代数入門演習　NO. 6　　2013. 11.12

6　合同式

6.1　解説編

定義 6.1. (合同式)　m を自然数とする．整数 a, b が与えられたとき,

$$m \mid (a-b), \qquad \text{つまり } \exists c \in \mathbb{Z} \text{ s.t. } a-b=mc$$

が成り立つならば,「**a と b は m を法として (mod m で) 合同である**」といい, 記号

$$a \equiv b \pmod{m}, \quad a \equiv b \mod m, \quad a \equiv b\ (m)$$

等で表わす.　□

合同式を考えることの有用性は**講義プリントの第 6.1 節**で語られているが, ここでは単純な事実であり, かつ重宝な命題6.1 を使って, いくつかの例を見る (命題6.2, 問題6.15, 問題6.16, 問題6.17).

命題 6.1 (**講義プリントの命題 6.3**)**.** a を任意の整数とする．このとき次が成り立つ.

(1) a が偶数, つまり a を 2 で割ったときに余りが 0 ならば, $a^2 \equiv 0 \mod 4$.

(2) a が奇数, つまり a を 2 で割ったときに余りが 1 ならば, $a^2 \equiv 1 \mod 8$ が成り立つ.

d を平方 (数) でない自然数, a を 0 でない整数とする．平方数とは整数の 2 乗として表される数のことである．不定方程式 $x^2 - dy^2 = a$ は「Pell 方程式」と呼ばれ, 古来から研究対象になっている[1]．Pell 方程式 $x^2 - dy^2 = 1$ $(a = 1)$ はいつも整数解をもつことが Lagrange(1767) により証明されている．$\sqrt{d}$ の連分数展開を利用するという Euler のアイデアを使って, Lagrange はそのすべての整数解の求め方を提示している．一方, Pell 方程式 $x^2 - dy^2 = -1$ $(a = -1)$ は必ずしも整数解をもつとは限らない．例えば, $x^2 - 2y^2 = -1$ は解をもつが, $x^2 - 3y^2 = -1$ は解をもたない．Legendre(1830), Dirichlet(1834) から始まって, Pell 方程式 $x^2 - dy^2 = -1$ が整数解をもつための種々の d に関する判定法 (十分条件) が与えられているが, **まだ万能な判定法は知られていない．** ($\sqrt{d}$ の連分数展開を利用すると (予測できない) 長い計算の後, 原理的には解の存在を判定はできる.) 命題6.1 を使うと, この Pell 方程式が整数解をもつための 1 つの必要条件がわかる (命題6.2).

e が 3 以上の奇数ならば, 命題6.2 により Pell 方程式 $x^2 - 2^e y^2 = -1$ は整数解をもたないことがわかる．例えば, $x^2 - 8y^2 = -1$, $x^2 - 32y^2 = -1$ は整数解をもたない．また, c を平方 (数) でない正の奇数, e を 2 以上の自然数とする．そのとき, 命題6.2 により Pell 方程式 $x^2 - 2^e cy^2 = -1$ は整数解をもたない．例えば, $x^2 - 12y^2 = -1$, $x^2 - 20y^2 = -1$ は整数解をもたない.

---

[1]その歴史については No.5, p.5 の脚注で紹介した, 小林昭七氏の著作の第 3.11 節を参照. d が平方数のときは $d = e^2$ をみたす整数 e が存在する．そのとき,

$$(x + ey)(x - ey) = x^2 - e^2y^2 = x^2 - dy^2 = a$$

となり, a の約数を調べることに帰着して問題が極端に易しくなってしまう．問題 4.3 を参照.

命題 6.2. Pell 方程式 $x^2 - dy^2 = -1$ が整数解をもつならば, d は奇数か, または $2 \parallel d$ をみたす. ここで記号「$2 \parallel d$」は $2 \mid d$, しかし $2^2 \nmid d$ となることを意味する. つまり, $v_2(d) = 1$.

[証明]　$x^2 - dy^2 = -1 \ \cdots (*)$ をみたす整数 x, y が存在すると仮定する. x の偶奇で場合分けして考える. まず次の簡単な事実に注意する. 整数 a について, $a^2 - a = a(a-1)$ で, a と $a-1$ のどちらか 1 つは 2 で割り切れるから, $a^2 \equiv a \mod 2$ が成り立つ.

