平方剰余の相互法則と
2次(または3次)合同方程式の解について

青山学院大学 理工学部 物理・数理学科

小野 駿輝 学籍番号:15118029

西山研究室

2023年2月20日

目 次

1 序論

1.1 背景

私が本研究を行った動機は，初等整数論に興味を持っておりその初等整数論の華とも言える平方剰余の相互法則について学んだ際に，さらに深く学びたいと思ったからである．

1775 年にオイラーがゴールドバッハ宛の手紙で $x^2 + Ny^2$ の形の整数を割る素数 p を求める問題について書いたのが始まりである．オイラーは実験的にいくつかの結果を得たが，それを現在使われる平方剰余の相互法則の形に定式化して証明したのがガウスである．

平方剰余の相互法則を使うことによって 2 次合同方程式に解が存在するかどうかの判定が簡単に出来ることを小林昭七先生の教科書『なっとくするオイラーとフェルマー』[小林] によって学んだ．2 次合同方程式に解が存在しないことがある．2 次合同方程式の解の判定方法がわかった為，次は解が存在する 2 次合同方程式の個数について研究し結果を得た．さらに 2 次合同方程式について学んでいる中で 3 次合同方程式についても興味を持ち始めた．平方剰余と 2 次合同方程式についての文献やサイトは数多く存在しているが，立法剰余と 3 次合同方程式についてのものは少ない．そこで卒業研究で行った議論や結果，またその証明をここに報告する．

1.2 主結果

本論文で得られた主な結果を述べる．このうち (1),(2) は [小林] によって学んだことの報告である．(3),(4) については自分で工夫して研究を行った．

(1) p を奇素数とするとき 2 次合同方程式

$$ax^2 + bx + c \equiv 0 \pmod{p} \quad (a, b, c \in \mathbb{Z}, \quad a \not\equiv 0 \pmod{p})$$

が解を持つための必要十分条件は，判別式 $D = b^2 - 4ac$ が p を法として平方剰余になることである．(定理 3.11)

(2) $\sharp\{$ 解を持つ 2 次合同方程式 $\quad x^2 + bx + c = 0\} = \dfrac{p(p+1)}{2}$

$\sharp\{$ 解を持たない 2 次合同方程式 $\quad x^2 + bx + c = 0\} = \dfrac{p(p-1)}{2}$

ただし方程式は有限体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ で考えた．(定理 3.14)

(3) 3 次合同方程式

$$x^3 + bx + c \equiv 0 \pmod{p} \quad (b, c \in \mathbb{Z})$$

が解を持つ十分条件は

判別式 $D = 81c^2 + 12b^3$ が p を法として平方剰余かつ $t_{\pm} = \dfrac{c}{2} \pm \dfrac{\sqrt{D}}{18}$ が p を法として立法剰余になることである．(必要条件であることの証明は出来なかった．)（定理 4.4）

(4) $\sharp\{$ 解を持つ 3 次合同方程式　$x^3+ax^2+bx+c\} = \dfrac{p(2p^2+1)}{3}$

$\sharp\{$ 解を持たない 3 次合同方程式　$x^3+ax^2+bx+c\} = \dfrac{p(p^2-1)}{3}$

ただし方程式は有限体 $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ で考えた.（定理 4.4）

1.3　本論文の構成

環とイデアルについて知っておくことで平方剰余が理解しやすくなるので，§2 では整数環とイデアルについて述べる．§3 では，まず平方剰余を定義し，その性質と相互法則を紹介する．次に 2 次合同方程式の解の存在について調べ実際に計算する．また解が存在する 2 次合同方程式の個数を述べる．§4 では §3 と同様にまず立法剰余を定義し，その性質を紹介する．次に 3 次合同方程式の解の存在について調べ，実際に計算する．そして解が存在する 3 次合同方程式の個数を述べる．最後に §5 では研究結果のまとめと今後の課題について述べる．

