北数教“第 101 回数学教育実践研究会”

【高校生にもわかる】

（多項式版）フェルマーの大定理の証明

＜ ABC 定理の紹介＞

レポート

平成 29 年 6 月 3 日 (土)

北海道大学　情報教育館３Ｆ
スタジオ型多目的中講義室

千歳科学技術大学　安田富久一

1　（多項式版）フェルマーの定理

【 フェルマーの大定理（最終定理） 】

n を 3 以上の整数とする。このとき、

$$a^n + b^n = c^n$$

を満たす正の整数は存在しない。

はあまりにも有名なフェルマーの大定理（最終定理）。フェルマーがこの予想をしたのは江戸時代初め頃で、ワイルズが 1994 年に証明を完成させるまでの約 400 年間、未解決の難問であり続けた。その証明にはものすごく高度な数学の修養を要するらしい。

この定理の整数の部分を多項式に変えてみると

【 （多項式版）フェルマーの定理 】

n を 3 以上の整数とする。このとき、

$$X^n + Y^n = Z^n$$

を満たす多項式 X, Y, Z で、全てが定数ではなく、どの 2 つも互いに素なものは存在しない。

となる。整数よりも多項式の方が難しい（整数は小学校から習ってるけれど、多項式は高校に入ってからやから、感覚的に難しいやろう）から、この多項式版のフェルマーの定理はもっと難しい、という気がする。

しかし、19 世紀後半には既に知られており、さらに簡単な証明が 20 世紀も終わりかけの頃に見つかった。その証明に使われるのが、**『ABC 定理』**である。『ABC 定理』の証明は高校生にもわかる程度であるにもかかわらず、発見と証明がごく最近のことであり、このようなことは他にほとんどない。

そのために、高校の授業等に活かせる可能性がありそうなので、紹介したい。今回のレポートは、

共立出版社創立９０周年記念出版　数学講座　数学探検　第 6 巻
山崎隆雄　著　『初等整数論』数論幾何への誘い

の 第 2 章 多項式 の中の ABC 定理 及びそれに関する内容の紹介であり、自分の学習としてまとめ直したものである。私の解釈ミスや説明のまずさ等があるといけないので、興味があれば是非読んで確認していただけると幸いである。また、私のミス等があれば教えていただけるとさらに幸いである。

この本では、最大公約数等を環のイデアルにより定義してある。本レポートの内容については、特にイデアルを持ち出す必要はないので、高校までの用語で書いた。ただ、最近は多項式・整式に関する約数・倍数等の言葉を余り使わないようなので、確認のため、本レポートで使った用語を、5 ページにまとめておいた。

2　『ABC 定理』

『ABC 定理』は多項式に関する定理である。多項式の係数は有理数のみ、実数のみ、または複素数のみ、のいずれを採用しても構わないが、話しを複雑にしないために、実数係数の多項式のみを考えることにしよう。

『ABC 定理』を紹介する前に記号等について準備しておく。

【 記号 】

- $\deg A$：多項式 A の次数を示す。
  ＜例＞ $A = 2x^3 - 3x + 1$ なら、$degA = 3$
- radA：A の素因子全ての積を示す。
  ＜例＞ $A = x^3 - 3x^2 + 4$ のとき、$A = (x+1)(x-2)^2$ なので、$\mathrm{rad}A = (x+1)(x-2)$
  $B = x^5 - 2x^3 + x$ のとき、$B = x(x+1)^2(x-1)^2$ なので、$\mathrm{rad}B = x(x+1)(x-1)$

【 **ABC 定理** 】

A, B, C は実数係数の多項式で、どの 2 つも互いに素であり、しかも全てが定数ではないとする。

このとき、$A + B = C$ なら

$$\max\{\deg A, \deg B, \deg C\} < \deg \mathrm{rad}(ABC)$$

が成り立つ。

だからどうした、と言われてしまいそうだが、この『ABC 定理』を利用して（多項式版）フェルマーの大定理が簡単に導けるのである。$Stothers$, $Mason$ 両氏による定理らしい。『ABC 定理』を利用すると、（多項式版）フェルマーの大定理よりも強い次の定理が証明できる。

【 定理 1 】

自然数 p, q, r が $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leqq 1$ を満たすとき、

$$X^p + Y^q = Z^r$$

を満たす多項式 X, Y, Z で、全てが定数ではなく、どの 2 つも互いに素なものは存在しない。

この定理の特別な場合として、p, q, r のどれもが 3 以上の自然数 n に等しいときが、（多項式版）フェルマーの定理になっている。

3　ABC 定理 の証明

ABC 定理 の証明はさぞかし難解だろうと思いきや、微分の基本性質を知っていれば理解できる程度のもの。しかも、そんなに長くはない。多項式をアルファベット大文字で表し、例えば A の微分を普通通り A' で表すことにする。微分に関する使う知識を命題として示しておく。

