として $q = 6k + 5$ と表される。

$$2^q+q^2=2^5\cdot\left(2^6\right)^k+(6k+4)^2\equiv 32\cdot 1^k+16=48\equiv 0 \pmod 3$$

したがって，$q\geqq 5$ のとき，2^q+q^2 は，3 より大きく，3 の倍数となるから，素数ではない。

以上より，p^q+q^p と表される素数は 17 のみである。

[2014 一橋大学]

(1) a,b,c がすべて 3 以上のとき

a,b,c はすべて奇数であるから，$a-b-8$，$b-c-8$ は共に偶数の素数である。

よって

$$a-b-8=2,\quad b-c-8=2$$

すなわち

$$b=c+10,\quad a=c+20$$

したがって，$c,c+10,c+20$ はすべて素数である。

$c=3$ のとき，

$$b=13,\quad a=23$$

であるから，題意を満たす。

$c\geqq 5$ のとき

c は 3 の倍数でないから，n を 2 以上の自然数として，$3n-1$ または $3n+1$ と表される。

$c=3n-1$ と表されるとき

$$b=c+10=3n+9=3(n+3)$$

より，b は素数ではない。

$c=3n+1$ と表されるとき

$$a=c+20=3n+21=3(n+7)$$

より，a は素数ではない。

(2) a,b,c の少なくとも 1 つが 2 のとき

$a-b-8>0$，$b-c-8>0$ であるから $a>b>c$

よって　　$c=2$

このとき　　$b-c-8=b-10$

さらに，a,b は共に奇数の素数となるから $a-b-8$ は偶数の素数である。よって

$$a-b-8=2$$

すなわち

$$a=b+10$$

したがって，$b-10,b,b+10$ がすべて素数である。

$b-10=p$ と置くと， $p,\ p+10,\ p+20$ のすべてが素数となる。

このとき，(1)と同様にして， $p=3$， $b=p+10=13$， $a=p+20=23$

以上より， $(a,b,c)=(23,13,2),(23,13,3)$

[2015 東京大学]

$$ {}_{2015}C_m=\frac{{}_{2015}P_m}{m!}=\frac{2015\cdot2014\cdot2013\cdots\cdots(2016-m+1)(2016-m)}{1\cdot2\cdot3\cdots\cdots(m-1)m}$$

$$=\frac{2015}{1}\cdot\frac{2014}{2}\cdot\frac{2013}{3}\cdots\cdots\frac{(2016-m)}{m}$$

この積において，偶数番目の項だけを抜き出し，分子と分母の素因数 2 の個数を数える。

分子	2014	2012	2010	2008	2006	2004	2002	2000	1998	1996
2 の個数	1	2	1	3	1	2	1	4	1	2
分母	2	4	6	8	10	12	14	16	18	20
2 の個数	1	2	1	3	1	2	1	4	1	2

分子の 2 の個数が分母の 2 の個数を上回るまで表を作ればよいが，次のような考察をする。

$$\frac{2016-m}{m}=\frac{2^5\cdot3^2\cdot7-m}{m}$$

ここで， m を 2 以上の偶数として， $m=2^k\cdot a$ （k は自然数， a は奇数）と表す。すると

$$2^5\cdot3^2\cdot7-m=2^5\cdot3^2\cdot7-2^k\cdot a$$

$k\leqq4$ のとき

$$2^5\cdot3^2\cdot7-2^k\cdot a=2^k(2^{5-k}\cdot3^2\cdot7-a)$$

$2^{5-k}\cdot3^2\cdot7$ は偶数， a は奇数であるから， $2^{5-k}\cdot3^2\cdot7-a$ は奇数である。

よって，分子と分母の 2 の個数は一致する。

$k=5$ のとき

$$2^{5-k}\cdot3^2\cdot7-a=3^2\cdot7-a$$

は偶数となるから，分子の 2 の個数は分母の 2 の個数を上回る。

$m<32=2^5$ のときは， $k<5$ であり， $m=32$ で初めて $k=5$ となるので，求める m は $m=32$ である。

[2007 大阪府立大学]

(1) mod 11で考える。

$$m=\sum_{k=1}^{n}10^{k-1}a_k=\sum_{k=1}^{n}(11-1)^{k-1}a_k\equiv\sum_{k=1}^{n}(-1)^{k-1}a_k$$

よって，mが 11 の倍数であることと，$\sum_{k=1}^{n}(-1)^{k-1}a_k$ が 11 の倍数であることは同値であるから，$\frac{1}{11}\sum_{k=1}^{n}(-1)^{k-1}a_k$ が整数であることは，m が 11 で割り切れるための必要十分条件である

