代数的整数論 Fermat の最終定理へ

アルゴドゥー　@alg_d

2013 年 3 月 9 日

目次

0　お話

まず，代数的整数論は何をやりたい理論なのか，ということについて述べます．早く数学的な話に入りたい方は飛ばして先に進んで構いません．(といっても，そちらは最後の証明を除いては必要最小限のことしか書いていないのですが．)

代数的整数論の始まりは Gauss だといわれています．整数論には「平方剰余の相互法則」と呼ばれる法則が古くから知られており (しかし証明はされていなかった)，Gauss が平方剰余の相互法則の証明を初めて与えたそうです．Gauss は平方剰余の相互法則を「整数論の基本定理」と呼び，生涯で 8 つの異なる証明 (1796 年には第一証明を見つけていたらしい) を与えました．

さて，平方剰余の相互法則が証明できれば当然それらの一般化，即ち三次 (立方) 剰余の相互法則，四次剰余の相互法則，……，n 次剰余の相互法則，…を考えることになります．三次剰余の相互法則については Jacobi(1827) が，四次剰余の相互法則については Gauss(1828〜1832) が考えたそうです (しかし証明はしてないらしい)．

そのとき Gauss は四次剰余の相互法則を扱うに当たっては整数環 $\mathbb{Z}$ よりも，「複素整数環」$\mathbb{Z}[i] = \{x + yi \mid x, y \in \mathbb{Z}\}$ で考えるのが自然であることに気付きました．(現在では $\mathbb{Z}[i]$ は Gauss の整数環と呼ばれています．) $\zeta_n := \exp\left(\dfrac{2\pi i}{n}\right)$ とすれば $i = \zeta_4$ ですが，実はこの 4 というのが「四」次剰余の四から来ているのです．実際三次剰余の相互法則の場合は $\mathbb{Z}[\zeta_3] = \{x + y\zeta_3 \mid x, y \in \mathbb{Z}\}$ を考えると上手くいくことが知られています．(Jacobi (1837))

※ $\mathbb{Z}[i]$ や $\mathbb{Z}[\zeta_3]$ を考えると上手くいきそうだ，ということに気付き定式化しただけで，証明は Gauss も Jacobi もしていないそうです．この三次剰余，四次剰余の相互法則の証明をしたのは Eisenstein だそうです．

このことから n 次剰余の相互法則については $\mathbb{Z}[\zeta_n]$ を考えれば良さそうだ，ということが分かります．この $\mathbb{Z}[\zeta_n]$ を使えば n 次剰余の相互法則だけでなく，Fermat の最終定理も証明できると一時は考えられていました．しかし，この理論には困難があります．それは《素因数分解の一意性 (に相当する性質)》が一般の $\mathbb{Z}[\zeta_n]$ では成り立たないことです (即ち，$\mathbb{Z}[\zeta_n]$ が UFD とは限らないということ)．

※ この事実に気付くのが遅れたのは，「$\mathbb{Z}[\zeta_n]$ が《素因数分解の一意性》を満たさないような最小の n」が 23 で結構大きいからしいです．ちなみに「《素因数分解の一意性》が成り立つ n」は有限個しかなく，最大の n は 84 です．

$\mathbb{Z}[\zeta_{23}]$ が《素因数分解の一意性》を満たさないことを確かめるのは大変なので，ここでは別の例で「《素因数分解の一意性》が成り立たない可能性があること」を見てみます．

※ この例で扱う $\mathbb{Z}[\sqrt{-5}]$ は勿論 $\mathbb{Z}[\zeta_n]$ とは違うのですが，これらの環は「整数環」と呼ばれる環であり，その意味で $\mathbb{Z}[\sqrt{-5}]$ と $\mathbb{Z}[\zeta_n]$ は仲間であると考えることが出来ます．

例. $\mathbb{Z}[\sqrt{-5}] := \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}\}$ と置く．この環で 6 を考えると

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{1}$$

と二通りに分解され，しかもこの分解に現れている $2,\ 3,\ 1 + \sqrt{-5},\ 1 - \sqrt{-5}$ はどれもこれ以上分解できない (即ち既約元である)． □

では $\mathbb{Z}[\zeta_n]$ で考えることは諦めなければいけないかというとそうではなく，Kummer が理想数 (ideale Zahlen, 1845〜) というものを考えてこの問題を乗り越えました．

