Fermat の最終定理

alg-d
http://alg-d.com/math/ac/

2013 年 11 月 10 日

目次

1 導入

Fermat の最終定理. $n \geq 3$ のとき，$x^n + y^n = z^n$，$xyz \neq 0$ は有理整数解を持たない.

Fermat の最終定理がスキームだかなんだか難しい概念を駆使して証明されたことは良く知られていて，私もその証明は全く分からないけれども，ある程度特殊な場合であればそれなりの知識で証明ができる．ここではそれを紹介する.

Fermat の最終定理は $n = p \geq 5$ が素数の場合のみ示せば十分である．($n = 3, 4$ の場合の証明はよく知られている．) このとき $p \nmid xyz$ と $p \mid xyz$ の二つの場合に分けられるが，前者を 1st case，後者を 2nd case という．この PDF では 1st case のみを扱う．(2nd case については [1] の Chapter 9 を参照．)

2　使用する事実について

定義. $\zeta_n := \exp\left(\frac{2\pi\sqrt{-1}}{n}\right)$.

定義. $\mathbb{Q}(\zeta_n)^+ := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

命題 1 ([1]Prop. 1.5.)**.** $\mathbb{Q}(\zeta_p)$ の単数 ε に対して，$\mathbb{Q}(\zeta_p)^+$ の単数 ε_1 と $m \in \mathbb{Z}$ が存在して $\varepsilon = \zeta_p^m \varepsilon_1$ と書ける. □

命題 2 ([1]Lem. 1.9.)**.** $\alpha := a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1} \in \mathbb{Z}[\zeta_p]$ として，少なくとも一つの a_i が 0 であるとする．このとき $n \mid \alpha$ ならば各 i について $n \mid a_i$ となる. □

命題 3 ([1]Thm. 4.14.)**.** 自然な写像 $Cl_{\mathbb{Q}(\zeta_n)^+} \longrightarrow Cl_{\mathbb{Q}(\zeta_n)}$ は単射である.

定義. B_n を Taylor 展開 $\dfrac{x}{e^x - 1} = \displaystyle\sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$ により定義する．B_n を Bernoulli 数という.

Bernoulli 数は有理数になることが知られている.

$$\frac{-x}{e^{-x}-1} = \frac{x}{1-e^{-x}} = \frac{xe^x}{e^x-1} = \frac{xe^x - x + x}{e^x - 1} = x + \frac{x}{e^x - 1}$$

により $n > 0$ に対して $B_{2n+1} = 0$ となることが分かる．$B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = -\frac{1}{30}$, $B_{10} = \frac{5}{66}$, $B_{12} = -\frac{691}{2730}$, ... となることが知られている.

命題 4 ([1]Thm. 4.2.)**.** $\zeta(s)$ を Riemann ゼータ関数とするとき，任意の正整数 n に対して $\zeta(1-n) = -\dfrac{B_n}{n}$. □

p を奇素数とする．$\chi\colon (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ を準同型とする．Taylor 展開

$$\sum_{a=1}^{p-1} \frac{\chi(a) x e^{ax}}{e^{px} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{x^n}{n!}$$

により $B_{n,\chi}$ を定める．$\chi = 1$ とすれば，$n \neq 1$ のとき $B_{n,1} = B_n$ である．また $B_{1,1} = 1/2$, $B_1 = -1/2$.

命題 5 ([1]Prop. 4.1.)**.** $B_{1,\chi} = \dfrac{1}{p}\displaystyle\sum_{a=1}^{p-1} \chi(a) a$. □

$a \in \mathbb{Z}$ が $p \nmid a$ を満たすとする．このとき 1 の $p-1$ 乗根 $\omega(a) \in \mathbb{Z}_p$ が一意に存在して $a \equiv \omega(a) \pmod{p}$ となる．これにより準同型 $\omega\colon (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{Z}_p$ が定まる．ω の像は代数的だから，$\omega\colon (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ とみなせる．(埋め込み $\overline{\mathbb{Q}} \longrightarrow \mathbb{C}_p$ を一つ固定しておく．) ω を Teichmüller 指標という．

