東大数学パトロール（05 回）

―整数の人工庭園の巡り（Ⅱ）

前回は比較的考え易い，定型的な整数問題を取り上げましたが，今回は少しハイレベルの整数問題を扱ってみたいと思います．中には，かなりの難問もありますが，難関校では“こういう問題も出題されるのだ”，という気持ちで付き合っていただければ，と考えています．

■実験・観察・発見

ここ数年，整数問題は多くの大学で出題されるようになりましたが，その大部分はパターン化でき，ある程度の定型的解法を身につけておけば，何とか正解に至り着くことができます．しかし，東大，京大，東工大などで出題されるものは，そうした定型的解法だけではどうにもならないものも相当数含まれます．そこで大切になるのは，

実験（具体化）　⇒　観察　⇒　発見

というプロセスです．定理，公式だけで数学の問題が解決できると考えるのは大きな誤りで，今回紹介する 12 題は，ある意味ではすべてその種の問題です．

ブダペスト生まれの物理化学学者マイケル・ポランニー（1891～1976）は，『暗黙知の次元』（ちくま学芸文庫・高橋勇夫訳）という本で「暗黙的認識をことごとく排除して，すべての知識を形式化しようとしても，そんな試みは自滅するしかないことを，私は証明できると思う」と記し，“数学理論”について以下のように述べています．

> **数学的理論は，ひたすらそれに先立つ暗黙的認識に依拠して構成されるしかなく，暗黙的認識という行為の内部でのみ理論として機能しうるのである．ちなみに，この際の暗黙的認識は，数学理論から，（数学理論が関係を有してはいるが）その理論以前に確立済みの経験へと注目を移すときに成り立つものだ．そういうわけで，暗黙的認識を撲滅して，経験を包括的に説明しようとする数学理論の理想は，自己矛盾で，論理的に不健全なものだと，証明されるのである．**

高校生にはいささか難しいもの言いと感じられるかもしれませんが，“暗黙知”とは要するに，体系的に言語化された理論以前の経験的直観知，非言語的認識知とも言うべきもので，端的に言えば，定理，公式だけに依拠して考えるだけではなく，具体的な試行錯誤の生み出す経験知を大切にして，数学の問題を考えることを忘れてはならない，と主張しているのです．このことは難関校を目指す受験生諸君に，是非肝に銘じておいて欲しいことです．

さて，そうしたことを踏まえた上で，まず今年（2020 年）の京大・文系の問題を紹介してみましょう．

【５・１】 a を奇数とし，整数 m,n に対して

$$f(m,n)=mn^2+am^2+n^2+8$$

とおく．$f(m,n)$ が 16 で割り切れるような整数の組 (m,n) が存在するための a の条件を求めよ．

［解説］ $f(m,n)$ の右辺を変形しても，a の条件をすぐに求めることは難しい．この種の問題ではまず，m,n の値を具体的に定め，条件を満たす a が存在するか，という実験から始めてみるのがよい．

$$f(1,1)=a+10,\qquad f(1,2)=a+16,$$
$$f(2,1)=4a+11,\qquad f(2,2)=4a+20$$

であり，a が奇数であることに注意すると，$f(1,1)$，$f(1,2)$，$f(2,1)$ のときは奇数だから，条件を満たす a は存在しない．$f(2,2)$ については，$a=3,7,11,\cdots$ のとき，条件を満たす (m,n) は存在することが分かる．すなわち，

$a\equiv 3 \pmod 4$ のとき，条件を満たす (m,n) が存在が存在する

かな，と予想される．以下，これ踏まえて解答を作ってみよう．

（ｉ）$m=2p+1$，$n=2q+1$ $(p,q\in\mathbb{Z})$ のとき；

$$f(m,n)=(2p+1)(2q+1)^2+a(2p+1)^2+(2q+1)^2+8$$
$$\equiv 2p+1+a+1+8\equiv a+(10+2p) \pmod 4$$

すなわち，

$$a+(10+2p)=4k\ (k\in\mathbb{Z})$$

a は奇数だから，これを満たす奇数 a は存在しない．

（ⅱ）$m=2p+1$，$n=2q$ $(p,q\in\mathbb{Z})$ のとき；

$$f(m,n)=(2p+1)\cdot 4q^2+a(2p+1)^2+4q^2+8\ \equiv a \pmod 4$$

したがって，奇数 a をどのように定めても，これを満たす奇数 a は存在しない．

（ⅲ）$m=2p$，$n=2q+1$ $(p,a\in\mathbb{Z})$ のとき；

$$f(m,n)=2p(2q+1)^2+a\cdot 4p^2+(2q+1)^2+8\equiv 1 \pmod 4$$

すなわち，

$$f(m,n)=4k+1\ (k\in\mathbb{Z})$$

であるから，奇数 a をどのように定めても，$4k+1=16l$ $(l\in\mathbb{Z})$ となることはない．したがって，条件を満たす奇数 a は存在しない．

（ⅳ）$m=2p$，$n=2q$ $(p,q\in\mathbb{Z})$ とき；

$$f(m,n)=2p\cdot 4q^2+a\cdot 4p^2+4q^2+8\ \equiv 0 \pmod 4$$

そこで，$8pq^2+4ap^2+4q^2+8=16k$ $(k\in\mathbb{Z})$ とおくと，

$$ap^2+(2pq^2+q^2+2)=4k\quad\cdots①$$

（イ）$a=4b+1$ $(b\in\mathbb{Z})$ のとき，①より

$$4bp^2+(p^2+2pq^2+q^2+2)=4k\quad\cdots②$$

ここで，p,q の偶奇に着目すると，

$p \equiv 0, q \equiv 0 \pmod 2$ のとき，$p^2 + 2pq^2 + q^2 + 2 \equiv 2 \pmod 4$

$p \equiv 1, q \equiv 0 \pmod 2$ のとき，$p^2 + 2pq^2 + q^2 + 2 \equiv 3 \pmod 4$

$p \equiv 0, q \equiv 1 \pmod 2$ のとき，$p^2 + 2pq^2 + q^2 + 2 \equiv 3 \pmod 4$

$p \equiv 1, q \equiv 1 \pmod 2$ のとき，$p^2 + 2pq^2 + q^2 + 2 \equiv 2 \pmod 4$

だから，②を満たす整数 p, q は存在しない．

（ロ） $a = 4b + 3$ $(b \in \mathbb{Z})$ のとき，①より

$$4bp^2 + (3p^2 + 2pq^2 + q^2 + 2) = 4k \quad \cdots ③$$

ここで，

$p \equiv 1, q \equiv 1 \pmod 2$ のとき，$3p^2 + 2pq^2 + q^2 + 2 \equiv 0 \pmod 4$

であるから，③を満たす整数 p, q は存在する．

以上の考察から，求める条件は，$a \equiv 3 \pmod 4$ □

（ロ）においては，

$p \equiv 1, q \equiv 0 \pmod 2$ のとき，$3p^2 + 2pq^2 + q^2 + 2 \equiv 1 \pmod 4$

$p \equiv 0, q \equiv 1 \pmod 2$ のとき，$3p^2 + 2pq^2 + q^2 + 2 \equiv 3 \pmod 4$

$p \equiv 0, q \equiv 0 \pmod 2$ のとき，$3p^2 + 2pq^2 + q^2 + 2 \equiv 2 \pmod 4$

であることも，容易に確認できるでしょう．

上の考察から分かることは，“$a \equiv 3 \pmod 4$ のときのみ，条件を満たす整数 m, n は存在し，その m, n はともに偶数である”ということです．実は，本問の難しさは“m, n の偶奇に着目して議論を進める”という**“視点の発見”**であり，実はこの視点さえ見えてしまえば，むしろ易しい問題です．そして，この視点の発見のために，［解説］の冒頭で述べたような実験が必要なのです．

次も，今年（2020 年）の東工大の問題で，一見難しそうに感じられますが，具体的な実験を忘れなければ，案外すんなり解決する“易しい”問題です．

【５・２】（１） $\left|x^2 - x - 23\right|$ の値が，3 を法として 2 に合同である正の整数 x をすべて求めよ．

（２） k 個の連続した正の整数 $x_1, \cdots, x_k$ に対して，$\left|x_j^{\,2} - x_j - 23\right|$ $(1 \leq j \leq k)$ がすべて素数になる k の最大値と，その k に対する連続した正の整数 $x_1, \cdots, x_k$ をすべて求めよ．

ここで，k 個の連続した整数とは，$x_1, x_1 + 1, x_1 + 2, \cdots, x_1 + k - 1$ となる列のことである．

［解説］（１） $f(x) = x^2 - x - 23$ $(x \in \mathbb{N})$ とおくと，

$f(x) < 0 \Leftrightarrow x(x-1) < 23 \Leftrightarrow x = 1, 2, 3, 4, 5$ ，

$f(x) > 0 \Leftrightarrow x(x-1) > 23 \Leftrightarrow x = 6, 7, 8, , 9, 10, \cdots,$

（ｉ） $f(x) < 0$ のとき；（すべて，mod 3 で考える）

$\left|f(1)\right| = \left|-23\right| \equiv 2$ ， $\left|f(2)\right| = \left|-21\right| \equiv 0$ ， $\left|f((3)\right| = \left|-17\right| \equiv 2$ ，

