ISSN 1881-6134

鳥取大学数学教育研究

Tottori Journal for Research in Mathematics Education

http://www.rs.tottori-u.ac.jp/mathedu

ウィルソンの定理を題材とした高校数学における教材開発

松岡　学　*Manabu Matsuoka*

vol.17, no.5
Aug. 2014

ウィルソンの定理を題材とした高校数学における教材開発

松岡　学
大阪樟蔭女子大学

要 約：整数論におけるウィルソンの定理は，定理で述べられていること自身は，高校生にも理解しやすいものである。しかし，その証明には様々な要素が含まれており，必ずしも理解が容易ではない。一般に，ウィルソンの定理の証明は合同式の式変形で記述されることが多いが，その記述方法では合同式を学習していない者には理解が難しい。そのようなことから，本研究においては合同式を用いずに，ウィルソンの定理を題材とした初等的な教材を開発することを目的とする。具体的には，多項式の展開を用いる証明とペアの考えを用いる証明の２通りの方法で教材を作成する。

キーワード：ウィルソンの定理，フェルマーの小定理，多項式の展開，ペア，素数

１　研究目的

ウィルソンの定理は整数論において有名な定理である。ラグランジュによって定理が証明され，ガウスにより一般化されている。参考文献としては Dickson（1952）や Turnage（2008）などがある。

また，ウィルソンの定理は近年においても様々な研究がされている。組合せ論的な研究としては András（2011）や Tripathi（2006）があり，代数関数体を用いたものは Laššák（2000）がある。また，有限環の立場からのアプローチとしては，Hirano・Matsuoka（2013）がある。

高校数学の教材としては，ウィルソンの定理は高校生にも理解できる内容であり，適切な題材といえる。しかし，若干理解しづらい内容を含んでおり，教材作成には注意を要する。一般的に，ウィルソンの定理を証明する際，合同式（mod p）を用いて記述することが多い。合同式の記号を使うことで，式変形が簡便になるという長所があるが，合同式を学習していない者にとっては理解が難しい。また，合同式を用いた機械的な式変形で記述されるため，証明の数学的な意味が分かりにくいという側面もある。そこで，本研究においては，合同式を用いずに，数学の予備知識があまりない高校生にも理解できるような教材を作成することを目的とする。ただし，数学的に曖昧な部分がないように，正確な表現を心がける。

ウィルソンの定理を切っ掛けに，高校生の整数論への理解が定着し，さらに，数学に対して深い興味をもたせることが，本研究の最終的な目的である。

２　教材開発の内容

数学の教育現場において，時として問題の解法パターンを暗記させるような指導に陥ることがある。しかし，数学において重要なのは，数学的な対象をじっくり時間をかけて考察し，その仕組みや構造を理解することである。また，予備知識の部分も暗記するのではなく，根本的な部分から考えることが重要である。

そのようなことを踏まえて，次の 3 点に重点を置いて教材を開発する。

・数学的内容の意味が明確な教材
・数学的に正確に記述されている教材
・整数問題特有の証明方法に慣れるための教材

本研究は合同式を用いずに教材を作成するため，機械的な式変形ではなく，問題や式変形の意味を考えながら学習できるように配慮する。また，

高校数学における「整数の性質」は直観的に扱いやすい分野であるが，本教材においては数学的に正確な記述を試みる。具体的には，素因数分解の一意性や数学的帰納法などを用いて，正確な定式化を行う。整数問題は他の分野とは違った独特の証明法があるので，そのような手法に慣れておくことは，高校生にとって有意義であると思われる。

ウィルソンの定理の証明は何種類もあるが，高校数学の範囲では，“多項式の展開を用いる証明”と“ペアの考えを用いる証明”の 2 種類が適切であると思われる。どちらの証明法も重要であるため，本研究においては両方の方法で教材を作成する。

