数をめぐる冒険

木曜第 4 時限 井上尚夫

0　はじめに

この講義では数 (整数) の作る美しい世界を探ってみる。方法は「思考と論理」である。あえて「冒険」としたのは、講義の内容を単に事実として受け止めるだけではなく、君たちにも、「思考と論理」を武器に主体的に考えて欲しいからだ。予備知識はいらない。数学への先入観を持たずに参加して欲しい。

1　素数について

1.1　約数と倍数

数の世界には**四則演算**という 4 つの演算がある。まずこれを整理してみよう。

加法　$a+0=0+a=a$ の様に、0 は加えても変わらない。このことから 0 を**加法についての単位元**[1]と呼ぶ。

a について、$a+(-a)=(-a)+a=0=$(単位元) が成り立つ。このことから$-a$ を a の加法についての**逆元**という。

a に b の逆元を加えることを加法の逆演算 (減法) という。

乗法　$a\times 1=1\times a=a$ の様に、1 は掛けても変わらない。このことから 1 を**乗法についての単位元**と呼ぶ。

a について、$a\times b=b\times a=1=$(単位元) が成り立つとき、b を a の乗法についての**逆元**という。

a に b の逆元を掛けることを乗法の逆演算 (除法) という。

(加法、減法) と (乗法、除法) はきわめて類似した構造を持っている。しかし、まったく同じではない。それは分配法則が対称ではないためで、その結果 0 には乗法の逆元が存在しないからだ。

命題 1　乗法の逆元について次が成り立つ。

(1)　0 の逆元は存在しない。

(2)　整数の範囲で考えれば、逆元が存在するのは ± 1 のみである。

(3)　有理数全体の世界で考えれば、0 以外のすべての数について逆元が存在する。

さて、整数全体の集合を $\boldsymbol{Z}$ と表すとき、$\boldsymbol{Z}$では和、差、積は自由に行えるが商は必ずしも定義されない。これを手がかりに整数のことを詳しく考えてみたい。

定義 1　二つの整数 a と b について、a が b の**倍数**であるとは、$a=kb$ となる整数 k が存在することをいう。またこのとき、b は a の**約数**という。

命題 2　(1)　逆元を持つ数は単位元 (即ち 1) の約数である。(これを**単元**という。)

(2)　どんな数も単元を約数に持つ。どんな数も単元の倍数である。

(3)　a に単元を掛けたもの (これを a の **同伴元**という) は a の約数である。

(4)　0 はすべての数の倍数である。**どんな数も 0 の約数である。**

[1]聞きなれない言葉だと思うかもしれない。しかし、数学の用語は考えるための整理の手段である。

1.2 素数とは

定義 2 0 と単元以外の数 a について

(1) 単元と a の同伴元を自明な約数という。

(2) 自明な約数以外に約数を持たない数を素数という。

(3) 自明な約数以外に約数が存在するとき、合成数という。

(4) a の約数で素数のものを a の素因数という。

整数の世界では単元は± 1 であり、a の同伴元は$\pm a$ である。そのため、a が素数であるとき、$-a$ も素数となるが、この二つは同じ素数と見なすのである。

問 1 有理数係数の多項式全体のなす世界で、単位元、逆元、単元、同伴元、約数、素数はどういう意味になるのだろうか。

1.3 素数の判定

与えられた数が素数であるか否かを判定する方法については第 4 節でいくつか述べる。ここでは、もっとも単純な方法に触れるにとどめる。

命題 3 a を 2 以上の自然数とする。a が素数であるための必要十分条件は a が$\sqrt{a}$以下の素因数を持たないことである。

1.4 素数の分布

定理 1.1 素数は無限に多く存在する。

$p(n)$ を n 以下の素数の個数と定める。この定理は

$$\lim_{n\to\infty} p(n) = \infty$$

を意味する。19 世紀末になってさらに強く次が証明されている。

定理 1.2 (素数定理)

$$\lim_{n\to\infty} \frac{p(n)\log n}{n} = 1$$

ただし、log　は、自然対数（底を $e = 2.71828\cdots$とする対数）である。

この定理は n が十分大きければ、$p(n)$ はほぼ$\dfrac{n}{\log n}$に等しいことを述べている。この証明はとても難しいので講義では扱えない。整数の話に自然対数がでてくることの不思議さを感じて欲しい。