命題 6 ([1]Cor. 5.15.)**.** n が奇数で $n \not\equiv -1 \pmod{p-1}$ ならば $B_{1,\omega^n} \equiv \dfrac{B_{n+1}}{n+1} \pmod{p}$ で，またこれらは p 進整数である． □

3 Fermat の最終定理

まず，Kummer が証明した次の定理を証明する．

定理 7. 素数 $p \geq 5$ が $p \nmid h_{\mathbb{Q}(\zeta_p)}$ を満たすとき，$x^p + y^p = z^p,\ p \nmid xyz$ は有理整数解を持たない．

証明. 有理整数解が存在すると仮定する．即ち $x, y, z \in \mathbb{Z}$ が存在してとして $x^p + y^p = z^p$, $p \nmid xyz$ となる．$\zeta := \zeta_p$ として $\mathbb{Z}[\zeta]$ で考えると $\displaystyle\prod_{i=0}^{p-1}(x + \zeta^i y) = z^p$ と分解できる．故にイデアルの式として $\displaystyle\prod_{i=0}^{p-1}(x + \zeta^i y) = (z)^p$ が成り立つ．$i \neq j$ に対してイデアル $(x + \zeta^i y)$ と $(x + \zeta^j y)$ は互いに素であることが分かる．故に素イデアル分解の一意性から，あるイデアル $\mathfrak{a}$ を使って $(x + \zeta y) = \mathfrak{a}^p$ と書ける．今 $p \nmid h_{\mathbb{Q}(\zeta)}$ であるから，$\alpha \in \mathbb{Z}[\zeta]$ が存在して $\mathfrak{a} = (\alpha)$ と書ける．従って $(x + \zeta y) = (\alpha)^p = (\alpha^p)$．故にある $\varepsilon \in E_{\mathbb{Q}(\zeta)}$ が存在して $x + \zeta y = \varepsilon\alpha^p$ となる．命題 1 により，ある $\varepsilon_1 \in \mathbb{Q}(\zeta)^+$ と $r \in \mathbb{Z}$ が存在して $\varepsilon = \zeta^r \varepsilon_1$ と書ける．よって $x + \zeta y = \zeta^r \varepsilon_1 \alpha^p$ である．$\alpha = a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1} \quad (a_i \in \mathbb{Z})$ と書けば $\bmod p$ で

$$\alpha^p \equiv a_0^p + a_1^p \zeta_p^p + \cdots + a_{p-1}^p \zeta_p^{p(p-1)} = a_0^p + \cdots + a_{p-1}^p =: a.$$

故に $x + \zeta y = \zeta^r \varepsilon_1 \alpha^p \equiv \zeta^r \varepsilon_1 a$ である．一方複素共役を考えると $x + \zeta^{-1} y = \zeta^{-r} \varepsilon_1 \overline{\alpha}^p \equiv \zeta^{-r} \varepsilon_1 a$ だから

$$\zeta^{-r}(x + \zeta y) \equiv \zeta^r (x + \zeta^{-1} y)$$

即ち

$$x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \equiv 0.$$

今，$1, \zeta, \zeta^{2r-1}, \zeta^{2r}$ が互いに異なると仮定する．つまりこれらは $\mathbb{Q}$ 上一次独立である．

$x+\zeta y-\zeta^{2r}x-\zeta^{2r-1}y=p\beta$ ($\beta\in\mathbb{Z}[\zeta]$) と書く．$\beta=b_0+b_1\zeta+\cdots+b_{p-1}\zeta^{p-1}$ ($b_i\in\mathbb{Z}$) とすれば $x+\zeta y-\zeta^{2r}x-\zeta^{2r-1}y=pb_0+\cdots+pb_{p-1}\zeta^{p-1}$ である．表現の一意性から $p\mid x$ となり $p\nmid xyz$ に矛盾.

故に同じになるペアがある．明らかに $1\neq\zeta$, $\zeta^{2r-1}\neq\zeta^{2r}$ だから起こるのは次の三通り．

(i) $1=\zeta^{2r}$ のとき.

$x+\zeta y-x-\zeta^{-1}y\equiv 0\pmod p$ だから $\zeta y-\zeta^{p-1}y\equiv 0\pmod p$ である．よって先と同様にして $p\mid y$ が導かれ矛盾する.