2　整数環とイデアル

飯高茂先生の『環論，これはおもしろい -素因数分解と循環小数への応用-』[飯高] を参考に環とイデアルについて述べる．

以下 R は集合とする．

2.1　整数環

定義 2.1 (環)**.** R が**環**であるとは，2 種類の演算加法と乗法が定義されていて，以下 7 つの条件を満たす時にいう．

(1) 加法の結合律:　$(a+b)+c = a+(b+c) \quad (a,b,c \in R)$

(2) 加法の単位元: $\exists z \in R$ が存在して, $a+z = z+a = a \quad (a \in R)$ を満たす．以下 z を 0 と書く．

(3) 加法の逆元: $a \in R$ に対して $\exists b \in R$ が存在して，$a+b = b+a = 0$ を満たす．

(4) 加法の可換律:　$a+b = b+a \quad (a,b \in R)$

(5) 乗法の結合律:　$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad (a,b,c \in R)$

(6) 乗法の単位元: $\exists u \in R$ が存在して，$a \cdot u = u \cdot a = a \quad (a \in R)$ を満たす．以下 u を 1 と書く．

(7) 分配法則:　$a \cdot (b+c) = (a \cdot b) + (a \cdot c), (a+b) \cdot c = (a \cdot c) + (a \cdot b) \quad (a,b,c \in R)$

さらに乗法の可換律:　$ab = ba \quad (a, b \in R)$ を満たすとき**可換環**という.

定義 2.2 (単元). R を環とする.
$x \in R$ が**単元**とは, $xx^{-1} = x^{-1}x = 1$ となる乗法の逆元　x^{-1}　が存在する時に言う.

定義 2.3 (整域). R を環とする. $a, b \in R$ に対して,

$$ab = 0 \quad \text{ならば} \quad a = 0 \quad \text{または} \quad b = 0$$

の時, R を**整域**と言う.

定義 2.4 (既約元). R を整域とする. $a, b, c \in R\,(a \neq 0)$ に対して,
$a = bc$　(b または c が単元)　の時 a を**既約元**と言う.
$a = bc$　(b, c がともに非単元)　の時 a を**可約元**と言う.

2.2　イデアル

定義 2.5 (イデアル). R を環,　$P \subseteq R$ とする.
P が次の三つの条件を満たすとき, P は R の**イデアル**であるという.

(1) $P \neq \emptyset$

(2) $\alpha, \beta \in P \quad$ ならば $\quad \alpha + \beta \in P$

(3) $r \in R, \alpha \in P \quad$ ならば $\quad r\alpha \in P$

一般にイデアル P を (P) と書く.

定義 2.6 (素イデアル). R を環, (P) を R のイデアルとする.
$a, b \in R$ に対して,

$$ab \in (P) \quad \text{ならば} \quad a \in (P) \quad \text{または} \quad b \in (P)$$

の時, (P) を**素イデアル**と言う.

定義 2.7 (素元). R を整域とする. 非単元 $p \in R$ に対して,

$$ab \in (P) \quad \text{ならば} \quad a \in (P) \quad \text{または} \quad b \in (P)$$

の時, p を**素元**という.

定義 2.8 (一意分解整域). R を整域, $a \in R$ を 0 でない非単元, $a_1, a_2, \ldots, a_n$ を素元とする.

$$a = a_1 a_2 \cdots a_n$$

と素元の積で分解できる時 R を**一意分解整域**または**素元分解整域**と言い, **UFD** と書く.

3　平方剰余と相互法則

平方剰余とその相互法則について，[小林] を参考に述べる．

以下 p を奇素数　$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ を標数 p の有限体 (素体) とする．

3.1　平方剰余

例えば $p = 7$ のとき，通常の意味では 2 は平方数ではないが，$4^2 = 16 \equiv 2 \pmod 7$ と考えると，2 は平方 4^2 と 7 を法として合同である．このようなときに 2 を 7 を法とする**平方剰余**という．もっと一般的に次のように定義する．

