内容解説資料

じつきょう

数学資料 No. 76

変な時計とその仲間たち

早稲田大学教育学部教授　谷山公規

数学の楽しさ・美しさを高校生に伝える題材の一つとして，代数学のいくつかの命題に基づく数遊びを紹介します。

図1(13)では1から12までが円周上に奇妙な順番で並んでいます。筆者はこれを「変な時計」と呼んでいます。これはどのような順番でしょうか。

図2（次ページ）をご覧ください。1から時計回りに2，4，8までは順に2倍した数になっています。次の3というのは8の2倍の16を13で割った余りです。次の6はまた3の2倍になっています。6を13で割った余りは6ですから，3の2倍の6を13で割った余り，ということも出来ます。

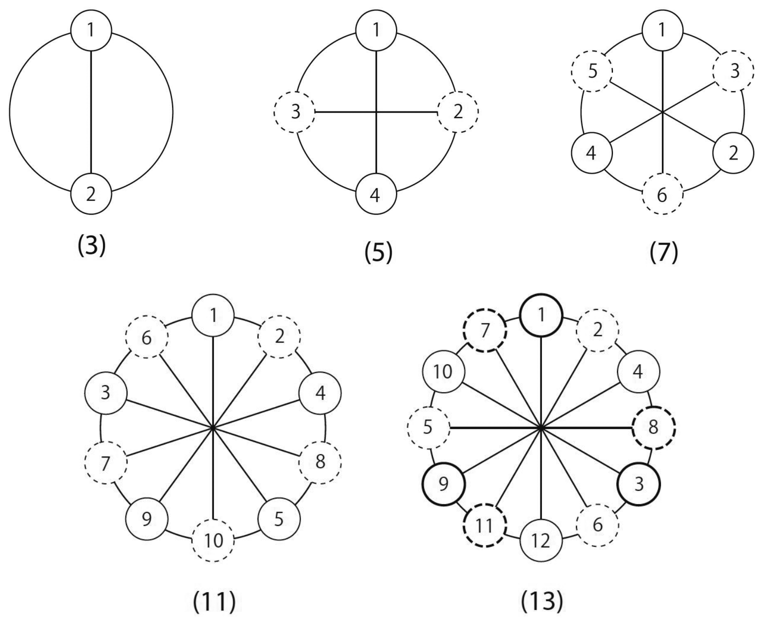

図1　変な時計とその仲間たち

もくじ

論説
変な時計とその仲間たち…………………………… 1
特集
エビデンスに基づく政策形成と統計学………… 5
特集
「大学入学共通テスト（新テスト）」に向けて… 9
実践記録
数学の苦手な生徒を対象にした三角比の導入方法について… 13
新訂版教科書のご案内……………………………… 15
ワンポイント教材
ベクトルの内積の利用……………………………… 16

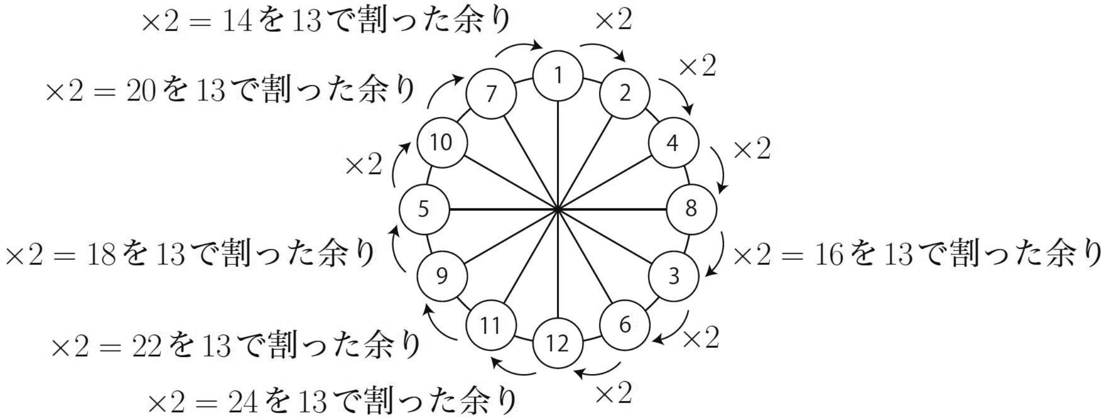

図２　変な時計の数字の並び方のルール

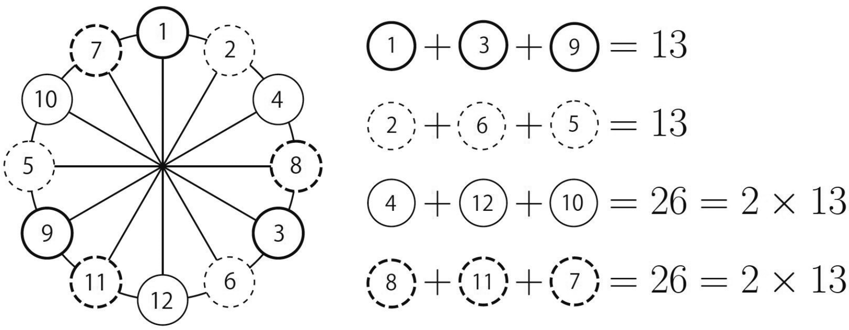

図３　変な時計の持つ性質

一般に時計回りに x の次を y とすると，y は x の２倍の $2x$ を 13 で割った余り，になっています。12 番目の７についても，７の２倍の 14 を 13 で割った余りが１，で７の次が１となり元に戻っています。

