余りの数学に関する一考察

―フェルマーの小定理の活用を通して―

横山　政道（よこやま　まさみち）

§0．はじめに

入試問題を解いていると，大学の教養レベルの知識を知っていれば，問題の背景が分かり見通しがつきやすい問題は多い。中でも剰余の問題や周期数列的な問題等では，フェルマーの小定理や合同式が威力を発揮します。これらが背景になっている入試問題等について考察していきます。

§1．フェルマーの小定理について

［問題1］　p を素数とする。k は自然数で $k<p$ であるとき，二項係数 ${}_pC_k$ は p で割り切れることを証明せよ。　〔03 大阪教育大(後期)〕

〔解〕　$k<p$ で

${}_pC_k=\dfrac{p(p-1)(p-2)\cdots\cdots(p-k+1)}{k!}$ は自然数で，

p は素数であるから $k!$ の因数で割り切れない。

すなわち，${}_pC_k$ は p の倍数である。㊦

フェルマーの小定理を理解するには合同式の意味を知っておく必要があるので簡単に説明します。

合同式

2つの整数 a と b を2以上の自然数 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＞　$21\equiv1\pmod5$　$100\equiv2\pmod7$

$a-b$ が n の倍数になっている。

では有名定理を導いていくことにします。

［二項定理］　$(a+b)^p=a^p+\sum_{k=1}^{p-1}{}_pC_ka^{p-k}\cdot b^k+b^p$

において，p が素数のとき，［問題1］から ${}_pC_k$ は p の倍数であるから次の式が成り立つ。

$(a+b)^p\equiv a^p+b^p\pmod p$

同様にして，m 個の場合は

$(\underbrace{a+b+c+\cdots}_{m\text{個}})^p\equiv\underbrace{a^p+b^p+c^p+\cdots\cdots}_{m\text{個}}$

$a=b=c=\cdots\cdots=1$ とおくと，

$(\underbrace{1+1+1+\cdots\cdots}_{m\text{個}})^p\equiv\underbrace{1^p+1^p+\cdots\cdots+1^p}_{m\text{個}}\pmod p$

すなわち　$m^p\equiv m\pmod p$

［フェルマーの小定理］

p を素数，a を任意の自然数とすると，

$a^p\equiv a\pmod p$

（どんな数 a も p 乗すると自分自身にもどる）

また，a と p が互いに素つまり a が p の倍数でないときは，両辺を a で割った式 $a^{p-1}\equiv1\pmod p$ も成立する。

㊟　ここで，注意すべきことは p が素数であること，素数でない数の場合はフェルマーの小定理を拡張したオイラーの定理が使われます。

§2．具体例

［問題2］　2^{2005} を5で割った余りを求めよ。　〔類02 法政大〕

フェルマーの小定理より

$2^5\equiv2\pmod5$

2と5は互いに素より

$2^4\equiv1\pmod5$ また $2005=4\times501+1$ から

$2^{2005}=(2^4)^{501}\cdot2\equiv1\cdot2\pmod5$

よって，求める余りは　2

［問題3］　n を正の整数とし，3^n を17で割ったときの余りを $r(n)$ とする。

(1)　$r(3)$，$r(5)$，$r(8)$，$r(11)$ の値を求めよ。また，$r(25)$，$r(2005)$ の値を求めよ。

(2)　任意の正の整数 n について $r(n)=r(n+k)$ が成り立つような正の整数 k を考える。このよ

うな k のうち最小のものを求めよ。

(3) 整数 a, b が $0 \leqq b < a \leqq 20$ を満たすとする。このとき，3^a+3^b が 17 で割り切れるような組 (a, b) の中で a, b が素数である組を a の値が大きいほうから順に並べると，(□, □), (□, □), (□, □) である。〔類04 近畿大・理工〕

(1) [解] 3^3 を 17 で割った余りは 10 であり，合同式で表していくと $3^3 \equiv 10 \pmod{17}$

以下合同式の計算法則を使って，

$3^4 \equiv 30 \equiv 13 \pmod{17}$, $3^5 \equiv 39 \equiv 5 \pmod{17}$

……, $3^8 \equiv 16 \pmod{17}$, $3^9 \equiv 48 \equiv 14 \pmod{17}$

$3^{11} \equiv 126 \equiv 7 \pmod{17}$

よって，$r(3)=10$, $r(5)=5$, $r(8)=16$, $r(11)=7$

[フェルマーの小定理]より

$3^{17} \equiv 3 \pmod{17}$ また，3 と 17 は互いに素から $3^{16} \equiv 1 \pmod{17}$ が成り立つ。

合同式の計算法則から

$3^{16} \equiv 1 \pmod{17}$ の両辺に 3^9 をかけると

$3^{25} \equiv 3^9 \equiv 14 \pmod{17}$ すなわち，$r(25)=14$

また，$r(2005)$ の値は

$3^{2005} \equiv 3^{16\times 125+5} \equiv (3^{16})^{125} 3^5 \equiv 1 \cdot 5 \equiv 5 \pmod{17}$