(ii) $\zeta=\zeta^{2r-1}$ のとき.

$x+\zeta y-\zeta^2x-\zeta y\equiv 0\pmod p$ だから $x-\zeta^2x\equiv 0\pmod p$ である．よって先と同様にして $p\mid x$ が導かれ矛盾する.

(iii) $1=\zeta^{2r-1}$ (このとき $\zeta=\zeta^{2r}$) のとき.

$x+\zeta y-\zeta x-y\equiv 0\pmod p$ だから $(x-y)+\zeta(y-x)\equiv 0\pmod p$ である．よって先と同様にして $x\equiv y\pmod p$ を得る．$x^p+(-z)^p=(-y)^p$ として同様の議論を行うと $x\equiv -z\pmod p$ を得る．よって $x^p+y^p=z^p$ から $x^p+x^p\equiv -x^p\pmod p$，よって $3x^p\equiv 0\pmod p$ を得る．今 $p\geq 5$ だから $p\mid x$ となり，矛盾. □

定義. $p\nmid h_{\mathbb{Q}(\zeta_p)}$ となる素数 p を正則素数という.

つまり，Kummer は「正則素数 p については Fermat の最終定理が成立する」ことを示したことになる．更に，Kummer は素数 p が正則になる為の必要十分条件を与えている.

定理 8. p が正則素数 $\Longleftrightarrow n=2,4,\cdots,p-3$ に対して $p\nmid B_n$.

例えば，$691\mid B_{12}$ であるから 691 は非正則素数である．非正則素数は小さいほうから順に $37,59,67,101,103,131,149,157,233,\cdots$.

Fermat の最終定理が正則素数の場合に解決したので，次は非正則素数について取り組みたいわけであるが，非正則素数についてもある程度は解決できる．前定理による正則素数の性質から，素数の《非正則度》を次のように定めるのは自然であろう.

定義. $i(p):=\#\{0<n<p-1\mid n\text{ は偶数},\ p\mid B_n\}$ を p の index of irregularity という.

このとき，《非正則度》$i(p)$ が十分小さい素数については，Fermat の最終定理 (の 1st case) が証明できるのである (定理 15)．この証明には Herbrand の定理 (定理 13) を使うので，まずそれを示す.

4 Herbrand の定理

$M/\mathbb{Q}$ を有限次アーベル拡大とする．Kronecker-Weber の定理により，ある $m \in \mathbb{N}$ が存在して $M \subset \mathbb{Q}(\zeta_m)$ となる．このような m のうち最小のものを取っておく．$G := \mathrm{Gal}(M/\mathbb{Q})$ は $(\mathbb{Z}/m\mathbb{Z})^\times$ の剰余群とみなせる．$x \in \mathbb{R}$ の小数部分を $\{x\}$ で表す．M の Stickelberger 元を $\theta = \theta(M) := \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \left\{\frac{a}{m}\right\} \sigma_a^{-1} \in \mathbb{Q}[G]$ で定める．$I(M) := \mathbb{Z}[G] \cap \theta\mathbb{Z}[G]$ を Stickelberger イデアルと呼ぶ．

例. $M = \mathbb{Q}(\zeta_m)$ の場合，$J \subset \mathbb{Z}[G]$ を $\{c - \sigma_c \mid (c, m) = 1\}$ で生成されるイデアルとすれば $I(\mathbb{Q}(\zeta_m)) = \theta J$ である． □

$x = \sum_{\sigma \in G} x_\sigma \sigma \in \mathbb{Z}[G]$ のイデアル類群 Cl_M への作用を $A^x := \prod_{\sigma \in G} (A^\sigma)^{x_\sigma}$ で定める．

定理 9 (Stickelberger の定理，[1]Thm. 6.10.)**.** M の Stickelberger イデアルは M のイデアル類群を消す．即ち，M の任意の分数イデアル $\mathfrak{a} \subset M$ と $\beta\theta \in I(M)$ $(\beta \in \mathbb{Z}[G])$ に対して $\mathfrak{a}^{\beta\theta}$ は単項イデアルとなる． □