普通の自然数の範囲でも，分解が完全でない場合，二通りの分解が起こることがありえ

ます．$12 = 2\cdot 6 = 3\cdot 4$ など．そこで，Kummer は分解 (1) は分解の仕方が不完全であると考えました．しかし，先に言った通りこれ以上の分解は存在しません．そこで (数学では度々やることですが) 存在しないものは作ってしまえばよいのです． つまり，「理想数」と呼ばれる架空の数 A, B, C, D が存在して

$$2 = AB,\ 3 = CD,\ 1+\sqrt{-5} = AC^{\dagger},\ 1-\sqrt{-5} = BD$$

$$6 = (AB)(CD) = (AC)(BD)$$

と分解されると考えるわけです．そして実際，この考えは上手く行って，Kummer は次のような結果を残しました．

定理 (Kummer, 1847)**.** $p \geq 3$ を素数とする．$\mathbb{Z}[\zeta_p]$ の「(理想数を使わない) 素因数分解の出来なさ (後述)」があまり大きくなければ，$x^p + y^p = z^p,\ xyz \neq 0$ は有理整数解を持たない．

この定理の画期的なところは，Fermat の最終定理を複数の p について同時に証明したところです．

※ Fermat の最終定理については Kummer 以前にもいくつか結果がありますが，$n = 4$ の場合 (Fermat)，$n = 3$ の場合 (Euler)，$n = 5$ の場合 (Dirichlet，Legendre)，$n = 14$ の場合 (Dirichlet)，$n = 7$ の場合 (Lamé) など，どれも個別の n に対するものでした．ちなみに，「素因数分解の出来なさ」が大きい素数は小さい方から順に $37, 59, 67, 101, 103, 131, 149, 157, 233, \cdots$ です．

そこでこの PDF ではこの Kummer の結果 (の一部) を目標にします．その為に理想数についてやるのですが，今日では理想数そのものでなくて，それを書き直した「イデアル」(Dedekind による) が使われています．なのでここでもイデアルを使います．

Dedekind のイデアルのポイントは「集合」を上手く使うことです．集合という概念が明確に現れだしたのは丁度この頃で，Dedekind は集合を積極的に使っていった一人だったのです．Dedekind というと「Dedekind の切断」がよく知られていますが，アレは「実数を有理数の集合を使って定義する」というもので，やはり集合が使われているのです．

先ほどの例 $\mathbb{Z}[\sqrt{-5}]$ を取って説明すると，Dedekind は $\mathbb{Z}[\sqrt{-5}]$ の理想数 A を集合 $\{\alpha \in \mathbb{Z}[\sqrt{-5}] \mid \alpha \text{ は } A \text{ の倍数 }\}$ とみなすことにしました．つまり「イデアル」=「とある理想数の倍数全体」です．このようにすると，もし集合 $\{\alpha \in \mathbb{Z}[\sqrt{-5}] \mid \alpha \text{ は } A \text{ の倍数 }\}$

† これはたまたまで，選択公理は関係ありません

が定まれば，この集合の元は $\mathbb{Z}[\sqrt{-5}]$ の元であり良く知っているものですから，簡単に扱うことができます．

問題はこの集合 $\{\alpha \in \mathbb{Z}[\sqrt{-5}] \mid \alpha \text{ は } A \text{ の倍数 }\}$ を定めることで，我々は理想数 A というのが何なのかよく分かっていないのですから，その倍数全体を決めろといわれてもよく分かりません．そこで「倍数」について考えます．

簡単のために，普通の整数の範囲で考えてみると，$n \in \mathbb{Z}$ の倍数というのは

(1) n の倍数 $\pm$ n の倍数 $=$ n の倍数
(2) n の倍数の何倍か $=$ n の倍数

を満たします．そこで，このような条件を満たす集合を「イデアル」と呼ぶことにするのです．次の節から，$\mathbb{Z}[\sqrt{-5}]$ の場合にイデアルを定義して，理想数の役割を果たしていることを見ていきます．

