生徒の質問から

横山（よこやま）　政道（まさみち）

§1．はじめに

［問題1］　m，n がともに自然数のとき，$3^n-3^m=24$　を満たす n，m の値を求めよ。

センター試験1ケ月前の追い込みの時期，対数の関係式から導かれた上記の問題の解説の中で，「穴埋めは適当に代入していけば答えが求まることもある」と言ったところ，生徒からこんな質問があった。それはもっと大きな数が答えになるときはどうするのですか？という内容である。そこで，数を大きくして一般的に考えていくことにする。

［問題2］　2005^n-2005^m が1000の倍数になるように，最小の自然数 m，n の値を求めよ。

§2．オイラーの定理および用語の説明

(a)　**合同式**

2つの整数 a と b を自然数 n で割った余りが同じであるとき，a と b は n を法として合同であるといい，記号 $a\equiv b\pmod{n}$ と書く。

＜例＞　$21\equiv1\pmod{5}$　　$100\equiv2\pmod{7}$

$a-b$ が n の倍数になっている。

(b)　**オイラー関数とオイラーの定理**（証明略）

オイラー関数 $\psi(n)$ ➡ n を正の整数とするとき，$1\sim n-1$ までの整数で n と互いに素な整数の個数を表す。ただし，$\psi(1)=1$ と約束する。

$n=a^p\times b^q\times c^r\times d^s\times\cdots\cdots$ と素因数分解の式で表されるとき

$$\psi(n)=n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\left(1-\frac{1}{d}\right)\cdots\cdots$$

＜例＞　$n=15$ の場合　$15=3\times5$ から，

$\psi(15)=15\times\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=8$　実際に書き並べると $\{\underline{1},\ 2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14\}$ の8個。

オイラーの定理　n を正の整数とし，a と n が互いに素な整数のとき　$a^{\psi(n)}\equiv1\pmod{n}$

(c)　**位数の意味と位数法則について**

位数 ➡ $a^e\equiv1\pmod{n}$ となる最小の自然数 e

＜例＞　フェルマーの小定理から導かれる式 $2^6\equiv1\pmod{7}$ において，$2^3\equiv1\pmod{7}$ であるから，mod7 における2の位数は3である。

位数法則 ➡ mod n での a の位数を e とするとき

$a^n\equiv1\pmod{n}$ ならば，e は n の約数

§3．問題2の解答

それでは問題2の解答に入ります。

［解］　$1000=2^3\times5^3$　$2005=5\times401$

$2005^n-2005^m=2005^m(2005^{n-m}-1)$

$=5^m\cdot401^m\cdot(2005^{n-m}-1)=5^m\cdot401^m\times$(偶数)

は，$2^3\times5^3$ の倍数であるから，$m\geqq3$ でなければならない。また m は最小の数であるから　$m=3$

このとき，$2005^{n-m}-1$ は8の倍数であり，合同式で表すと，$2005^{n-3}\equiv1\pmod{8}$ である。

$n-3=k$ とおいて，$2005^k\equiv1\pmod{8}$ を満たす最小の自然数 k の値を求める。

オイラー関数から，　$\psi(8)=8\left(1-\frac{1}{2}\right)=4$

オイラーの定理から　$2005^4\equiv1\pmod{8}$ が成り立ち，位数の法則より，求める最小の数は4の約数にあるから，それぞれ調べていく。ただし，$2005\equiv5\pmod{8}$ から5で計算を行うと，（計算が楽）

1のとき　$2005^1\equiv5^1\fallingdotseq1\pmod{8}$

2のとき　$2005^2\equiv5^2\equiv1\pmod{8}$　よって，$k=2$

したがって，最小の自然数 m，n は，$m=3$，$n=5$

《参考文献》

〔1〕　数学オリンピック事典　野口廣　監修

〔2〕　センター試験対応模試　数学Ⅰ・A，Ⅱ・B×8　改訂版　Z会出版

（宮崎県立宮崎南高等学校）