この定理を認めて，Herbrand の定理を証明する．

G を有限アーベル群とし，$\widehat{G} := \hom(G, \mathbb{C}^\times)$ と置く．$\chi \in \widehat{G}$ に対して $\varepsilon_\chi := \frac{1}{|G|} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1} \in \mathbb{Q}[G]$ と定める．

命題 10. (1) $\varepsilon_\chi \varepsilon_\psi = \begin{cases} \varepsilon_\chi & (\chi = \psi \text{のとき}) \\ 0 & (\chi \neq \psi \text{のとき}) \end{cases}$

(2) $1 = \sum_{\chi \in \widehat{G}} \varepsilon_\chi$

(3) $\varepsilon_\chi \sigma = \chi(\sigma)\varepsilon_\chi$

証明. (1) $\sum_{\sigma \in G} \chi(\sigma) = \begin{cases} |G| & (\chi = 1 \text{ のとき}) \\ 0 & (\chi \neq 1 \text{ のとき}) \end{cases}$ である．

$\because$) $\chi \neq 1$，即ち $\chi(\tau) \neq 1$ なる $\tau \in G$ が存在すれば

$$\chi(\tau) \sum_{\sigma \in G} \chi(\sigma) = \sum_{\sigma \in G} \chi(\tau\sigma) = \sum_{\sigma \in G} \chi(\sigma)$$

により $(\chi(\tau)-1)\sum_{\sigma\in G}\chi(\sigma)=0$, よって $\sum_{\sigma\in G}\chi(\sigma)=0$ である.

故に

$$\begin{aligned}
\varepsilon_\chi\varepsilon_\psi &= \left(\frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1}\right)\left(\frac{1}{|G|}\sum_{\sigma\in G}\psi(\sigma)\sigma^{-1}\right)\\
&= \frac{1}{|G|^2}\sum_{\sigma,\tau\in G}\chi(\sigma)\psi(\tau)\sigma^{-1}\tau^{-1}\\
&= \frac{1}{|G|^2}\sum_{\rho,\tau\in G}\chi(\rho\tau^{-1})\psi(\tau)\rho^{-1}\\
&= \frac{1}{|G|^2}\sum_{\rho,\tau\in G}\chi(\rho)\chi(\tau)^{-1}\psi(\tau)\rho^{-1}\\
&= \frac{1}{|G|^2}\sum_{\rho\in G}\chi(\rho)\rho^{-1}\sum_{\sigma\in G}\chi^{-1}\psi(\tau)\\
&= \frac{1}{|G|}\varepsilon_\chi\sum_{\sigma\in G}\chi^{-1}\psi(\tau)\\
&= \begin{cases}\varepsilon_\chi & (\chi=\psi\text{のとき})\\ 0 & (\chi\neq\psi\text{のとき})\end{cases}.
\end{aligned}$$

(2) $\sum_{\chi\in\widehat{G}}\chi(\sigma)=\begin{cases}|G| & (\sigma=e\text{ のとき})\\ 0 & (\sigma\neq e\text{ のとき})\end{cases}$ である.

$\ddots$) $\sigma\neq e$ のとき $\psi(\sigma)\neq 1$ なる $\psi\in\widehat{G}$ を取れば

$$\psi(\sigma)\sum_{\chi\in\widehat{G}}\chi(\sigma)=\sum_{\chi\in\widehat{G}}\psi\chi(\sigma)=\sum_{\chi\in\widehat{G}}\chi(\sigma)$$

により $(\psi(\sigma)-1)\sum_{\chi\in\widehat{G}}\chi(\sigma)=0$, よって $\sum_{\chi\in\widehat{G}}\chi(\sigma)=0$ である.