【 命題 】

(i) A が定数でなければ、$\deg A' = \deg A - 1$

(ii) B が A^n の倍数なら、B' は A^{n-1} の倍数である（n は自然数)。

(iii) $AB' = BA'$ であることと、$A = cB$ となる 0 ではない実数 c があることとは同値である。

【 **ABC 定理 の証明** 】

先ず流れを示す。次の (1)〜(4) を順に示し証明する。

(1) $AB' - BA' = AC' - CA' = CB' - BC' \neq 0$ である。
（この等しい 3 つの多項式を D とおく)。

(2) $\max(\deg A, \deg B, \deg C) + \deg D < \deg(ABC)$

(3) $A_1 = \frac{A}{\mathrm{rad}A}$, $B_1 = \frac{B}{\mathrm{rad}B}$, $C_1 = \frac{C}{\mathrm{rad}C}$ とおくと、D は A_1, B_1, C_1 の公倍数である。

(4) $\deg(ABC) \leqq \deg D + \deg \mathrm{rad}(ABC)$

＜ **(1)** について＞

$A + B = C$ の両辺を微分すると、$A' + B' = C'$ なので、

$$AB' - BA' = A(C' - A') - (C - A)A' = AC' - CA'$$

同様にして、$AB' - BA' = CB' - BC'$ であることもわかる。

次に、もし $D = AB' - BA' = 0$ なら、命題の (iii) より、ある実数が存在して $A = cB$ となる。これは A, B が互いに素であることに反するので、$D \neq 0$ であり、(1) が示された。

＜ **(2)** について＞

$$\begin{aligned}\deg(D) &= \deg(AB' - BA') \\ &\leqq \max\{\deg(AB'), \deg(BA')\} \\ &= \deg(A) + \deg(B) - 1 \qquad (\because \text{命題 (i)}) \\ &= \deg(AB) - 1\end{aligned}$$

$$\therefore\ \deg(C) + \deg(D) < \deg(ABC)$$

ここで、$C + (-A) = B$, $C + (-B) = A$ と見れば、今得た不等式の左辺の C は A や B に変えても成り立つので、(2) が示された。

＜ **(3)** について＞

D が A_1 の倍数であることを示せば、D は残りの B_1, C_1 の倍数でもあることは、A, B, C の対称性から明らか。A_1 についてのみ示せばよい。

A を素式分解して、

$$A = \epsilon(A) P_1^{e_1} \cdots P_r^{e_r} \qquad (P_1, \cdots, P_r : \text{互いに素で、} e_1, \cdots, e_r \text{ は自然数})$$

とする。このとき、$A_1 = \epsilon(A) P_1^{e_1 - 1} \cdots P_r^{e_r - 1}$ である。$1 \leqq i \leqq r$ である任意の i について、A, A' は共に $P_i^{e_i - 1}$ の倍数なので、D は $P_i^{e_i - 1}$ の倍数となり、D は A_1 の倍数である（同様に B_1 や C_1 の倍数でもある)。よって、(3) が示された。

＜ **(4)** について＞

A_1, B_1, C_1 はどの 2 つも互いに素なので、(3) より D は $A_1 B_1 C_1$ の倍数であることがわかるので、$D\,\mathrm{rad}(ABC)$ は ABC の倍数であり、(4) が成り立つことがわかる。

今示した (2),(4) から ABC 定理が成り立つことは明らか。　　（証明終わり）

4　ABC 定理 の応用

定理 1（2 ページ）は、ABC 定理を用いると次のように が証明できる。

【 定理 1 の証明 】

背理法により示す。

$A=X^p, B=Y^q, C=Z^r$ として ABC 定理 を適用すると、

$$\begin{aligned}\max\left(\deg\left(X^p\right),\deg\left(Y^q\right),\deg\left(Z^r\right)\right) &< \deg\mathrm{rad}(X^pY^qZ^r)\\ &= \deg\mathrm{rad}(XYZ)\\ &\leqq \deg\left(XYZ\right)\end{aligned}$$

$$\therefore\quad p\deg X<\deg\left(XYZ\right)\ ,\ q\deg Y<\deg\left(XYZ\right)\ ,\ r\deg Z<\deg\left(XYZ\right)$$

$$\therefore\quad \deg\left(XYZ\right)=\deg(X)+\deg(Y)+\deg(Z)<\left(\frac{1}{p}+\frac{1}{q}+\frac{1}{r}\right)\deg\left(XYZ\right)\ \cdots\cdots\cdots\ ①$$

$\deg(XYZ)>0$ なので、①より $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}>1$ となり、矛盾が導けた。　　（証明終わり）