(1) 多項式の展開を用いる教材

最初に，多項式の展開を用いる教材について考察する。組合せからの準備として，「表 1」にあるような問題プリントから始めることとする。

表 1

整数　問題プリント 1

問題 1

p を素数，r を $1 \leqq r \leqq p-1$ である自然数とする。このとき，${}_pC_r$ は p の倍数であることを証明せよ。

（問題 1 の解答）

$r=1$ のとき，${}_pC_1 = p$ であり題意は成り立つので，r を 2 以上の自然数とする。

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

${}_pC_r$ は p 個から r 個とる組合わせの総数なので，自然数である。

ここで，p は素数であり，$2 \leqq r \leqq p-1$ より，p は $r, r-1, \cdots, 2$ のいずれでも割り切れない。したがって

$t = \dfrac{(p-1)\cdots(p-r+1)}{r(r-1)\cdots 2\cdot 1}$ とおくと，

t は整数であり，

$${}_pC_r = pt$$

よって，${}_pC_r$ は p の倍数である。

（解答終）

問題 1 は基本的な命題であるが，素数の性質を確認するための題材として，高校生にとって適切な問題である。問題 1 を踏まえて，多項式の展開の考えを用いる方法で，ウィルソンの定理を証明することができる。

表 2

整数　問題プリント 2

問題 2

次の問いに答えよ。

(1) $(x+1)(x+2)\cdots(x+p-1)$

$= x^{p-1} + a_1 x^{p-2} + a_2 x^{p-3} + \cdots a_{p-2}x + a_{p-1}$

とする。p が 3 以上の素数であるとき，$a_1, a_2, \cdots, a_{p-2}$ はそれぞれ p で割り切れることを証明せよ。

(2) 素数 p に対して，$(p-1)!$ を p で割ったときの余りは -1 であることを証明せよ。

（問題 2 の解答）

(1) 与えられた式を x の代わりに $x+1$ で考え，両辺に $x+1$ をかけると，

$(x+1)(x+2)\cdots(x+p)$

$= (x+1)^p + a_1(x+1)^{p-1} + \cdots + a_{p-1}(x+1)$

この式の右辺と与えられた式の両辺に $x+p$ をかけたものを考えることで

$(x+1)^p + a_1(x+1)^{p-1} + \cdots + a_{p-1}(x+1)$

$= (x+p)(x^{p-1} + a_1 x^{p-2} + \cdots a_{p-2}x + a_{p-1})$

を得る。
これは x に関する恒等式より
両辺を展開して，x に関する係数を比べることで，次の関係式を得る。

$a_1 = {}_pC_2$

$2a_2 = {}_pC_3 + a_1 \cdot {}_{p-1}C_2$

$3a_3 = {}_pC_4 + a_1 \cdot {}_{p-1}C_3 + a_2 \cdot {}_{p-2}C_2$

……

$(p-2)a_{p-2} = p + (p-1)a_1 + \cdots + 3a_{p-3}$

$(p-1)a_{p-1} = 1 + a_1 + a_2 + a_3 + \cdots a_{p-2}$

ここで，問題 1 より，

$a_1 = {}_pC_2$ は p で割り切れる。

次に，a_1，${}_pC_3$ が p で割り切れるので，

$2a_2$，すなわち a_2 は p で割り切れる。
同様に，

$a_3, \cdots, a_{p-2}$ は p で割り切れる。

よって，$a_1, a_2, \cdots, a_{p-2}$ はそれぞれ p で割り切れる。

(2) $p = 2, 3$ のとき題意は成り立つので，
p を 5 以上の素数とする。(1)より

$(p-1)a_{p-1} = 1 + a_1 + a_2 + a_3 + \cdots a_{p-2}$ であり，

$a_1, a_2, \cdots, a_{p-2}$ は p で割り切れるので，

$(p-1)a_{p-1}$ を p で割った余りは 1 である。

$(p-1)a_{p-1} = pa_{p-1} - a_{p-1}$ より

$-a_{p-1}$ を p で割った余りは 1 である。

よって，a_{p-1} を p で割った余りは -1 である。

ここで，$a_{p-1} = (p-1)!$ より

$(p-1)!$ を p で割ったときの余りは -1 である。

（解答終）

高校生が問題 2(2)を問題 1 から自力で解くことは難しい。このことから問題 2 は誘導形式とした。ただし，問題 2 (1)の解答はやや技巧的であり，少し難易度が高い。問題 2 (2)により証明された事実を，ウィルソンの定理という。ウィルソンの定理として「表 3」に明記しておく。