13 は素数です。同様に素数 $p=3, 5, 7, 11$ のそれぞれについて図１(p)では１から $p-1$ までが似たようなルールで並んでいます。つまり**時計回りに x の次を y とすると，y は x の a 倍の ax を p で割った余り，になっています。**ここで図１(3)と図１(5)と図１(11)では $a=2$，図１(7)では $a=3$ です。

このルールだけでしたら小学生にも説明出来ますが，１から $p-1$ までがちょうど１回現れるのは不思議ですね。理由は後で説明することにして，この「変な時計とその仲間たち」の持つ美しい性質をさらに見ていきます。「変な時計」では，１と 12，２と 11，４と９，８と５，３と 10，６と７のように，円の反対側にある数を足すとちょうど 13 になっています。一般に図１(p)では円の反対側にある数を足すと p になっています。また，実線の丸で囲まれた数を全て足すと p の倍数になっています。例えば図１(11) では $1+4+5+9+3=22$ と 11 の倍数になっています。同様に点線の丸で囲まれた数を全て足しても p の倍数になっています。例えば図１(11) では $2+8+10+7+6=33$ とこれも 11 の倍数になっています。さらに図３のように「変な時計」では 1, 3, 9 や 2, 6, 5 や 4, 12, 10 や 8, 11, 7 のように円周を３等分する位置にある３つの数の和も全て 13 の倍数になっています。以上の性質は全て次のようにまとめて述べることが出来ます。d を $p-1$ の約数とします。このとき図１(p)において円周を d 等分する位置にある d 個の数の和は全て p の倍数になります。

この「変な時計とその仲間たち」の持つ性質

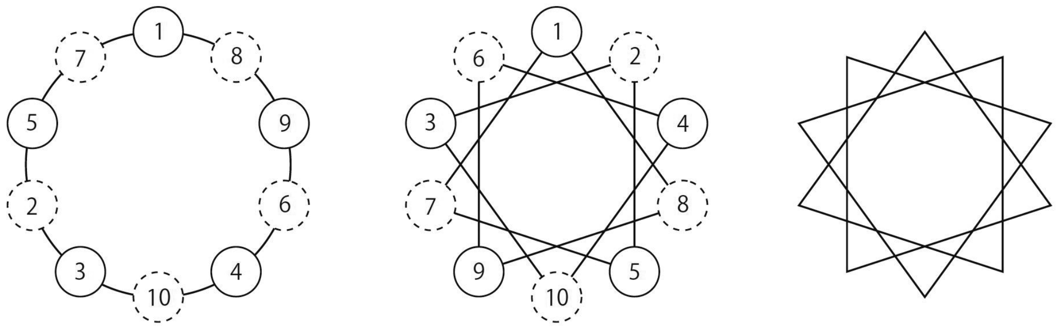

図４　生成元の取り替えで現れる星形

は，加減乗除を知っている人にでしたら誰にでも説明することが出来ます。それで，このように数を並べることが出来ることを不思議に思ってもらえればよいです。さらに，何故このように並べることが出来るのか，その背景にある理論を知りたいと思ってもらえれば尚よいです。以下にその理由を代数学の言葉で説明します。

p を素数とします。図１では $p \leq 13$ ですが $p > 13$ でも同様の事が成立します。整数 m，n に対して，$m-n$ が p の倍数であるとき m と n は p を法として合同であるといい $m \equiv n \pmod{p}$ と記しました。すると「変な時計」の数字の並びは

$$2^0 \equiv 1 \pmod{13},$$
$$2^1 \equiv 2 \pmod{13},$$
$$2^2 \equiv 4 \pmod{13},$$
$$2^3 \equiv 8 \pmod{13},$$
$$2^4 \equiv 3 \pmod{13},$$
$$2^5 \equiv 6 \pmod{13},$$
$$2^6 \equiv 12 \pmod{13},$$
$$2^7 \equiv 11 \pmod{13},$$
$$2^8 \equiv 9 \pmod{13},$$
$$2^9 \equiv 5 \pmod{13},$$
$$2^{10} \equiv 10 \pmod{13},$$
$$2^{11} \equiv 7 \pmod{13},$$
$$2^{12} \equiv 1 \equiv 2^0 \pmod{13}$$