よって

$$\begin{aligned}\sum_{\chi\in\widehat{G}}\varepsilon_\chi &= \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1}\\ &= \frac{1}{|G|}\sum_{\sigma\in G}\Big(\sigma^{-1}\sum_{\chi\in\widehat{G}}\chi(\sigma)\Big)\\ &= 1.\end{aligned}$$

(3) $\varepsilon_\chi\sigma = \dfrac{1}{|G|}\displaystyle\sum_{\tau\in G}\chi(\tau)\tau^{-1}\sigma = \frac{1}{|G|}\sum_{\rho\in G}\chi(\sigma\rho)\rho = \chi(\sigma)\varepsilon_\chi$ である． □

命題 11. R を $\{\chi(\sigma)\mid \chi\in\widehat{G},\ \sigma\in G\}\cup\{1/|G|\}\subset R$ となる可換環，M を $R[G]$ 加群とする．$\chi\in\widehat{G}$ に対して $M_\chi := \varepsilon_\chi M$ と置けば $M = \displaystyle\bigoplus_{\chi\in\widehat{G}} M_\chi$.

証明. 命題 10 の 2 より明らかに $M = \displaystyle\sum_{\chi\in\widehat{G}} M_\chi$ である．$m_\chi\in M_\chi$ が $\displaystyle\sum_{\chi\in\widehat{G}} m_\chi = 0$ を満たしたとする．$m_\chi = \varepsilon_\chi a_\chi$ となる a_χ が存在する．このとき $\displaystyle\sum_{\chi\in\widehat{G}}\varepsilon_\chi a_\chi = 0$ だから，任意の $\psi\in\widehat{G}$ を取ると

$$\begin{aligned}0 &= \varepsilon_\psi 0\\ &= \sum_{\chi\in\widehat{G}}\varepsilon_\psi\varepsilon_\chi a_\chi\\ &= \varepsilon_\psi a_\psi\end{aligned}$$

となり $a_\psi = 0$ である，即ち各 $\psi\in\widehat{G}$ に対して $m_\psi = 0$ である． □

p を奇素数とする．$G := \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ として ω を Teichmüller 指標とすれば $\widehat{G} = \{\omega^i \mid 0\le i\le p-2\}$ となる．$\varepsilon_i := \varepsilon_{\omega^i}\in\mathbb{Z}_p[G]$ と書く．また

$$\varepsilon_- := \sum_{2\not| i}\varepsilon_i = \frac{1}{2} - \frac{1}{2}\sigma_{-1},\quad \varepsilon_+ := \sum_{2|i}\varepsilon_i = \frac{1}{2} + \frac{1}{2}\sigma_{-1}$$

と定める．これを使えば $M = M^-\oplus M^+$ と分解する．

$\theta = \displaystyle\sum_{a=1}^{p-1}\frac{a}{p}\sigma_a^{-1}\in\mathbb{Q}[G]$ を Stickelberger 元とすれば，命題 5 を使って

$$\varepsilon_i\theta = \sum_{a=1}^{p-1}\frac{a}{p}\varepsilon_i\sigma_a^{-1} = \frac{1}{p}\sum_{a=1}^{p-1}a\omega^{-i}(a)\varepsilon_i = B_{1,\omega^{-i}}\varepsilon_i$$

となる．よって $(c-\sigma_c)\theta \in I(\mathbb{Q}(\zeta_p))$ $((c,p)=1)$ に対して

$$\varepsilon_i(c-\sigma_c)\theta = (c-\omega^i(c))B_{1,\omega^{-i}}\varepsilon_i$$

である．$A :=$「$\mathbb{Q}(\zeta_p)$ のイデアル類群の p-Sylow 部分群」とする．今 A の演算を加法で表せば，十分大きい n に対して $p^nA = 0$ であるから，$\sum_n x_n p^n \in \mathbb{Z}_p$ と $a \in A$ に対して $\Big(\sum_{n=0}^{\infty} x_n p^n\Big)a := \sum_{n=0}^{\infty}(x_n p^n a)$ が定義できる．この $\mathbb{Z}_p$ の作用と G の作用により A は $\mathbb{Z}_p[G]$ 加群となる．よって前命題により $A_i := \varepsilon_i A$ として $A = \bigoplus_{i=0}^{p-2} A_i$ と分解する．

Stickelberger の定理によれば $(c-\sigma_c)\theta A = 0$，よって各 i について $(c-\sigma_c)\theta A_i = 0$ である．今，$\varepsilon_i(c-\sigma_c)\theta = (c-\omega^i(c))B_{1,\omega^{-i}}\varepsilon_i$ だったから，任意の $\varepsilon_i a \in A_i$ に対して

$$(c-\omega^i(c))B_{1,\omega^{-i}}(\varepsilon_i a) = \varepsilon_i(c-\sigma_c)\theta a = \varepsilon_i 0 = 0.$$