※ 今回は PDF の目的上 Fermat の最終定理について強調しましたが，Kummer は n 次剰余の相互法則についても理想数を使い示しています．

定理 (Kummer, 1850)**.** $p \geq 3$ を素数とする．$\mathbb{Z}[\zeta_p]$ の「素因数分解の出来なさ」があまり大きくなければ，p 次剰余の相互法則が成立する．即ち，p と素な理想素数 λ_1, λ_2 に対して $\left(\dfrac{\lambda_1}{\lambda_2}\right) = \left(\dfrac{\lambda_2}{\lambda_1}\right)$ が成り立つ．

1 $\mathbb{Z}[\sqrt{-5}]$ の場合

ここでは「イデアル」の話を $\mathbb{Z}[\sqrt{-5}]$ に限ってする．勿論ここの話はもっと一般的な (代数体の整数環と呼ばれる種類の) 環について成り立つのであるが，この PDF ではその中でも $\mathbb{Z}[\sqrt{-5}]$ と $\mathbb{Z}[\zeta_n]$ しか登場しないし，雰囲気を知るには $\mathbb{Z}[\sqrt{-5}]$ の場合だけでも大丈夫だろう，多分．一応次の節で一般の代数体の整数環の場合について書いてあるが，あまり詳しくは書いてない．

定義 (念のため)**.** $a, b \in \mathbb{Z}$ に対して

$$a \mid b \Longleftrightarrow a \text{ が } b \text{ を割り切る}$$

定義. $\mathfrak{a} \subset \mathbb{Z}[\sqrt{-5}]$ が次を満たすとき，$\mathfrak{a}$ をイデアルという．

(1) $\mathfrak{a}$ は加法について $\mathbb{Z}[\sqrt{-5}]$ の部分群である．
(2) $\alpha \in \mathfrak{a}$, $\gamma \in \mathbb{Z}[\sqrt{-5}]$ ならば $\gamma\alpha \in \mathfrak{a}$

$\mathfrak{a}, \mathfrak{b}$ をイデアルとするとき

$$\mathfrak{a}+\mathfrak{b} := \{\alpha+\beta \mid \alpha \in \mathfrak{a},\ \beta \in \mathfrak{b}\}$$
$$\mathfrak{ab} := \left\{\sum_{i=0}^{n} \alpha_i\beta_i \;\middle|\; \alpha_i \in \mathfrak{a},\ \beta_i \in \mathfrak{b}\right\}$$

としてイデアルの和と積を定義する.

※ $\mathfrak{ab} := \{\alpha\beta \mid \alpha \in \mathfrak{a},\ \beta \in \mathfrak{b}\}$ と定義してしまうと，これはイデアルにならない．(加法で閉じてないから．) 加法で閉じるようにするために和 $\sum \alpha_i\beta_i$ の全体を考える必要がある.

$\alpha_0, \cdots, \alpha_n \in R$ に対して

$$(\alpha_0, \cdots, \alpha_n) := \{x_0\alpha_0 + \cdots + x_n\alpha_n \mid x_i \in R\}$$

と置けば，これは $\mathbb{Z}[\sqrt{-5}]$ のイデアルになる．これを $\alpha_0, \cdots, \alpha_n$ で生成されるイデアルと呼ぶ．一つの元 α で生成されるイデアル (α) を単項イデアルという．このとき明らかに

$$(\alpha_0) + \cdots + (\alpha_n) = (\alpha_0, \cdots, \alpha_n)$$
$$(\alpha_0, \cdots, \alpha_n)(\beta_0, \cdots, \beta_m) = (\alpha_0\beta_0, \alpha_0\beta_1, \cdots, \alpha_n\beta_m)$$

等が成り立つ．また $(0) = \{0\}$ や $(1) = \mathbb{Z}[\sqrt{-5}]$ もイデアルである.

定義. イデアル $\mathfrak{p}$ が素イデアル
$\iff \mathfrak{p} \subsetneq \mathbb{Z}[\sqrt{-5}]$ であり，かつ $\alpha\beta \in \mathfrak{p}$ ならば $\alpha \in \mathfrak{p}$ または $\beta \in \mathfrak{p}$

定理 (素イデアル分解の一意性)**.** 0 でないイデアル $\mathfrak{a} \subset R$ に対して，素イデアル $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ と正整数 $e_1, \cdots, e_g$ が一意に存在して $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ と書ける.