表 3

定理 1（ウィルソンの定理）
素数 p に対して，$(p-1)!$ を p で割ったときの余りは -1 である。

これで，ウィルソンの定理を多項式の展開を用いて証明することができた。内容としては，「素数の性質」や「多項式の展開」「組合せ」などの数学的な事柄を含んでいる。

また，この方法の応用として，フェルマーの小定理を証明することができるので，こちらも「表 4」に挙げておく。

表 4

整数　問題プリント 3

問題 3
p を素数，n を自然数とする。

このとき，$n^p - n$ は p で割り切れることを証明せよ。

問題 4

次の命題(1)と(2)が同値であることを証明せよ。

(1) p を素数，n を自然数とするとき，

$n^p - n$ は p で割り切れる。

(2) p を素数，n を p と互いに素な自然数とするとき，$n^{p-1} - 1$ は p で割り切れる。

（問題 3 の解答）

$p = 2$ のとき，$n^2 - n = (n-1)n$ であり，

連続する整数の積なので，

$p = 2$ で割り切れる。

よって，p を 3 以上の素数とする。

n を自然数とするとき，問題 2 (1)の等式において $x = n$ とすると，

$$(n+1)(n+2)\cdots(n+p-1)$$

$$= n^{p-1} + a_1 n^{p-2} + a_2 n^{p-3} + \cdots + a_{p-2} n + a_{p-1}$$

を得る。ここで，

$$n(n+1)(n+2)\cdots(n+p-1) - (n^p - n)$$

$$= a_1 n^{p-1} + \cdots a_{p-2} n^2 + (a_{p-1} + 1)n \quad \cdots ①$$

連続する p 個の整数の積なので，

すべての自然数 n に対して

$n(n+1)(n+2)\cdots(n+p-1)$

は p で割り切れる。

また，ウィルソンの定理より

$a_{p-1} = (p-1)!$ を p で割ったときの余りは -1 より，$a_{p-1} + 1$ は p で割り切れる。

ここで，$a_1, a_2, \cdots, a_{p-2}$ は p で割り切れるので，

$a_1 n^{p-1} + \cdots + a_{p-2} n^2 + (a_{p-1} + 1)n$

はすべての自然数 n に対して p で割り切れる。

よって，①より $n^p - n$ は p で割り切れる。

（解答終）

（問題 4 の解答）

(1) ⇒ (2) の証明。

p を素数，n を p と互いに素な自然数とする。

(1)より，

$n^p - n = pk$ となる整数 k が存在する。

したがって $n(n^{p-1} - 1) = pk$

ここで，$k = 0$ のとき，$n^{p-1} - 1 = 0$ は p で割り切れるので，題意は成り立つ。

よって，$k \neq 0$ とする。

右辺は p で割り切れ，

n と p は互いに素であるから

素因数分解の一意性より

$n^{p-1} - 1$ は p で割り切れる。

したがって，$k \neq 0$ のときも題意は成り立つ。

よって，(2)が証明された。

(2) ⇒ (1) の証明。

p を素数，n を自然数とする。

[Ⅰ] n が p の倍数であるとき

$n^p - n$ は明らかに，p で割り切れる。

[Ⅱ] n と p が互いに素であるとき

(2)より $n^{p-1} - 1 = pm$ となる整数 m が存在する。

両辺に n をかけると

$n^p - n = pnm$

よって $n^p - n$ は p で割り切れる。

[Ⅰ][Ⅱ]より

(1)が証明された。

（解答終）

問題 3 における p が 3 以上の場合の解答は，p が 2 の場合においても成立する。しかし，解答の

途中で $a_1, a_2, \cdots, a_{p-2}$ を扱うので，高校生の混乱を避けるために，p が2の場合と3以上の場合で，場合分けをする解答を採用した。

問題 4 の(1)と(2)が同じ内容を表していることは直観的には明らかであるが，数学的に正確に同値性を証明することは重要であるので，問題 4 を用意した。問題 4 の(2)は，フェルマーの小定理といわれている。フェルマーの小定理として「表 5」に明記しておく。