2 素因数分解

2.1 素因数分解とそのアルゴリズム

定義 3 0 と± 1 以外の数を素数の積として表すことを **素因数分解**という。

素因数分解に関連して問題になるのは次の二つの事項である。

可能性: 2 以上のすべての自然数は素因数分解できる。

一意性: 素因数分解の方法は素数の順序を除いて一通りである。

ここではまず前者について考えよう。

命題 4 a を 0 と± 1 以外の数とする。a の 2 以上の正の約数で、最小のものは素数である。

この命題により、与えられた数を素因数分解するアルゴリズムが得られる。

2.2 素因数分解の一意性からわかること

一意性を示す前に一意性が正しければどういうことが分かるのかについて述べよう。

2.2.1 様々な無理数

$\sqrt{2}$が無理数であることは習っただろう。しかし、もっと一般に次が成り立つのだ。

定理 2.1 p の k 乗根は p 自身が k 乗数でない限り無理数である。

結局、$\sqrt[3]{4}$も$\sqrt{21}$も無理数なのだ。この事実を示すために、まず、次の主張を証明しよう。

命題 5 (1) a と b が互いに素かつ ab が k 乗数ならば、a も b も k 乗数である。

(2) ab が c の倍数で b と c が互いに素ならば a は c の倍数である。

定理 2.2 整数係数方程式の有理数解は

$$\pm\frac{\text{最低次の項の係数}}{\text{最高次の項の係数}}$$

の形に限る。それ以外の実数解は無理数である。

2.2.2 ピタゴラス数とフェルマーの定理

辺の長さが $3, 4, 5$ である三角形は直角三角形である。これはピタゴラスの定理からわかることだ。もっと一般にしよう。

定義 4 $x^2 + y^2 = z^2$を満たす自然数の組を **ピタゴラス数**という。

定理 2.3 互いに素なピタゴラス数の組は

$$m^2 - n^2, \quad 2mn, \quad m^2 + n^2 \qquad m \text{ と } n \text{ は互いに素で一方は偶数}$$

の形に限る。

証明の要点

1) x と z が奇数で y が偶数の場合を考えればよい。

2) $y^2 = (z+x)(z-x)$ において、y, $z+x$, $z-x$ はすべて偶数なので、次のように置き直す。

$$y = 2a, \quad z + x = 2b, \quad z - x = 2c, \Rightarrow a^2 = bc$$

3)　b と c は互いに素であり、それぞれ平方数になる。

$$b = m^2, \quad c = n^2 \Rightarrow \text{定理の結論}$$

$n \neq 2$ のとき $x^n + y^n = z^n$ を満たす自然数の組があるか否かという問題は 17 世紀の数学者フェルマーによって考察された。彼は、1630 年頃、ディオファントスの「アリスマティカ」のピタゴラス数にの項の欄外に次の書き込みをした。

> これに反し、立方を二つの立方に、二重平方を二つの二重平方に分かつこと、一般に平方より大きい任意のべきを二つの同一べきのものに分かつことはできない。そのことの真に驚くべき証明を見つけたが、この余白に書くには狭すぎる。

言い換えれば、

> $n > 2$ のとき、$x^n + y^n = z^n$ を満たす自然数の組は存在しない。

と述べているのだ。しかし、その後彼は、n が 3 と 4 の場合を除いて、その証明を記すことはなかった。これが、「フェルマーの最終定理 (もしくは、大定理、予想)」として 350 年間にわたって多くの数学者を悩ませた問題の発端である。
3 年前ワイルズは、モーデル予想の特別な場合を証明することによって、その一つの帰結として、フェルマーの最終定理を証明した。ワイルズの証明は代数幾何学の最新の成果に基づいており、専門家にしか理解し得ないものだ。この講義では、自然数のついての素朴な議論のみでわかる $n = 4$ の場合を扱うことにする。