＜注＞

この定理 1、及び（多項式版）フェルマーの大定理において、“X,Y,Z の全てが定数ではなく、どの 2 つも互いに素ではない” という条件を省くと、自明な解が存在する。ここで、自明な解 X,Y,Z というのは、$a^n+b^n=c^n$ となる 0 ではない定数 a,b,c 及び、任意の多項式 W について、

$$X=aW\ ,\ Y=bW\ ,\ Z=cW$$

として与えられるもので、これは $X^n+Y^n=Z^n$ を満たし、解になっている。

【 その他の応用例 】　定理 1 の証明に ABC 定理を用いたが、例えば次の問題に応用できる。

＜応用問題例＞次の等式を満たす多項式 A , B を求めよ。

$$\mathrm{A}^2=\mathrm{B}^5+x^2\ \cdots\cdots\cdots\ ②$$

＜解答＞

(1)　A,B,x のどの 2 つも互いに素のとき、つまり、A,B が互いに素でしかも x を因数に持たないとき、ABC 定理より、

$$\max\left(\deg\mathrm{A}^2,\deg\mathrm{B}^5,\deg\mathrm{x}^2\right)<\deg\mathrm{rad}(\mathrm{A}^2\mathrm{B}^5x^2)$$

$$\therefore\quad\begin{cases}2\deg\mathrm{A}<\deg\mathrm{A}+\deg\mathrm{B}+1\\ 5\deg\mathrm{B}<\deg\mathrm{A}+\deg\mathrm{B}+1\\ 2<\deg\mathrm{A}+\deg\mathrm{B}+1\end{cases}$$

これから、$0<\deg\mathrm{B}<\frac{2}{3}$ となり、これを満たす整数 $\deg\mathrm{B}$ は存在しない。

(2)　A,B,x のうちの 2 つで、互いに素ではないものがあるとき、この場合は②より、A,B が共に x を因数に持つときに限る。そこで、$\mathrm{A}=x\widetilde{\mathrm{A}}$, $\mathrm{B}=x\widetilde{\mathrm{B}}$ とおくと、②は、

$$\widetilde{\mathrm{A}}^2=x^3\widetilde{\mathrm{B}}^5+1\ \cdots\cdots\cdots\ ③$$

となる。$\widetilde{\mathrm{A}}\neq 0$, $\widetilde{\mathrm{B}}\neq 0$ ならば、③より $\widetilde{\mathrm{A}}^2$ と $x^3\widetilde{\mathrm{B}}^5$ は互いに素なので、ABC 定理より、

$$2\deg\widetilde{\mathrm{A}}<\deg\widetilde{\mathrm{A}}+\deg\widetilde{\mathrm{B}}+1\ ,\ 3+5\deg\widetilde{\mathrm{B}}<\deg\widetilde{\mathrm{A}}+\deg\widetilde{\mathrm{B}}+1$$

となり、$\deg\widetilde{\mathrm{B}}<-\frac{1}{3}$ である。これは矛盾。よって、$\widetilde{\mathrm{A}}=0$ または $\widetilde{\mathrm{B}}=0$ であるが、③より $\widetilde{\mathrm{A}}=0$ は明らかに不適なので、$\widetilde{\mathrm{B}}=0$ 。また、このとき③より $\widetilde{\mathrm{A}}=\pm 1$ 。

$$A=\pm x\ ,\ B=0\ 。$$

以上 (1),(2) より、求める多項式 A,B は、$A=\pm x$, $B=0$ ……(答)

5　用語

多項式に関する用語について、高校では余り使わないものをまとめておく（書物により定義に異同があるものがあるので、要注意：例えば、零多項式 0 の次数を ∞ と定義する流儀もあるらしい）。

次数・最高次の係数・モニック

多項式

$$A = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 \quad （但し、a_n \neq 0）$$

について、n を A の次数、a_n を最高次の係数と言い、それぞれ $\deg A$, $\epsilon(A)$ と表す

$$\deg A = n \, , \, \epsilon(A) = a_n$$

（注）

零多項式 $A = 0$ の次数は考えない。零多項式と次数が 0 の多項式を定数と呼ぶ。

また、　$\epsilon(A) = 1$ である多項式 A をモニックと呼ぶ。

約数・倍数

多項式 A, B について、$A = BQ$ を満たす多項式 Q が存在するとき、A を B の倍数、B を A の約数と言う。

互いに素

零多項式ではない多項式 A, B について、A と B に共通な公約数が定数しかない場合、A と B は互いに素という。

（注）本では、この定義を次のような同値条件で書いてある。

$AX + BY = 1$ となる多項式 X, Y が存在するとき、A と B は互いに素という。

既約多項式

多項式 P について、P の約数が定数または P の定数倍以外にないとき、P を既約多項式と言う。

素式

モニック（最高次の係数が 1）な既約多項式を素式と言う。

素式分解

零多項式ではない多項式 A について、

$$A = \epsilon(A) P_1 P_2 \cdots P_r$$

を満たす素式 $P_1, P_2, \cdots, P_r$ が存在する（証明は省略）。これを A の素式分解と言い、$P_1, \cdots, P_r$ を A の素因子と言う。