表 5

定理 2（フェルマーの小定理）
p を素数，n を p と互いに素な自然数とするとき，$n^{p-1}-1$ は p で割り切れる。

フェルマーの小定理は，ウィルソンの定理を用いることなく直接証明することもできる。こちらの証明も高校生にとっては適切な内容であるため，問題 5 として用意しておく。

表 6

整数　問題プリント 4

問題 5
p を素数，n を自然数とする。
このとき，n^p-n は p で割り切れることを（ウィルソンの定理を用いずに）証明せよ。

（問題 5 の解答）
n に関する数学的帰納法で証明する。
[Ⅰ] $n=1$ のとき，
$1^p-1=1-1=0$ より
明らかに p で割り切れる。
よって，$n=1$ のとき題意は成り立つ。
[Ⅱ] $n=k$ のとき，題意が成り立つと仮定する（$k \geqq 1$）。

すなわち，$k^p-k=pm$ となる整数 m が存在するとする。
$n=k+1$ のとき，

$$
\begin{aligned}
&(k+1)^p-(k+1)\\
&={}_pC_0k^p+{}_pC_1k^{p-1}+\cdots\cdots+{}_pC_{p-1}k+{}_pC_0-k-1\\
&=k^p-k+{}_pC_1k^{p-1}+\cdots\cdots+{}_pC_{p-1}k\\
&=pm+{}_pC_1k^{p-1}+\cdots\cdots+{}_pC_{p-1}k
\end{aligned}
$$

ここで，問題 1 より，
${}_pC_1$，${}_pC_2$，…，${}_pC_{p-1}$ はすべて p の倍数である。
よって　$(k+1)^p-(k+1)$ は p で割り切れる。
よって，$n=k+1$ のときも題意は成り立つ。
[Ⅰ][Ⅱ]より
すべての自然数 n に対して，題意が成り立つことが証明された。

（解答終）

問題 5 の解答では，数学的帰納法を用いてフェルマーの小定理を証明したが，こちらの方が一般的な証明方法であるため，問題 3 だけではなく，問題 5 を扱うことは，高校生にとって有効であると思われる。

ウィルソンの定理の証明だけではなく，フェルマーの小定理の証明にも触れることで，内容としては，「数学的帰納法」や「同値性の証明」など，数学的に大切な事柄を学習できる。そのことから，問題 1 から問題 5 を順に理解することで，学習者は自然と整数論の考え方や扱い方が身につくものと思われ，整数問題の教材としては妥当であると思われる。

(2)ペアの考えを用いる教材

多項式の展開を用いることで，比較的短いプロセスでウィルソンの定理が証明できる。その反面，多項式の扱い方などがやや技巧的であり，証明自体のポイントが分かりにくいという難点もある。

それらのことを鑑みて，ここではペアの考えを用いる直接的な方法を考察する。最初に，次のような“余り”に関する基本的な性質から始める。

表 7

整数　問題プリント 5

問題 6

整数 a, b, t に対して，a，b を t で割ったときの余りをそれぞれ r，s とする。このとき，ab を t で割ったときの余りと，rs を t で割ったときの余りは等しいことを証明せよ。

（問題 6 の解答）

条件より　$a = yt + r$，　$b = zt + s$

となる整数 y, z が存在する。

$$ab = yzt^2 + yst + rzt + rs$$

$$= (yzt + ys + rz)t + rs$$

ここで，$(yzt + ys + rz)t$ は　t　で割り切れる。

よって，ab を t で割ったときの余りと，rs を t で割ったときの余りは等しい。

（解答終）

問題 6 は直観的には明らかな事柄であるが，数式を用いて正確に表現することが大切であるので，問題として用意した。次に，“ペアの考え方”を導入する。

表 8

整数　問題プリント 6

問題 7

p を素数とする。1 以上 $p-1$ 以下の任意の整数 a に対して，ab を p で割ると 1 余るような 1 以上 $p-1$ 以下の整数 b がただ 1 つ存在することを証明せよ。