定理 2.4 $x^4 + y^4 = z^2$ を満たす自然数の組は存在しない。

証明

1) そのような自然数の組が存在したとしてその中で一番小さいものをとる。

2) $x^2, y^2, z,$ は互いに素なピタゴラス数なので、

$$x^2 = m^2 - n^2,\ y^2 = 2mn\, z = m^2 + n^2$$

3)　x, n, m も互いに素なピタゴラス数であり、偶奇を考えて

$$x = p^2 - q^2,\ n = 2pq,\ m = p^2 + q^2$$

4)　$y^2 = 4pqm$ に着目すれば、p, q, m は互いに素なので

$$p = a^2, \quad q = b^2, \quad m = c^2 \Rightarrow a^4 + b^4 = c^2$$

5)　a, b, c はもとの x, y, z より小さいので、矛盾

3　素因数分解の一意性の証明

前節では、素因数分解の一意性を利用してそれから分かる事実を紹介した。この節では素因数分解の一意性の証明を目指す。

3.1　ユークリッドの互除法

二つの整数 a と b について、その共通な約数を**公約数**という。$a = b = 0$ の場合を除き、公約数には最大のものが存在する。それを**最大公約数**と呼び、

$$(a, b)$$

と表す。まず、基本的な事項をいくつか。

- a と b が互いに素 $\Longleftrightarrow (a, b) = 1$
- $a \neq 0$ のとき、$(a, 0) = |a|$

定理 3.1 $a = bp + r$ が成り立つ時、a と b の公約数は一致する。特に、

$$(a, b) = (b, r)$$

この事実を使えば、最大公約数の計算のためには割り算を繰り返し実行すればよい。

例　2485 と 3955 の最大公約数を求めよう。

$$\begin{array}{lcccl}
3955 \div 2485 = 1 \cdots 1470 & \Rightarrow & 3955 = 1 \times 2485 + 1470 & \Rightarrow & (3955, 2485) = (2485, 1470) \\
2485 \div 1470 = 1 \cdots 1015 & \Rightarrow & 2485 = 1 \times 1470 + 1015 & \Rightarrow & (2485, 1470) = (1470, 1015) \\
1470 \div 1015 = 1 \cdots 455 & \Rightarrow & 1470 = 1 \times 1015 + 455 & \Rightarrow & (1470, 1015) = (1015, 455) \\
1015 \div 455 = 2 \cdots 105 & \Rightarrow & 1015 = 2 \times 455 + 105 & \Rightarrow & (1015, 455) = (455, 105) \\
455 \div 105 = 4 \cdots 35 & \Rightarrow & 455 = 4 \times 105 + 35 & \Rightarrow & (455, 105) = (105, 35) \\
105 \div 35 = 3 \cdots 0 & \Rightarrow & 105 = 3 \times 35 + 0 & \Rightarrow & (105, 35) = (35, 0) = 35
\end{array}$$

この様に、次々と割り算をしていけば剰余はだんだん小さくなるのでいつかは割り切れる。その時の割る数が最大公約数なのだ。この方法を **ユークリッドの互除法**という。また、上の定理から

a と b の公約数は最大公約数 (a, b) の約数である。

ということも分かる。

3.2　ユークリッドの互除法を逆にたどる

前節での例の結果を利用して

$$\begin{array}{rcll}
35 & = & 455 - 4 \times 105 & \\
 & = & 455 - 4 \times (1015 - 2 \times 455) & = 9 \times 455 - 4 \times 1015 \\
 & = & 9 \times (1470 - 1015) - 4 \times 1015 & = 9 \times 1470 - 13 \times 1015 \\
 & = & 9 \times 1470 - 13 \times (2485 - 1470) & = 22 \times 1470 - 13 \times 2485 \\
 & = & 22 \times (3955 - 2485) - 13 \times 2485 & = 22 \times 3955 - 35 \times 2485
\end{array}$$