故に $(c-\omega^i(c))B_{1,\omega^{-i}}$ は A_i を消す．

$i \neq 0$ で i が偶数ならば，$B_{1,\omega^{-i}} = 0$ であるからこれは自明である．$i = 0$ のとき，$B_{1,1} = 1/2$ だから $(c-1)/2$ が A_0 を消す，即ち $A_0 = 0$ が分かる．(これは ε_0 の定義からも明らか．) 次に i が奇数の場合．まず $i = 1$ とする．$c = 1+p$ と取れば $\bmod p$ で

$$(c-\omega(c))B_{1,\omega^{-1}} = pB_{1,\omega^{-1}} = \sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv p-1 \not\equiv 0.$$

A_1 は p 群だったから，$A_1 = 0$ が分かった．奇数 $i \neq 1$ のとき，c として p の原始根で $c \not\equiv c^i \equiv \omega^i(c) \pmod p$ となるものを取れば次の定理が得られる．

命題 12. $i = 3, 5, \ldots, p-2$ に対して $B_{1,\omega^{-i}}$ は A_i を消す．

これにより次の定理が分かる．

定理 13 (Herbrand の定理)**.** $i = 3, 5, \ldots, p-2$ に対して，$A_i \neq 0 \Longrightarrow p | B_{p-i}$.

証明. $A_i \neq 0$ とすれば，A_i は p 群だから $p \mid B_{1,\omega^{-i}}$ でなければならない．命題 6 により $B_{1,\omega^{-i}} \equiv \dfrac{B_{p-i}}{p-i} \pmod p$ だから，$p \mid B_{p-i}$ である． □

※ 実は逆も成り立つことが知られている．

定理 14 (Ribet の定理)**.** $i = 3, 5, \ldots, p-2$ に対して，$p | B_{p-i} \Longrightarrow A_i \neq 0$. □

この定理により p-rank$(Cl_{\mathbb{Q}(\zeta_p)}) \geq i(p)$ が分かる．

5 Fermat の最終定理 2

いよいよ次の定理が証明できる．

定理 15. 素数 p が $i(p) < \sqrt{p} - 2$ を満たすならば $x^p + y^p = z^p,\ p \nmid xyz$ は有理整数解を持たない．

証明. $x^p + y^p = z^p$ とする．$\zeta := \zeta_p$ と書く．$i = 0, 1, \ldots, p-1$ に対して $\mathbb{Q}(\zeta)$ のイデアル $\mathfrak{a}_i$ が存在して $(x + \zeta^i y) = \mathfrak{a}_i^p$ と書ける．$C \subset Cl_{\mathbb{Q}(\zeta)}$ を $[\mathfrak{a}_1], \ldots, [\mathfrak{a}_{p-1}]$ で生成される部分群とする．C は $\mathbb{Z}_p[G]$ 加群である．$\sigma_i \mathfrak{a}_1 = \mathfrak{a}_i$ としてよい．よって C は $\mathbb{Z}_p[G]$ 上 $[\mathfrak{a}_1]$ で生成される．$C = \bigoplus_i \varepsilon_i C$ と分解するから，$\varepsilon_i \mathfrak{a}_1$ で生成される部分群を $\langle \varepsilon_i \mathfrak{a}_1 \rangle$ と書けば $C = \bigoplus_i \langle \varepsilon_i \mathfrak{a}_1 \rangle$ である．また $C^- = \bigoplus_{2 \nmid i} \langle \varepsilon_i \mathfrak{a}_1 \rangle$ である．

$$\begin{aligned} p\text{-}\operatorname{rank}(C^-) &= \#\{1 \leq i \leq p-1 \mid 2 \nmid i,\ \varepsilon_i \mathfrak{a}_1 \neq 0\} \\ &\leq \#\{1 \leq i \leq p-1 \mid 2 \nmid i,\ A_i \neq 0\} \end{aligned}$$