と規則的であることが分かります。整数全体の集合 $\mathbb{Z}$ の p を法とした合同類全体の集合 $\mathbb{Z}/p\mathbb{Z}$ は体になります。この体は p 個の元 $[0]_p$, $[1]_p$, $\cdots$, $[p-1]_p$ からなります。これらを $0, 1, \cdots, p-1$ と略記することにします。$\mathbb{Z}/p\mathbb{Z}$ は体なので加減乗除が出来ます。例えば $p=13$ のときには $3 \times 6 = 5$ となります。これは $3 \times 6 = 18$ と $18 \equiv 5 \pmod{13}$ を合わせて略記しています。このとき体 $\mathbb{Z}/p\mathbb{Z}$ の乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ は 0 以外の $p-1$ 個の元 $1, 2, \cdots, p-1$ からなります。一般に，体 K の乗法群 $K^\times$ の有限部分群は巡回群となることが知られています。代数学のどの入門書にも載っているような基本的な定理です。体 $\mathbb{Z}/p\mathbb{Z}$ は p 個の元からなる有限体で，乗法群 $(\mathbb{Z}/p\mathbb{Z})^\times$ は $p-1$ 個の元からなる有限群です。よって $(\mathbb{Z}/p\mathbb{Z})^\times$ は巡回群になるので，図１(p) のように円周上に１から $p-1$ までをルールに従って並べることが出来る訳です。ここでルールにおける a がこの巡回群の生成元です。この巡回群の生成元が何になるかは原始根問題といって簡単ではないことが知られています。計算してみると $p=3$ のときは 2，$p=5$ のときは 2 と 3，$p=7$ のときは 3 と 5，$p=11$ のときは 2 と 6 と 7 と 8，$p=13$ のときは 2 と 6 と 7 と 11 が生成元になることが分かります。図１は，これらのうち最小のものを生成元として選んで巡回群を Cayley graph として表示して，それを少し加工したものです。円周上で１の次の数 $a=2$ または $a=3$ が生成元です。別の生成元を使っても同様なことが出来ます。例えば $p=11$ のときに $a=8$ を生成元として選ぶと図４（左図）のような Cayley graph になります。これと同型な Cayley graph を図１(11) と同じ数の位置で描いてみると図４（中図）になります。どちらの図

でも実線の丸で囲まれた数と点線の丸で囲まれた数が円周上交互に並んでいます。この実線の丸で囲まれた数は，素数 $p=11$ を法として平方剰余である数になっています。平方剰余に関するいくつかの命題は，このように幾何的にイメージするすることで理解することが出来ます。図４（中図）の数字を消すと図４（右図）のように星形の図形が得られます。円状に等間隔に並んでいる 10 個の点の３つ隣り同士を結んで得られる図形なので $(10,\ 3)-\mathrm{star}$ と筆者は呼んでいます。ここで 10 と３は互いに素です。このような構成をするといつでも互いに素になります。

では次に図１(p) において円周を d 等分する位置にある d 個の数の和は p の倍数になることを説明します。これら d 個の数からなる集合を S とします。S の元 s を一つ任意に選びます。$q=(p-1)/d$ として $X=a^q$ とおきます。すると

$S=\{s,\ sX,\ sX^2,\ \cdots,\ sX^{d-1}\}$ と表せることが分かります。さて $X^d=(a^q)^d=a^{q\cdot d}=a^{p-1}=1$ ですから $X^d=1$ です。よって $X^d-1=0$ です。

$X^d-1=(X-1)(X^{d-1}+X^{d-2}+\cdots+X+1)$ と因数分解出来ます。よって

$(X-1)(X^{d-1}+X^{d-2}+\cdots+X+1)=0$ ですが，

$X\neq 1$ ですから $X-1\neq 0$ です。よって

$X^{d-1}+X^{d-2}+\cdots+X+1=0$ です。ここで体は整域であるという性質を使いました。この

$X^{d-1}+X^{d-2}+\cdots+X+1$ は円周等分多項式，略して円分多項式と呼ばれています。よって S の元すべての和は

$$s+sX+sX^2+\cdots+sX^{d-1}$$
$$=s(1+X+X^2+\cdots+X^{d-1})=s\cdot 0=0$$

となり，これが p の倍数であることが示せました。

本稿で述べた事は特に新しい事ではありませんが，このように円周上に数字を配置していろいろな性質を説明する方法は数年前から筆者が行っているものです。例えば早稲田大学数学教育学会大会（2016 年 12 月）での講演でも紹介しています。同学会誌にその講演記録 [1] が収録されています。それと同じものは

http://www.f.waseda.jp/taniyama/number-placement-web.pdf

で読むことが出来ます。そこには関連する巡回数 142857 についての記述もあります。また 2017 年に出版された本 [2] に本稿のように円周上に数字を配置してある図がたくさんあります。本稿の内容を全て含んではいないようですが，とても楽しそうな本です。

以上見てきましたように「変な時計」についていろいろと考えていると時の経つのも忘れてしまいますね。

参考文献

[1] 谷山公規 , 数並べ（素人の数遊び）, 早稲田大学数学教育学会会誌 , 第 35 巻 (2017), 3-9.

[2] M.Weissman, An illustrated theory of numbers, *American Mathematical Society*, Providence, RI, 2017.