例. $\mathbb{Z}[\sqrt{-5}]$ で $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ だった.

$$\mathfrak{p}_1 := (2, 1+\sqrt{-5}),\ \mathfrak{p}_2 := (3, 1+\sqrt{-5}),\ \mathfrak{p}_3 := (3, -1+\sqrt{-5})$$

と置けばこれらは素イデアルで

$$(2) = \mathfrak{p}_1^2.\ (3) = \mathfrak{p}_2\mathfrak{p}_3,\ (1+\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_2,\ (1-\sqrt{-5}) = \mathfrak{p}_1\mathfrak{p}_3,\ (6) = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$$

となる.

※ お話での記号と対応させて言えば理想数 A, B に対応するイデアルが $\mathfrak{p}_1$ で，C に対応するイデアルが $\mathfrak{p}_2$ で，D に対応するイデアルが $\mathfrak{p}_3$ ということ.

例えば $(2) = (2, 1+\sqrt{-5})^2$ を示してみる．

˙.˙)

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

なので $(2) = (4, 2+2\sqrt{-5}, -4+2\sqrt{-5})$ を示せばよい．$\mathfrak{a}$:=(右辺) と置く．

$(2) \subset \mathfrak{a}$ について

$2 \in \mathfrak{a}$ を示せばよい．$\mathfrak{a} \ni (2+2\sqrt{-5}) - (-4+2\sqrt{-5}) - 4 = 2$.

$(2) \supset \mathfrak{a}$ について

$4, 2+2\sqrt{-5}, -4+2\sqrt{-5} \in (2)$ を示せばよい．しかしそれは明らか．

$\mathfrak{p}_1 = (2, 1+\sqrt{-5})$ は単項イデアルでない．

˙.˙) $(2, 1+\sqrt{-5}) = (a+b\sqrt{-5})$ とかけたとする．$\subset$ からある $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ が存在して $2 = (a+b\sqrt{-5})\alpha$, $1+\sqrt{-5} = (a+b\sqrt{-5})\beta$ と書ける．絶対値の自乗を取ると $4 = (a^2+5b^2)|\alpha|^2$, $6 = (a^2+5b^2)|\beta|^2$ である．故に $a^2+5b^2 \mid 2$，従って $a^2+5b^2 = 1$ である．よって $a = \pm 1, b = 0$ だから $(2, 1+\sqrt{-5}) = (1)$ である．故に $\supset$ から $2(x+y\sqrt{-5}) + (1+\sqrt{-5})(z+w\sqrt{-5}) = 1$ と書ける．$(2x+z-5w) + (2y+z+w)\sqrt{-5} = 1$ だから $1 = 2x + (-2y-w) - 5w = 2(x-y-3w)$ となり矛盾．

つまり，2 は普通の数の範囲では分解できないけれども，理想数 (イデアル) の範囲では $2 = A^2$ と分解されるのである．理想数の等式 $2 = A^2$ に対応するイデアルの等式が $(2) = \mathfrak{p}_1^2$ というわけ．

定義. $\mathbb{Q}(\sqrt{-5}) := \{x+y\sqrt{-5} \mid x, y \in \mathbb{Q}\}$ とする．$\mathfrak{a} \subset \mathbb{Q}(\sqrt{-5})$ が $\mathbb{Q}(\sqrt{-5})$ の分数イデアルとは次を満たすこと．

(1) $\mathfrak{a}$ は加法について $\mathbb{Q}(\sqrt{-5})$ の部分群である．
(2) $\alpha \in \mathfrak{a}$, $\gamma \in \mathbb{Z}(\sqrt{-5})$ ならば $\gamma\alpha \in \mathfrak{a}$
(3) ある $\alpha(\neq 0) \in \mathbb{Z}(\sqrt{-5})$ が存在して $\alpha\mathfrak{a} \subset \mathbb{Z}(\sqrt{-5})$

分数イデアルについても，イデアルと同様にして和や積や単項分数イデアルを定義することができる．$I_{\mathbb{Q}(\sqrt{-5})}$:=「0 でない $\mathbb{Q}(\sqrt{-5})$ の分数イデアル全体」は分数イデアルの積でアーベル群になる．$P_{\mathbb{Q}(\sqrt{-5})} := \{(\alpha) \mid \alpha \in \mathbb{Q}(\sqrt{-5}) \setminus \{0\}\}$ はその部分群．剰余群