(i) x が偶数のとき. いまのことから $x^2 \equiv x \equiv 0$, $y^2 \equiv y \mod 2$ に注意して, $(*)$ の両辺を mod 2 で考えると, $0 - dy \equiv -1 \mod 2$ (問題 6.3). 両辺に -1 をかけて (あるいは移項して), $dy \equiv 1 \mod 2$ となる (問題 6.3). d が偶数であると仮定すると, $0 \equiv d \mod 2$ だから,

$$0 = 0y \equiv dy \equiv 1 \mod 2$$

(問題 6.3), よって, $0 \equiv 1 \mod 2$ となり (問題 6.1(3)) 矛盾を得る (問題 6.2). ゆえに, d は奇数となる.

(ii) x が奇数のとき. 命題 6.1(2) により $x^2 \equiv 1 \mod 8$ だから, $(*)$ の両辺を mod 8 で考えると, $1 - dy^2 \equiv -1 \mod 8$ (問題 6.3). したがって, $dy^2 \equiv 2 \mod 8 \ \cdots (**)$(問題 6.3). とくに, $dy^2 \equiv 2 \mod 4$(問題 6.4(1)). y が偶数であると仮定すると, 命題 6.1(1) により $0 \equiv y^2 \mod 4$ だから,

$$0 = d0 \equiv dy^2 \equiv 2 \mod 4$$

(問題 6.3), よって, $0 \equiv 2 \mod 4$ となり (問題 6.1(3)) 矛盾を得る (問題 6.2). ゆえに, y は奇数となる. 再び命題 6.1(2) (と問題 6.1(2)) により $1 \equiv y^2 \mod 8$ だから, $(**)$ により,

$$d = d1 \equiv dy^2 \equiv 2 \mod 8$$

(問題 6.3). したがって, $d \equiv 2 \mod 8$(問題 6.1(3)). ゆえに, $d - 2 = 8z$ をみたす整数 z が存在する. そのとき $d = 2(1 + 4z)$ で, $1 + 4z$ は奇数だから, $2 \parallel d$ をみたす.

(i), (ii) により主張がわかる. $\square$

6.2　問題編

問題 6.1. m を自然数, a, b, c を整数とする. 次を示せ.

(1) [反射律] $a \equiv a \mod m$.

(2) [対称律] $a \equiv b \mod m \Longrightarrow b \equiv a \mod m$.

(3) [推移律] $a \equiv b \mod m$ かつ $b \equiv c \mod m \Longrightarrow a \equiv c \mod m$.

問題 6.2. m を自然数, a, b を整数とする. $a \equiv b \mod m$ が成り立つための必要十分条件は, a と b をそれぞれ m で割ったときの余りが一致することである. これを証明せよ.
(ヒント: 問題 6.1 を使う.)

問題 6.3. m を自然数, a, b, c, d を整数とし, $a \equiv b \mod m$ かつ $c \equiv d \bmod m$ をみたすと仮定する. 次を示せ.

(1) $a \pm c \equiv b \pm d \mod m$.

(2) $ac \equiv bd \mod m$.

問題 6.4. m, n を自然数, a, b, ℓ を整数とする. 次を示せ.

(1) $m \mid n$ のとき, $a \equiv b \mod n \Longrightarrow a \equiv b \mod m$.

(2) $\ell \neq 0$ のとき, $a \equiv b \mod m \Longleftrightarrow a\ell \equiv b\ell \mod m\ell$.

問題 6.5. m を自然数とし, a, b, c を整数とする. $d := \gcd(c, m)$ とするとき,

$$ac \equiv bc \mod m \text{ ならば, } a \equiv b \mod \frac{m}{d}$$

が成り立つことを示せ. とくに $\gcd(c, m) = 1$ のときは $a \equiv b \mod m$ となるから, c で割り算して良い.
(ヒント: 問題 **3.3** を使う.)

問題 6.6. a を整数, m を自然数とする. a の法 m に関する逆元 (**講義プリントの定義 5.4**) は存在すればただ 1 つであることを示せ.

問題 6.7. 次の整数 a の法 m に関する逆元は存在するか? 存在する場合それを求めよ.
(1) $a = 10$, $m = 13$　(2) $a = 18$, $m = 57$　(3) $a = 35$, $m = 109$

問題 6.8. 法 m に関する逆元を使って次の合同式を解け.
(1) $4x \equiv 1 \bmod 15$　(2) $8x \equiv 3 \bmod 9$

問題 6.9. n を自然数とする. 合同式の計算を使って次を示せ.
(1) $39 \mid (53^{103} + 103^{53})$.　(2) $7 \mid (5^{2n} + 3 \cdot 2^{5n-2})$.