※ 問題 7 のような整数 a, b を，素数 p に関するペアと呼び $\{a,b\}$ と表す。

問題 8

素数 p に関するペア $\{a,b\}$ について，自分自身がペアとなる整数は，1，$p-1$ であり，この２つに限ることを証明せよ。

（問題 7 の解答）

最初に，存在を証明する。

p は素数であり，a は 1 以上 $p-1$ 以下より，

a と p は互いに素。

よって，$ax + py = 1$ を満たす整数 x, y が存在する。

$ax = p(-y) + 1$ より，

ax は p で割ると 1 余るような整数である。

ここで，

…，$a(x-p)$，ax，$a(x+p)$，…

はすべて，p で割ると 1 余る整数であるので，

…，$x-p$，x，$x+p$，$x+2p$, …

の中から 0，1，2，3，…，$p-1$　のいずれかになるものを b とすると，ab を p で割ったときの余りは 1 になる。

ここで，$b = 0$ とすると，

$a \times 0 = pz + 1$ となる整数 z が存在する。

$p \times (-z) = 1$ となり，

p は素数であり，$-z$ は整数であるので矛盾。

したがって，b は 0 でない。

よって，ab を p で割ると 1 余るような整数 b を 1，2，3，…，$p-1$　の中から取ることができる。

よって，整数 b の存在が証明された。

次に，一意性を証明する。

b, c は，1 以上 $p-1$ 以下の整数であり，ab, ac は共に p で割ると 1 余るような整数とする。

ここで，便宜的に $c \leqq b$ としてよい。

条件より，整数 u, v が存在し，

$ab = pu + 1$,　　$ac = pv + 1$　となる。

両辺の差を取ると，

$a(b-c) = p(u-v)$

ここで，$u = v$ のとき，

$b - c = 0$ から $b = c$ となり一意性がいえるので，

$u \neq v$とする。
pは素数であり，aとpは互いに素であるから素因数分解の一意性より，
$b-c=pw$ となる整数wが存在する。

ここで，$0 \leqq b-c \leqq p-2$ より $w=0$

したがって $b-c=0$ より $b=c$
よって，整数bの一意性が証明された。

（解答終）

（問題 8 の解答）
$1\cdot 1=p\times 0+1$，$(p-1)(p-1)=p(p-2)+1$
であり，$1\cdot 1$と$(p-1)(p-1)$は共にpで割ったときの余りが1である。
よって 1，$p-1$は自分自身がペアとなる
逆に，aを自分自身がペアとなる整数とする。
すなわち，$a\cdot a=pu+1$となる整数uが存在するとする（$1 \leqq a \leqq p-1$）。

$a^2-1=pu$より，$(a+1)(a-1)=pu$

ここで，$u=0$のとき，
$a=\pm 1$から$a=1$となる
よって，$u \neq 0$とする。
pは素数であり，素因数分解の一意性より
$a+1=pk$ または $a-1=pm$となる。
（ただし，k,mは整数）
すなわち，$a=pk-1$ または $a=pm+1$

ここで，$1 \leqq a \leqq p-1$より，

$a=pk-1$の場合，$k=1$であり，$a=p-1$
$a=pm+1$の場合，$m=0$であり，$a=1$
よって，$a=1$，$p-1$
以上より，自分自身がペアとなる整数は，1，$p-1$であり，この２つに限る。

（解答終）

問題 7 および問題 8 においては，ペアという新しい概念を定めたが，解答自体は初等的な式変形で解くことができる。ただし，問題 7 においては，高校数学ではあまり扱わない「存在」と「一意性」を示すことが解答の鍵であり，学習者はこの考え方を問題 7 で理解することが重要である。また，式変形も整数論独特のものであり，問題を解くことで学習者はこのような式変形の手法に慣れることができる。問題 8 においても，$a=1$，$p-1$のときを確かめるだけではなく，“逆に，この 2 つに限る”ことを証明する必要があり，「必要十分条件の証明」というテーマを含んでいる。

これらのように，問題 7 および問題 8 は，数学的に重要な題材を内包している。そして，ペアの考えを用いることで，ウィルソンの定理をより直接的に証明することができる。

