

科学・技術の世界 – Fermat の大定理を巡って –

第12回 平成17年7月5日(火)

先週の復習 (1/5)

- Fermat の大定理には Case I と Case II がある.
- Case I は $x^p + y^p = z^p$ の整数解 x, y, z で x, y, z すべて p で割り切れないものはない, という主張.
- Case II は $x^p + y^p = z^p$ が整数解 x, y, z で x, y, z のうち少なくとも一つは p で割り切れる, というものはないという主張.

先週の復習 (2/5)

- l を奇素数とし, $\zeta = \exp(2\pi i/l)$ とする. $z^l = 1$ である (Euler の公式を使えばわかる).
- 円分整数 $f(\zeta)$ とは

$$a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{l-1}\zeta^{l-1}$$

と定義される複素数.

- 円分整数の和, 積は円分整数を複素数と思ってやれば良い.

先週の復習 (3/5)

- 任意の円分整数が素元への一意分解を持つとする. このとき, 以下のことが証明できる.

補題 1 $x^p + y^p = z^p$ をみたす整数 x, y, z で x, y, z いずれも p で割り切れないものが存在したとする. このとき, 以下が成立する.

$$x \equiv y \pmod{p}$$

- この補題を $x^p + y^p = z^p$ を変形した式 $x^p + (-z)^p = (-y)^p$ に適用することで, 次のこともわかる.

$$x \equiv -z \pmod{p}$$

先週の復習 (4/5)

- よって以下の計算ができる.

$$x^p + y^p = z^p$$

$$x^p + x^p \equiv (-x)^p \pmod{p}$$

$$x + x \equiv -x \pmod{p}$$

$$3x \equiv 0 \pmod{p}$$

二行目から三行目への変形は Fermat の小定理から出ることに注意.

先週の復習 (5/5)

- p は奇素数であり, x は p で割り切れないので,

$$3 \equiv 0 \pmod{p}$$

これは $p = 3$ を意味するが, $x^3 + y^3 = z^3$ をみたす整数解は存在しないことがわかっているので, 矛盾である.

- 以上のように素元への一意分解性を仮定すれば Fermat の Case I は証明できる (Case II はもう少し仮定が必要). が, 一般の円分整数に対して素元分解の一意性は成立しない!

ノルムの計算 (1/11)

ζ を 1 の l 乗根, すなわち $\zeta = \exp(2\pi i/l)$ とおく.
円分整数 $f(\zeta)$ に対してそのノルム $Nf(\zeta)$ は次のように定義される.

$$Nf(\zeta) = f(\zeta)f(\zeta^2) \cdots f(\zeta^{l-1})$$

このノルムに対して $l = 5$ の場合にいくつか計算を試みる.

問題 1 $f(\zeta) = 3\zeta^3 + 4\zeta^2 + 7\zeta + 1$ に対して $Nf(\zeta)$ を求めよ.

ノルムの計算(2/11)

問題の解答を与える前に一つ準備が必要である. ζ および ζ^2 は

$$x^4 + x^3 + x^2 + x + 1 = 0$$

の解である. 上の式を変形して,

$$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0$$

$$\left(x^2 + 2 + \frac{1}{x^2}\right) + \left(x + \frac{1}{x}\right) - 1 = 0$$

$$\left(x + \frac{1}{x}\right)^2 + \left(x + \frac{1}{x}\right) - 1 = 0$$

ノルムの計算 (3/11)

前項の式に ζ および ζ^2 を代入すると,

$$(\zeta + \zeta^{-1})^2 + (\zeta + \zeta^{-1}) - 1 = 0$$

$$(\zeta^2 + \zeta^{-2})^2 + (\zeta^2 + \zeta^{-2}) - 1 = 0$$

これから $\zeta + \zeta^{-1}$ および $\zeta^2 + \zeta^{-2}$ は方程式

$$X^2 + X - 1 = 0$$

の二つの解である.

ノルムの計算 (4/11)

解答.

$$\begin{aligned} Nf(\zeta) &= f(\zeta)f(\zeta^2)f(\zeta^3)f(\zeta^4) \\ &= (f(\zeta) \cdot f(\zeta^4))(f(\zeta^2) \cdot f(\zeta^3)) \end{aligned}$$

と考えると, まず $f(\zeta)f(\zeta^4)$ を計算する.