定義 3.1 (平方剰余)**.** $a \in \mathbb{Z}$ が p を法として**平方剰余**とは $\exists x \in \mathbb{Z}$ が存在して $x^2 \equiv a \pmod p$ を満たすときに言う．a が平方剰余でないとき**平方非剰余**という．

例 3.2. $p = 5$ を法とする平方剰余を調べる．$x = 0, 1, 2, 3, 4$ に対してその平方 $x^2 \pmod 5$ を計算してみると，$1^2 = 1$, $2^2 = 4$, $3^2 = 9 \equiv 4$, $4^2 = 16 \equiv 1$ より 5 を法として平方になっているのは $a = 1, 4$ しかない．したがって 5 を法とする平方剰余は $0, 1, 4$ だけである．$2, 3$ は平方非剰余である．

定理 3.3 (平方剰余の個数)**.** $p = 2s + 1\,(s \in \mathbb{N})$ を奇素数とする．

(1) 法 p の平方剰余の全体は $\{1^2, 2^2, 3^3, \ldots, s^2\} \pmod p$ に一致する．

(2) ${\mathbb{F}_p}^\times$ の中で平方剰余の元の個数は $s = \dfrac{p-1}{2}$ である．

証明. $2s + 1 \equiv 0$ より

$$s + 1 \equiv -s,\ \ s + 2 \equiv -(s-1),\ \ s + 3 \equiv -(s-2),\ \ldots,\ 2s \equiv -1$$

となるので，平方剰余として $1^2, 2^2, 3^2, \ldots, s^2$ を p で割った余りだけを考えればよい．

そこで $1^2, 2^2, 3^2, \ldots, s^2$ を p で割った余りが全て相異なることを背理法で証明する．

$$\exists m, n \in \mathbb{N} \text{ s.t. } 1 \le m < n \le s, m^2 \equiv n^2 \pmod p$$

と仮定する．$n^2 - m^2 \equiv (n-m)(n+m) \equiv 0 \pmod p$ より $n - m, n + m$ の少なくとも一方は p で割り切れる．$1 \le m < n \le s$ から $0 < n - m \le s$ より $2 \le 2m < n + m \le 2s$．したがって

$$n - m \not\equiv 0 \pmod p \quad \text{かつ} \quad n + m \not\equiv 0 \pmod p$$

より矛盾．　■

例 3.4. $p = 13$ を法とする平方剰余を調べる．
$s = 6$ より $x = 1, 2, 3, 4, 5, 6$ の 2 乗を p で割った余りを計算すればよい．

$$1^2 = 1,\ 2^2 = 4,\ 3^2 = 9,\ 4^2 = 16 \equiv 3,\ 5^2 = 25 \equiv 12,\ 6^2 = 36 \equiv 10$$

より $\{1, 3, 4, 9, 10, 12\}$ が平方剰余となる．したがって 13 を法とする平方剰余は $s = 6$ 個存在する．

定理 3.5. $p = 2s + 1\,(s \in \mathbb{N})$ を奇素数とする．

(1) 1 は常に平方剰余である

(2) $a, b \in \mathbb{F}_p$ が共に平方剰余ならば，積 ab も平方剰余である．

(3) $a \in \mathbb{F}_p^{\times}$ が平方剰余ならば，$\exists b \in \mathbb{F}_p^{\times}$ (b は p を法として平方剰余) がただ 1 つ存在して $ab = 1$ を満たす．(平方剰余の逆元はまた平方剰余である．)

証明. (1) $1^2 = 1$ より明らか．

(2) a, b が平方剰余より $\exists \alpha, \beta \in \mathbb{F}_p$ s.t. $(a = \alpha^2) \wedge (b = \beta^2)$ より $ab = (\alpha\beta)^2$ も平方剰余である．

(3) p が奇素数である．そこで $a \not\equiv 0$ ならばフェルマーの小定理 $(a^{p-1} \equiv 1 \pmod{p})$ より
$a \times a^{p-2} = a^{p-1} \equiv 1$　　$a = \alpha^2$ であるから $b = a^{p-2}$ とおくと $b = (\alpha^2)^{p-2} = (\alpha^{p-2})^2$
ただ一つであることは逆元の一意性より明らか．