$Cl_{\mathbb{Q}(\sqrt{-5})} := I_{\mathbb{Q}(\sqrt{-5})}/P_{\mathbb{Q}(\sqrt{-5})}$ を $\mathbb{Q}(\sqrt{-5})$ のイデアル類群という．

定理． $\mathbb{Q}(\sqrt{-5})$ のイデアル類群は有限群である．

この定理により自然数であることが分かった $h_{\mathbb{Q}(\sqrt{-5})} := |Cl_{\mathbb{Q}(\sqrt{-5})}|$ を $\mathbb{Q}(\sqrt{-5})$ の類数という．実は，$h_{\mathbb{Q}(\sqrt{-5})} = 2$ 即ち $Cl_{\mathbb{Q}(\sqrt{-5})} \cong \mathbb{Z}/2\mathbb{Z}$ であることが知られている．($2 \mid h_{\mathbb{Q}(\sqrt{-5})}$ であることは先の例から分かる．)

この定理は一般の代数体について成り立つ．例えば $\mathbb{Q}(\zeta_n)$ についても $Cl_{\mathbb{Q}(\sqrt{-5})}$ は有限群である．

2　一般の代数体の場合

一応一般的な場合の定義を書いておく．(というか，このレジュメの前の版で書いたのをそのまま残しておいただけである．) 飛ばして次に進んでもらって問題ない (…と思う…)．

定義． 有理数体 $\mathbb{Q}$ の有限次拡大体 k を代数体という．

定義． $\alpha \in \mathbb{C}$ が代数的数 $\Longleftrightarrow$ ある有理数係数多項式 f が存在して $f(\alpha) = 0$.

α を代数的数とする．定義から $f(\alpha) = 0$ となる多項式 f が存在するが，そのような f のうち「次数が最小」で「最高次係数が 1」なものは唯一つしか存在しない．これを α の最小多項式と呼び，P_α で表す．P_α の係数が全て有理整数となるような α を代数的整数という．

定義． 代数体 k の部分環 $\mathcal{O}_k := \{\alpha \in k \mid \alpha \text{ は代数的整数 }\}$ を k の整数環という．

命題． 正整数 n に対して $\zeta_n := \exp(\frac{2\pi i}{n})$ と置く．$\mathbb{Q}(\zeta_n) :=$ ($\mathbb{Q}$ と ζ_n を含む最小の体) は代数体である．その整数環は $\mathbb{Z}[\zeta_n] :=$ ($\mathbb{Z}$ と ζ_n を含む最小の環) である．

定義． k を代数体とする．$\mathfrak{a} \subset \mathcal{O}_k$ が次を満たすとき，$\mathfrak{a}$ を k のイデアルという．

(1) $\mathfrak{a}$ は加法について $\mathcal{O}_k$ の部分群である．
(2) $\alpha \in \mathfrak{a}$, $\gamma \in \mathcal{O}_k$ ならば $\gamma\alpha \in \mathfrak{a}$

$\mathfrak{a}, \mathfrak{b}$ を k のイデアルとするとき

$$\mathfrak{a}+\mathfrak{b} := \{\alpha+\beta \mid \alpha \in \mathfrak{a},\ \beta \in \mathfrak{b}\}$$
$$\mathfrak{a}\mathfrak{b} := \left\{\sum_{i=0}^{n} \alpha_i\beta_i \;\middle|\; \alpha_i \in \mathfrak{a},\ \beta_i \in \mathfrak{b}\right\}$$

としてイデアルの和と積を定義する．$\alpha_0, \cdots, \alpha_n \in \mathcal{O}_k$ に対して

$$(\alpha_0, \cdots, \alpha_n) := \{x_0\alpha_0 + \cdots + x_n\alpha_n \mid x_i \in \mathcal{O}_k\}$$

と置けば，これは k のイデアルになる．これを $\alpha_0, \cdots, \alpha_n$ で生成されるイデアルと呼ぶ．一つの元 α で生成されるイデアル (α) を単項イデアルという．このとき明らかに

$$(\alpha_0) + \cdots + (\alpha_n) = (\alpha_0, \cdots, \alpha_n)$$
$$(\alpha_0, \cdots, \alpha_n)(\beta_0, \cdots, \beta_m) = (\alpha_0\beta_0, \alpha_0\beta_1, \cdots, \alpha_n\beta_m)$$

