素数のべき乗和に関する性質

札幌創成高校
外山　尚生

§０　はじめに

１９９５年の京都大学の入試問題第４問に次のような問題が出ていた。

> 自然数 n 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 $f(n^7)=f(n)$ 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。

自分で得点を決められるというなんとも面白い問題だ。

今回、この問題の 「7」 を別な数字にして同じことをしてみた。すると、なんとも興味深い結果がでたのでここで報告したい。

§１　合同式

今回のレポートではあまりについて議論していくので、先に合同式について触れておこう。

[定義１．１]

> 整数aとbを0でない整数nで割った余りが等しいことを$a\equiv b$（mod n）と書く。

すると、この合同式について次の命題が成り立つ。

[命題１．２]

> a、b、c、d、nを整数、mを自然数とする。
> $a\equiv b$（mod n）、$c\equiv d$（mod n）のとき次のことが成り立つ。
> １　$a+c\equiv b+d$（mod n）
> ２　$a-c\equiv b-d$（mod n）
> ３　$ac\equiv bd$　（mod n）
> ４　$a^m\equiv b^m$　（mod n）

[証明]

$a\equiv b$（mod n）、$c\equiv d$（mod n）は整数q、rを用いて$a=nq+b$、$c=nr+d$と書ける。

１は$a+c=nq+b+nr+d=n(q+r)+(b+d)$より証明できる。２も同様にして証明できる。

３は$ac=(nq+b)(nr+d)=n(nqr+qd+rb)+bd$より証明できる。

４は３を$c=a$、$d=b$にして繰り返すことで証明できる。㊮

[命題１．３]

$ab \equiv ac \pmod{n}$ で、aとnが互いに素ならば、$b \equiv c$

[証明]

$ab = nq + ac$より、$a(b-c) = nq$。aとnが互いに素だから$b-c$はnの倍数である。

よって、$b-c \equiv 0 \pmod{n}$ より$b \equiv c$。㊮

今回の問題の$f(n)$はmod 7の時を考えればよいから、次の命題が成り立つ。

[命題１．４]

自然数a、a_1、a_2、…、a_nについて

1　$f(a_1+a_2) \equiv f(a_1)+f(a_2) \pmod{7}$

2　$f\left(\sum_{k=1}^{n} a_k\right) \equiv \sum_{k=1}^{n} f(a_k) \pmod{7}$

3　$f(a^n) \equiv \{f(a)\}^n \pmod{7}$

これらの命題を使って先に紹介した京都大学の問題を解き、分析していきたい。

§ 2　京都大学の問題を解いてみる

まずは京都大学の問題を解いて、この問題の面白さを味わおう。

[問題]

自然数 n 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 $f(n^7) = f(n)$ 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。

[解答]

（１） n を 7 で割った余りについて分類して求める。

$f(n) = 0$ のとき、 $f(n^7) = f(0^7) = f(0) = 0$

$f(n) = \pm 1$ のとき、 $f(n^7) = f((\pm 1)^7) = f(\pm 1) = \pm 1$ （複合同順）

$f(n) = \pm 2$ のとき、 $f(n^7) = f((\pm 2)^7) = f(\pm 128) = \pm 2$（複合同順）

$f(n) = \pm 3$ のとき、 $f(n^7) = f((\pm 3)^7) = f(\pm 2187) = \pm 3$ （複合同順）

以上より $f(n^7) = f(n)$　㊮

（２）（１）より任意の自然数 m について $f(n^{6+m}) = f(n^m)$ が成り立つから、$1 \leqq n \leqq 6$ のときを考えれば十分である。そこで$1 \leqq n \leqq 6$ のときの $f(k^n)$ の値を命題１．４を使って求め、その和を求めると、次ページの表のようになる。

	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$\sum_{k=1}^{7} f(k^n)$	$f\left(\sum_{k=1}^{7} k^n\right)$
$n=1$	1	2	3	4	5	6	0	21	0
$n=2$	1	4	2	2	4	1	0	14	0
$n=3$	1	1	6	1	6	6	0	21	0
$n=4$	1	2	4	4	2	1	0	14	0
$n=5$	1	4	5	2	3	6	0	21	0
$n=6$	1	1	1	1	1	1	0	6	6

上の表より mを自然数として、$g(n)=\begin{cases}0 & (n \neq 6m)\\ 18 & (n=6m)\end{cases}$ であることがわかる。