■

定理 3.6 (平方剰余による因数分解)． $p = 2s + 1\,(s \in \mathbb{N})$ とする．p を法とする相異なる平方剰余を $a_1, a_2, a_3, ..., a_s$ とすると

$$x^{s-1} \equiv (x - a_1)(x - a_2)...(x - a_s) \pmod{p}$$

証明. $f(x) = x^s - 1$ とおいて，　$a_i\,(1 \leq i \leq s)$ を p を法とする平方剰余とする．

$$\exists \alpha_i \text{ s.t. } a_i \equiv \alpha_i^2 \pmod{p}$$
$$\therefore\ f(a_i) = a_i^s - 1 \equiv \alpha_i^{2s} - 1 \equiv \alpha_i^{p-1} - 1 \equiv 0 \pmod{p}$$

$f(x)$ を $(x - a_1)$ で割った商を $f_1(x)$，　余りを c_1 とすると
$f(x) = f_1(x)(x - a_1) + c_1$ であるが $x = a_1$ の時 $f(a_1) = c_1$
一方で $f(a_1) \equiv 0 \pmod{p}$ より $c_1 \equiv 0 \pmod{p}$ よって

$$f(x) = f_1(x)(x - a_1)$$

と書き直せる．

次に $x = a_2$ の時

$$f(a_2) = f_1(a_2)(a_2 - a_1) \equiv 0 \pmod{p}$$

$a_2 - a_1 \not\equiv 0 \pmod{p}$ よって $f_1(a_2) \equiv 0 \pmod{p}$ である

上記と同様に考えると

$$f_1(x) \equiv f_2(x)(x - a_2) \pmod{p}$$

と書き直せる. これより

$$f(x) = f_2(x)(x - a_2)(x - a_1)$$

次に $x = a_3$ とおき同様の議論を繰り返せばよい. ■

定理 3.7 (平方剰余の判別). $p = 2s + 1 (s \in \mathbb{N})$ を奇素数よして有限体 $\mathbb{F}_p$ で考える.

(1) $a \in \mathbb{F}_p^\times$ が平方ならば $a^s = 1$ である.

(2) $a \in \mathbb{F}_p^\times$ が平方でなければ $a^s = -1$ である.

証明. フェルマーの小定理より

$$a^{p-1} = a^{2s} = (a^s - 1)(a^s + 1) = 0$$

だから $a^s = 1$ または $a^s = -1$

定理 3.6 より $x^s \equiv 1 \pmod{p}$ の解は s 個存在しそれらは平方剰余である. ■

定理 3.8 (平方剰余の積). $a, b \in \mathbb{F}_p$ とする.

(1) a, b が共に平方剰余又は共に平方非剰余ならば積 ab は平方剰余である.

(2) a, b の一方が平方剰余, 他方が平方非剰余ならば積 ab は平方非剰余である.

証明. 定理 3.7 より明らか. ■

3.2 相互法則

一般にある数 a が平方剰余であるかどうかを何も知らずに判定するのは，むつかしいことが多い．簡単に判定する方法の一つが，ガウスが発見した平方剰余の相互法則である．それを紹介しよう.

定義 3.9 (ルジャンドル記号). 素数 p と $a \in \mathbb{Z}$ に対して

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \exists x \in \mathbb{Z} \text{ s.t. } x^2 \equiv a \pmod{p} \\ 0 & a \equiv 0 \pmod{p} \\ -1 & \nexists x \in \mathbb{Z} \text{ s.t. } x^2 \equiv a \pmod{p} \end{cases}$$

と定義して，この記号を**ルジャンドル記号**と呼ぶ.

定理 3.10 (平方剰余の相互法則: ガウス)**.** q を p と相異なる奇素数とする． 次の 3 つの関係式が成り立つ.