この方法はどの a と b についても適用可能なので次が分かる。

定理 3.2 (1) 二つの自然数 a, b について

$$Ma + Nb = (a, b)$$

を満たす整数 M, N が存在する。
(2)a と b が互いに素 $\Longleftrightarrow$ $Ma + Nb = 1$ を満たす整数 M, N が存在する。

3.3 素因数分解の一意性の証明

まず、前節の結果を用いて次を示そう。

定理 3.3 p は素数であるとする。
(1)ab が p の倍数であれば、a と b の少なくとも一方は p の倍数である。
(2)$a_1 a_2 \cdots a_n$が p の倍数であれば、$a_1, a_2, \cdots, a_n$の少なくとも一つは p の倍数である。

さて、背理法で素因数分解の一意性を証明しよう。

1. 自然数 n が二通りの方法で素因数分解できたとする。

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

2. $n = q_1 q_2 \cdots q_s$が p_1の倍数なので、$q_1, q_2, \cdots, q_s$のどれか一つは p_1の倍数である。それを仮に q_1とする。
3. $n/p_1 = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$であり、$n/p_1$も二通りの方法で素因数分解されたことになる。
4. この議論を繰り返せば、二通りの方法で素因数分解できる数の列でどんどん小さくなるものが存在することになる。ある数より小さい自然数は有限個しかないからこれは矛盾である。

4 整数についてのその他の話題

4.1 約数のリストアップ

定理 4.1 自然数 n の素因数分解を

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \qquad p_1 < p_2 < \cdots < p_r$$

とおく。このとき、n の (正の) 約数は全部で $(k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$ 個あり、それらは

$$p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}, \qquad 0 \leq \ell_j \leq k_j$$

と表せる。

証明の概略

1. n の約数を a とし、$n = ab$ とおく。
2. $p_1, p_2 \cdots p_r$以外の素数が a と b の素因数に」なることはない。
3. $a = p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r}$, $b = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ とおくと、

$$\ell_j + m_j = k_j, \qquad 1 \leq j \leq r$$

4.2 約数の総和

自然数 n について、

$$\varphi(n) = n \text{ の約数の総和}$$

と定める。n が一つの素因数しか持たないときは、これは等比級数であり

$$\varphi(p^k) = \frac{p^{k+1}-1}{p-1}.$$

一般の場合には、前項での結果から

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \qquad p_1 < p_2 < \cdots < p_r$$

のとき、

$$\varphi(n) = \frac{p_1^{k_1+1-1}}{p_1-1}\frac{p_2^{k_2+1-1}}{p_2-1}\cdots\frac{p_r^{k_r+1-1}}{p_r-1}.$$

である。a と b が互いに素である時、

$$\varphi(ab) = \varphi(a)\varphi(b).$$

4.3 完全数

約数の総和が自分自身の 2 倍よりちょうど等しくなる数を **完全数**という。ギリシャの数学において、この数はもっとも美しい数とされ、完全数を見つけるための様々な努力がなされた。

n	n の約数	$\varphi(n)$	
6	1,2,3,6	12	完全数
8	1,2,4,8	15	不足数
12	1,2,3,4,6,12	28	過剰数

では、偶数が完全数になるための条件を考察しよう。

1. $n = 2^k m$ (ただし $k \geq 1$ で m は奇数) が完全数であるとする。
2. $\varphi(n) = (2^{k+1}-1)\varphi(m) = 2n = 2^{k+1}m.$
3. $\varphi(m) = m + \dfrac{m}{2^{k+1}-1}.$
4. 上の式で左辺は整数であるから $2^{k+1}-1$ は m の約数である。
5. $k \geq 1$ より $\dfrac{m}{2^{k+1}-1}$ は m より小さな m の約数であるから、右辺は m の二つの約数の和である。これが約数の総和に等しいのだから m はこの二つの約数しか持たない。

$$m = 2^{k+1}-1, \quad m \text{ は素数.}$$

4.4 メルセンヌの素数

$2^p - 1$ の形の素数を **メルセンヌの素数**という。$2^p - 1$ が素数になるためには p 自身が素数でなければならない。しかし、p が素数であっても $2^p - 1$ が素数になるとは限らない。

