剰余類のちょっとした小手技

札幌新川高等学校　中村文則

○強引ぐ(Going) my way

<先　生>今日の授業は「連続する整数の積」に関する話題について考えてみよう。

連続する整数とは

……, −8, −7, −6, −5, −4, −3, −2, −1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, ……

なる整数列の並びから、

3, 4, 5, 6, 7, 8, 9, 10

のように、適当な長さで切り取った一部分の整数列です。これを一定間隔で切り取ってみると面白い性質が見えてくる。例えば間隔2とは、(1, 2), (4, 5), (7, 8) のように切り取ることだけど、その2つの数をみると偶数と奇数のpairになる。すなわち部分列は2の倍数を必ず含んでいる。同様に (3, 4, 5), (7, 8, 9), (8, 9, 10) のように間隔3の場合は、どんな倍数を含んでいるだろうか。

<まなぶ>やっぱり2の倍数です。

<よしお>3の倍数も含んでいると思います。

<先　生>その通り。よしおのいうように3の倍数を含んでいるね。ではこうやってどんどん切り取る間隔を延ばしていったらどうなるだろう。下の図を見て各自考えてごらん。

整　数	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2の倍数	○		○		○		○		○		○		○		○		○		○		○		○		○
3の倍数		△			△			△			△			△			△			△			△		
4の倍数	□				□				□				□				□				□				□
5の倍数					☆					☆					☆					☆					☆

<かず子>分かりました。間隔が5だと5の倍数。間隔が6だと6の倍数のように「間隔の倍数」を含んでいます。

<先　生>もっと具体的にいってみよう。間隔が n の場合は n の倍数を含んでいるということだね。ところで実は、先ほどまなぶがいっていたことも重要なことなんだ。間隔3ということは、間隔2を延ばしたものだね。だから2の倍数も含むことになる。間隔5ではどうだろう。

<まなぶ>2の倍数、3の倍数、4の倍数、5の倍数を含みます。

<先　生>したがって、間隔n は、k(k=1,2,3,……,n)の倍数を含む。これから間隔 n に含まれるすべての数の積を計算すると、2の倍数、3の倍数、…、nの倍数の積を含むわけだから、「連続する n 個の整数の積」は

$$n\times(n-1)\times(n-2)\times(n-3)\times\cdots\cdots\times3\times2\times1 \qquad \cdots\cdots(*)$$

で割りきれることが分かるんだ。

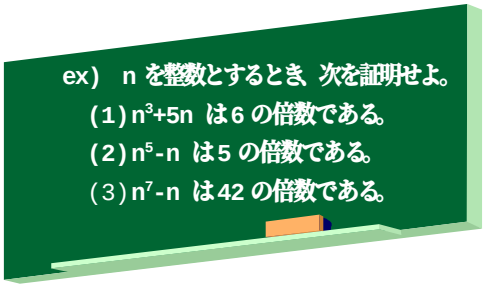
さて、(*)の計算を圧縮して表現し、n!と書くことにしよう。読みかたは n の階乗(n factorial)「ひゃくとおりある」なんて語路合せで覚えればよい。

<生徒達>……

<先　生>……まっ、冗談はさておき、まとめると

「連続する n 個の整数の積は n！で割りきれる」

ということだが、次にこれを利用した問題を解いてみよう。



<先　生>まず(1)を考えてみよう。3!=6 だから、与式は連続する 3 個の整数の積になっていればいいことがわかる。

$$n^3+5n=n(n^2+5)$$

となるけど、さて連続する 3 個の整数の積をどうやって作ればいいだろう。n をそのひとつとして考えてみよう。

<よしお> n,n+1,n+2 でしょうか。

<先　生>うん、そうすると、与式の中の因数には(n+1)(n+2) すなわち n^2+3n+2 が足りないことになるから

(与式)=$n(n^2+5)$

=$n\{(n+1)(n+2)-(n^2+3n+2)+n^2+5\}$

=$n\{(n+1)(n+2)-3(n+1)\}$

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

ここで、n(n+1)(n+2)は連続する 3 個の整数の積だから 6 の倍数となる。また、n(n+1)は連続する2個の整数の積だから 2 の倍数、したがって 3n(n+1)は 6 の倍数。よって、以上より与式は 6 の倍数であることがわかる。ところで他のみんなもよしおと同じような連続する3つの整数を考えたのかな。

