代数入門演習　NO. 11　　2014. 1.14

11　2 次合同式と平方剰余の理論

11.1　解説編

1 次合同式 $ax \equiv b \mod m\,(a \neq 0)$ はその解法を統一的に述べることができる (**No.9 の定理 9.1**). とくに a と m が互いに素なときは, $a \bmod m$ の逆元を a^{-1} で書くことにすれば $x \equiv a^{-1}b \mod m$ という形で唯 1 つの解を求めることができる. 次に 2 次合同式を考えてみる. 2 次合同式の一般形は $ax^2 + bx + c \equiv 0 \mod m\,(a \neq 0)$ であるが, 平方完成をすると $x^2 \equiv a \mod m$ を考えることが基本となる. 1 次合同式の場合と違ってその解の様子は複雑である.

- $x^2 \equiv 4 \mod 8$ をみたす x は $x \equiv 2, 6 \bmod 8$ の 2 つ.
- $x^2 \equiv 1 \mod 8$ をみたす x は $x \equiv 1, 3, 5, 7 \bmod 8$ の 4 つ.
- $x^2 \equiv 3 \mod 8$ をみたす整数 x は存在しない.

任意の整数を 8 で割ったときの「余り」は 0, ±1, ±2, ±3, 4 となるから, mod 8 でその平方が取り得る値は, 0, 1, 4 となる. これによりわかる. このような状況を記述するために**平方剰余**および**平方剰余記号** (または **Legendre 記号**) というものを導入する.

定義 11.1. p を奇素数, a を p と互いに素な整数とする.

1. 2 次合同式 $x^2 \equiv a \mod p$ が整数解をもつとき a は法 p に関して**平方剰余**である, という. 平方剰余でないときは**平方非剰余**であるという.
2. p と a に対して**平方剰余記号**または **Legendre 記号** $\left(\dfrac{a}{p}\right)$ を次のように定義する:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ は平方剰余,} \\ -1 & a \text{ は平方非剰余.} \end{cases}$$

a が p と互いに素でない場合, すなわち $p \mid a$ のときは $\left(\dfrac{a}{p}\right) = 0$ と定義する. □

平方剰余記号に関しては次の基本性質がある.

命題 11.1. p を奇素数, a, b を p と互いに素な整数とする.

(1) $a \equiv b \mod p$ ならば $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$.

(2) (**講義プリントの補題 12.3**)　$\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$.

(3) (**講義プリントの定理 12.4**)　$\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

(4) (**講義プリントの定理 12.5: 第 1 補充法則**)　$\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

(5) (**講義プリントの定理 12.5: 第 2 補充法則**)　$\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

ある整数が平方剰余であるかを判定するのは意外に面倒である．とくに, 法が大きいときは 2 次合同式の解をやみくもに求めることはもちろん, 上で見たような順次代入していくという方針も気が遠くなる．この基本性質をうまく使うことでその効率を上げることができる．つまり, 命題 11.1 の性質 (1) から a を p より小さい自然数にすることができ, 命題 11.1 の性質 (2) から素因数分解を考えて各素因子ごとに平方剰余かどうかを判定すればよいことがわかる．そのような状況では次の定理が有効となる．

定理 11.2. (**講義プリントの定理 12.5: 平方剰余の相互法則**)　p と q を相異なる奇素数とするとき次が成立する．

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

相互法則は p と q の差が大きいときなどは強力な道具となる．理論的な観点からも, p を法とする既約剰余類群 $(\mathbb{Z}/p\mathbb{Z})^\times$ と q を法とする既約剰余類群 $(\mathbb{Z}/q\mathbb{Z})^\times$ という全く異なる世界をつなぐという意味でこの「相互法則」はとても美しい定理である．なお, Euler, Legendre が予想した定理 11.2 は Gauss(1801) により初めて証明され, 現在では 200 種類を超える証明が知られている．平方剰余の相互法則の背後には巨大な理論 (類体論) が存在し, この定理は整数論の王道を築いて来た．幾通りもの証明がある理由の 1 つは, このような歴史的背景から来るのだろう．

問題.　$x^2 \equiv 203 \bmod 47$ をみたす整数 x は存在するか?