$\left|f(4)\right| = \left|-11\right| \equiv 2$, $\left|f(5)\right| = \left|-3\right| \equiv 0$

（ⅱ） $f(x) > 0$ のとき；（すべて， $\mathrm{mod}\,3$ で考える）

$f(x) = x(x-1) - 24 + 1$ だから，

$x \equiv 0$ ならば $f(x) \equiv 1$

$x \equiv 1$ ならば $f(x) \equiv 1$

$x \equiv 2$ ならば $f(x) \equiv 0$ ・・・（＊）

したがって，この場合， $f(x) \equiv 2 (\mathrm{mod}\,3)$ となる x は存在しない．

以上，（ⅰ），（ⅱ）から， $x = 1,3,4$ □

（2）（1）の結果を参考にして具体的に調べる．

$\left|f(3)\right| = 17$, $\left|f(4)\right| = 11$, $\left|f(5)\right| = 3$, $\left|f(6)\right| = 7$, $\left|f(7)\right| = 19$ はすべて素数．

$\left|f(8)\right| = 33$, $\left|f(9)\right| = 49$, $\left|f(10)\right| = 67$ （素数）， $\left|f(11)\right| = 87$, ・・・

したがって， k の最大値は 5 と予想される．しかるに，

$x \geq 6$ のとき，（1）の（＊）より，

$x = 3n + 2$ $(n = 2,3,4,\cdots)$ ならば， $f(x) \equiv 0 (\mathrm{mod}\,3)$

すなわち，

$f(6)$ ， $f(7)$ ， $\boxed{f(8)}$ ， $f(9)$ ， $f(10)$ ， $\boxed{f(11)}$ ， $f(12)$ ， $f(13)$ ， $\boxed{f(14)}$ ，・・・

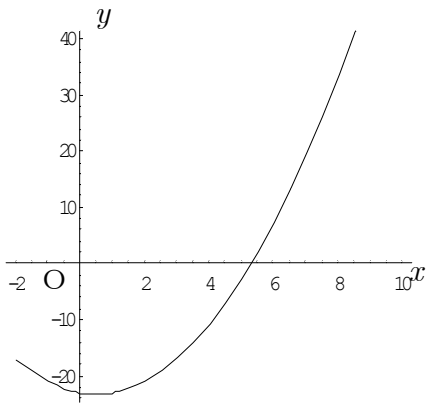
において，四角で囲った数は，3 の倍数であるから， $k \leq 4$ である．

よって， k の最大値は，5 □

また，このときの連続した正の整数は，

（3，4，5，6，7） □

不等式 $x^2 - x - 23 < 0$ を解こうとして，



解の公式を機械的に利用して

$$\frac{-1-\sqrt{93}}{2} < x < \frac{-1+\sqrt{93}}{2}$$

とし，開平法計算により

$$\sqrt{93} = 9.64\cdots$$

を利用しようとする人を多く見かけるが， x は“正の整数”だから，［解説］のように考えていくのが，ベストです．また，

$y = x^2 - x - 23$ （右上図）

のグラフを考えてみるのも，この問題の解決の一助になるのではないかと思います．このグラフを丁寧に調べれば，$x \geq 6$ のときは，$k \leq 4$ となることは，簡単に予想できるはずです．要するに，素朴な実験が大切であり，下手に大上段に構えた議論は禁物だ，ということです．地に足をつけた思考を忘れないでいただきたい．

次の問題も今年（2020 年）の京大・理系の問題．やはり，実験がものをいう問題で，私自身は，【５・１】の文系の問題よりも考え易いのでは，と感じています．

【５・３】正の整数aに対して，

$$a = 3^b c \quad (b,c \text{は整数で} c \text{は} 3 \text{で割り切れない})$$

の形に書いたとき，$B(a) = b$と定める．例えば，$B(3^2 \cdot 5) = 2$である．

m,nは整数で次の条件を満たすとする．

（ⅰ）$1 \leq m \leq 30$　（ⅱ）$1 \leq n \leq 30$　（ⅲ）nは3で割り切れない．

このような(m,n)について$f(m,n) = m^3 + n^2 + n + 3$とするとき，

$A(m,n) = B(f(m,n))$の最大値を求めよ．また，$A(m,n)$の最大値を与えるような(m,n)をすべて求めよ．

［解説］$A(m,n)$の最大値をMとすると，少し実験して分かるように，$M \geq 2$となる．実際，

$$f(3,2) = 27 + 4 + 2 + 3 = 3^2 \cdot 4$$

であり，このとき$A(3,2) = 2$である．さらに，

$$m \text{が} 3 \text{の倍数のとき，} 3^3 \mid m^3$$

であるから，$3^3 \mid (n^2 + n + 3)$となるような，nが存在すれば，$M \geq 3$となる．ところが，$n = 3k + 2$ $(k \in \mathbb{Z})$のとき，

$$n^2 + n + 3 = (3k+2)^2 + (3k+2) + 3 = 9k^2 + 15k + 9$$

だから，たとえば，$k = 3$とすると，

$$9k^2 + 15k + 9 = 135$$

となって，これは$3^3 = 27$で割り切れる．したがって，ここまでの素朴な実験から，$M \geq 3$であることが分かる．

（ⅰ）$n = 3k + 1$ $(k = 0,1,2,\cdots,8,9)$のとき；

$$f(m,n) = m^3 + (3k+1)^2 + (3k+1) + 3$$
$$= (m^3 + 5) + 9k(k+1) \quad \cdots ①$$

ここで，

$m \equiv 0 \pmod 3$ならば，$m^3 + 5 \equiv 5 \pmod 9$

$m \equiv 1 \pmod 3$ならば，$m^3 + 5 \equiv 6 \pmod 9$

$m \equiv 2 \pmod 3$ならば，$m^3 + 5 \equiv 4 \pmod 9$

$\therefore \quad 9 \nmid (m^3 + 5)$

$\therefore \quad 9 \nmid f(m,n)$　（$\because$　①より，$m^3 + 5 = f(m,n) - 9k(k+1)$）

（ⅱ）$n = 3k + 2$ $(k = 0,1,2,\cdots,9)$のとき；

$$f(m,n) = m^3 + (3k+2)^2 + (3k+2) + 3$$
$$= m^3 + (9k^2 + 15k + 9) \quad \cdots ②$$

ここで，

$k \equiv 0 \pmod 3$ならば，$9 \mid (9k^2 + 15k + 9)$

$k \equiv 1,2 \pmod 3$ならば，$9 \nmid (9k^2 + 15k + 9)$

したがって，$f(m,n)$を最大にするkは，

$$k = 3l \ (l = 1,2,3), \quad m = 3a \ (a \in \mathbb{Z})$$

が必要で，このとき，

$$m^3+9k^2+15k+9=(3a)^3+9(3l)^2+15(3l)+9$$
$$=9\{3a^3+(9l^2+5l+1)\}$$

（イ）$l=1$ のとき，

$$3a^3+(9l^2+5l+1)=3a^3+15$$

したがって，$a\equiv 1 \pmod 3$ のとき，

$$9\mid(3a^3+15),\quad 27\nmid(3a^3+15)$$

（ロ）$l=2$ のとき，

$$3a^3+(9l^2+5l+1)=3a^3+37 \qquad \therefore \quad 9\nmid 3a^3+37$$

（ハ）$l=3$ のとき，

$$3a^3+(9l^2+5l+1)=3a^3+97 \qquad \therefore \quad 9\nmid 3a^3+97$$

以上の考察から，

$$m=3(3b+1)\quad (b=0,1,2,3),\qquad n=3\cdot 3l+2\quad (l=1)$$

よって，

$$M=\max A(m,n)=4\ \square$$
$$(m,n)=(3,11),(12,11),(21,11),(30,11)\ \square$$

本問での大切な考察は，実験から $M\geq 3$ であることを見抜くことで，これが見えれば，本問の眼目は，$M\geq 4$ かつ $M<5$ であることを示すことに絞られます．そして，これを示すことは，［解説］からも分かるようにそんなに難しいことではないのです．

本節の最後に，これまた今年（2020 年），名古屋大学の理系の問題を考えてみましょう．さほど難しいものではありません．

【５・４】 ３つの数 2，m^2+1，m^4+1 が相異なる素数となる正の整数 m が１つ固定されているものとする．

（１）３つの数 2，m^2+1，m^4+1 のうち，１つを a とし，残りの２つを b,c とする．このとき $a^2<bc$ となる a をすべて求めよ．

（２）正の整数 x,y が $(x+y)(x^2+2y^2+2xy)=2(m^2+1)(m^4+1)$ を満たしているとき x,y を求めよ．

［解説］（１）３つの数が相異なるので，$m\geq 2$ であることに注意する．

（ⅰ）$a=2$ のとき；

$$bc-a^2=(m^2+1)(m^4+1)-4\geq 5\cdot 17-4=81>0 \quad \therefore \quad bc>a^2$$

（ⅱ）$a=m^2+1$ のとき；

$$bc-a^2=2(m^4+1)-(m^2+1)^2=(m^2-1)^2>0 \qquad \therefore \quad bc>a^2$$

（ⅲ）$a=m^4+1$ のとき；

$$bc-a^2=2(m^2+1)-(m^4+1)^2$$
$$=-\{(m^8-1)+2m^2(m^2-1)\}<0 \qquad \therefore \quad bc<a^2$$