等が成り立つ．また $(0) = \{0\}$ や $(1) = \mathcal{O}_k$ もイデアルである．

定義． イデアル $\mathfrak{p}$ が素イデアル $\Longleftrightarrow \alpha\beta \in \mathfrak{p}$ ならば $\alpha \in \mathfrak{p}$ または $\beta \in \mathfrak{p}$

定理． 0 でないイデアル $\mathfrak{a} \subset \mathcal{O}$ に対して，素イデアル $\mathfrak{p}_1, \cdots, \mathfrak{p}_g$ と正整数 $e_1, \cdots, e_g$ が一意に存在して $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ と書ける．

※ この定理を証明するにあたって重要なのは，整数環の次の三つの性質である．

(1) 0 でない素イデアルは極大イデアルである．(即ち，次元が 1 である．)
(2) Noether 環である．
(3) 整閉整域である．

そこで逆に，この三つの性質を持つ環を Dedekind 環と呼ぶ．一般の Dedekind 環でも素イデアル分解の一意性が成立する．

定義． $\mathfrak{a} \mid \mathfrak{b} \Longleftrightarrow$ あるイデアル $\mathfrak{c}$ が存在して $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ となる．

命題． $\mathfrak{a} \mid \mathfrak{b} \Longleftrightarrow \mathfrak{a} \supset \mathfrak{b}$

定義． k を代数体とする．$\mathfrak{a} \subset k$ が分数イデアルとは次を満たすこと．

(1) $\mathfrak{a}$ は加法について k の部分群である．
(2) $\alpha \in \mathfrak{a},\ \gamma \in \mathcal{O}_k$ ならば $\gamma\alpha \in \mathfrak{a}$

(3) ある $\alpha(\neq 0) \in \mathcal{O}_k$ が存在して $\alpha\mathfrak{a} \subset \mathcal{O}_k$

$I_k :=$「k の 0 でない分数イデアル全体」はイデアルの積でアーベル群になる．$P_k := \{(\alpha) \mid \alpha \in k^\times\}$ はその部分群．$Cl_k := I_k/P_k$ を k のイデアル類群という．また $E_k := \{\alpha \in \mathcal{O}_k \mid \alpha^{-1} \in \mathcal{O}_k\}$ を k の単数群という．

定理 (代数的整数論の基本定理)．代数体 k について

(1) イデアル類群は有限群
(2) $E_k \cong \mathbb{Z}/w\mathbb{Z} \times \mathbb{Z}^r$ (Dirichlet の単数定理)

自然数 $h_k := |Cl_k|$ を k の類数という．

3 Fermat の最終定理

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

Fermat の最終定理を示すには $n = 4$ の場合と n が素数 $p \geq 3$ の場合に示せばよい．

˙.˙) $n = 4$ の場合と $n = p \geq 3$ の場合に示せたとしよう．今 $n \geq 3$ を一般の自然数とする．

(i) ある素数 $p \geq 3$ によって $p \mid n$ となるとき．$n = pm$ と書くと

$$x^n + y^n = z^n \Longrightarrow (x^m)^p + (y^m)^p = (z^m)^p$$

だから，もし $x^n + y^n = z^n$ が解を持てば $x^p + y^p = z^p$ が解を持つ事になり矛盾．

(ii) そうでないとき．この場合 $n = 2^m$ $(m \geq 2)$ と書ける．よって

$$x^n + y^n = z^n \Longrightarrow (x^{2^{m-2}})^4 + (y^{2^{m-2}})^4 = (z^{2^{m-2}})^4$$

となり同様に矛盾である．

$n = 3$ については Euler が，$n = 4$ については Fermat が解決している．故に $n = p \geq 5$ の場合のみ考えればよい．さらに $\begin{cases} p \nmid xyz & \text{(1st case)} \\ p \mid xyz & \text{(2nd case)} \end{cases}$ の二つの場合に分けることができる．今回は 1st case についてのみ考える．