$f(\zeta) = 3\zeta^3 + 4\zeta^2 + 7\zeta + 1$ なので,

$$\begin{aligned} f(\zeta^4) &= 3\zeta^{12} + 4\zeta^8 + 7\zeta^4 + 1 \\ &= 7\zeta^4 + 4\zeta^3 + 3\zeta^2 + 1 \end{aligned}$$

これから次のような筆算を行う.

ノルムの計算 (5/11)

0	3	4	7	1
7	4	3	0	1
0	3	4	7	1
12	21	3	0	9
28	4	0	12	16
7	0	21	28	49
47	28	28	47	75
19	0	0	19	47

上記の計算から次を得る.

$$f(\zeta)f(\zeta^4) = 19\zeta^4 + 19\zeta + 47$$

ノルムの計算 (6/11)

式

$$f(\zeta)f(\zeta^4) = 19\zeta^4 + 19\zeta + 47$$

で ζ を ζ^2 で取り替えると,

$$f(\zeta^2)f(\zeta^8) = 19(\zeta^2)^4 + 19\zeta^2 + 47$$

$$f(\zeta^2)f(\zeta^3) = 19\zeta^3 + 19\zeta^2 + 47$$

を得る. ここで $X_0 = \zeta + \zeta^4$, $X_1 = \zeta^2 + \zeta^3$ とおき,
 X_0, X_1 を用いて $f(\zeta)f(\zeta^4), f(\zeta^2)f(\zeta^3)$ を書き直すと, 以下のようになる.

$$f(\zeta)f(\zeta^4) = 19X_0 + 47, f(\zeta^2)f(\zeta^3) = 19X_1 + 47$$

ノルムの計算 (7/11)

X_0, X_1 は方程式

$$X^2 + X - 1 = 0$$

の解であったので,

$$\begin{aligned} Nf(\zeta) &= f(\zeta)f(\zeta^4) \cdot f(\zeta^2)f(\zeta^3) \\ &= (19X_0 + 47)(19X_1 + 47) \\ &= 361X_0X_1 + 893(X_0 + X_1) + 2209 \\ &= -361 - 893 + 2209 \\ &= 955 \end{aligned}$$

を得る. 上の式変形で二次方程式の解と係数の関係を使ったことに注意せよ.

ノルムの計算 (8/11)

問題 2 $g(\zeta) = \zeta^4 + \zeta^2 + 1$ のノルム $Ng(\zeta)$ を計算せよ.

解答. 先程と同じように

$$Ng(\zeta) = g(\zeta)g(\zeta^4) \cdot g(\zeta^2)g(\zeta^3)$$

のうち, $g(\zeta)g(\zeta^4)$ をまず計算する.

$$g(\zeta^4) = \zeta^{16} + \zeta^8 + 1 = \zeta + \zeta^3 + 1$$

から次のような筆算をする.

ノルムの計算 (9/11)

$$\begin{array}{rrrrr} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ \hline 1 & 2 & 2 & 1 & 3 \\ -1 & 0 & 0 & -1 & 1 \end{array}$$

上の計算から

$$g(\zeta)g(\zeta^4) = -\zeta^4 - \zeta + 1$$

を得る.

ノルムの計算(10/11)

$$g(\zeta)g(\zeta^4) = -\zeta^4 - \zeta + 1$$

の ζ を ζ^2 におきかえることで,

$$g(\zeta^2)g(\zeta^8) = -\zeta^8 - \zeta^2 + 1$$

$$g(\zeta^2)g(\zeta^3) = -\zeta^3 - \zeta^2 + 1$$

を得る.

$$X_0 = \zeta + \zeta^4, X_1 = \zeta^2 + \zeta^3$$

とおき, 上の式を書き換えると, 以下のようになる.

$$g(\zeta)g(\zeta^4) = -X_0 + 1, g(\zeta^2)g(\zeta^3) = -X_1 + 1$$

ノルムの計算(11/11)

よって

$$\begin{aligned} Ng(\zeta) &= g(\zeta)g(\zeta^4)g(\zeta^2)g(\zeta^3) \\ &= (-X_0 + 1)(-X_1 + 1) \\ &= X_0X_1 - (X_0 + X_1) + 1 \end{aligned}$$

となるが, X_0, X_1 は方程式

$$X^2 + X - 1 = 0$$

の解なので, 解と係数の関係から

$$Ng(\zeta) = -1 - (-1) + 1 = 1$$

素数 p の因数分解 (1/15)

ここから素数 p を円分整数の積に分解することを考える.