以上より，$a=2$，m^2+1 $\square$

（2）2，m^2+1，$m^4+1\,(m\geq 2)$が相異なる３つの素数であるから，

$m^4+1\,|\,x+y$　または　$m^2+1\,|\,x+y$　または　$2\,|\,x+y$

に注意する．

（ｉ）$x+y=k(m^4+1)\ (k\in\mathbb{N})$のとき；

仮定から，$k(m^4+1)(x^2+2y^2+2xy)=2(m^2+1)(m^4+1)$

$\therefore\quad k(x^2+2y^2+2xy)=2(m^2+1)<(m^4+1)^2$　（$\because$　（１）の結果）

ところが，

$k(x^2+2y^2+2xy)=k\{(x+y)^2+y^2\}>k^3(m^4+1)^2\geq(m^4+1)^2$

すなわち，　$(m^4+1)^2<(m^4+1)^2$

となり，これは不合理である．

（ⅱ）$x+y=k(m^2+1)\ (k\in\mathbb{N})$のとき；

仮定から，$k(m^2+1)(x^2+2y^2+2xy)=2(m^2+1)(m^4+1)$

$\therefore\quad k((x+y)^2+y^2\}=2(m^4+1)$

2，m^4+1は素数だから，$k=1$　または　2　または　m^4+1

$k=m^4+1$とすると，$(x+y)^2+y^2=2$となり，これは不合理．

$k=2$とすると，$4(m^2+1)^2+y^2<m^4+1$なり，これは不合理．

したがって，$k=1$．このとき，$x+y=m^2+1$で

$(m^2+1)^2+y^2=2(m^4+1)$　　$\therefore\quad y^2=(m^2-1)^2$

$\therefore\quad x=2$，$y=m^2-1$（$\because\quad y>0$）

（ⅲ）$x+y=2k\ (k\in\mathbb{N})$のとき；

仮定から，$k\{(x+y)^2+y^2\}=(m^2+1)(m^4+1)$

m^2+1とm^4+1が素数だから，$k=1$　または　m^2+1　または　m^4+1

（イ）$k=1$のとき，$x=1$，$y=1$となって，このときは明らかに不合理．

（ロ）$k=m^2+1$のとき，$4(m^2+1)^2+y^2=m^4+1$となって，不合理．

（ハ）$k=m^4+1$のとき，$4(m^4+1)^2+y^2=m^2+1$となって，不合理．

以上の考察から，$x=2$，$y=m^2+1$ □

“東大数学パトロール”のはずが，本節では，今年の，京大，東工大，名大の問題を紹介しましたが，ここで噛みしめてほしかったのは，はじめに紹介したポランニーの言葉です．定理，公式に裏打ちされた“理論”だけでは，難関校の初見の入試問題には太刀打ちできません．“理論”が出来上がる背後には，素朴かつ具体的な試行錯誤，多くの実験があり，その混沌たる現場を数多く体験することにより，ポランニーの言うところの“暗黙知”が知らず知らずのうちに育まれます．そして，その“暗黙知”こそ，数学的直観力であり，私が，“言語認識”（これもまた大切！ですが）とともに，難関校志望の受験生に身につけて欲しいものなのです．

次節からは，最後の［５・１２］を除いてすべて，東大の入試問題です．

■整数問題と数列

整数問題と数列（あるいは漸化式）との融合問題は，東大数学の頻出テーマです．本節で紹介する３題は，いずれもその典型問題ですが，並みの受験生には相当の難問と言っても過言ではありません．

最初は，2011 年東大・理科の問題です．なお，（１），（２）までは文科でも出題されていて，（３）が理科固有の小問（？）です．問題文を読んで頂ければお分かりになるように，実は問題そのものが，“実験，観察，発見”の流れに沿って作られています．

【５・５】実数xの小数部分を，$0 \leq y < 1$かつ$x-y$が整数となる実数yのこととし，これを記号$\langle x \rangle$で表す．実数aに対して，無限数列$\{a_n\}$の各項$a_n\ (n=1,2,3,\cdots)$を次のように順次定める．

（ⅰ）$a_1 = \langle a \rangle$　　（ⅱ）$\begin{cases} a_n \neq 0 \quad \text{のとき，} \ a_{n+1} = \left\langle \dfrac{1}{a_n} \right\rangle \\ a_n = 0 \quad \text{のとき，} \ a_{n+1} = 0 \end{cases}$

（１）$a = \sqrt{2}$のとき，数列$\{a_n\}$を定めよ．

（２）任意の自然数nに対して$a_n = a$となるような$\dfrac{1}{3}$以上の実数aをすべて求めよ．

（３）aが有理数であるとする．aを整数pと自然数qを用いて$a = \dfrac{p}{q}$と表すとき，q以上のすべての自然数nに対して，$a_n = 0$であることを示せ．

[解説]（１）$1 < \sqrt{2} < 2$であるから，$a = \sqrt{2}$のとき，

$$a_1 = \langle \sqrt{2} \rangle = \sqrt{2} - 1\ ,$$

$$a_2 = \left\langle \frac{1}{a_1} \right\rangle = \left\langle \frac{1}{\sqrt{2}-1} \right\rangle = \langle \sqrt{2}+1 \rangle = \left(\sqrt{2}+1\right) - 2 = \sqrt{2} - 1 = a$$

$$\therefore \quad a_n = \sqrt{2} - 1\ (n = 1,2,3,\cdots)\ \square$$

（２）$a_n = a$（for all $n \in \mathbb{N}$）となる必要十分条件は

$$a_2 = a_1 \quad \therefore \quad \left\langle \frac{1}{a} \right\rangle = a \ \cdots ①$$

$a \geq \dfrac{1}{3}$と$0 \leq a < 1$とから，

$$\frac{1}{3} \leq a < 1 \qquad \therefore \quad 1 < \frac{1}{a} \leq 3$$

したがって，$\dfrac{1}{a}$の整数部分は 1，2，3 のいずれかであるが，整数部分が 3 とすると，

$\left\langle \dfrac{1}{a} \right\rangle = 0$ となって，これは①を満たさない．

（ｉ）整数部分が 1 のとき；

①より　$\dfrac{1}{a} - 1 = a \qquad \therefore \quad a^2 + a - 1 = 0$

よって，$\dfrac{1}{3} \leq a < 1$ より，　$a = \dfrac{-1+\sqrt{5}}{2}$ □

（ⅱ）整数部分が 2 のとき；

①より　$\dfrac{1}{a} - 2 = a \qquad \therefore \quad a^2 + 2a - 1 = 0$

よって，$\dfrac{1}{3} \leq a < 1$ より　$a = -1 + \sqrt{2}$ □

（3）整数 p を自然数 q で割ったときの商を k_1，余りを r_1 とすると，

$$p = qk_1 + r_1 \ (0 \leq r_1 < q) \text{・・・②}$$

$$\therefore \quad a = \frac{p}{q} = k_1 + \frac{r_1}{q} \quad \left(0 \leq \frac{r_1}{q} < 1\right)$$

$r_1 = 0$ ならば，$a_1 = \langle a \rangle = 0$，

$r_1 \neq 0$ ならば，$a_1 = \langle a \rangle = \dfrac{r_1}{q} \qquad \therefore \quad \dfrac{1}{a_1} = \dfrac{q}{r_1}$

$r_1 \neq 0$ のとき，q を r_1 で割ったときの商を k_2，余りを r_2 とすると，

$$q = r_1 k_2 + r_2 \ (0 \leq r_2 < r_1) \text{・・・③}$$

$$\therefore \quad \frac{1}{a_1} = \frac{q}{r_1} = k_2 + \frac{r_2}{r_1} \quad \left(0 \leq \frac{r_2}{r_1} < 1\right)$$

$r_2 = 0$ ならば，$a_2 = \left\langle \dfrac{1}{a_1} \right\rangle = 0$，

$r_2 \neq 0$ ならば，$a_2 = \left\langle \dfrac{1}{a_2} \right\rangle = \dfrac{r_2}{r_1} \qquad \therefore \quad \dfrac{1}{a_2} = \dfrac{r_1}{r_2}$

以下同様に割り算を実行していくと，②，③から分かるように，単調に減少する余りの列；　$0 \leq r_i < r_{i-1} < \cdots < r_1 < q$ ・・・④

が得られて，

$r_i = 0$ ならば，$a_i = \left\langle \dfrac{1}{a_{i-1}} \right\rangle = 0$，

$r_i \neq 0$ ならば，$a_i = \left\langle \dfrac{1}{a_{i-1}} \right\rangle = \dfrac{r_i}{r_{i-1}}$

となる．④は，0 または自然数列であるから，ある $i\,(1 \leq i \leq q)$ が存在して，$r_i = 0$ とな

り，このとき，$a_i = 0$ である．よって，q 以上のすべての自然数 n に対して，$a_n = 0$ であることが示された．□

本問の背景にあるのは，“ユークリッドの互除法の原理”であり，これはさらに“連分数”のお話に関連しています．

たとえば，$a = \dfrac{8}{5}$（有理数）のとき，a は

$$a = \frac{8}{5} = 1 + \frac{3}{5} = 1 + \frac{1}{\frac{5}{3}} = 1 + \frac{1}{1 + \frac{2}{3}} = 1 + \frac{1}{1 + \frac{1}{\frac{3}{2}}} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}$$