(2) $9876543210123456789=\sum_{k=1}^{19}10^{k-1}a_k$ により a_k を定めると

$$\sum_{k=1}^{19}(-1)^{k-1}a_k=9-8+7-6+5-4+3-2+1-0+1-2+3-4+5-6+7-8+9=10$$

よって，$\sum_{k=1}^{19}(-1)^{k-1}a_k$ は 11 で割り切れないから，(1)により $9876543210\ \ 123456789$ は 11 で割り切れない。

(3) $$\sum_{k=1}^{19}(-1)^{k-1}a_k=2\cdot9-2\cdot8+2\cdot7-0+2(-a_4+a_5-a_6+a_7-a_8+a_9)$$

$$=2(-a_4+a_5-a_6+a_7-a_8+a_9)+16$$

$$=2(-a_4+a_5-a_6+a_7-a_8+a_9+8)$$

2 と 11 は互いに素であるから，$-a_4+a_5-a_6+a_7-a_8+a_9+8$ が 11 の倍数であればよい。

$$1+2+3-4-5-6\leqq-a_4+a_5-a_6+a_7-a_8+a_9\leqq6+5+4-3-2-1$$

であるから，

$$-9\leqq-a_4+a_5-a_6+a_7-a_8+a_9\leqq9$$

よって

$$-1\leqq-a_4+a_5-a_6+a_7-a_8+a_9+8\leqq17$$

したがって，$-a_4+a_5-a_6+a_7-a_8+a_9+8$ が 11 の倍数となるのは

$$-a_4+a_5-a_6+a_7-a_8+a_9+8=0,11$$

のときである。これより

$$-a_4+a_5-a_6+a_7-a_8+a_9=-8,3$$

すなわち

$$(a_5+a_7+a_9)-(a_4+a_6+a_8)=-8,3\quad\cdots①$$

また，$a_4, a_5, a_6, a_7, a_8, a_9$ は相違なる 1 以上 6 以下の自然数であるから

$$(a_5+a_7+a_9)+(a_4+a_6+a_8)=21\quad\cdots②$$

$a_5+a_7+a_9, a_4+a_6+a_8$ は共に整数であるから，①，②より

$$a_5+a_7+a_9=12, a_4+a_6+a_8=9$$

相違なる 1 以上 6 以下の 3 つの自然数の和が 12 となる組み合わせは

6，5，1 と 6，4，2 と 5，4，3

の 3 通りあり，それぞれに対して a_5, a_7, a_9 の決め方は 3! 通りある。また，残りの 3 数 a_4, a_5, a_6 の決め方は 3! 通りあるので， $a_4, a_5, a_6, a_7, a_8, a_9$ の場合の数は

$$3\times(3!)\times(3!)=108$$

通りある。よって，自然数 m で 11 で割り切れるものは 108 個ある。

[2012　東京大学]

(1) 連続する 2 個の自然数を $k, k+1$ とおく。この 2 数の積が n 乗数であると仮定すると，整数 m を用いて

$$k(k+1)=m^n \quad \cdots①$$

と表される。ここで， $k, k+1$ は互いに素であるから，①より $k, k+1$ は共に n 乗数である。 $k+1>k$ であるから， $k=a^n, k+1=(a+h)^n$ （ただし， a, h は自然数）と置くと，

$$(k+1)-k=(a+h)^n-a^n={}_nC_1a^{n-1}h+{}_nC_2a^{n-2}h^2+\cdots\cdots+{}_nC_1a^{n-1}h^{n-1}+h^n>1$$

となり，これは， $(k+1)-k=1$ であることに矛盾する。

ゆえに，連続する 2 個の自然数の積は n 乗数ではない。

(2) 連続する n 個の自然数を $k, k+1, k+2, \cdots\cdots, k+n-1$ とおく。この n 個の数の積が n 乗数であると仮定すると，整数 m を用いて

$$k(k+1)(k+2)\cdots\cdots\cdots(k+n-1)=m^n \quad \cdots①$$

と表される。

$$k^n<k(k+1)(k+2)\cdots\cdots\cdots(k+n-1)<(k+n-1)^n$$

であるから，

$$k^n<m^n<(k+n-1)^n \quad \text{これより} \quad k<m<k+n-1$$

よって， m は $k+1, k+2, \cdots\cdots, k+n-2$ のどれかと一致する。

したがって，①の両辺を m で割ると，

$$k\cdots\cdot(m-1)\cdot(m+1)\cdots\cdot(k+n-1)=m^{n-1} \quad \cdots②$$

このとき， $n-1\geqq 1$ ， $m\geqq 2$ かつ $m+1$ と m は互いに素であるから，等式②は成り立たない。

ゆえに，連続する n 個の自然数の積は n 乗数ではない。

[2016 慶應義塾大学]

(1) 等式は

$$\cos\frac{2k}{5}\cdot 2\pi+i\sin\frac{2k}{5}\cdot 2\pi=\cos\frac{1}{5}\cdot 2\pi+i\sin\frac{1}{5}\cdot 2\pi$$