であるから, 定理の仮定と Herbrand の定理により $p\text{-}\operatorname{rank}(C^-) \leq i(p) < \sqrt{p} - 2$ となる．$r := [\sqrt{p}] - 1 (> \sqrt{p} - 2)$ として $\mathfrak{a}_1^{b_1} \cdots \mathfrak{a}_r^{b_r}$ $(0 \leq b_i < p)$ を考える．$p^r > p^{p\text{-}\operatorname{rank}(C^-)} = |C^-|$ だから，Dirichlet の抽斗論法により，異なる組 $(b_1, \ldots, b_r)$，$(c_1, \ldots, c_r)$ が存在して $\mathfrak{a}_1^{b_1} \cdots \mathfrak{a}_r^{b_r}$ と $\mathfrak{a}_1^{c_1} \cdots \mathfrak{a}_r^{c_r}$ の C^- 成分が一致するようにできる．このとき $a_i := b_i - c_i$ とすれば $[\mathfrak{a}_1^{a_1} \cdots \mathfrak{a}_r^{a_r}] \in C^+$ である．よってある $\rho \in \mathbb{Q}(\zeta)$ とイデアル $\mathfrak{b}$ が存在して

$$\mathfrak{a}_1^{a_1} \cdots \mathfrak{a}_r^{a_r} = \rho \mathfrak{b}, \quad \mathfrak{b}^{\sigma_{-1}} = \mathfrak{b}$$

とできる．各 $\mathfrak{a}_i$ は p と互いに素だから，ρ と $\mathfrak{b}$ も p と互いに素としてよい．両辺を p 乗して

$$\prod_{i=1}^{r} (x + \zeta^i y)^{a_i} = \rho^p \mathfrak{b}^p$$

となる．故に $\mathbb{Q}(\zeta)$ の中で $\mathfrak{b}^p$ は単項イデアルである．命題 3 により，$\mathbb{Q}(\zeta)^+$ の中で $\mathfrak{b}^p$ が単項イデアルとなることが分かる．$\mathfrak{b}^p = (\alpha)$，$\alpha \in \mathbb{Q}(\zeta)^+$ と書く．

$$\prod_{i=1}^{r} (x + \zeta^i y)^{a_i} = (\rho^p \alpha)$$

であるが，$\mathbb{Q}(\zeta)$ の単数は $\zeta^m\varepsilon$ ($m \in \mathbb{Z}$, ε は実単数) と書ける (命題 1) ので

$$\prod_{i=1}^{r}(x+\zeta^i y)^{a_i} = \zeta^m \varepsilon \rho^p \alpha$$

と書ける．複素共役を取れば

$$\prod_{i=1}^{r}(x+\zeta^{-i} y)^{a_i} = \zeta^{-m} \varepsilon \bar{\rho}^p \alpha$$

となる．mod p で $\rho^p \equiv \bar{\rho}^p$ だから

$$\prod_{i=1}^{r}\left(\frac{x+\zeta^i y}{x+\zeta^{-i} y}\right)^{a_i} \equiv \zeta^{2m} \pmod{p}$$

で，また $v \geq 0$ を $v \equiv 2m - \sum_{i=1}^{r} i a_i \pmod{p}$ となるように取れば

$$\prod_{i=1}^{r}\left(\frac{x+\zeta^i y}{y+\zeta^i x}\right)^{a_i} \equiv \zeta^{v} \pmod{p}$$

となる．

$$x_i := \begin{cases} y & (a_i < 0) \\ x & (a_i \geq 0) \end{cases}, \quad y_i := \begin{cases} x & (a_i < 0) \\ y & (a_i \geq 0) \end{cases}$$

として $F(T) := \prod(x_i + T^i y_i)^{|a_i|}$，$G(T) := \prod(y_i + T^i x_i)^{|a_i|}$ と置く．$F(\zeta) \equiv \zeta^v G(\zeta) \pmod{p}$ となる．即ち，ある $K(T) \in \mathbb{Z}[T]$ が存在して $F(\zeta) = \zeta^v G(\zeta) + pK(\zeta)$ となる．よってある $H(T) \in \mathbb{Z}[T]$ が存在して $F(T) = T^v G(T) + pK(T) + (1 + T + \cdots + T^{p-1})H(T)$ と書ける．両辺に $1 - T$ を掛けて T で微分し，T に ζ を代入し，mod p を取れば

$$(1-\zeta)F'(\zeta) - F(\zeta) \equiv (1-\zeta)\zeta^v G'(\zeta) - \zeta^v G(\zeta) + v(1-\zeta)\zeta^{v-1} G(\zeta)$$