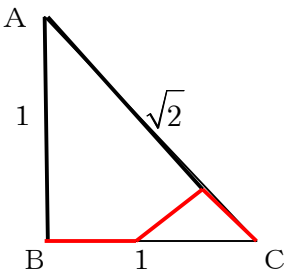
のように，**“有限連分数”**で表され，$a_4 = 0$ だから，$a_n = 0\ (n \geq 4)$ となります．

また，$a = \sqrt{2}$ のとき，上の（1）から分かるように，$a_n \neq 0\,(\text{for all}\ \ n \in \mathbb{N})$ だから

$$a = \sqrt{2} = 1 + \left(\sqrt{2} - 1\right) = 1 + \frac{1}{\sqrt{2} + 1}$$

$$= 1 + \frac{1}{2 + \left(\sqrt{2} - 1\right)} = 1 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}$$

$$= 1 + \frac{1}{2 + \frac{1}{2 + \left(\sqrt{2} - 1\right)}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}}$$



となり，以下同様に繰り返されるので，この場合，a は**“無限連分数”**になります．．

なお，数列 $\{x_n\}$ を，

$$x_{n+1} = 1 + \frac{1}{x_n + 1}\ (n \geq 1),\quad x_1 = 1$$

で定めると，これは $\sqrt{2}$ に収束する“有理数”の数列を構成していきます．この漸化式は 1 次分数形の漸化式で定型的解法によって，簡単に一般項を求めることができますが，具体的に調べると

$$x_2 = \frac{3}{2} = 1.5,\quad x_3 = \frac{7}{5} = 1.4,\quad x_4 = \frac{17}{12} = 1,4166\cdots,$$

$$x_5 = \frac{41}{29} = 1.41379\cdots \qquad x_6 = \frac{99}{70} = 1.41428\cdots,\quad x_7 = \frac{239}{169} = 1.41420\cdots$$

のようになり，確かに $\sqrt{2}$ にどんどん近づいていることが“予感”できます．さらに，この

漸化式は，右上図のような，３辺の長さが，1，1，$\sqrt{2}$ の直角二等辺三角形を利用して幾何学的に導くこともできます．ここでは，解説しませんが，興味のある方は，拙著『古代ギリシアの数理哲学への旅』（現代数学社）の 61 頁を参照してください．

本問の補足解説の最後に，1993 年早大・理工で出題された連分数と整数の問題および答のみを紹介しておきます．解答は，各自の練習問題ということにしておきましょう．

［１］α,β を互いに素な正の整数とする．

（１）$\alpha x-\beta y=0$ の整数解をすべて求めよ．

（２）$\dfrac{\alpha}{\beta}=a_1+\dfrac{1}{a_2+\dfrac{1}{a_3+\dfrac{1}{a_4}}}$ （a_1,a_2,a_3,a_4 は正の整数）と書けるとする．

$a_1+\dfrac{1}{a_2+\dfrac{1}{a_3}}$ を通分して得られる分子 $a_1a_2a_3+a_1+a_3$ を p，分母 a_2a_3+1 を q とするとき，$\alpha q-\beta p$ の値を求めよ．

［２］$157x-68y=3$ の整数解をすべて求めよ．

≪答≫［１］（１）α,β が互いに素であることから，$(x,y)=(\beta k,\alpha k)\ (k\in\mathbb{Z})$ □

（２）$\alpha q-\beta p=1$ □

［２］$(x,y)=(39+68k,90+157k)$ （$k\in\mathbb{Z}$） □

次は，二項係数に関する 2009 年東大・理科の問題です．（１），（２）は文科との共通問題で，前問同様，（３）が理科固有の問いです．二項係数は，東大数学の頻出テーマであることは，これまでの“東大数学パトロール”の読者の方々は先刻ご承知でしょう．

【５・６】自然数 $m\geq 2$ に対し，$m-1$ 個の二項係数

$${}_m\mathrm{C}_1,\ {}_m\mathrm{C}_2,\ \cdots,\ {}_m\mathrm{C}_{m-1}$$

を考え，これらすべての最大公約数を d_m とする．すなわち d_m はこれらすべてを割り切る最大の自然数である．

（１）m が素数ならば，$d_m=m$ であることを示せ．

（２）すべての自然数 k に対し，k^m-k が d_m で割り切れることを，k に関する数学的帰納法によって示せ．

（３）m が偶数のとき d_m は１または２であることを示せ．

［解説］（１）　$r!\,{}_m\mathrm{C}_r=m\times(m-1)\cdots\cdots(m-r+1)\ (r=1,2,\cdots,m-1)$

だから，m が素数であることから

$$m\mid {}_m\mathrm{C}_r\quad (r=1,2,\cdots,m-1)$$

すなわち，m は $m-1$ 個の二項係数の公約数である．しかるに，

$$ {}_m\mathrm{C}_1 = m $$

であるから，m は $m-1$ 個の二項係数の最大公約数である．よって，

$$ d_m = m \ \square $$

（2）$k=1$ のときは明らかに成り立つので，1以上のある k について，

$$ d_m \mid (k^m - k) $$

が成り立つとする．このとき，

$$ (k+1)^m - (k+1) = k^m - k + \sum_{r=1}^{m-1} {}_m\mathrm{C}_r k $$

であるから，帰納法の仮定と d_m の定義により，

$$ d_m \mid (k+1)^m - (k+1) $$

よって，すべての自然数 k に対して，

$$ d_m \mid k^m - k \ \square $$

（3）$m = 2n \ (n \in \mathbb{N})$ とおくと，

$$ \sum_{r:odd} {}_{2n}\mathrm{C}_r = {}_{2n}\mathrm{C}_1 + {}_{2n}\mathrm{C}_3 + {}_{2n}\mathrm{C}_5 + \cdots\cdots + {}_{2n}\mathrm{C}_{2n-1} = 2^{2n-1} \quad \cdots (*) $$

が成り立つことに注意する．（2）において，$m = 2n \ (n \in \mathbb{N})$，$k = 2$ とおくと，

$$ 2^m - 2 = 2^{2n} - 2 = 2(2^{2n-1} - 1) $$

であり，（2）の結果より，$d_m \mid (2^m - 2)$ だから

$$ d_m \mid 2(2^{2n-1} - 1) \qquad \therefore \quad 2^i \nmid d_m \ (i \geq 2) \quad \cdots ① $$

一方，（*）と d_m の定義により，

$$ d_m \mid 2^{2n-1} $$

となり，d_m は2の冪乗の形である．よって，　①より，

$$ d_{2m} = 1, 2 \ \square $$

等式（*）は，よく知られた結果で，n を自然数とすると，一般に，

$$ \sum_{k:even} {}_n\mathrm{C}_r = {}_n\mathrm{C}_0 + {}_n\mathrm{C}_2 + {}_n\mathrm{C}_4 + \cdots = 2^{n-1} $$

$$ \sum_{k:odd} {}_n\mathrm{C}_r = {}_n\mathrm{C}_1 + {}_n\mathrm{C}_3 + {}_n\mathrm{C}_5 + \cdots = 2^{n-1} $$

が成り立ちます．難関校受験生は，証明，結果とも常識にしておきたいものです．

（3）は次のように，背理法で証明することもできます．いま m を偶数とし，$d_m \geq 3$ とします．また，$f(k) = k^m - k$ とおきます．このとき，$d_m - 1 \geq 2$ で，

$$ f(d_m - 1) = (d_m - 1)^m - (d_m - 1) \equiv (-1)^m - (-1) = 2 \pmod{d_m} $$

したがって，$f(d_m-1)$ を d_m で割ると２余り，これは（２）の結果と矛盾します．すなわち，$d_m<3$，つまり，m が偶数のとき，$d_m=1,2$ が示されたことになります．

次は，2014 年の東大・理科の問題．これも（１）～（３）は文科との共通問題です．（４）は少々厄介ですが，**“鳩の巣論法あるいはディリクレの引き出し論法”**が鍵になります．やはり，並みの受験生には難しいかもしれませんが，東大，京大，東工大レベルを志す受験生には，学んでおいてほしい知識です．

【５・７】 r を 0 以上の整数とし，数列 $\{a_n\}$ を次のように定める．

$$a_1=r,\quad a_2=r+1,\quad a_{n+2}=a_{n+1}(a_n+1)\quad (=1,2,3,\cdots)$$

また，素数 p を１つとり，a_n を p で割った余りを b_n とする．ただし，０を p で割った余りは０とする．

（１）自然数 n に対し，b_{n+2} は $b_{n+1}(b_n+1)$ を p で割った余りと一致することを示せ．

（２）$r=2$，$p=17$ の場合に，10 以下のすべての自然数 n に対して，b_n を求めよ．

（３）ある２つの異なる自然数 n,m に対して，$b_{n+1}=b_{m+1}>0$，$b_{n+2}=b_{m+2}$ が成り立ったとする．このとき，$b_n=b_m$ が成り立つことを示せ．