(1) 相互法則: $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

(2) 第一補充法則: $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(3) 第二補充法則: $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

証明. 小林昭七先生の『なっとくするオイラーとフェルマー』の p190 を参照して下さい． ■

3.3 2 次合同方程式の解の存在

目的: $ax^2 + bx + c \equiv 0 \pmod{p} \quad (a, b, c \in \mathbb{Z}, \quad a \not\equiv 0 \pmod{p})$ の解の存在を調べる.

p が素数,a と p が互いに素であるから $\mathbb{F}_p$ では a の逆元が存在する．両辺に a の逆元を掛けた 2 次合同方程式を改めて

$$x^2 + bx + c \equiv 0 \pmod{p}$$

とおいてこの方程式について調べる.

(I) 2 次方程式の解は

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

であるが，$\mathbb{F}_p$ では 2 の逆元が存在するから, $\frac{1}{2}$ は $\mathbb{F}_p$ の元で表すことが出来る.

(II) よって平方根 $x = \sqrt{b^2 - 4c}$ が存在すること，つまり $D \equiv b^2 - 4c \pmod{p}$ が平方剰余かどうか調べれば良い.

これをまとめると次の定理を得る.

定理 3.11. 二次合同方程式

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

が解を持つための必要十分条件は，判別式 $D = b^2 - 4ac$ が p を法として平方剰余になることである.

例 3.12.

$$p = 17, \quad x^2 + 13x + 10 \equiv 0 \pmod{17}$$

に解が存在するかどうか判定するために D が平方剰余かどうか調べる.

解の公式より $x = \dfrac{-13 \pm \sqrt{13^2 - 4 \cdot 10}}{2}$ である.

次に判別式を調べると，$= D = 13^2 - 4 \cdot 10 \equiv (-4)^2 + 4 \cdot 7 \equiv 10 \pmod{17}$

$\left(\frac{10}{17}\right) = \left(\frac{-7}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{7}{17}\right)$

第一補充法則を使うと　$\left(\frac{-1}{17}\right) = (-1)^{\frac{17-1}{2}} = 1$ となる．

さらに相互法則を使うと　$\left(\frac{7}{17}\right) = \left(\frac{17}{7}\right)(-1)^{\frac{17-1}{2}\cdot\frac{7-1}{2}} = \left(\frac{3}{7}\right) = -1$ と計算できる．

まとめると $\left(\frac{10}{17}\right) = 1 \cdot -1 = -1$.

したがって D は平方非剰余なのでこの 2 次合同方程式に解はない.

例 3.13.

$$p = 17, \quad x^2 + 3x + 11 \equiv 0 \pmod{17}$$

に解が存在するかどうか判定する．

同様に判別式を計算すると $D \equiv -1 \pmod{17}$ となり例 3.12 より $\left(\frac{-1}{17}\right) = 1$

したがって D は平方剰余なのでこの 2 次合同方程式に解が存在する．$(x = 5, 9)$

3.4　解を持つ 2 次合同方程式の個数の決定

定理 3.14 (解を持つ 2 次合同方程式の個数). 2 次合同方程式を $\mathbb{F}_p$ 上の 2 次方程式と考えたとき，解が存在する 2 次方程式と解が存在しない 2 次方程式の個数はそれぞれ以下のように表せる．

(1) $\sharp\{$ 解を持つ 2 次合同方程式　$x^2 + bx + c = 0\} = \dfrac{p(p+1)}{2}$

(2) $\sharp\{$ 解を持たない 2 次合同方程式　$x^2 + bx + c = 0\} = \dfrac{p(p-1)}{2}$ ■

証明. $P(x) = x^2 + bx + c \quad (b, c \in \mathbb{F}_p)$ とおく．まず解を持つ 2 次合同方程式の個数を考える．解が存在することと因数分解出来ることは同値だから，因数分解された式を数える．

(I)　$(x - \alpha)^2 = 0 \quad (\alpha \in \mathbb{F}_p)$ となる α は p 個.