したがって、得点を得るためには $g(6)=18$ を答えればよい。㊟

（２）の問題は nが6で割り切れないときは $g(n)=0$ で、 $g(n)\neq 0$ となるのはnが6で割り切れるとき のみであるのが面白い。

ここで、（１）はフェルマーの小定理の特別な場合である。

[定理２.１] フェルマーの小定理

pを素数とする。任意のpと互いに素な整数aに対して
1　$a^p \equiv a \pmod p$
2　$a^{p-1} \equiv 1 \pmod p$

この定理を証明するためには次の補題が必要である。

[補題２．２]

pを素数とするとき
${}_pC_k$（$k=1,2,\cdots,p-1$）はpで割り切れる。

[証明]${}_pC_k=\dfrac{p\times(p-1)\times(p-2)\times\cdots\times(p-k+1)}{(p-k)\times(p-k-1)\times(p-k-2)\times\cdots\times3\times2\times1}$

ここでpは素数だから1から$p-k$（$<p$）の全ての整数はpと互いに素である。

よって、${}_pC_k$はpで割り切れる。㊟

この補題を用いて、定理２．１は証明できる。

[定理２．１の証明]

１は数学的帰納法で証明する。

$a=1$のときは明らかに成り立つ。

$a=k$のとき$k^p \equiv k$…①が成り立つと仮定する。

二項定理より$(k+1)^p=\sum_{k=0}^{p} {}_pC_k p^k = 1+k^p+\sum_{k=1}^{p-1} {}_pC_k p^k$であるから、

補題２．２より$\sum_{k=1}^{p-1} {}_pC_k p^k$は$p$で割り切れる。

よって①より$(k+1)^p \equiv 1+k^p \equiv 1+k$が成り立つ。

２は$a^p \equiv a \pmod p$から、aとpは互いに素だから命題１．３より$a^{p-1} \equiv 1 \pmod p$である。㊟

§３　7を他の数字にして同じことをしてみる。

さて、この京都大学の問題をさらに発展させてみよう。

そこで「7」を別の数字にして同じような操作をしてみた。$f_a(n)$、$g_a(n)$を次のように定義する。

[定義３．１]

> ２以上の自然数aと、自然数nに対し、$f_a(n)$、$g_a(n)$を次のように定義する。
>
> $f_a(n)$＝nをaで割った余り
>
> $g_a(n)=f_a\left(\sum_{k=1}^{a} k^n\right)$

京都大学の問題は$a=7$の時と同じような操作である。

（京都大学の問題は$g_7(n)=3f_7\left(\sum_{k=1}^{7} k^n\right)$となっているが、3は本質とは関係ないため、無視した）

aの値にいろいろな数字を入れて$g_a(n)$を計算すると、次のようになる。

（１）$a=2$のとき

	$k=1$	$k=2$	$\sum_{k=1}^{a} f_a(k^n)$	$g_a(n)$
$n=1$	1	0	1	1

（２）$a=3$のとき

	$k=1$	$k=2$	$k=3$	$\sum_{k=1}^{a} f_a(k^n)$	$g_a(n)$
$n=1$	1	2	0	3	0
$n=2$	1	1	0	2	2

（３）$a=4$のとき

	$k=1$	$k=2$	$k=3$	$k=4$	$\sum_{k=1}^{a} f_a(k^n)$	$g_a(n)$
$n=1$	1	2	3	0	6	2
$n=2$	1	0	1	0	2	2
$n=3$	1	0	3	0	4	0

（４）$a=5$のとき

	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$\sum_{k=1}^{a} f_a(k^n)$	$g_a(n)$
$n=1$	1	2	3	4	0	10	0
$n=2$	1	4	4	1	0	10	0
$n=3$	1	3	2	4	0	10	0
$n=4$	1	1	1	1	0	4	4

（5）$a=6$のとき

	$k=1$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$\sum_{k=1}^{a} f_a(k^n)$	$g_a(n)$
$n=1$	1	2	3	4	5	0	15	3
$n=2$	1	4	3	4	1	0	13	1
$n=3$	1	2	3	4	5	0	15	3
$n=4$	1	4	3	4	1	0	13	1
$n=5$	1	2	3	4	5	0	15	3