（４）$a_2,a_3,a_4,\cdots$ に p で在り切れる数が現れないとする．このとき，a_1 も p で割り切れないことを示せ．

［解説］（１）仮定より，$a_{n+1}\equiv b_{n+1}(\mathrm{mod}\,p)$，$a_n+1\equiv b_n+1(\mathrm{mod}\,p)$ だから，

$$a_{n+1}(a_n+1)\equiv b_{n+1}(b_n+1)(\mathrm{mod}\,p)$$

一方，$a_{n+2}\equiv b_{n+2}(\mathrm{mod}\,p)$，$a_{n+2}=a_{n+1}(a_n+1)$

$$\therefore\quad b_{n+2}\equiv b_{n+1}(b_n+1)(\mathrm{mod}\,p)\ \square$$

（２）$r=2$，$p=17$ のとき，b_n の定義と（１）の結果とを用いると，

$a_1=2\quad\therefore\quad b_1=2\ \square$

$a_2=2+1=3\quad\therefore\quad b_2=3\ \square$

$b_3=$［$3(2+1)=9$ を 17 で割った余り］$=9\ \square$

$b_4=$［$9(3+1)=36$ を 17 で割った余り］$=2\ \square$

$b_5=$［$2(9+1)=20$ を 17 で割った余り］$=3\ \square$

以下，同様の，2，3，9 の繰り返しだから，

$b_6=9$，$b_7=2$，$b_8=3$，$b_9=9$，$b_{10}=2\ \square$

（３）$b_{n+1}=b_{m+1}(>0)$・・・①　　$b_{n+2}=b_{m+2}$・・・②

（１）の結果より，k，l を整数として，

$$b_{n+2}-b_{n+1}(b_n+1)=kp\ \text{・・・③}$$

$$b_{m+2}-b_{m+1}(b_m+1)=lp\ \text{・・・④}$$

③，④を辺々引いて，

$$b_{n+2}-b_{m+2}-b_{n+1}b_n+b_{m+1}b_m-b_{n+1}+b_{m+1}=(k-l)p$$

①，②を用いると，

$$b_{m+1}(b_m-b_n)=(k-l)p \quad \cdots ⑤$$

したがって，⑤の左辺はpで割り切れ，

$$0<b_{m+1}\leq p-1,\ -(p-1)\leq b_m-b_n\leq p-1$$

で，かつpが素数だから，

$$b_m-b_n=0 \qquad \therefore \quad b_m=b_n \ \square$$

（4）数列$b_1,b_2,b_3,b_4,\cdots$対して，隣り合う2数を組とする

$$\text{順序対}(b_i,b_{i+1})\ (i=1,2,3,\cdots)$$

を考える．仮定より，$1\leq b_i\leq p-1$，$1\leq b_{i+1}\leq p-1$であるから，(b_i,b_{i+1})の相異なる組は高々$(p-1)^2$個である．したがって，$q=(p-1)^2+1$個の順序対

$$(b_1,b_2),\ (b_2,b_3),\cdots,\ (b_q,b_{q+1})$$

の中には，必ず同じものが存在する（鳩の巣論法あるいはディリクレ論法）．すなわち，

$$(b_s,b_{s+1})=(b_t,b_{t+1})\ (s<t),$$

となる自然数s,tが存在する．すなわち，

$$b_s=b_t \quad \text{かつ} \quad b_{s+1}=b_{t+1}$$

いま．このようなsのうち最小のものを考える．$s>1$とすると，（3）の結果より

$$(b_{s-1},b_s)=(b_{t-1},b_t)$$

が成り立つので，これはsの最小性に反する．したがって，$s=1$で，このとき，

$$b_1=b_t(t>1)$$

となり，$b_t\neq 0$より$b_1\neq 0$だから，

$$p\nmid a_1 \quad （a_1\text{は}p\text{で割り切れない}）$$

よって，題意は示された．□

本問の（4）の［解説］で用いた“鳩の巣論法”とは，小学生でも理解できる原理です．それは要するに，

n羽の鳩とm個の巣箱があり，$n>m$のとき，鳩が一斉に巣箱に入ったとき，どの巣箱かは分からないけれど，（巣箱の中で鳩ぽっぽが共食いしない限り！）少なくとも1つの巣箱には鳩が2羽以上入っている

という，きわめて当たり前の理屈です．

上の解説では，

$$q=(p-1)^2+1\text{個の順序対}(b_1,b_2),\ (b_2,b_3),\cdots,\ (b_q,b_{q+1})$$

が鳩であり，巣箱は，$b_i\ (1\leq b_i\leq p-1)$と$b_{i+1}\ (1\leq b_{i+1}\leq p-1)$から作った，$(p-1)^2$の順序対にほかなりません．

これに関連して思い出すのは，筆者が高校生のとき考えたことのある，以下のような

の問題です.

$$a_1 = a_2 = 1,\ \ a_{n+1} = a_n + a_{n-1}\,(n \geq 2)$$

で定まる数列$\{a_n\}$をフィボナッチ数列といいますが，**この数列の中には任意の自然数kの倍数が必ず存在**します．この不思議な事実？を証明してみよというのが，その問題です.

まず，任意の自然数kに対して,

$$a_i \equiv a_j(\mathrm{mod}k),\ \ a_{i+1} \equiv a_{j+1}(\mathrm{mod}k),\ \ i < j \quad \cdots(*)$$

を満たす自然数i，jが存在することを示してみます.

a_nをkで割った余りをr_nとすると，r_nの取り得る値は高々k通りであるから，順序対$(r_n, r_{n+1)})$の種類は高々k^2通りです．したがって，$l = k^2 + 1$とすると，l個の順序対

$$(r_1, r_2),\ \ (r_2, r_3), \cdots,\ \ (r_l, r_{l+1})$$

の中には，鳩の巣論法により必ず同じものが存在します．いまその２つを

$$(r_i, r_{i+1}),\ \ (r_j, r_{j+1}),\ \ i < j$$

とすると,

$$\begin{cases} r_i = r_j \\ r_{i+1} = r_{j+1} \end{cases} \Leftrightarrow \begin{cases} a_i \equiv a_j\,(\mathrm{mod}\,k) \\ a_{i+1} \equiv a_{j+1}\,(\mathrm{mod}\,k) \end{cases} \cdots(**)$$

となり，（$*$）を満たすi, jが存在することが分かりました.

いま，このようなiの最小値をpとし，$p > 2$とします．すると，（$**$）とフィボナッチ数列の定義から

$$a_{p+1} - a_p \equiv a_{j+1} - a_j(\mathrm{mod}k) \qquad \therefore \quad a_{p-1} \equiv a_{j-1}(\mathrm{mod}k)$$

$$\therefore \quad r_{p-1} = r_{j-1} \qquad \therefore \quad \begin{cases} r_{p-1} = r_{j-1} \\ r_p = r_j \end{cases}$$

すなわち，これは，pの最小性に反します．したがって，$p = 1$となり，このとき，$a_1 = a_2 = 1$とから,

$$\begin{cases} a_1 \equiv a_j(\mathrm{mod}\,k) \\ a_2 \equiv a_{j+1}\,(\mathrm{mod}\,k) \end{cases} \quad \therefore \quad \begin{cases} 1 \equiv a_j(\mathrm{mod}\,k) \\ 1 \equiv a_{j+1}(\mathrm{mod}\,k) \end{cases}$$

したがって，$0 \equiv a_{j+1} - a_j(\mathrm{mod}\,k) \qquad \therefore \quad a_{j-1} \equiv 0(\mathrm{mod}k)$

つまり，a_{j-1}はkの倍数であり，当初の目標が示されたことになります.

$k = 3$として，少し具体的に説明してみます．フィボナッチ数列$\{a_n\}$は,

$a_1 = 1,,\ \ a_2 = 1,\ \ a_3 = 2,\ \ a_4 = 3,\ \ a_5 = 5,\ \ a_6 = 8,\ \ a_7 = 13$

$a_8 = 21,\ \ a_9 = 34,\ \ a_{10} = 55,\ \ a_{11} = 89,\ \ a_{12} = 144$. ・・・・・

のようになり，したがって,

$(r_1, r_2) = (1,1)$，$(r_2, r_3) = (1,2)$，$(r_3, r_4) = (2,0)$，$(r_4, r_5) = (0,2)$，$(r_5, r_6) = (2,2)$，
$(r_6, r_7) = (2,1)$，$(r_7, r_8) = (1,0)$，$(r_8, r_9) = (0,1)$，$(r_9, r_{10}) = (1,1)$，$(r_{10}, r_{11}) = (1,2)$，

となります．このとき，$\begin{cases} a_i \equiv a_j \pmod 3 \\ a_{i+1} \equiv a_{j+1} \pmod 3 \end{cases}$ を満たす i の最小値は，$i = 1$ で，それゆえ $j = 9$ となります．つまり，

$$1 \equiv 34 \pmod 3,\ 1 \equiv 55 \pmod 3 \quad \text{より} \quad 0 \equiv 21 \pmod 3$$

となって，確かに $21 (= a_8)$ は 3 の倍数で，これはフィボナッチ数列の第 5 項です．

$k = 3$ のときは，こんなことをしなくてもその倍数を見つけることは容易ですが，たとえば“$k = 2020$”の倍数が存在するか，ということになれば，これは具体的に実験して調べると相当時間がかかりそうです．やはり，上で述べてきたような“理論”も大切で，あらためて人生というものは一筋縄ではいかないことが実感できるでしょう．