定理 (Kummer)．素数 $p \geq 3$ が $p \nmid h_{\mathbb{Q}(\zeta_p)}$ を満たすとき，$x^p + y^p = z^p$，$xyz \neq 0$ は有理整数解を持たない．

証明. 1st case (即ち $p \nmid xyz$ の場合) のみ示す．先に述べたとおり $p \geq 5$ としてよい．

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 $x^p + y^p = z^p,\ xyz \neq 0$ となる．$\zeta := \zeta_p$ として $\mathbb{Z}[\zeta]$ で考えると $\prod_{i=1}^{p}(x + \zeta^i y) = z^p$ と分解できる．故にイデアルの式として $\prod_{i=1}^{p}(x + \zeta^i y) = (z)^p$ が成り立つ．

※ 左辺の $(x + \zeta^i y)$ は $x + \zeta^i y$ で生成された単項イデアルである．念のため．

$i \neq j$ 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．

˙.˙) $(x + \zeta y) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g},\ \prod_{i=2}^{p}(x + \zeta^i y) = \mathfrak{q}_1^{a_1} \cdots \mathfrak{q}_s^{a_s},\ (z) = \mathfrak{r}_1^{b_1} \cdots \mathfrak{r}_t^{b_t}$ と素イデアル分解したとする．$\prod_{i=0}^{p-1}(x + \zeta^i y) = (z)^p$ から

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \mathfrak{q}_1^{a_1} \cdots \mathfrak{q}_s^{a_s} = (\mathfrak{r}_1^{b_1} \cdots \mathfrak{r}_t^{b_t})^p = \mathfrak{r}_1^{pb_1} \cdots \mathfrak{r}_t^{pb_t}$$

である．$1 \leq u \leq g$ とする．今，$2 \leq i \leq p$ に対して $(x + \zeta y)$ と $(x + \zeta^i y)$ は互いに素であるから，$\mathfrak{q}_1, \cdots, \mathfrak{q}_s$ の中に $\mathfrak{p}_u$ は現れない．よって，素イデアル分解の一意性からある番号 $1 \leq v \leq t$ が存在して $\mathfrak{p}_u = \mathfrak{r}_v,\ e_u = pb_v$ である．

簡単のため，$\mathfrak{r}_v$ の番号を付け直して，$\mathfrak{p}_u = \mathfrak{r}_u,\ e_u = pb_u$ としておく．このとき $\mathfrak{a} := \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_g^{b_g}$ と置けば

$$(x + \zeta y) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} = \mathfrak{p}_1^{pb_1} \cdots \mathfrak{p}_g^{pb_g} = \mathfrak{a}^p$$

である．

今仮定により $p \nmid h_{\mathbb{Q}(\zeta)}$ であるからある $\alpha \in \mathbb{Z}[\zeta]$ が存在して $\mathfrak{a} = (\alpha)$ と書ける．

˙.˙) イデアル $\mathfrak{b} \in I_{\mathbb{Q}(\zeta)}$ に対して，$\mathfrak{b}$ の属する同値類 $\in Cl_{\mathbb{Q}(\zeta)}$ を $[\mathfrak{b}]$ で表すことにする．すると $(x + \zeta y) = \mathfrak{a}^p$ から $[(x + \zeta y)] = [\mathfrak{a}^p] = [\mathfrak{a}]^p$ である．イデアル類群の定義より $[(x + \zeta y)] = 1$ であるから $[\mathfrak{a}]^p = 1$ である．故に $[\mathfrak{a}] \in Cl_{\mathbb{Q}(\zeta)}$ の位数は p または 1 である．群論により「(元の位数) | (群の位数)」であるから

$$([\mathfrak{a}] \text{ の位数}) \mid (Cl_{\mathbb{Q}(\zeta)} \text{の位数}) = h_{\mathbb{Q}(\zeta)}$$

となる．今仮定により $p \nmid h_{\mathbb{Q}(\zeta)}$ であるから ($[\mathfrak{a}]$ の位数) $= 1$ しかありえない．故に

$[\mathfrak{a}]$ は単位元である，即ち $\mathfrak{a}$ は単項イデアルである．よってある $\alpha \in \mathbb{Z}[\zeta]$ が存在して $\mathfrak{a} = (\alpha)$ と書ける．