表 9

整数　問題プリント 7
問題 9 pを素数とする。$(p-1)!$をpで割ったときの余りは-1であることを証明せよ。

（問題 9 の解答）
$p=2,3$のとき題意は成り立つので，
pを5以上の素数とする。
すなわち，pは奇数とする。

$2 \leqq a_1 \leqq p-2$である任意の整数a_1に対して，ペアb_1が存在する。

ここで，$a_1 \neq b_1$であり，$2 \leqq b_1 \leqq p-2$である。

次に，$2 \leqq a_2 \leqq p-2$でありa_1，b_1と異なる任意の整数a_2に対して，ペアb_2が存在する。
同様の操作を繰り返すと，pは奇数より，
{2，3，4，……，$p-2$}
={a_1，b_1，a_2，b_2，……，a_m，b_m }
となり，2から$p-2$までの整数がペアの組に分けられる。
したがって，
$(p-1)!=(p-1)(p-2)\cdots\cdots 3\cdot 2\cdot 1$
$=(p-1)\cdot 1\cdot a_1b_1a_2b_2\cdots\cdots a_mb_m$

ここで問題 6 より
$(p-1)!$を p で割ったときの余りは
$(p-1)\cdot 1\cdot 1\cdot 1\cdots\cdots 1 = p-1$
となる。
すなわち，余りは-1となる。

（解答終）

ペアの考えを用いることで，ウィルソンの定理をより直接的に証明できる教材を作成することができた。こちらの方法では，証明のプロセスが明確であり，ウィルソンの定理の証明の仕組みがはっきりとしている。ただし，問題 7，問題 9 の解答の難易度が少し高いことが難点である。また，ペアという新しい概念を定める必要があり，直接証明できる反面，高校生にとっては馴染みにくい側面もある。

3　成果と課題

本研究により得られた成果と課題は次の 7 点である。

①数学的に正確な記述

一般的に，ウィルソンの定理の証明は，合同式を用いて記述されることが多いが，本研究においては合同式を用いずに，高校数学の範囲の知識で理解できるような教材を作成することができた。これにより合同式を学習していない者も，順を追うことで自然にウィルソンの定理の証明を，数学的に正確に理解することができる。

②2 通りの証明方法による教材

多項式の展開を用いる証明とペアの考えを用いる証明の 2 通りの証明法による教材を与えることができた。

前者には，「素数の性質」「多項式の展開」「ウィルソンの定理とフェルマーの小定理の関連」などの数学的な題材が含まれており，後者には，「素数の性質」「存在と一意性」「ペアの概念」などの数学的な題材が含まれている。これらのように，ウィルソンの定理を題材とした教材を通して，学習者は数学的に重要な内容を学ぶことができるようになっている。また，整数問題特有の証明に慣れることができる。

③内容の精選

発展的な内容を扱っていることもあり，問題の解答などで若干理解しづらい部分もある。内容の精選や証明の記述方法の改良などが今後の課題である。

④整数論への興味・関心の育成

整数論への興味・関心を育成するため，具体的に理解しやすいウィルソンの定理やフェルマーの小定理などを題材とした教材を開発することができた。合同式などの発展的な記号を使わずに，初等的な方法だけで問題を解き，整数問題に自然と慣れ親しむことで，興味・関心を育成することを意図している。

今後は，授業実践等で興味・関心の育成に有効であるかどうかを検証する必要がある。

⑤授業実践

本研究で開発した教材をもとに，実際に模擬授業等を行い，教材の有効性を検証する必要がある。発展的な内容を扱っているため，高校の科学クラブ等，意識の高い高校生を対象に模擬授業を実施することが有効であると思われる。

⑥ガウスによる一般化を題材とした教材

ウィルソンの定理は，ガウスにより一般化されている。今後は，それらを題材とした教材を考察することが考えられる。

⑦環論の立場からの教材

ウィルソンの定理やガウスによる一般化は，さらに，現代数学の環論の立場から一般化される。今後，現代数学の啓蒙的な意味からも，このような流れを意識した教材を考察することが考えられる。

A　付録

ウィルソンの定理の証明は，オイラーの公式を用いて記述することもできる。しかし，“取り込みと押し出しの方法”がオイラーの公式の証明の鍵であり，確率や集合の考え方に通じている。そのようなことから，本研究の主題の 1 つである“整数問題特有の証明方法に慣れるための教材”から少し外れるため付録として挙げておく。