■整数の応用問題

この節では，“整数の応用問題”を紹介してみます．最初は，1989 年の東大・理科の問題です．問題文の $3^{21} = 10460353203$ がヒントになります．

【５・８】 $\dfrac{10^{210}}{10^{10} + 3}$ の整数部分の桁数と，一の位の数字を求めよ．ただし，$3^{21} = 10460353203$ を用いてよい．

［解説］ $N = \dfrac{10^{210}}{10^{10} + 3}$ とおくと，$10^{10} < 10^{10} + 3 < 10^{11}$ であるから，

$$10^{199} = \frac{10^{210}}{10^{11}} < N < \frac{10^{210}}{10^{10}} = 10^{200}$$

$\therefore$　（N の整数部分の桁数）＝200 □

また，$a = 10^{10}$（百億），$b = 3$ とおくと，

$$N = \frac{a^{21}}{a+b} = \frac{a^{21} + b^{21} - b^{21}}{a+b}$$

$$= \frac{(a+b)(a^{20} - a^{19}b + \cdots\cdots - ab^{19} + b^{20})}{a+b} - \frac{b^{21}}{a+b}$$

$$= (a^{20} - a^{19}b + \cdots\cdots - ab^{19} + b^{20}) - \frac{b^{21}}{a+b}$$

ここで，上式の（　）内の一の位の数字は

$$b^{20} = 3^{20} = (3^4)^5 = 81^5 \text{ の一の位の数字は } 1$$

に等しく，

$$\frac{b^{21}}{a+b}=\frac{3^{21}}{10^{10}+3}=\frac{10460353203}{10000000003}=1.046\cdots\cdots$$

である．よって，

（N の一の位の数字）＝9□

ちょっと，トリッキーな問題ですが，この種の問題も東大では，思い出したようにときどき出題されます．なお，n が奇数のとき，

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

という分解は常識にしておきたいものです．これは，因数定理から明らかでしょう．

次は，2002 年東大・理科の問題．シャッフルに関するもので，これは“数論”ではしばしば登場してくるテーマです．

【５・９】 N を正の整数とする．$2N$ 個の項からなる数列

$$\{a_1,a_2,\cdots\cdots,a_N,b_1,b_2,\cdots\cdots,b_N\}$$

を

$$\{b_1,a_1,b_2,a_2,\cdots\cdots\cdots\cdots,b_N,a_N\}$$

という数列に並べ替える操作を「シャッフル」と呼ぶことにする．並べ替えた数列は b_1 を初項とし，b_i の次に a_i，a_i の次に b_{i+1} が来るようなものになる．また，数列 $\{1,2,\cdots\cdots,2N\}$ をシャッフルしたときに得られる数列において，数 k が現れる位置を $f(k)$ で表す．

たとえば，$N=3$ のとき，$\{1,2,3,4,5,6\}$ をシャッフルすると $\{4,1,5,2,6,3\}$ となるので，$f(1)=2, f(2)=4, f(3)=6, f(4)=1, f(5)=3, f(6)=5$ である．

（１）数列 $\{1,2,3,4,5,6,7,8\}$ を３回シャッフルしたときに得られる数列を求めよ．

（２）$1\le k\le 2N$ を満たす任意の整数 k に対し，$f(k)-2k$ は $2N+1$ で割り切れることを示せ．

（３）n を正の整数とし，$N=2^{n-1}$ のときを考える．数列 $\{1,2,3,\cdots\cdots,2N\}$ を $2n$ 回シャッフルすると，$\{1,2,3,\cdots\cdots,2N\}$ に戻ることを証明せよ．

［解説］（１）具体的に調べると，

１回後は，$\{5,1,6,2,7,3,8,4\}$

２回後は，$\{7,5,3,1,8,6,4,2\}$

よって，３回シャッフルして得られる数列は，

$\{8,7,6,5,4,3,2,1\}$ □

（２）（ｉ）$1\le k\le N$ のとき；

$\{1,2,\cdots\cdots,k,\cdots\cdots,N,N+1,N+2,\cdots\cdots,N+k,\cdots\cdots,2N\}$

をシャッフルすると，

$\{N+1,1,N+2,2,N+3,3,\cdots\cdots\cdots,N+k,k,\cdots\cdots\cdots,2N,N\}$

だから，

$$f(k)=2k \Leftrightarrow f(k)-2k=0$$

$\therefore \quad 2N+1 \mid (f(k)-2k)$

（ⅱ） $N+1 \le k \le 2N$ のとき；

$k = N + (k-N)$ に注意すると，

$$\{1, 2, \cdots\cdots\cdots, N, N+1, \cdots\cdots, N+(k-N), \cdots\cdots\cdots, 2N\}$$

をシャッフルすると，

$$\{N+1, 1, N+2, 2, \cdots\cdots, N+(k-N), k-N, \cdots\cdots\cdots, 2N\}$$

だから，

$$f(k) = 2(k-N)-1 \Leftrightarrow f(k)-2k = -2N-1$$

$$\therefore \quad 2N+1 \mid (f(k)-2k)$$

よって，題意は示された．□

（3） $1 \le k \le 2N (k \in \mathbb{N})$ とする．いま非負整数 i に対して，

$$f^0(k) = k, \quad f^i(k) = f(f^{i-1}(k)) \ (i \ge 1)$$

のように定めると， $f^i(k)$ は i 回シャッフルしたときの k の位置である．（2）より，

$$f(k) \equiv 2k \pmod{2N+1}$$

であるから，これを用いると，

$$f^2(k) = f(f(k)) \equiv 2f(2k) \equiv 2^2 f(k) \pmod{2N+1}$$

$$f^3(k) = f(f^2(k)) \equiv 2f(2^2 f(k)) \equiv 2^3 f(k) \pmod{2N+1}$$

以下，同様に考えると，

$$f^{2n}(k) \equiv 2^{2n} k \pmod{2N+1} \quad \cdots ①$$

一方，仮定から $N = 2^{n-1}$ だから， $2N+1 = 2^n + 1$.

$$\therefore \quad 2^{2n}k - k = (2^n+1)(2^n-1)k = (2N+1)(2^n-1)k$$

$$\therefore \quad 2^{2n}k \equiv k \pmod{2N+1} \quad \cdots ②$$

①，②から， $f^{2n}(k) \equiv k \pmod{2N+1}$

f の定義により， $1 \le f^{2n}(k) \le 2N$ であるから，

$$f^{2n}(k) = k \quad (\text{for all } k).$$

よって，題意は示された．□

唐突ですが，シャッフルの問題は 2000 年の日本数学オリンピックの“本選”でも，出題されています．この際ですから，紹介してみます．

左から順に $a_1, a_2, \cdots, a_{3n}$ と書かれた $3n$ 枚のカードが並んでいるとき，以下のような（ⅰ），（ⅱ）の操作をすることを，シャッフルと呼ぶことにする．

（ⅰ）次の（B）のように，（A）を３つの行に分ける．

$$a_1, a_2, a_3, \ a_4, a_5, a_6, \ a_7, a_8, a_9, \ \cdots, \ a_{3n-2}, a_{3n-1}, a_{3n} \qquad (A)$$

$$a_1, \ a_4, \ a_7, \ \cdots \ , \ a_{3n-2}$$

$$a_2, \ a_5, \ a_8, \ \cdots \ , \ a_{3n-1} \qquad (B)$$

$$a_3, \ a_6, \ a_9, \ \cdots \ , \ a_{3n}$$

（ⅱ）次の（C）のように，上の（B）の３つの行をつなげる．

$$a_3, a_6, a_9, \cdots, a_{3n}, \ a_2, a_5, a_8, \cdots, a_{3n-1}, \ a_1, a_4, a_7, \cdots, a_{3n-2} \qquad (C)$$

例えば，左から 1，2，3，4，5，6 と並んだ６枚のカードを１回，２回，・・・とシャッ

フルしていくと，

1，2，3，4，5，6
3，6，2，5，1，4
2，4，6，1，3，5
・・・・・・

となっていく．このとき，以下の問に答えよ．
問　左から 1，2，3，4，・・・，190，191，192 と並んだ 192 枚のカードを何回かシャッフルすると，これが 192，191，190，・・・，4，3，2，1 の順番になることがあるか．

“8 回のシャッフル”によって，題意のような順番になりますが，興味関心のある方は，拙著『整数の理論と演習』（現代数学社）の 286，287 頁を参照して下さい．

さて，次はベクトル，三角形の絡む整数問題．2010 年の東大・文理共通問題です．さほど難しいものではありません．

【５・１０】C を半径１の円周とし，Ａを C 上の１点とする．３点Ｐ，Ｑ，ＲがＡを時刻 $t=0$ に出発し，C 上を各々一定の速さで，Ｐ，Ｑは反時計回りに，Ｒは時計回りに，時刻 $t=2\pi$ まで動く．Ｐ，Ｑ，Ｒの速さは，それぞれ $m,1,2$ であるとする．（したがって，Ｑは C をちょうど一周する．）ただし，m は $1\leq m\leq 10$ を満たす整数である．△ＰＱＲがＰＲを斜辺とする直角二等辺三角形となるような速さ m と時刻 t の組をすべて求めよ．