<かず子>あのう、私は、n-1とnとn+1 を考えました。

<先　生>では、かず子の考えた整数について、どうなるか計算してみよう。

(与式)=$n(n^2+5)$

=$n(n^2-1+6)$

=$(n-1)n(n+1)+6n$

(n-1)n(n+1)は連続する 3 個の整数の積だから明らかに与式も 6 の倍数だね。こちらの方が分かり易いかもしれない。では、まなぶはどう考えたのだろう。

<まなぶ>あのう、ぼくは、nをもとにするのを忘れて、n+1,n+2,n+3 にしてしまったんですけど。

<先　生>話をよく聞いていないということだが、でも間違いではないよ。ちょっとやってみよう。

$(n+1)(n+2)(n+3)=n^3+6n^2+11n+6$

だから、

(与式)=n^3+5n

=$(n^3+6n^2+11n+6)-6n^2-6n-6$

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

ほら、できてしまった。要は、方針を決めたら初志貫徹、何が何でもその方向へ式を変形するって気持ちを持つことだ。数学はエレガントだけでなくこういった強引さも必要なんだ。これを強引ぐ(Going)my way という。

<生徒達>……

<先　生>……まっ、とにかく(1)はできたから、次は(2)。まず与式を因数分解してみよう。

(与式)=$n(n^4-1)$

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

=$(n-1)n(n+1)(n^2+1)$　……(**)

さて、ここで、(n-1)n(n+1)は連続する 3 個の整数の積だ。5 の倍数であることを示すには連続する 5 個の整数の積を作ればいい。では残りの2つの整数はなんだろう。

<よしお> (n+2),(n+3)です。

<先　生>確かにそうだけど、もう少し計算しやすいものはないかな。

<かず子>n-2とn+2 のほうがいいと思います。

<先　生>そう、その通り。(n-1)n(n+1)の前後の数を考えればいいね。そうすると(n-2)(n-1)n(n+1)(n+2)という連続する 5 個の整数の積が作られる。さあ、それでは変形しよう。

(与式)=$(n-1)n(n+1)\{(n^2-4)+5\}$

=$(n-2)(n-1)n(n+1)(n+2)+5(n-1)n(n+1)$

あとは、もう明らかだよな。

ところで、(**)を見てごらん。この式の(n-1)n(n+1)は連続する 3 個の整数の積であるわけだから、実は与式は 6 の倍数でもある。したがって、与式は5の倍数かつ6の倍数、すなわち30の倍数になっているんだ。

さあ、それでは最後の問題(3)だ。まなぶ、まず因数分解をしてみよう。

<まなぶ> (与式)=$n(n^6-1)$

=$n(n^2-1)(n^4+n^2+1)$

=$(n-1)n(n+1)(n^4+n^2+1)$

となります。

<先　生>OK!。この段階で6の倍数であることが分かるね。したがって42の倍数であるには、あとは7の倍数であることを示せばよい。さあ、それでは連続する 7 個の整数の積を作ってみよう。よしお、どうする。

<よしお> (n-1)n(n+1) の前後に、(n-3),(n-2),(n+2),(n+3)を掛けます。

<先　生>だいぶ、要領良くなってきたな。

(n-3)(n-2)(n+2)(n+3)=(n-3)(n+3)(n-2)(n+2)

$=(n^2-9)(n^2-4)$

$=n^4-13n^2+36$

だから、

(与式)=(n-1)n(n+1)(n^4+n^2+1)