となる．$F(\zeta) \equiv \zeta^v G(\zeta)$ だったから

$$(1-\zeta)\frac{F'(\zeta)}{F(\zeta)} - 1 \equiv (1-\zeta)\frac{G'(\zeta)}{G(\zeta)} - 1 + v(1-\zeta)\zeta^{-1}$$

が分かる．これを計算すると

$$(1-\zeta)\sum_{i=1}^{r} i a_i \zeta^i \left(\frac{y}{x+\zeta^i y} - \frac{x}{y+\zeta^i x}\right) \equiv v(1-\zeta)$$

が分かる．$a_i \neq 0$ となる最小の番号 i を i_0 とする．両辺に $\prod_{i=1}^{r}(x+\zeta^i y)(y+\zeta^i x)$ を掛けて分母を払う．左辺は ζ について $1 + i_0 + r(r+1) - 2i_0 = 1 + r(r+1) - i_0$ 次の多

項式で，最高次係数は $i_0 a_{i_0}(x^2-y^2)x^r y^r$ である．一方右辺は $1+r(r+1)$ 次で最高次係数は $-x^r y^r v$ である．ここで r の取り方から $1+r(r+1)<1+(\sqrt{p}-1)\sqrt{p}<p-1$ である．よって命題 2 により $v\equiv 0 \pmod p$ が分かる．即ち右辺は (mod p で) 0 になる．よって左辺も 0 である．故に $x^2\equiv y^2$，即ち $x\equiv \pm y$ が分かった．

y と z を入れ替えて以上の議論を行えば $x\equiv \pm z$ が分かる．故に $x^p \pm x^p \equiv \pm x^p$ となるが，これは $p>3$ では矛盾する． □

ところで，この $i(p)<\sqrt{p}-2$ という条件はどのくらいの素数が満たすのだろうか．コンピュータによる計算に依れば，12×10^6 以下の素数について，$i(p)=0,1,2,\ldots$ となる素数 p の個数が以下のようになることが知られている ([2])．

$i(p)$	p の個数
0	477616
1	239483
2	59710
3	9824
4	1282
5	127
6	13
7	4

これを見ると，殆どの素数は $i(p)<\sqrt{p}-2$ を満たしそうに感じられる．

またここで，$p \mid B_j$ となるのは $1/p$ の確率であると仮定してみる．すると $i(p)=k$ となる確率は

$$ {}_{\frac{p-3}{k}}C_k \left(1-\frac{1}{p}\right)^{\frac{p-3}{2}-k}\left(\frac{1}{p}\right)^k $$

となるから，$p\to\infty$ とすれば $\dfrac{1}{2^k}\dfrac{e^{-1/2}}{k!}$ である．よって素数 p が $i(p)>\sqrt{p}-2$ を満たす確率は

$$ \sum_{k>\sqrt{p}-2}\frac{1}{2^k}\frac{e^{-1/2}}{k!} $$

となり，これは $\dfrac{1}{2^N}\dfrac{1}{N!}$ $(N:=[\sqrt{p}]-1)$ で抑えられる．Fermat の最終定理の 1st case は $p<6\times 10^9$ では成り立つことが知られているから，Fermat の最終定理の 1st case が成り立たない素数 p の割合は高々

$$ \sum_{p>6\times 10^9}\frac{1}{2^N}\frac{1}{N!} $$

程度だと考えることができて，これは $10^{-300000}$ 以下である．

参考文献

[1] L. C. Washington, Introduction to Cyclotomic Fields, GTM 83, Springer, 1997

[2] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, M. A. Shokrollahi, Irregular Primes and Cyclotomic Invariants to 12 Million, J. Symbolic Computation (2001) 31, 89–96, http://www.sciencedirect.com/science/article/pii/S0747717199910118