$\therefore \quad r(2005)=5$

このように，桁数が大きい場合，この定理は有効です。

(2) (解説) 定理より導かれた $3^{16} \equiv 1 \pmod{17}$ から $k=16$ になりそうな気がしますが，実際にはそうならない場合もありますので注意が必要です。一つ例を挙げると，フェルマーの小定理から導かれる式 $2^6 \equiv 1 \pmod{7}$ において，$2^3 \equiv 1 \pmod{7}$ です。因みに，最小の数 3 を mod 7 における 2 の位数といいます。

その最小の数の求め方ですが，位数の法則というのがあって，一般に約数の中に存在することが分かっています。つまり 16 の約数を一つ一つ調べていくと，求める最小の数 16 が求まります。

[解] $3^{16} \equiv 1 \pmod{17}$ より，16 の約数 1, 2, 4, 8, 16 について，それぞれ調べていくと，$3^1 \equiv 3$, $3^2 \equiv 9$, $3^4 \equiv 13$, $3^8 \equiv 16 \pmod{17}$ よって，$k=16$

(3) [解] (1)(2)の結果から (以下 (mod17) を省略)

$3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 10$, $3^5 \equiv 5$, $3^7 \equiv 11$, $3^{11} \equiv 7$, $3^{13} \equiv 12$, $3^{16} \equiv 1$, $3^{17} \equiv 3$, $3^{19} \equiv 10$, …… 周期 16 で繰り返される。

この中で条件に合う素数 a, b の値を求めていくと

$3^{19}+3^{11} \equiv 17$, $3^{13}+3^5 \equiv 17$, $3^{11}+3^3 \equiv 17 \pmod{17}$

したがって，$(a, b)=(19, 11), (13, 5), (11, 3)$ の 3 組。

その他，整数に関する証明問題でもフェルマーの小定理は現れます。例をあげると，

[問題 4] 正の整数 n について，$2n^3-3n^2+7n$ ……① は 6 の倍数であることを証明せよ。

いろいろと解法が考えられますが，基本的かつ重要な解法には整数を 6 で割った余りに分けて一つ一つ丁寧に調べていく方法や，隣接する整数の積の定理を用いるために因数分解をする方法などがあります。ここではフェルマーの小定理を含めて 2 つの方法で解いてみることにします。

[解 1]

隣接する k 個の整数の積は $k!$ で割り切れる。

$$\begin{aligned} 2n^3-3n^2+7n &= n(2n^2-3n+7) \\ &= n\{(n-1)(n+1)+n^2-3n+8\} \\ &= n\{(n-1)(n+1)+(n-1)(n-2)+6\} \\ &= (n-1)n(n+1)+(n-2)(n-1)n+6n \end{aligned}$$

$(n-1)n(n+1)$, $(n-2)(n-1)n$ は隣接 3 整数の積より 6 の倍数であり，$6n$ も 6 の倍数であるから，①は成り立つ。

[解 2]

p を素数，n を任意の自然数とすると，

$n^p \equiv n \pmod{p}$ [フェルマーの小定理]

$$2n^3-3n^2+7n = 6\left(\frac{n^3}{3}-\frac{n^2}{2}+\frac{7n}{6}\right)$$

$$= 6\left(\frac{n^3-n}{3}-\frac{n^2-n}{2}+\frac{n}{3}-\frac{n}{2}+\frac{7}{6}n\right)$$

$$= 6\left(\frac{n^3-n}{3}-\frac{n^2-n}{2}+n\right)$$

定理より，n^3-n, n^2-n はそれぞれ 3 と 2 で割り切れるから，①は 6 の倍数である。

《参考文献》

〔1〕 モノグラフ 20 整数 宮原 繁 著 科学新興社

〔2〕 2004 数学ⅠⅡAB入試問題集 数研出版

〔3〕 2003 数学ⅠⅡAB入試問題集 数研出版

(宮崎県立宮崎南高等学校)