［解説］円の中心をＯとすると，ＯＡを始線とするときの

$\overrightarrow{\mathrm{OP}}$，$\overrightarrow{\mathrm{OQ}}$，$\overrightarrow{\mathrm{OR}}$ の偏角はそれぞれ，mt，t，$-2t$

である．△ＰＱＲがＰＲを斜辺とする直角二等辺三角形となる条件は，ＰＲが円の直径で，ＯＱ⊥ＯＲとなることであるから，

$$mt+2t=\pi+2k\pi \quad \cdots ①$$

$$3t=\frac{\pi}{2}+l\pi \qquad \cdots ② \qquad (k,l\in\mathbb{Z})$$

②と $0\leq t\leq 2\pi$ より，$t=\dfrac{2l+1}{6}\pi\ (l=0,1,2,3,4,5)$ ・・・③

③を①に代入して整理すると，

$$(m+2)(2l+1)=6(2k+1)$$

$$\therefore\quad (m+2)(2l+1)-6\equiv 0 \pmod{12} \quad \cdots ④$$

④を満たす $m\ (1\leq m\leq 10)$ を求めると，

$l=0$ のとき，$m=4$，　$l=1$ のとき，$m=4,8$
$l=2$ のとき，$m=4$，　$l=3$ のとき，$m=4$
$l=4$ のとき，$m=4,8$，　$l=5$ のとき，$m=4$

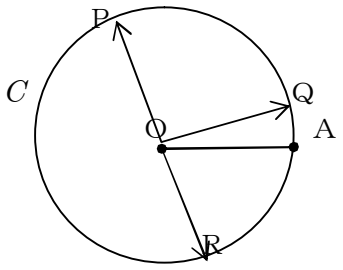
よって，m と t の組 (m,t) は，

$$(m,t)=\left(4,\frac{\pi}{6}\right),\left(4,\frac{\pi}{2}\right),\left(8,\frac{\pi}{2}\right),\left(4,\frac{5\pi}{6}\right),\left(4,\frac{7\pi}{6}\right),\left(4,\frac{3\pi}{2}\right),\left(8,\frac{3\pi}{2}\right),\left(4,\frac{11\pi}{6}\right)\ \square$$

題意を図示すると．右下図のようになり

ます．ポイントは，直角二等辺三角形の条件をどのように数式で表現するか，であり，これが，上の［解説］の①，②になります．

後半のポイントは④で，これは簡単な合同式にほかなりません．



文理共通問題ということで，理系の受験生はこの程度の問題は完答してほしいのですが，こういう問題では謂わば**“数学言語のリテラシー”**が問われています．日頃から幾何学的条件，代数的条件，解析的条件などをどのように表現するか，意識的に考える習慣をつけてほしいものです．

次は，2008 年東大・理科の“レピュニット数(repeated unit number)”についての問題です．易しいとは言えませんが，興味深い面白いテーマです．果敢に挑戦してほしいものです．

【５・１１】自然数 n に対し，$\dfrac{10^n-1}{9}=\overbrace{111\cdots111}^{n個}$ を $\boxed{n}$ で表す．たとえば $\boxed{1}=1$，$\boxed{2}=11$，$\boxed{3}=111$ である．

（1） m を 0 以上の整数とする．$\boxed{3^m}$ は 3^m で割り切れるが，3^{m+1} では割り切れないことを示せ．

（2） n が 27 で割り切れることが，$\boxed{n}$ が 27 で割り切れるための必要十分条件であることを示せ．

［解説］（1）数学的帰納法で示す．

$m=0$ のとき，$\boxed{3^0}=\boxed{1}=1$

だから成り立つ．そこで，0 以上のある整数 m に対して

$$\boxed{3^m}=\frac{10^{3^m}-1}{9}=\frac{10^a-1}{9}\ (a=3^m)$$

が 3^m で割り切れるが，3^{m+1} で割り切れないとする．このとき，

$$\boxed{3^{m+1}}=\frac{10^{3^{m+1}}-1}{9}=\frac{10^{3a}-1}{9}=\frac{10^a-1}{9}(10^{2a}+10^a+1)$$

$$=\boxed{3^m}(10^{2a}+10^a+1)$$

であり，$10=9+1$ であるから，２項定理より

$$10^{2a}+10^a+1=9K+3\ （K\text{ は整数}）$$

とおけるので，

$$\boxed{3^{m+1}}=\boxed{3^m}\times3(3K+1)$$

と書けて，帰納法の仮定より $\boxed{3^{m+1}}$ は 3^{m+1} で割り切れ，3^{m+2} では割り切れない．

よって，題意は示された．□

（2） n が 27 で割り切れるとし，$n=27q$ （q は自然数）とおく．このとき，

$$\boxed{n}=\boxed{27q}=\frac{10^{27q}-1}{9}=\frac{(10^{27})^{q}-1}{9}$$

$$=\frac{10^{27}-1}{9}\left(10^{27(q-1)}+10^{27(q-2)}+\cdots+10^{27}+1\right)$$

$$=\boxed{3^3}\times\left(10^{27(q-1)}+10^{27(q-2)}+\cdots+10^{27}+1\right)$$

であるから，（1）の結果から $\boxed{n}$ は 27 で割り切れる．

逆に，$\boxed{n}$ が 27 で割り切れるとする．いま，$n=27q+r\ (0\le r\le 26)$ とする．このとき，$\boxed{0}=0$ と定めておくと，

$$\boxed{n}=\frac{10^{27q+r}-1}{9}=\frac{10^{27q+r}-10^{r}+10^{r}-1}{9}$$

$$=\frac{10^{27q}-1}{9}\times 10^{r}+\frac{10^{r}-1}{9}$$

$$=\boxed{27q}\times 10^{r}+\boxed{r}$$

したがって，$\boxed{r}$ が 27 で割り切れるための条件を考えておけばよい．

$r=0$ のときは，$\boxed{r}$ は 27 で割り切れるので，$1\le r\le 26$ とする．

$$\boxed{r}=10^{r-1}+10^{r-2}+\cdots+10+1$$

$$=(9+1)^{r-1}+(9+1)^{r-2}+\cdots+(9+1)+1$$

だから，2項定理より，

$$\boxed{r}=9L+r\ （L\text{ は整数}）$$

とおけるので，$\boxed{r}$ が 27 で割り切れるならば 9 でも割り切れるので，$r=9,18$ である．

$r=9$ のとき，$\boxed{r}=\boxed{3^2}$ だから（1）の結果より不適である．

$r=18$ のとき，$\boxed{r}=\dfrac{10^{18}-1}{9}=\dfrac{10^{9}-1}{9}(10^{9}+1)=\boxed{3^2}\times(10^{9}+1)$

となり，$10^{9}+1=3M+2$ （M は整数）とおけるので，不適．すなわち，

$$n=27q$$

となって，n は27 で割り切れる．

以上より，題意は示された．□

本問で取り上げたタイプの数を**レピュニット数**（unit＝1 が続く数という意味）と言います．いまこれを

$$R_n=\boxed{n}=\frac{10^{n}-1}{9}=\overbrace{111\cdots111}^{n\text{個}}$$

と書くことにするとき，数列 $\{R_n\}\ (n=1,2,3,\cdots)$ には，一体，どれくらいの頻度で素数が

存在するのでしょうか？

実は，これは現在でも十分解明されていない（はずの）問題で，今から 13 年前の 2007 年の時点でレピュニット素数は

$$R_2,\ R_{19},\ R_{23},\ R_{317},\ R_{1031},\ R_{49081},\ R_{86453},\ R_{109297},\ R_{270343}$$

の９個しか見つかっていません．このようなタイプの素数がごく稀にしか存在しないのは分かりますが，このタイプの素数が無限個存在するか否か，またR_nが素数であるためのnの条件等は，全く分かっていません．

高校生でも証明できるレピュニット数に関する命題に以下のようなものがあります．

（ⅰ）$n \mid m$ ならば，$R_n \mid R_m$ である．

（ⅱ）D が R_n と R_m の公約数であれば，$D \mid R_{m+n}$ である．

（ⅲ）$\gcd(n,m)=1$ ならば，$\gcd(R_n,R_m)=1$ である．

（ⅳ）$\gcd(n,m)=d$ ならば，$\gcd(R_n,R_m)=R_d$ である．

これらの命題の証明はここでは割愛しますが，興味のある方は拙著『整数問題の解法研究』（聖文新社）の 188，189 頁を参照して下さい．

この他にも，第１回目のブログの【１・４】(1998 年)，【１・５】(2015 年）で紹介した二項係数と整数に関する東大の問題も是非チェックしておいて下さい．

さて，今回のブログの最後は，以下の 2002 年慶應大学・医の“$4k+1$ 型の素数”の問題です．2000 年前後の慶大・医の問題は特に難しく，この問題も含めて試験時間内で全４題を完答することは至難の業，200%（？）不可能で，いまは亡き畏友の数学講師と“正気の沙汰ではない”と話し合ったことを思い出します．とは言え，以下の問題は“教育的”には大変興味深い問題で，読者諸君もそのつもりで付き合ってみて下さい．入試問題の“上限”が垣間見える問題です．

【５・１２】 ４で割ると余りが１になるような素数p，$p=4k+1$，を１つとる．これに対し，等式

$$\text{（Q）}\quad a^2+4bc=p$$

を満たす自然数３つの組(a,b,c)の全体を考える．両辺の絶対値を比べれば分かるように，このような自然数３つの組の可能性は有限通りしかありえない．

いま等式（Q）を満たす自然数３つの組(a,b,c)から新しく自然数３つの組を作る手続きを次の（ⅰ），（ⅱ），（ⅲ）により定める．

（ⅰ）$a<b-c$ ならば$(a+2c,c,b-a-c)$ を作る．

（ⅱ）$b-c<a<2b$ ならば$(2b-a,b,a-b+c)$ を作る．

（ⅲ）$a>2b$ ならば$(a-2b,a-b+c,b)$ を作る．

（１）(a,b,c)が等式（Q）を満たす自然数の組でさらに（ⅰ）の条件$a<b-c$を満たすとする．このとき，上の（ⅰ）より得られる$(a+2c,c,b-a-c)$ もまた等式（Q）を

満たすことを示しなさい.