問題 3 $\zeta = \exp(2\pi i/5)$ とする. 11 を $\mathbb{Z}[\zeta]$ の積に分解せよ.

解答. まず次の方程式を解く.

$$x^5 \equiv 1 \pmod{11}.$$

これを満す解で最も絶対値が小さいものは $x = -2$ となる. そこで

$$f(\zeta) = \zeta + 2$$

とおく.

素数 p の因数分解 (2/15)

$f(\zeta)$ のノルムを計算する. 先程と同様にまず $f(\zeta)f(\zeta^4)$ を計算すると,

$$\begin{aligned} f(\zeta)f(\zeta^4) &= (\zeta + 2)(\zeta^4 + 2) \\ &= 1 + 2(\zeta + \zeta^4) + 4 \\ &= 5 + 2(\zeta + \zeta^4) \end{aligned}$$

となる. 上式の ζ に ζ^2 を代入することで,

$$f(\zeta^2)f(\zeta^3) = 5 + 2(\zeta^2 + \zeta^3)$$

を得る.

素数 p の因数分解 (3/15)

$X_0 = \zeta + \zeta^4, X_1 = \zeta^2 + \zeta^3$ とおき, 前項の式を書き換えると,

$$f(\zeta)f(\zeta^4) = 5 + 2X_0, f(\zeta^2)f(\zeta^3) = 5 + 2X_1$$

となる. X_0, X_1 は

$$X^2 + X - 1 = 0$$

の解なので, 解と係数の関係から,

$$X_0 + X_1 = -1, \quad X_0X_1 = -1$$

素数 p の因数分解 (4/15)

よって

$$\begin{aligned} Nf(\zeta) &= (5 + 2X_0)(5 + 2X_1) \\ &= 25 + 10(X_0 + X_1) + 4X_0X_1 \\ &= 25 - 10 - 4 = 11 \end{aligned}$$

左辺をもう一度見直すと,

$$(\zeta + 2)(\zeta^2 + 2)(\zeta^3 + 2)(\zeta^4 + 2) = 11$$

という分解が得られていることがわかる. □

素数 p の因数分解 (5/15)

問題 4 $\zeta = \exp(2\pi i/5)$ とする. 31 を $\mathbb{Z}[\zeta]$ の積に分解せよ.

解答. まず次の方程式を解く.

$$x^5 \equiv 1 \pmod{31}.$$

これを満す解で最も絶対値が小さいものは $x = 2$ となる. そこで

$$f(\zeta) = \zeta - 2$$

とおく.

素数 p の因数分解 (6/15)

$f(\zeta)$ のノルムを計算する. 先程と同様にまず $f(\zeta)f(\zeta^4)$ を計算すると,

$$\begin{aligned} f(\zeta)f(\zeta^4) &= (\zeta - 2)(\zeta^4 - 2) \\ &= 1 - 2(\zeta + \zeta^4) + 4 \\ &= 5 - 2(\zeta + \zeta^4) \end{aligned}$$

となる. 上式の ζ に ζ^2 を代入することで,

$$f(\zeta^2)f(\zeta^3) = 5 - 2(\zeta^2 + \zeta^3)$$

を得る.

素数 p の因数分解 (7/15)

$X_0 = \zeta + \zeta^4, X_1 = \zeta^2 + \zeta^3$ とおき, 前項の式を書き換えると,

$$f(\zeta)f(\zeta^4) = 5 - 2X_0, f(\zeta^2)f(\zeta^3) = 5 - 2X_1$$

となる. X_0, X_1 は

$$X^2 + X - 1 = 0$$

の解なので, 解と係数の関係から,

$$X_0 + X_1 = -1, \quad X_0X_1 = -1$$

素数 p の因数分解 (8/15)

よって

$$\begin{aligned} Nf(\zeta) &= (5 - 2X_0)(5 - 2X_1) \\ &= 25 - 10(X_0 + X_1) + 4X_0X_1 \\ &= 25 + 10 - 4 = 31 \end{aligned}$$

左辺をもう一度見直すと,

$$(\zeta - 2)(\zeta^2 - 2)(\zeta^3 - 2)(\zeta^4 - 2) = 31$$

という分解が得られていることがわかる.