故に $(x+\zeta y) = (\alpha)^p = (\alpha^p)$．従ってある $\varepsilon \in E_{\mathbb{Q}(\zeta)}$ が存在して $x+\zeta y = \varepsilon\alpha^p$ となる．この ε に対して，ある $\varepsilon_1 \in \mathbb{Q}(\zeta+\zeta^{-1}) \subset \mathbb{R}$ と $r \in \mathbb{Z}$ が存在して $\varepsilon = \zeta^r\varepsilon_1$ と書けることが知られている．よって $x+\zeta y = \zeta^r\varepsilon_1\alpha^p$ である．$\alpha = a_0+a_1\zeta+\cdots+a_{p-1}\zeta^{p-1} \quad (a_i \in \mathbb{Z})$ だから

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

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

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

即ち

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

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．$\equiv 0 \pmod{p}$ だから $x+\zeta y-\zeta^{2r}x-\zeta^{2r-1}y = p\beta$ $(\beta \in \mathbb{Z}[\zeta])$ と書ける．$\beta = b_0+b_1\zeta+\cdots+b_{p-1}\zeta^{p-1}$ $(b_i \in \mathbb{Z})$ 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) $1 = \zeta^{2r-1}$ $(\zeta = \zeta^{2r})$ 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．

$$\frac{x}{e^x-1}=\sum_{n=0}^{\infty}B_n\frac{x^n}{n!}$$

と Taylor 展開したとき，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．最初のほうについては，$B_0=1,\ B_1=-\frac{1}{2},\ B_2=\frac{1}{6},\ B_4=-\frac{1}{30},\ B_6=\frac{1}{42},\ B_8=-\frac{1}{30},\ B_{10}=\frac{5}{66},\ B_{12}=-\frac{691}{2730},\ \cdots$

こう言われてもなんのこっちゃという感じであるが，実は Bernoulli 数というのはあのゼータなのである．

定理. $\zeta(s)$ を Riemann ゼータ関数とするとき, 任意の正整数 n に対して $\zeta(1-n)=-\dfrac{B_n}{n}$

このゼータにより，正則素数が次のように判定される．

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

例えば，$691\mid(B_{12}$ の分子$)$ 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むわけであるが，非正則素数についてもある程度解決されている．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. $i(p):=\left|\{2\le n\le p-3\mid n\text{ は偶数},\ p\mid B_n\}\right|$ を p の index of irregularity という．

このとき,《非正則度》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．即ち

定理 ([4]p107)**.** 素数 p が $i(p)<\sqrt{p}-2$ を満たすならば $x^p+y^p=z^p,\ p\nmid xyz\neq 0$ は有理整数解を持たない．

参考文献

[1] 石田 信, 『代数的整数論』, 森北出版, 1974 年
代数的整数論の入門書．Galois 理論の基本定理を知っている位の知識があれば多分読める．特殊な場合 (下の体が $\mathbb{Q}$ の場合) しか基本的に扱っていないので，その分わかりやすくなっている．

[2] 高木 貞治, 『代数的整数論 一般論及類体論』, 岩波書店, 1971 年
こちらは一般の場合 (下の体が $\mathbb{Q}$ でないの場合) でやっている．また類体論が書いてある．類体論については初めにこの本でどんな物か知るのが良いと思うのだけれど，どうだろう．

[3] Neukirch,『代数的整数論』，シュプリンガージャパン，2003 年
代数的整数論の辞書としても使えるらしい教科書．”代数学の基礎だけを仮定して”と書かれているが，初めに読むには難しすぎると思う．面白い本なのだけれども．

[4] L. C. Washington, Introduction to Cyclotomic Fields, GTM 83, Springer, 1997
岩澤理論の教科書．今回やらなかった Fermat の最終定理の 2nd case について，また非正則素数の場合についても書いてある．

[5] 斎藤 毅,『フェルマー予想』，岩波書店，2009 年
買って本棚に飾りましょう．私はまだ 22 ページしか読めてない．

[6] 河田 敬義,『19 世紀の数学 整数論』，共立出版，1992 年
歴史的な部分についてはこの本を参考にした．

[7] 倉田 令二朗,『平方剰余の相互法則—ガウスの全証明』，日本評論社，1992 年
三次剰余，四次剰余についても書いてある．