問題の構成としては，「表 A」にあるように問題 A を(1)と(2)に分けて誘導形式とした。また，

高校生が自力でオイラーの公式を証明することは難しいため，“異なる$n+1$個の箱に，異なるn個の球を入れる方法を考えることにより”というヒントをつけた。

表 A

整数　問題プリント A

問題 A

(1) nを自然数とする。異なる$n+1$個の箱に，異なるn個の球を入れる方法を考えることにより，次のオイラーの公式

$$n!={}_nC_0(n+1)^n-{}_nC_1n^n+{}_nC_2(n-1)^n-\cdots\cdots$$
$$\cdots\cdots+(-1)^{n-1}{}_nC_{n-1}\cdot2^n+(-1)^n{}_nC_n\cdot1^n$$

を証明せよ。ただし，同じ箱に複数の球を入れてもよく，逆に空の箱があってもよいものとする。

(2) pを素数とする。$(p-1)!$をpで割ったときの余りは-1であることを証明せよ

（問題 A の解答）

(1)箱1から箱nまでに空の箱ができないような入れ方の総数を考えると$n!$通りである。

また，全事象をUとし，箱iが空である事象をA_iとすると，箱1から箱nまでが空にならない事象は$U\setminus A_1\cup\cdots\cup A_n$であり，その総数は

$$n(U\setminus A_1\cup\cdots\cup A_n)=n(U)-n(A_1\cup\cdots\cup A_n)$$

である。

ここで，$n(U)=(n+1)^n$，

$$n(A_1\cup\cdots\cup A_n)$$
$$={}_nC_1\cdot n(A_1)-{}_nC_2\cdot n(A_1\cap A_2)$$
$$+{}_nC_3\cdot n(A_1\cap A_2\cap A_3)-\cdots\cdots$$
$$\cdots\cdots+(-1)^{n-1}\cdot{}_nC_n\cdot n(A_1\cap\cdots\cap A_n)$$

であることから，

$$n(U\setminus A_1\cup\cdots\cup A_n)$$
$$=(n+1)^n-{}_nC_1\cdot n^n+{}_nC_2\cdot(n-1)^n$$
$$-{}_nC_3\cdot(n-2)^n+\cdots\cdots+(-1)^n{}_nC_n\cdot1^n$$

となる。よって

$$n!=(n+1)^n-{}_nC_1\cdot n^n+{}_nC_2\cdot(n-1)^n$$
$$-{}_nC_3\cdot(n-2)^n+\cdots\cdots+(-1)^n\cdot{}_nC_n\cdot1^n$$

を得る。

(2) $p=2$のとき題意は成り立つので，

pを3以上の素数とする。

(1)におけるオイラーの公式において，

$n=p-1$のときを考えると

$$(p-1)!=p^{p-1}-{}_{p-1}C_1(p-1)^{p-1}$$
$$+{}_{p-1}C_2(p-2)^{p-1}-\cdots\cdots$$
$$\cdots\cdots+(-1)^p\cdot{}_{p-1}C_{p-2}\cdot2^{p-1}+(-1)^{p-1}$$

となる。

フェルマーの小定理より

${}_{p-1}C_i(p-i)^{p-1}$と${}_{p-1}C_i$はpで割ったときの余りが等しい（$1\leqq i\leqq p-2$）。

よって，$(p-1)!$をpで割ったときの余りは

$$-{}_{p-1}C_1+{}_{p-1}C_2-{}_{p-1}C_3+\cdots\cdots$$
$$\cdots\cdots+(-1)^p\cdot{}_{p-1}C_{p-2}+(-1)^{p-1}$$

である。

ここで，二項定理

$$(a+b)^{p-1}={}_{p-1}C_0a^{p-1}+{}_{p-1}C_1a^{p-2}b$$
$$+{}_{p-1}C_2a^{p-3}b^2+\cdots\cdots+{}_{p-1}C_{p-1}b^{p-1}$$