(II)　$(x - \alpha)(x - \beta) = 0 \quad (\alpha, \beta \in \mathbb{F}_p, \alpha \neq \beta)$ となる α, β の組み合わせは $\begin{pmatrix} p \\ 2 \end{pmatrix}$ $= \dfrac{p(p-1)}{2}$ である.

したがって (I) と (II) をあわせると

$$p + \frac{p(p-1)}{2} = \frac{p(p+1)}{2}$$

が解を持つ 2 次方程式の総数である.

次に 2 次方程式の総数を数える．b, c の選び方はそれぞれ p 通りであるから

$$\sharp\{P(x)\} = p^2$$

このことから解を持たない 2 次方程式の個数は

$$p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}$$

である． ■

4 立法剰余

平方剰余を一般化して立法剰余と 3 次合同方程式について述べる．
ここでも p を奇素数，　$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ を標数 p の有限体 (素体) とする．

4.1 立法剰余

定義 4.1 (立法剰余)**.** $a \in \mathbb{Z}$ が p を法として**立法剰余**とは $\exists x \in \mathbb{Z}$ が存在して $x^3 \equiv a \pmod{p}$ を満たすときである．a が立法剰余でないとき**立法非剰余**という．

定義 4.2 (立法剰余のルジャンドル記号)**.** 素数 p と $a \in \mathbb{Z}$ に対して次のように定義する．

$$\left[\frac{a}{p}\right]_3 = \begin{cases} 1 & \exists x \in \mathbb{Z} \text{ s.t. } x^3 \equiv a \pmod{p} \\ 0 & a \equiv 0 \pmod{p} \\ -1 & \nexists x \in \mathbb{Z} \text{ s.t. } x^3 \equiv a \pmod{p} \end{cases}$$

定理 4.3. (立法剰余の個数)

(1) $p \equiv 2 \pmod 3$ のとき任意の $a \in {\mathbb{F}_p}^\times$ に対して　$\left[\frac{a}{p}\right]_3 = 1$
したがって ${\mathbb{F}_p}^\times$ の中の立法剰余の元の個数は ${\mathbb{F}_p}^\times = p - 1$ である．

(2) $p \equiv 1 \pmod 3$ のとき ${\mathbb{F}_p}^\times$ の中の立法剰余の元の個数は $\frac{p-1}{3}$ である．

証明.　(1) 立法写像

$$\begin{array}{rccc} f\colon & \mathbb{F}_p & \to & \mathbb{F}_p \\ & \cup & & \cup \\ & a & \mapsto & a^3 \end{array}$$

が全単射であることを示せばよい．　単射ならば全射であるから単射を示す．
f が単射であることの必要十分条件は

$$m, n \in {\mathbb{F}_p}^\times, f(m) = f(n) \quad \text{ならば} \quad m = n$$

が成り立つことである．そこで　$f(m) = m^3 = n^3 = f(n)$　$(m, n \in \mathbb{F}_p{}^{\times})$ とすると
$0 = m^3 - n^3 = (m-n)(m^2+mn+n^2)$ だから

$m = n$　または　$m^2 + mn + n^2 = 0$ である．
$\dfrac{n}{m} = A$ とおいて，$1 + A + A^2 = 0$ の解の存在を調べる．
定理 3.11 より $D = 1 - 4 = -3$

$\left(\dfrac{-3}{p}\right) = \left(\dfrac{-1}{p}\right)\left(\dfrac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\dfrac{p}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}} = \left(\dfrac{p}{3}\right) =$ となって $p \equiv 2 \pmod 3$ なので $\left(\dfrac{p}{3}\right) = \left(\dfrac{2}{3}\right) = -1$ である．したがって $m = n$

(2) (1) と同様に考えると最後のルジャンドル記号は $p \equiv 1 \pmod 3$ だから $\left(\dfrac{-3}{p}\right) = 1$
$1 + A + A^2 = 0$ の解を λ, μ とすると，$n = m,\ m\lambda,\ m\mu$　の 3 つの解が存在する．
したがって f は 3 : 1 の写像になるので立法剰余は $\dfrac{p-1}{3}$ 個