メルセンヌの素数が完全数と関わりがあることは前項で述べたが、この形の数は素数か否かの判定が比較的やさしいので大きな素数の発見に利用されている。

p(素数)	2	3	5	7	11	13	17	19
2^p-1	3	7	31	127	2047	8191	131071	524287
判定	素数	素数	素数	素数	23×89	素数	素数	素数
完全数	6	28	496	8128		33550336	8589869056	137438691328

以下、2^p-1 が素数になる事が知られているのは、

$p = 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941,$
$11213, 19937, 21701, 23209, 44497, 132049, 216091, 756839, 859433$

$2^{859433}-1$ は 258690 桁の数で 1993 年に素数であることが証明された。

5 合同式と剰余系

5.1 合同式とその扱い

m を 2 以上の自然数とする。二つの整数 a と b の差が m の倍数である時、 **a と b は m を法として合同であるといい、**

$$a \equiv b \pmod{m}$$

と表す。以下の等式が成り立つ。

命題 6 $a \equiv b \pmod{m}$ かつ $c \equiv d \pmod{m}$ ならば

$$a \pm c \equiv b \pm d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

$p(x)$ を整数係数の多項式とする。$a \equiv b \pmod{m}$ ならば

$$p(a) \equiv p(b) \pmod{m}$$

応用として、倍数の判定法を解説する。

5.2 合同方程式

まず、一次合同方程式

$$ax \equiv b \pmod{m}$$

を考えよう。ただし、a と b は 0 から $m-1$ までの整数を考えれば十分である。

- a と m が互いに素な場合
- b が (a, m) の倍数の場合
- b が (a, m) の倍数でない場合

特に m が素数の場合は

$$a \not\equiv 0 \pmod{m} \Longrightarrow ax \equiv b \pmod{m} \text{ はただ一つの解を持つ。}$$

m が素数の場合、合同式の取り扱いは普通の数の場合とほとんど同じようになる。

- $a \not\equiv 0 \pmod{m}$ ならば $ab \equiv 1 \pmod{m}$ となる b が存在する。
- $ab \equiv 0 \pmod{m}$ ならば a と b の少なくとも一方は 0 と合同

このことから m が奇数の素数であるときは、2 次の合同方程式も同様に解ける。さらに次も証明できる。

定理 5.1 (ウィルソンの定理)
p を 2 以上の自然数とする。

$$p \text{ が素数である} \iff (p-1)! \equiv -1 \pmod{p}$$

この定理は素数の判定には役に立たないが、素数であるための必要十分条件を一つの式で与える唯一のものである。

5.3 中国式剰余定理

「5 で割って 2 余り、7 で割って 3 余り、9 で割って 4 余るような整数を求めよ。」
このような問題は中国で 1 世紀頃に考察されており、中国式剰余定理と呼ばれている。これを定理の形で書けば

定理 5.2 (中国式剰余定理) $m_1, m_2, \cdots, m_n$をどの二つも互いに素な自然数の組とするとき、1 次合同連立方程式

$$\begin{aligned} x &\equiv r_1 \pmod{m_1} \\ x &\equiv r_2 \pmod{m_2} \\ &\cdots \\ x &\equiv r_n \pmod{m_n} \end{aligned}$$

は $M = m_1 m_2 \cdots m_n$ を法としてただ一つの解を持つ。

この方程式の解は、

$$M = m_1 M_1 = m_2 M_2 = \cdots = m_n M_n$$

$$M_k t_k \equiv 1 \pmod{m_k}$$

で、M_k及び t_kを定めることにより

$$x \equiv r_1 M_1 t_1 + r_2 M_2 t_2 + \cdots + r_n M_n t_n \pmod{M}$$

と表せる。

応用　部分分数展開
中国式剰余定理を応用して、52/105 を部分分数に展開できる。この方法を多項式の世界で行えば、有理関数の不定積分の計算に応用できる。