において，$a=1$，$b=-1$ とおくと，

$$0=1-{}_{p-1}C_1+{}_{p-1}C_2-\cdots\cdots+(-1)^{p-1}\cdot{}_{p-1}C_{p-1}$$

となる。

したがって

$$-{}_{p-1}C_1+{}_{p-1}C_2-{}_{p-1}C_3+\cdots\cdots$$
$$\cdots\cdots+(-1)^p\cdot{}_{p-1}C_{p-2}+(-1)^{p-1}=-1$$

を得る。

よって，$(p-1)!$をpで割ったときの余りは-1で

ある。

（解答終）

（1）のオイラーの公式の証明においては，和集合の要素の個数に関する公式を用いることで，“取り込みと押し出しの方法”を数学的に正確に記述することができることから，そちらを採用することとした。オイラーの公式は一般に「表 B」のようになる。

表 B

オイラーの公式

自然数 n と実数 a に対して，次の等式が成り立つ。

$$n!={}_nC_0\cdot a^n-{}_nC_1(a-1)^n+{}_nC_2(a-2)^n-\cdots$$
$$\cdots+(-1)^{n-1}\cdot{}_nC_{n-1}(a-n+1)^n$$
$$+(-1)^n\cdot{}_nC_n(a-n)^n$$

一般の場合のオイラーの公式も，$n\leqq a$ のときは問題 A(1)の解答と同様に「箱 1～箱 a」と「球 1～球 n」を考えることで証明することができる。このとき，等式は $n\leqq a$ であるすべての自然数 a で成り立つことから，a に関する恒等式になる。このことから，すべての実数 a で等式が成り立つことが分かる。

オイラーの公式を一般的な形で記述してもよいが，2 変数のため高校生への負担が大きくなることから，問題 A(1)においては $a=n+1$ の特別な場合を提示した。この場合，1 変数になるため高校生への負担が少ないと思われる。

以上によりウィルソンの定理をオイラーの公式を用いて証明することができた。内容としては「オイラーの公式」「フェルマーの小定理」「和集合の要素の個数に関する公式」などの数学的な事柄を含んでいる。

参考文献

András Szilárd (2011), A Combinatorial Generalization of Wilson's Theorem, Australasian Journal of Combinatorics, Volume 49, 265-272.

Dickson Leonard Eugene (1952), History of the Theory of Numbers, Volume 1, Chelsea Publishing Company, New York.

Hirano Yasuyuki and Matsuoka Manabu (2013), Finite Rings and Wilson’s Theorem, Turkish Journal of Mathematics, Volume 37, Issue 4, 571-576.

Laššák Miroslav (2000), Wilson's Theorem in Algebraic Number Fields, Mathematica Slovaca Volume 50, Number 3, 303-314.

Tripathi　Amitabha (2006), A Combinatorial Proof of Wilson's Theorem, Ars Combinatoria Volume 80, 201-204.

Turnage Caroline LaRoch　(2008), Selected Proofs of Fermat's Theorem and Wilson's Theorem, A Thesis for the Degree of Master of Arts, Wake Forest University.

鳥取大学数学教育研究　　**ISSN 1881–6134**

Site URL：http://www.rs.tottori-u.ac.jp/mathedu

投稿規定

- ❖ 本誌は，次の稿を対象とします。
  - 鳥取大学数学教育学研究室において作成された卒業論文・修士論文，またはその抜粋・要約・抄録
  - 算数・数学教育に係わる，理論的，実践的研究論文／報告
  - 鳥取大学，および鳥取県内で行われた算数・数学教育に係わる各種講演の記録
  - その他，算数・数学教育に係わる各種の情報提供
- ❖ 投稿は，どなたでもできます。投稿された原稿は，編集委員による審査を経て，採択が決定された後，随時オンライン上に公開されます。
- ❖ 投稿は，編集委員まで，e-mailの添付書類として下さい。その際，ファイル形式は，PDFとします。
- ❖ 投稿書式は，バックナンバー（vol.9 以降）を参照して下さい。

鳥取大学数学教育学研究室

〒 680-8551　鳥取市湖山町南 4-101

TEI & FAX 0857-31-5101（溝口）

http://www.rs.tottori-u.ac.jp/mathedu/