と変形できるから，

$$2k \equiv 1 \pmod 5$$

を満たす最小の正の整数kを求めればよい。よって，$k=3$である。

(2) 事実 F より

$$\left(\cos\frac{2a}{b}\pi + i\sin\frac{2a}{b}\pi\right)^l = \cos\frac{1}{b}\cdot 2\pi + i\sin\frac{1}{b}\cdot 2\pi$$

となる整数lが存在するから，nを任意の整数として，$k=nl$すれば

$$z = \left(\cos\frac{2a}{b}\pi + i\sin\frac{2a}{b}\pi\right)^k = \left\{\left(\cos\frac{2a}{b}\pi + i\sin\frac{2a}{b}\pi\right)^l\right\}^n$$

$$= \left(\cos\frac{1}{b}\cdot 2\pi + i\sin\frac{1}{b}\cdot 2\pi\right)^n = \cos\frac{n}{b}\cdot 2\pi + i\sin\frac{n}{b}\cdot 2\pi$$

特に，$n=0,1,2,\cdots\cdots,b-1)$ととれば，$b$個の$z$はすべて異なり，また，$z$はこれ以外の値を取れないから，集合 P の要素の個数$n(P)$はbである。（zは複素数平面上の原点を中心として点 1 を 1 つの頂点とする正b角形の，すべての頂点を取り得るので，b個である。）

(3) a, bは互いに素な整数であるから，

$$ak + bl = 1$$

となる整数k, lが存在する。よって，

$$ak = 1 - bl$$

このk, lを用いると

$$\left(\cos\frac{2a}{b}\pi + i\sin\frac{2a}{b}\pi\right)^k = \cos\frac{2ak}{b}\pi + i\sin\frac{2ak}{b}\pi$$

$$= \cos\frac{2(1-bl)}{b}\pi + i\sin\frac{2(1-bl)}{b}\pi$$

$$= \cos\left(\frac{2}{b}\pi - 2\pi l\right) + i\sin\left(\frac{2}{b}\pi - 2\pi l\right)$$

$$= \cos\frac{2}{b}\pi + i\sin\frac{2}{b}\pi$$

(4) 事実 F によりQ_1, Q_2は

$$Q_1 = \left\{ z \;\middle|\; z\text{は整数}k\text{を用いて}\left(\cos\frac{2}{b_1}\pi + i\sin\frac{2}{b_1}\pi\right)^k\text{と表される複素数} \right\}$$

$$Q_2=\left\{ z \;\middle|\; z\text{は整数}l\text{を用いて}\left(\cos\frac{2}{b_2}\pi+i\sin\frac{2}{b_2}\pi\right)^{l}\text{と表される複素数}\right\}$$

となる。

$$\left(\cos\frac{2}{b_1}\pi+i\sin\frac{2}{b_1}\pi\right)^{k}=\cos\frac{2k}{b_1}\pi+i\sin\frac{2k}{b_1}\pi$$

$$\left(\cos\frac{2}{b_2}\pi+i\sin\frac{2}{b_2}\pi\right)^{l}=\cos\frac{2l}{b_2}\pi+i\sin\frac{2l}{b_2}\pi$$

であるから，集合Q_1の要素と集合Q_2の要素の積で表される複素数は

$$\left(\cos\frac{2k}{b_1}\pi+i\sin\frac{2k}{b_1}\pi\right)\left(\cos\frac{2l}{b_2}\pi+i\sin\frac{2l}{b_2}\pi\right)$$

$$=\cos\left(\frac{2k}{b_1}+\frac{2l}{b_2}\right)\pi+i\sin\left(\frac{2k}{b_1}+\frac{2l}{b_2}\right)\pi$$

$$=\cos\left(\frac{(kb_2+lb_1)}{b_1b_2}\cdot 2\pi\right)+i\sin\left(\frac{(kb_2+lb_1)}{b_1b_2}\cdot 2\pi\right)$$

b_1とb_2が互いに素ならば，k,lがすべての整数値をとるときkb_2+lb_1はすべての整数値をとるから，集合 R の要素の個数$n(R)$はb_1b_2である。

b_1とb_2の最大公約数が d ならば，k,lがすべての整数値をとるときkb_2+lb_1はすべての d の倍数の値をとるから，整数mを用いて

$$kb_2+lb_1=md$$

と表される。よって

$$\frac{(kb_2+lb_1)}{b_1b_2}=\frac{md}{b_1b_2}=\frac{m}{\frac{b_1b_2}{d}}$$

ここで，mはすべての整数値を取るから，集合 R の要素の個数$n(R)$は$\frac{b_1b_2}{d}$である。

註　$\frac{b_1b_2}{d}$はb_1とb_2の最小公倍数である。