合同式

【例題】
aを自然数とすると，a^3を **3** で割った余りと，aを **3** で割った余りは等しいことを示せ．
（慶応大・理工）

解法は主に 3 通りあるが，すべてをマスターしてほしい．まずは，一番一般的な解法を説明する．数式に 3 を登場させるために，$3k, 3k+1, 3k+2$などのように分類して，式に 3 を登場させるやり方である．

【解答１】
$a=1$のとき，$a^3=1$ より成り立つ．$a=2$のとき，$a^3=8$ より成り立つ．それ以外の自然数は，$a=3k, 3k+1, 3k+2$ (kは自然数) のいずれかで表せる．
ⅰ）$a=3k$のとき
$$a^3=3(9k^3)$$
より，余りはいずれも 0
ⅱ）$a=3k+1$のとき
$$a^3=(3k+1)^3=3(9k^3+9k^2+3k)+1$$
より，余りはいずれも 1
ⅲ）$a=3k+2$のとき
$$a^3=(3k+2)^3=3(9k^3+18k^2+12k+2)+2$$
より，余りはいずれも 2
以上より成り立つ．

※次の解答は，因数分解する解法であり，うまくはまるときれいにいくことも多い．また，3 で割った余りが等しいということは，引いたときに 3 の倍数になっているということであることを利用している．

【解答２】
$$a^3-a=a(a+1)(a-1)$$
であり，右辺は 3 連続する数なので，3 の倍数である．a^3とaの差が 3 の倍数であることは，3 で割った余りが等しいことを意味する．よって示された．

※最後の解答は，合同式とよばれる，次のようなものを導入する．今後の問題でフルに活用するので，マスターしてほしい．

一般に 2 つの整数a，bに対し，aとbをmで割った余りが等しいとき
$$a \equiv b \quad (mod\ m)$$
とかき，mを法として合同であるという．
合同式には，次の性質がある．
$$a \equiv b,\ c \equiv d \quad (mod\ m)$$
であるならば次の式が成り立つ．
$$a \pm c \equiv b \pm d,\ ac \equiv bd \quad (mod\ m)$$
特に$a \equiv b \quad (mod\ m) \Rightarrow a^n \equiv b^n \quad (mod\ m)$
が成り立つ．
大学で習う内容なので，解答には軽く定義を書いておく方がよい．

【解答３】
定数a, bを 3 で割った余りが等しいことを
$$a \equiv b \quad (mod\ 3)$$
と表すことにする．
ⅰ）$a \equiv 0\ (mod\ 3)$ のとき
$$a^3 \equiv 0^3 \equiv 0\ (mod\ 3)$$
より成り立つ．
ⅱ）$a \equiv 1\ (mod\ 3)$ のとき
$$a^3 \equiv 1^3 \equiv 1\ (mod\ 3)$$
より成り立つ．
ⅱ）$a \equiv 2\ (mod\ 3)$ のとき
$$a^3 \equiv 2^3 \equiv 8 \equiv 2\ (mod\ 3)$$
より成り立つ．よって示された．

【１】次の問に答えよ．ただし，数値は全て 10 進数とする．
(1) 7^{12}の 1 の位を求めよ．
(2) nが自然数のとき，117^nの 1 の位は 1，3，7，9のいずれかであることを証明せよ．
(3) 117^{2002}の 1 の位を求めよ．
（新潟大）

【解答】
(1) $7^2=49$，7^3の 1 の位は，7^2の 1 の位に 7 をかけた数の 1 の位になるから 3．7^4の 1 の位は，7^3の 1 の位に 7 をかけた数の 1 の位になるから 1. 同様に考えると7^5の 1 の位は 7, 7^6の 1 の位は 9 となり，以下，7, 9, 3, 1, 7, 9, 3, 1, …と繰り返しになる．
よって，mを 0 以上の整数とすると，
7^{4m+1}の 1 の位は 7
7^{4m+2}　〃　9
7^{4m+3}　〃　3
7^{4m+4}　〃　1
となるので，7^{12}の 1 の位は 1