問題 6.10. (チャレンジ問題)　6 桁の自然数 a が 7 で割り切れるならば, a の最下位の数を最上位に持っていって出来た数も 7 で割り切れることを示せ.
(ヒント: $1001 = 7 \cdot 11 \cdot 13$ に注意. a の上 5 桁を x, 下 1 桁を y とすると, $a = 10x + y$ と書ける. そのとき a の最下位の数を最上位に持っていって出来た数は, $b = y \times 10^5 + x$ となる. $10b \bmod 7$ を考えよ.)

問題 6.11. 自然数 n について合同式 $n \equiv 3 \mod 4$ が成り立つなら, n を割り切る素数 p で $p \equiv 3 \mod 4$ をみたすものが存在することを示せ.

問題 6.12. (チャレンジ問題)　初項が 5 で公差が 6 の等差数列

$$5,\ 11,\ 17,\ 23,\ 29,\ 35,\ 41,\ 47,\ 53, \ldots$$

の中には素数が無限個含まれることを証明せよ.
(ヒント: $6n+5$ ($n \geq 0$) の形の素数は有限個しかないと仮定し, それらを $p_0 := 5, p_1, p_2, \ldots, p_r$ とする. そのとき自然数 $6p_1p_2\cdots p_r + 5$ を考え矛盾を導く. 5 以上の素数は $6n+1$ の形か, $6n+5$ の形に限ることに注意する.)

問題 6.13. 自然数 a, b について

$$\gcd(2^a - 1,\ 2^b - 1) = 2^{\gcd(a,b)} - 1$$

が成り立つことを証明せよ.

問題 6.14. 平方数は 3 を法としてどんな合同式をみたすか答えよ. さらに 11 を法とする場合についても答えよ.

問題 6.15. d は $d \equiv 1 \mod 4$ をみたす平方 (数) でない自然数, a は $2 \parallel a$ をみたす 0 でない整数とする. すなわち, d を 4 で割ったときの余りは 1 で, $2 \mid a$ かつ $2^2 \nmid a$ をみたすとする. このとき Pell 方程式 $x^2 - dy^2 = a$ は整数解をもたないことを証明せよ.
(ヒント: mod 4 で考える.)

問題 6.16. (チャレンジ問題)　$m = 8n+7$ ($n \geq 0$) の形の自然数は 3 つの平方数の和に書けないことを示せ.
(ヒント: mod 8 で考えて命題 6.1 を使う. すべての自然数は 4 つの平方数の和として表せることが知られている (Lagrange の定理).)

問題 6.17. 整数 n は $n \equiv 3 \mod 4$ をみたすと仮定する. このとき, 不定方程式 $x^2+y^2 = nz^2$ は整数解をもたないことを示せ.
(ヒント: 命題 6.1 を使う.)

問題 6.18. $x^2 + y^2 = \dfrac{99}{100}$ をみたす有理数 x, y は存在しないことを示せ. つまり中心が $(0,0)$, 半径が $3\sqrt{11}/10$ の円周上には x-座標と y-座標が共に有理数となる点は存在しない.
(ヒント: $99 \equiv 3 \mod 4$. 問題 6.17 を使う.)

問題 6.19. 不定方程式 $x^3 - 7y^3 = 2$ は整数解をもたないことを示せ.
(ヒント: mod 7 で考える.)

問題 6.20. p を素数, $a, b, a_1, \ldots, a_n$ を整数とする. 次を示せ.

(1) $(a+b)^p \equiv a^p + b^p \mod p$.
(ヒント: 問題 5.6 を使う.)

(2) $(a_1 + \cdots + a_n)^p \equiv a_1^p + \cdots + a_n^p \mod p$.

問題 6.21. (チャレンジ問題)　p を素数, k を $0 \leq k \leq p-1$ をみたす整数とする. 次を示せ.

$$\binom{p-1}{k} \equiv (-1)^k \mod p.$$

(ヒント: $p-1 \equiv -1,\ p-2 \equiv -2,\ \ldots,\ p-k \equiv -k \mod p$.)