$=(n-1)n(n+1)\{(n^4-13n^2+36)+14n^2-35\}$

$=(n-3)(n-2)(n-1)n(n+1)(n+2)(n+3)+7(2n^2-5)(n-1)n(n+1)$

さあ、7の倍数であることが示されたね。

<あとがき>

現行指導要領で数学が、コア「数学Ⅰ」、オプション「数学A」に分かれてから、この分野の指導法は少し変わってきたと思う。

従来は、例えば6の倍数を示すには、剰余系を考え2と3を法(modulus)として分類し、場合分けで証明していたが、「数学Ⅰ」で並行して個数の処理を学ぶようになってからは、組合せを利用した方法も可能となってきた。

$$ {}_nC_k = \frac{n(n-1)(n-2)(n-3)\cdots\cdots(n-k+1)}{k!} $$

ここで、${}_nC_k$ は自然数であることから、右辺も自然数。よって、n(n-1)(n-2)(n-3)……(n-k+1)なる連続するk個の整数の積はk!で割りきれる。したがって、m(2≦m≦k)の倍数であるかどうかを示すには連続するk個の整数の積を作ればいいことになる。そして倍数問題は、この考え方の方が安易にそして簡単にできてしまうことが多いようだ。

もちろん場合分けというもっとも数学的な思考整理法は大切にしなければならないと思うが、中学校での場合分けの指導が単位数減の現状において段々と希薄になってきている関係から、高校現場では剰余類の概念を生徒に指導するのは困難になってきてもいる。もう少し思考を練り、そしてほぐす時間が欲しい。1年間を通して少しずつ場合分けの思考を育てていけばいいのではないだろうか。

ところで、本文の問題の(2),(3)は、フェルマーの小定理に関するものである。一般に

> pを素数とするとき
> $m^p \equiv n \pmod p \quad n \in N$ ……(#)

が成立する。以下、これを数学的帰納法により示そう。

proof)

P(n)=n^p-n とおく。

P(1)=0 より　明らかに成立

P(m)で成立すると仮定する。　すなわち　P(m)=$m^p-m\equiv 0 \pmod p$

$$ P(m+1)=(m+1)^p-(m+1) $$

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

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

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

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

ここで ${}_pC_k = \frac{p(p-1)(p-2)(p-3)\cdots\cdots(p-k+1)}{k!}$

連続するk個の整数の積p(p-1)(p-2)……(p-n+k)はk!で割り切れるが、

pは素数、　1≦k≦p-1

であるから、(p-1)(p-2)(p-3)……(p-k+1)が　k!で割り切れる。

∴ ${}_pC_k = pt_k \quad t_k \in N$ とおける。

$$P(m+1) = \sum_{k=1}^{p-1} {}_pC_k m^k + P(m)$$
$$= \sum_{k=1}^{p-1} pt_k m^k + p(m)$$
$$= p\sum_{k=1}^{p-1} t_k m^k + p(m)$$
$$\equiv 0 \pmod{p}$$

よって P(m+1) においても成立する。

以上より、すべての自然数 n において P(n)は成立する。

Q.E.D

この(#)から、

$n^p-n=ap$ $a \in N$ とおくと、

$n(n^{p-1}-1)=ap$

ここで(n,p)=1 であれば

$n^{p-1}-1 \equiv 0 \pmod{p}$

よって、フェルマーの小定理を得る。

> n を自然数、p を素数とする。n と p が互いに素であるとき、
> $n^{p-1} \equiv 1 \pmod{p}$

以上の証明は、剰余系の概念を必ずしも理解していなくても、十分高校生が理解できる内容であると思う。

具体的には、次のような問題にも応用できる。

ex) 2^{1999} を 19 で割った余りを求めよ。

解)

(2,19)=1 であるから、

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

$2^{1999}=(2^{18})^{111} \cdot 2$

$\equiv 2 \pmod{19}$

よって、余りは 2

フェルマーの小定理は、$M_p=2^p-1$ なるメルセンヌ数へと拡張し、「$2^{p-1} \cdot M_p$ は完全数である」というユークリッドの発見に回帰する。

初等整数論は時間の流れの中を揺れ動いているのである。フェルマーの大定理は、今世紀にその証明が完結したが、この分野はまだまだ興味をそそる題材が埋もれている。その探求が高校生の知識でも可能であるとしたら楽しいことである。ちょっとした興味で「数学の尻尾」に触れることができるのである。