（２）等式（Q）を満たす自然数の組(a,b,c)は$a=b-c$や$a=2b$を満たすことはないことを示しなさい.

（３）等式（Q）を満たす自然数の組(a,b,c)の中には，上の手続きを施しても変化しないという性質を持つものが存在する．$p=4k+1$と表すとき，この性質を持つ(a,b,c)をkを用いて具体的に与え，かつそれがただ１組しか存在しないことを示しなさい.

（４）等式（Q）を満たす自然数の組(a,b,c)に対して上の手続きを２回繰返して施すとどうなるか，結論を簡潔に説明しなさい．また，この観察をもとに等式（Q）を満たす自然数３つの組の全体の個数が偶数か奇数かを決定し，そう判断できる理由を述べなさい．ただし，等式（Q）を満たす自然数３つの組から上の手続きにより新しく作られた自然数３つの組は（ⅰ），（ⅱ），（ⅲ）のどの場合でも再び等式（Q）を満たすという事実についてはここでは証明なしに用いてよい.

（５）素数$p=4k+1$をある２つの自然数a,bにより$p=a^2+(2b)^2$と表すことができることを示しなさい.

［解説］解説に入る前に，集合Sと，題意の手続き（ⅰ）～（ⅲ）にしたがって写像σを以下のように定めておく.

$$S=\{(a,b,c)\,|\,a^2+4bc=p\ \cdots(\mathrm{Q})\}\ (\subset \mathbb{N}\times\mathbb{N}\times\mathbb{N}=\mathbb{N}^3)$$

ただし，pは$p=4k+1\ (k\in\mathbb{N})$の形の素数

$$\sigma:S\ni(a,b,c)\mapsto\begin{cases}(a+2c,c,b-a-c) & (a<b-c) \quad \cdots①\\ (2b-a,b,a-b+c) & (b-c<a<2b)\cdots②\\ (a-2b,c-b+c,b) & (a>2b) \quad \cdots③\end{cases}$$

なお，問題文で指摘されているように，素数$p=4k+1$を１つ固定したとき，集合Sは有限集合である.

（１）$(a,b,c)\in S$に対して，$(a_1,b_1,c_1)=(a+2c,c,b-a-c)$とおくと，

$$a_1^{\,2}+4b_1c_1=(a+2c)^2+4c(b-a-c)=a^2+4bc=p$$

$$\therefore\quad (a+2c,c,b-a-c)\in S$$

よって，題意は示された．□

＜注＞上は，①の場合に，写像σが，$\sigma:S\to S$であることを示したものであるが，②，③の場合についても，σはSからSへの写像，すなわち$\sigma(S)\subseteq S$であることが容易に示される.

（２）$(a,b,c)\in S$が$a=b-c$を満たすとすると，

$$a^2+4bc=(b-c)^2+4bc=(b+c)^2\ \neq\text{素数}$$

また，$a=2b$を満たすとすると，

$$a^2+4bc=(2b)^2+4bc=4b(b+c)\neq\text{素数}$$

となり，これは不合理である．よって，

$$a\neq b-c\quad\text{かつ}\quad a\neq 2b\ \square$$

（３）$\sigma((a,b,c))=(a,b,c)$が成り立つとき，第１成分が一致することが必要で，

$$a+2c>a,\quad a-2b<a$$

であるから，①，③の場合は，

$$\sigma((a,b,c))=(a,b,c)\ \cdots(*)$$

は成り立たない．したがって，（＊）が成り立つのは②の場合で，このとき，

$$(2b-a,b,a-b+c)=(a,b,c) \Leftrightarrow a=b$$

これを，$a^2+4bc=p$ に代入すると，

$$a^2+4ac=p \qquad \therefore \quad a(a+4c)=p$$

p は素数で，$a<a+4c$ であるから，$a=1$，$a+4c=p\ (=4k+1)$

$$\therefore \quad (a,b,c)=(1,1,k)$$

すなわち，写像 σ の“不動点”は $(1,1,k)$ に限られ，題意が示されたことになる．□

（4）実際に調べてみると，「2回の操作でもとに戻る」□

以下，上の結論を証明しておく．操作を $n(\geq 0)$ 回繰り返して得られる自然数の組を (a_n,b_n,c_n) とする．

(a,b,c) が①の条件を満たすとき，$(a_1,b_1,c_1)=(a+2c,c,b-a-c)$ で，

$$a_1=a+2c>2c=2b_1$$

であるから，③より，

$$a_2=a_1-2b_1=(a+2c)-2c=a$$

$$b_2=a_1-b_1+c_1=(a+2c)-c+(b-a-c)=b$$

$$c_2=b_1=c$$

$$\therefore \quad (a_2,b_2,c_2)=(a,b,c)$$

同様に，②，③の条件を満たす場合も，$(a_2,b_2,c_2)=(a,b,c)$ となる．

また，上の観察から，S の要素で $(a,b,c)\neq(a_1,b_1,c_1)$ の組；

$$\{(a,b,c),(a_1,b_1,c_1)\}$$

の個数を n とすると，$(a,b,c)=(a_1,b_1,c_1)$（σ の不動点）となるのは，（3）より

$$(a,b,c)=(1,1,k)$$

のみであるから，集合 S の要素の個数 $|S|$ は

$$|S|=2n+1$$

である．すなわち，

集合 S の要素の個数は奇数□

（5）“$(a,b,c)\in S \Leftrightarrow (a,c,b)\in S$ ”に注意する．集合 S の中に，$b=c$ となるものが存在しないとすると，

(a,b,c) と (a,c,b) $(b\neq c)$ とは1対1に対応する

ので，集合 S の要素の個数は偶数となる．しかるに，これは（4）の後半の結論と矛盾する．よって，S の中には $b=c$ となる自然数の組が存在し，これを用いると

$$p=a^2+4bc=a^2+(2b)^2$$

と表すことができ，題意は示された．□

本問は，オイラーが証明した有名な定理であり，“平方剰余に関する第1補充法則”を利用しても証明できます．［解説］の証明はドイツ，ハイデルベルグ生まれの数学者ザギエ氏（Don Zagier，1951～）によるもので，この証明は平方剰余（これについて興味のある人

は，拙著『整数の理論と演習』（現代数学社）を参照せよ）に一切触れることなく，高校生でも理解できる見事なものです.

要するに，ザギエ氏の証明は，**写像σの不動点を考え，この不動点によって集合Sの個数が奇数であることを確認し，一方，$b=c$であるようなSの要素が存在しないとすれば，Sの要素の個数は偶数となって，これは矛盾．それゆえ，$p=a^2+4\cdot b\cdot b$を満たす(a,b,b)が存在する**と主張しているのです．簡潔で鮮やかな証明で，脱帽するほかありません.

整数論は，20 世紀の前半までは“最も役に立たない数学”と考えられていましたが，20 世紀半ばから，数論はいわゆる“暗号理論”に応用されはじめ，実は今日では情報セキュリティーに関して，殆どの人（全世界の人類，と言っても大袈裟ではない！）がこの数論の御世話になっています.

いわゆる“ElGamal 暗号”の理論的背景にあるのが，離散対数という数論の理論で，これは，$a^y\equiv x(\mathrm{mod}\,p)$において$a$と$x$から$y$を求めることの難しさを利用したものです.

この他にも，巨大な整数の素因数分解の難しさを利用した“RSA 暗号”も有名です．これは，1978 年に Rivest，Shamir，Adleman の 3 人によって提案された暗号で，今日広く利用されています.

暗号理論に興味があれば，『暗号の数理』（一松信著・講談社），『素数入門』（講談社・芹沢正三著・講談社）などを参照されるといいでしょう．また，もう少し専門的な本として『暗号理論の基礎』（Douglas R.Stinson 著，櫻井幸一監訳・共立出版）なども大学入学後に読まれるといいかもしれません．この本の内容は，すべて“数論”と言っても過言ではありません．ちなみに，ちょっと自慢話をすると，芹沢先生の本は，著者ご本人から筆者に直接恵贈して頂き，一松先生からはかつて何通か直接お手紙を頂いたことがあります．お二人とも，不肖筆者の恩師だと，ご迷惑も省みずに勝手に考えています（笑）.

今回は，かなり重い問題を紹介しましたが，次回は空間図形と求積など，空間図形にまつわる標準問題について考えてみたいと思います.

（河田直樹・かわたなおき）