□

素数 p の因数分解 (9/15)

問題 5 $\zeta = \exp(2\pi i/5)$ とする. 41 を $\mathbb{Z}[\zeta]$ の積に分解せよ.

解答. これまでと同様,

$$x^5 \equiv 1 \pmod{41}$$

で絶対値が一番小さいものを取ると $x = -4$ となる. そこで

$$f(\zeta) = \zeta + 4$$

としてノルムを計算すると,

$$Nf(\zeta) = 205$$

となり 41 とはならない.

素数 p の因数分解(10/15)

そこで別の円分整数を取らなければならないが, それは次のようにする. -4 のべき乗を $\equiv \pmod{41}$ で見ると次のようになる.

$$-4, \quad (-4)^2, \quad (-4)^3 \equiv -23, \quad (-4)^4 \equiv 10$$

上の式から

$$(-4)^4 + 2 \cdot (-4) - 2 \equiv 0 \pmod{41}$$

となる. そこで

$$f(\zeta) = \zeta^4 + 2\zeta - 2$$

とおく. $f(\zeta)f(\zeta^4)$ を計算すると,

素数 p の因数分解 (11/15)

$$\begin{array}{rrrrr} 1 & 0 & 0 & 2 & -2 \\ 2 & 0 & 0 & 1 & -2 \\ \hline -2 & 0 & 0 & -4 & 4 \\ 0 & 0 & 2 & -2 & 1 \\ -4 & 2 & 0 & 0 & 4 \\ \hline -6 & 2 & 2 & -6 & 9 \\ -8 & 0 & 0 & -8 & 7 \end{array}$$

より

$$f(\zeta)f(\zeta^4) = -8(\zeta^4 + \zeta) + 7$$

よって ζ に ζ^2 を代入すれば,

$$f(\zeta^2)f(\zeta^3) = -8(\zeta^2 + \zeta^3) + 7$$

素数 p の因数分解 (12/15)

以上から

$$\begin{aligned} Nf(\zeta) &= (-8(\zeta + \zeta^4) + 7)(-8(\zeta^2 + \zeta^3) + 7) \\ &= 64(\zeta + \zeta^4)(\zeta^2 + \zeta^3) \\ &\quad - 56(\zeta + \zeta^4 + \zeta^2 + \zeta^3) + 49 \\ &= 41 \end{aligned}$$

となり, これから 41 の分解

$$41 = (\zeta^4 + 2\zeta - 2)(2\zeta^4 + \zeta - 2)(\zeta^3 + 2\zeta^2 - 2)(2\zeta^3 + \zeta^2 - 2)$$

を得る.

素数 p の因数分解 (13/15)

ここまでやってきた計算の手法をまとめると以下のようになる.

問題 **6** l を奇素数, $\zeta = \exp(2\pi i/l)$ とする. 別の素数 p で $p \equiv 1 \pmod{l}$ なるものを $\mathbb{Z}[\zeta]$ で分解せよ. という問題が与えられたとき,

- $x^l \equiv 1 \pmod{p}$ をみたす絶対値が一番小さい整数 k を見つける.

-

$$\sum_{i=0}^{l-1} a_i k^i \equiv 0 \pmod{p}$$

をみたす整数 $a_i, 0 \leq i \leq l-1$ を取る.

素数 p の因数分解 (14/15)

- 前項で求めた a_i に対して, 円分整数を

$$f(\zeta) = \sum_{i=0}^{l-1} a_i \zeta^i$$

とおく.

- ノルムを計算し,

$$Nf(\zeta) = p$$

となれば終了. そうでない場合は a_i を取り直す.

素数 p の因数分解 (15/15)

- Kummer はこの計算を $l \leq 23, p < 1000$ について行なった. これがどれだけ大変か想像して欲しい.
- すると, 次のようなことがわかった.
命題 **1** $l = 23$ とする. このとき 47 はこの方法では分解できない.
- しかし, この困難から Kummer は「理想数」を考案し, さまざまな整数論の問題へ適用して行くのである.