このようにして aの値を1から13にしてそれぞれのnに対する$g_a(n)$の値をまとめたものが次の表である

nの値＼aの値	2	3	4	5	6	7	8	9	10	11	12	13
1	1	0	2	0	3	0	4	0	5	0	6	0
2		2	2	0	1	0	4	6	5	0	2	0
3			0	0	3	0	0	0	5	0	0	0
4				4	1	0	4	6	3	0	2	0
5					3	0	0	0	5	0	0	0
6						6	4	6	5	0	2	0
7							0	0	5	0	0	0
8								6	3	0	2	0
9									5	0	0	0
10										10	2	0
11											0	0
12												12

すると、次のことが予想される。

[予想]

> pが奇素数のとき
> 1　$g_p(p-1)=p-1$
> 2　$1\leqq n\leqq p-2$の全てのnについて$g_p(n)=0$

予想１はフェルマーの小定理（定理２．１）から簡単に証明できる。

[命題３．２]

> pが奇素数の時　$g_p(p-1)=p-1$

[証明]

pは素数だから$p-1$以下の自然数aは全てpと互いに素である。

よってフェルマーの小定理より$f_p(a)=1$。さらに、$f_p(p)=0$である。

よって$g_p(p-1)=p-1$である。㊍

次に予想２を証明したい。予想２を証明するにはべき乗和についての定理が必要になる。

[定理３．３]

> $\sum_{k=1}^{n} k^m=a_{m+1}n^{m+1}+a_m n^m+a_{m-1}n^{m-1}+\cdots+a_2 n^2+a_1 n$とすると、
>
> $a_{i+1}=\frac{m}{i+1}a_i$　$(i=1,2,3,\cdots,m)$　　$a_1+a_2+a_3+\cdots+a_{i+1}=1$

定理３．３を予想を証明できるように書き換えてみたい。

［命題３．４］

pを奇素数とする。

$\sum_{k=1}^{p} k^n = a_{n+1}p^{n+1} + a_n p^n + a_{n-1}p^{n-1} + \cdots + a_2 p^2 + a_1 p$　…①とすると

$a_{i+1} = \frac{n}{i+1} a_i$　…②　$(i = 1,2,3,\cdots,n)$　　$a_1 + a_2 + a_3 + \cdots + a_{i+1} = 1$　…③

となる。

ここで①式より、$\sum_{k=1}^{p} k^n = p(a_{n+1}p^n + a_n p^{n-1} + \cdots + a_2 p + a_1)$　…④と表すことができる。

また、$1 \leqq n \leqq p-2$となる自然数nについて②式より

$a_2 = \frac{n}{2} a_1$、$a_3 = \frac{n}{3} a_2$、$a_4 = \frac{n}{4} a_3$、……、$a_{p-1} = \frac{n}{p-1} a_{p-2}$となる。

つまり、$a_{p-1} = \frac{n^{p-2}}{(p-1)!} a_1$となる。分母に注目すると、$p$は素数であるから、$p$と$(p-1)!$は互いに素である。

さらに、$\sum_{k=1}^{p} k^n$は明らかに整数であるから、$a_{n+1}p^n + a_n p^{n-1} + \cdots + a_2 p + a_1$は整数である。

よって、④式より$\sum_{k=1}^{p} k^n$は$1 \leqq n \leqq p-2$となる自然数nについてpの倍数であることが証明されたので、$1 \leqq n \leqq p-2$となる自然数nについて$g_p(n) = 0$であることが証明された。

§４　おわりに

問題を見てみたときに自分で点数を決められるというユニークな京都大学の問題であったが、この問題をテーマにいろいろ実験してみた結果、面白い発見がたくさんでき、数学の奥の深さを感じることができた。

べき乗和は単純な数式であるが、ここから導かれる数学の世界はまだまだ未知な部分が多そうだ。研究対象としてこれからも考えていきたいテーマになりそうだ。

◆参考資料◆

- 「べき乗和の公式について」（改訂版）　片山　喜美
  http://ja9nfo.web.fc2.com/math/bekijouwa.pdf
- 「受験の月」　1995年　京都大学　後期　文系　第４問　自分の点数を自分で決められる？
  http://examist.jp/legendexam/1995−kyoto/
- 「高校数学の美しい物語」　フェルマーの小定理の証明と例題
  https://mathtrain.jp/fermat_petit