フェルマーの小定理の別証明について

6 年 C 組　山名 大二郎
指導教員　川口　　慎二

１．研究の背景と目的

私は昨年から「フェルマーの小定理」に興味をもち、自分で別証明を考えることでその定理に対して考察を深めた。

２．研究概要

2 つの整数 a と b に対して、a と b を p で割った余りが等しくなるとき、a と b は p を法として**合同**であるといい、$a \equiv b \pmod{p}$ と表す。本稿では、次のフェルマーの小定理に対して、独自に 3 つのアプローチから別証明の方針を与える。

<u>定理</u>（フェルマーの小定理）

p を素数、a は p と互いに素である自然数とするとき、$a^{p-1} \equiv 1 \pmod{p}$ が成り立つ。

■一般的に知られている証明

$a,\ 2a,\ 3a, \cdots, (p-1)a$ について考える。$sa \equiv ta \pmod{p}$ となる $s,\ t$ （$1 \leqq s-t \leqq p-1$, $s \neq t$）が存在すると仮定する。$(s-t)a \equiv 0 \pmod{p}$ なので、$1 \leq s-t \leq p-1$ から、a と p が互いに素であることに矛盾する。ゆえに、$a,\ 2a,\ 3a, \cdots, (p-1)a$ を p で割った余りはすべて異なる。したがって、$a^{p-1}(p-1)! \equiv (p-1)!$ なので、$a^{p-1} \equiv 1 \pmod{p}$.　　(Q.E.D.)

■別証明に共通するアイデア

はじめに、別証明に共通する考え方を示す。まず、ウィルソンの定理：「p を素数とするとき、$(p-1)! \equiv -1 \pmod{p}$ が成り立つ」を用いる。$a^{p-1}-1 \equiv 0 \pmod{p}$ を示すために、

$(a+1)(a+2)\cdots(a+p-1) \equiv a^{p-1}-1 \pmod{p}$ を示せばよい。ここで、

$$(a+1)(a+2)\cdots(a+p-1) = a^{p-1} + S_1 a^{p-2} + S_2 a^{p-3} + \cdots + S_{p-2} a + (p-1)!$$

と表すことができ、ウィルソンの定理：$(p-1)! \equiv -1 \pmod{p}$ により、

$(a+1)(a+2)\cdots(a+p-1) = a^{p-1} + S_1 a^{p-2} + S_2 a^{p-3} + \cdots + S_{p-2} a - 1$ であるため、

$S_1 \equiv S_2 \equiv \cdots \equiv S_{p-2} \equiv 0$ を証明すればよい。

■アプローチ①

$p=5,\ m=3$ の場合を例にアイデアを示す。$1+2+3+4 \equiv 0 \pmod 5$ なので、

$$(1+2+3+4)(1\cdot 2+1\cdot 3+1\cdot 4+2\cdot 3+2\cdot 4+3\cdot 4) \equiv 0 \pmod 5$$

ゆえ、$1\cdot 2\cdot 3+1\cdot 2\cdot 4+1\cdot 3\cdot 4+2\cdot 3\cdot 4 \equiv 0 \pmod 5$ である。このアイデアを一般の $p,\ m$ に対しても同様に適用して、証明することができた。

■アプローチ②

S_m を $1, 2, 3, \cdots,\ p-1$ の中から m 個の数を全通りの方法で取り出し、それぞれのグループ内での積を求めたときの各積の総和であると定める。例えば、$p=5,\ m=3$ のとき、

$$S_3 = 1\cdot 2\cdot 3+1\cdot 2\cdot 4+1\cdot 3\cdot 4+2\cdot 3\cdot 4 \equiv 0 \pmod 5$$

となる。このように、2 組で打ち消しあうことができ、m が奇数のときは $S_m \equiv 0 \pmod p$ である。しかし、m が偶数のときは一般には成立しない。

■アプローチ③

S_m を p と m の式で表し、数学的帰納法を用いて証明することを目指した。$S_1 \equiv S_2 \equiv \cdots \equiv S_{m-1} \equiv 0$ と仮定すると、$S_m = (-1)^{m-1} \sum_{k_{n-1}=1}^{p-m} \left(k_{n-1} \sum_{k_{n-2}=1}^{k_{n-1}} \left(k_{n-2} \cdots \sum_{k_2=1}^{k_3} \left(k_2 \sum_{k_1=1}^{k_2} k_1 \right) \cdots \right) \right)$

$$S_m = \alpha_{m+1}^{(m)}(p-m)\cdots p + \alpha_{m+2}^{(m)}(p-m-1)\cdots p + \cdots + \alpha_{2m}^{(m)}(p-2m+1)\cdots p$$

$$\alpha_{m+1}^{(m)} = \frac{1}{(m+1)!},\ \alpha_{2m}^{(m)} = \frac{1}{2^m \cdot m!},\ \alpha_{m+t}^{m} = \frac{1}{m+t}\left(\alpha_{m+t-2}^{(m-1)} + t\alpha_{m+t-1}^{(m-1)}\right)$$

のように漸化式で表せる。

３．考察

アプローチ②については、まだ証明を改良できる余地があるので、アプローチ①の考え方やアプローチ③で得られた S_m の式を用いるなど、引き続き考えてみたい。また、フェルマーの小定理を一般化したものであるオイラーの定理についても考察しようと思う。