■

4.2　3 次合同方程式の解の公式

$p = 2, 3$ のときは特殊だから別に考える．ここでは $p \neq 2, 3$ とする．
3 次合同方程式　$(p \neq 2, 3)$

$$x^3 + bx + c \equiv 0 \pmod p \quad (b, c \in \mathbb{Z})$$

を考える. どんな 3 次方程式もこの形に変形出来る.
3 次方程式の公式をまず導く．そのために恒等式

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x^2 + y^2 + z^2 - xy - yz - zx)$$

を利用する．　$-3yz = b,\quad y^3 + z^3 = c$　とおくと

$$x^3 + y^3 + z^3 - 3xyz = x^3 + bx + c$$

なのでこのような y, z が求まると恒等式の右辺に代入して (1 次式) × (2 次式) の因数分解が得られる．　y, z を求めよう.

$$y^3 z^3 = \frac{-b}{3} \qquad y^3 + z^3 = c$$

であることを用いると解と係数の関係より

$$(t - y^3)(t - z^3) = t^2 - ct - \frac{b^3}{27}$$

解の公式より

$$D = 81c^2 + 12b^3 \qquad t_{\pm} = \frac{c}{2} \pm \frac{\sqrt{D}}{18}$$

が y^3, z^3 に一致する．これが立法根を持てば，$y = \sqrt[3]{t_+}, z = \sqrt[3]{t_-}$ とおいて $x + y + z = 0$ に代入すると

$$x = -(\sqrt[3]{t_+} + \sqrt[3]{t_-}) \qquad (\sqrt[3]{t_+} \cdot \sqrt[3]{t_-} = \frac{-b}{3})$$

が得られる．

4.3 3 次合同方程式の解の存在

例として $b = 0$ の時をまず考えてみる．
このときは $x^3 + c \equiv 0 \pmod{p}$ より
$\left[\dfrac{-c}{p}\right]_3 = 1$ ならば解が存在する．

定理 4.4. 3 次合同方程式

$$x^3 + bx + c \equiv 0 \pmod{p} \quad (b, c \in \mathbb{Z})$$

が解を持つ十分条件は
2 次補助方程式の判別式 D が p を法として平方剰余であり，かつ $t_{\pm}$ が p を法として立法剰余になることである．

4.4 解を持つ 3 次合同方程式の個数の決定

例 4.5. $p = 2$ の時，3 次合同方程式の解の存在について調べる．
3 次合同方程式は $x^3 + bx + c \equiv 0 \pmod{2}$ と変形できるので，この 3 次合同方程式に解が存在する b, c の組み合わせとその解は下図のようになる．

b	c	x
0	0	0
1	0	0,1
0	1	1
1	1	×

例 4.6. $p = 3$ の時，3 次合同方程式の解の存在と個数について調べる．
c の値によって場合分けをする．

(1) まず $c = 0$ の時を考える．

任意の a, b に対して $x = 0$ が 3 次合同方程式の解になり，その個数は 9 である．

(2) 次に $c=1$ の時を考える．$x \neq 0$ ならば $x^2 \equiv 1$ であるから $x^3+ax^2+bx+c \equiv x+a+bx+c=(1+b)x+a+1=0$ と変形できる．

$x=1$ が解となる a,b の組み合わせを考える．b を決めると a の値が決まるため 3 通りである．

$x=2$ が解となる場合も同様に考えると 3 通りである．

$x=1,2$ がどちらも解になる a,b の組み合わせは 2 元 1 次方程式

$$\begin{cases} a+b=1 \\ a-b=0 \end{cases}$$

の解であるから，ただ 1 つである．

したがって $c=1$ の時，解が存在する 3 次合同方程式の個数は 5 である．

(3) $c=2$ の時は $c=1$ の時と同様の議論ができるため，3 次合同方程式の個数は 5 である．

したがって $p=3$ の時，解が存在する 3 次合同方程式は 19 個存在し，解が存在しない 3 次合同方程式は 8 個存在する．

定理 4.7 (解を持つ 3 次合同方程式の個数)．$\mathbb{F}_p$ を係数とする 3 次方程式 x^3+ax^2+bx+c に対して，解が存在する 3 次合同方程式と解が存在しない 3 次合同方程式の個数はそれぞれ以下のように表せる．