(2) $117^n=(110+7)^n$
$={}_nC_0(110)^n+{}_nC_1(110)^{n-1}\cdot 7+\cdots+{}_nC_n 7^n$
最後の項以外は 1 の位は全て 0 だから，117^nは7^nの 1 の位と同じになり(1)の説明より，1，3，7，9のいずれかになる．

(3) 7^{2002}の 1 の位と同じであり，$7^{4\times500+2}$より 9

※合同式を使うと(1)は
$7^2 \equiv 49 \equiv 9 \pmod{10}$，$7 \equiv 7 \pmod{10}$より
$$7^3 \equiv 7^2 \times 7 \equiv 9 \times 7 \equiv 3$$
以下は同様に$7^4 \equiv 1 \pmod{10}$
よって，$7^{12} = (7^4)^3 \equiv 1^3 \equiv 1 \pmod{10}$
(3)は，$117 \equiv 7 \pmod{10}$より
$117^{2002} \equiv 7^{2002} = (7^4)^{500} \cdot 7^2 \equiv 7^2 \equiv 9 \pmod{10}$
となる．

※なお，この解答では，$7^4 \equiv 1 \pmod{10}$という情報が非常に役立っている．このような式を作るのが1つの目標であろう．合同式の威力を知ってもらうために，次の問題をやっておこう．

【２】nを自然数とするとき，$3^{n+1} + 4^{2n-1}$は13で割り切れることを証明せよ．
（名古屋市立大）

合同式を使わない場合は，帰納法を用いる．ポイントは，計算できるように，3か4のどちらかにそろえることである．
【解答】
$$4^2 \equiv 16 \equiv 3 \pmod{13}$$
なので，
$$\begin{aligned} 3^{n+1} + 4^{2n-1} &\equiv 9 \cdot 3^{n-1} + 4 \cdot 4^{2(n-1)} \pmod{3} \\ &\equiv 9 \cdot 3^{n-1} + 4 \cdot 3^{n-1} \pmod{3} \\ &\equiv 13 \cdot 3^{n-1} \equiv 0 \pmod{3} \end{aligned}$$
よって示された．

【３】nを自然数，pを素数とするとき，次のことを示せ．
(1) ${}_pC_1$，${}_pC_2$，…${}_pC_{p-1}$はいずれもpの倍数であることを示せ．
(2)定数a, bに対し，$(a+b)^p$をpで割った余りと，$a^p + b^p$をpで割った余りが等しいことを示せ．
(3) $n^p - n$ はpの倍数であることを示せ．
（類題多数）

（１）kを$p-1$以下の自然数とする．
$$ {}_pC_k = \frac{p(p-1)\cdots(p-k+1)}{k!} $$
であり，これは組み合わせだから整数である．また，pは素数で，$p > k$であるのでpと$k!$は互いに素である．よって，いずれもpの倍数となる．

（２）定数a, bに対し，pで割った余りが等しいとき，
$$a \equiv b \pmod{p}$$
と表すことにする．
$$\begin{aligned} (a+b)^p &= a^p + {}_pC_1 a^{p-1}b + \cdots {}_pC_{p-1} ab^{p-1} + b^p \\ &\equiv a^p + b^p \pmod{p} \end{aligned}$$
（（１）の結果を用いた．）

（３）$(a+b)^p \equiv a^p + b^p \pmod{p}$
において，$a = a_1 + a_2$，$b = a_3$ とおくと，
$$(a_1 + a_2 + a_3)^p \equiv {a_1}^p + {a_2}^p + {a_3}^p \pmod{p}$$
順次行うと，帰納的に，
$$(a_1 + a_2 + \cdots + a_n)^p \equiv {a_1}^p + {a_2}^p + \cdots + {a_n}^p \pmod{p}$$
ここで，$a_1 = a_2 = \cdots = a_n = 1$ とすると，
$$n^p \equiv n \pmod{p}$$
となるから，$n^p - n$ はpの倍数．

※$n^p \equiv n \pmod{p}$ はnとpが互いに素ならnで割ることができることが知られており，
$$n^{p-1} \equiv 1 \pmod{p}$$
が成り立つ．これをフェルマーの小定理という．

【練習】
$n^5 - n$が5の倍数であることを確認せよ．
（南山大・経営，一部略）