[解答例]　$203 \equiv 15 \bmod 47$ だから, 元の 2 次合同式は $x^2 \equiv 15 \bmod 47$ と同値．素因数分解 $15 = 3\cdot 5$ と**命題 11.1(2)** により, $\left(\frac{15}{47}\right) = \left(\frac{3}{47}\right)\left(\frac{5}{47}\right)$．**定理 11.2** により

$$\left(\frac{3}{47}\right)\left(\frac{47}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{47-1}{2}} = (-1)^{1\cdot 23} = -1,$$
$$\left(\frac{5}{47}\right)\left(\frac{47}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{47-1}{2}} = (-1)^{2\cdot 23} = 1$$

だから, 平方剰余記号の値は ± 1 を取ることに注意して,

$$\left(\frac{3}{47}\right) = -\left(\frac{47}{3}\right), \qquad \left(\frac{5}{47}\right) = \left(\frac{47}{5}\right)$$

を得る．**命題 11.1(1)** と $(\pm 1)^2 \equiv 1 \mod 3$ により, $\left(\frac{47}{3}\right) = \left(\frac{2}{3}\right) = -1$．**命題 11.1(1)** と $(\pm 1)^2 \equiv 1, (\pm 2)^2 \equiv 4 \mod 5$ により, $\left(\frac{47}{5}\right) = \left(\frac{2}{5}\right) = -1$．したがって,

$$\left(\frac{3}{47}\right) = 1, \qquad \left(\frac{5}{47}\right) = -1.$$

ゆえに,

$$\left(\frac{15}{47}\right) = 1\cdot(-1) = -1.$$

よって $x^2 \equiv 203 \bmod 47$ をみたす整数 x は存在しない．　□

最後に, 平方剰余の理論の簡単な応用として No.6 で述べた Pell 方程式 $x^2 - dy^2 = -1$ の整数解を調べる．d を平方 (数) でない自然数とする．**命題 6.2** により, $x^2 - dy^2 = -1$ が整数解をもつならば, d は奇数か, または $2 \parallel d$ となる．さらに次の命題 11.3 により, $x^2 - dy^2 = -1$ が整数解をもつならば, d のすべての素因数 $p \neq 2$ は $\bmod 4$ で 1 と合同になる．

命題 11.3. d は mod 4 で 3 と合同な素因数をもつと仮定する．このとき Pell 方程式 $x^2 - dy^2 = -1$ は整数解をもたない．

[証明] $x^2 - dy^2 = -1$ をみたす整数 x, y が存在すると仮定して矛盾を導く．仮定により，$p \mid d$ かつ $p \equiv 3 \mod 4$ をみたす素数 p が存在する．$p \mid d$ により，等式 $x^2 - dy^2 = -1$ から $x^2 \equiv -1 \mod p$ がわかる．よって，$\left(\dfrac{-1}{p}\right) = 1$．一方，第 1 補充法則 (命題 11.1 (4)) により，

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1. \quad (\because p \equiv 3 \mod 4)$$

このように矛盾を得る． □

11.2 問題編

問題 11.1. a を奇数とする．次のことを確かめよ: $x^2 \equiv a \mod 2$ の整数解は存在し，それは唯 1 つである．また，$x^2 \equiv a \mod 4$ が整数解をもつための必要十分条件は，$a \equiv 1 \mod 4$．解が存在するときは，その個数は 2.

問題 11.2. 次の値を定義にしたがって求めよ．
(1) $\left(\dfrac{-1}{7}\right)$ (2) $\left(\dfrac{3}{11}\right)$

問題 11.3. 次の値を求めよ．
(1) $\left(\dfrac{5}{37}\right)$ (2) $\left(\dfrac{21}{23}\right)$ (3) $\left(\dfrac{35}{41}\right)$

問題 11.4. 次の合同式をみたす整数 x は存在するか?
(1) $x^2 + 100 \equiv 0 \mod 41$.
(2) $3x^2 + 5x + 1 \equiv 0 \mod 7$.
(3) $\begin{cases} x^2 + 3 \equiv 0 \mod 143, \\ x \equiv 0 \mod 12. \end{cases}$

問題 11.5. p を奇素数とする．mod p の平方剰余，非剰余はそれぞれ $(p-1)/2$ 個ずつあることを証明せよ．
(ヒント: **講義プリントの補題 12.2**.)

問題 11.6. p を奇素数とする．等式 $\displaystyle\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$ を証明せよ．

問題 11.7. p を 2 でも 3 でもない素数とするとき次の (1) と (2) は同値であることを示せ．

(1) ある整数 x が存在して $x^2 - 3$ は p で割り切れる．

(2) $p \equiv \pm 1 \mod 12$.