(1) $\sharp\{$ 解を持つ 3 次合同方程式　$x^3+ax^2+bx+c\} = \dfrac{p(2p^2+1)}{3}$

(2) $\sharp\{$ 解を持たない 3 次合同方程式　$x^3+ax^2+bx+c\} = \dfrac{p(p^2-1)}{3}$ ■

証明.　(1) 解が 3 個存在するものと,1 個のもので場合分けする．

重解を含む 3 次合同方程式の個数は

$$(x-\alpha)^3=0 \quad (\alpha \in \mathbb{F}_p) \quad \text{又は} \quad (x-\alpha)^2(x-\beta)=0 \quad (\alpha,\beta \in \mathbb{F}_p, \alpha \neq \beta)$$

と因数分解出来るものなので p^2 個ある．

異なる 3 つの解を持つ 3 次合同方程式の個数は

$$(x-\alpha)(x-\beta)(x-\gamma)=0 \quad (\alpha,\beta,\gamma \in \mathbb{F}_p, \alpha \neq \beta \neq \gamma)$$

となる α,β,γ の組み合わせである．

まず $\alpha > \beta > \gamma$, $\alpha = n$ の時の組み合わせは $A_n = 0+1+2+3+...+(n-1) = \dfrac{n(n-1)}{2}$

$n=1,2,...p-1$ までの和を計算すればよいから

$$S_n = \sum_{n=1}^{p-1} A_n = \frac{p(p-1)(p-2)}{6}$$

次に解を 1 つしか持たない 3 次合同方程式の個数を考える．

$$(x-\alpha)(x^2+Ax+B)=0 \quad (\alpha \in \mathbb{F}_p, \left(\frac{B^2-4A}{p}\right)=-1)$$

と因数分解出来るものなので

$$p \cdot \frac{p(p-1)}{2} = \frac{p^2(p-1)}{2}$$

したがって解が存在する 3 次合同方程式の個数は

$$p^2 + \frac{p(p-1)(p-2)}{6} + \frac{p^2(p-1)}{2} = \frac{p(2p^2+1)}{3}$$

(2) 解が存在しない 3 次合同方程式の個数を考える．$Q(x)=x^3+ax^2+bx+c \quad (a,b,c \in \mathbb{F}_p)$ とおくと a,b,c の選び方はそれぞれ p 通りであるから方程式の総数は

$$\sharp\{Q(x)\}=p^3$$

なので解が存在しない 3 次合同方程式の個数は

$$p^3 - \frac{p(2p^2+1)}{3} = \frac{p(p^2-1)}{3}$$

である．

■

5 将来の課題

5.1 将来の課題

(1) p が合成数の場合の合同方程式について，解の存在の判定を行う．
(中国式剰余定理を上手く使う必要があると思われる．)

(2) 4 次，5 次，…，n 次合同方程式に解が存在するかの判定方法と解が存在する方程式の個数について調べる．

(3) 定理 4.3 で得られた 3 次合同方程式の解の存在は必要十分条件になっているか調べる．

6 謝辞

1 年間ご指導して下さった西山先生に御礼申し上げます．私の数学力を上げて下さったり，研究のヒントを何度もくださったこと，感謝いたします．また，卒業研究発表の場で 4.3 が必要十分条件であるかどうかを質問して下さった谷口健二先生と，将来の課題 (2) の 5 次以上の合同方程式の場合は解の公式が存在しないので，別の方法を試すのか質問して下さった川崎盛道先生にも感謝いたします．

7　参考文献

参考文献

[小林] 小林昭七『なっとくするオイラーとフェルマー』講談社，2003.

[飯高] 飯高茂『環論，これはおもしろい –素因数分解と循環小数への応用–』共立出版，2013.