自然科学研究のための
整数論入門

2020 年 11 月 2 日

目次

1　はじめに

数の概念は、数学という学問の出発点に位置するものであるが、それゆえに最も困難な対象でもある。典型的な例はゴールドバッハ予想である。『偶数は２つ（以上）の素数の和でかける』こんなバカみたいにみえることが証明できない。宇宙がおわっても素数は汲み尽くせないといったことと関係しているのかもしれない。素数分布公式なるがあるが、たとえ、宇宙が存在する時間内に、１０の１０の１０の１０乗の桁で素数を確定することはできないかもしれない。実数全体という漠としたものとちがって、目の前に具体的数としてみせて意味があるというのが素数である。ここまでくると、認識論の問題になるかもしれない。

中学生にでもわかるものがなぜ何百年も解決しないのかこれが数学者を悩ませてきた。ある問題はきわめて簡単に解けるのに、隣あった問題は、もう同じやり方が使えないという不規則さになんとか理論づけようと、過去の数学者は努力してきたのであろう。

この講義では、数の現象を物理現象となぞらえて説明する試みをやってみたい。

なにごとによらず、学問というのは、事実の蒐集をもとにしているが、それのよって来る筋道あるいは理屈があるはずである。（実はないかもしれないが）さいわい、物理学には、これまでのところ一応の筋道がある。これが理論といわれるものである。力学、電磁気学、統計力学、量子力学。。。。これらは小数の基本原理、あるいは方程式から出発した入り込んだ構造体といえる。

数学は一見散発的な定理の集積のようにみえるが、そのように思わせるのは、社会背景あるいは教育のせいであろう。単に学校数学で技巧としてだけ教え込むと、脈絡なしにやることになる。そうすると、自分のなけなしの技巧だけで、難問に挑むことになる。あるいは、技巧だけを磨くことになる。

数学を少し気をつけて勉強すれば、小数の基本原理から構成された理論形式の構造体であることがうっすらとでも感得できるようになるであろう。

そして、一定の過程を踏むことにより、（じつは、かなりの時間と忍耐と修練を必要とするが)、たとえば、リーマン幾何、トポロジー、リー群（連続群）論などのように物理において直接関係すると思わせる極めて高度な内容を含む理論構造体であることが、個人の理解のレベルに応じて、わかる仕組みになっていると思う。

整数の理論に筋道をつけるとすれば、いったいなにかというと、やはり、『素数の概念』というもので、素数によって「ある程度」特徴ずけられるのではないか。力学の運動法則あるいは量子力学の重ね合わせの原理に対応するものとして?! 。

さしあたり、基本方針として、素数に関する特徴づけから出発して理論構成を行けるのではないか。

初等整数論は、有理整数に関する現象を扱うが、これの最終目的として、通常の行程に従って,『ガウスの平方剰余の相互律』の証明でひとくくりとしたい。それより上に進むと、いわゆる、代数体の話しに入る. 平方剰余の相互法則は、初等整数論で閉じない理由が隠されていて、それが代数体における素因数分解の真実を記述していることがわかる. これについても、簡単にふれたい。

2　整数論と物理学

『素数は幾何学』である。『幾何学は物理である』。ゆえに、素数は物理である？？ これは、整数論学者の小野孝教授の言われていることの受け売りである。

ある特定の問題を解くために、学問が発展する。

唐突に思えるが、数の全体というものを考える。これに対応する物理の対象としては、なんであろうか。

質点の描く閉じた軌跡（閉曲線＝閉軌道) の集合というものが考えられる。これは、結び目とも関連する。これは、数を代数方程式の根に限定したとき、つまり、それに対応したものとして、微分方程式（運動方程式）の解（軌道）が対応しているとみられるないこともない。

素数との関連で考えると, 素なる軌道と、それを何回か繰り返した軌道が考えられるが、それは、合成数とみられる。

素数の情報をひとつにまとめて内包した関数がある。これが、ゼータ関数である。それは、すこし変わった級数で書かれる：

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

ここで、s は複素変数で、級数が収束するためには, $\mathrm{Re}s > 1$ という制限がつく。このように、s の複素関数としてとらえたのが、リーマンであるがそのもとをたどれば、オイラーまで遡るようである。

素数が内蔵されていることは、これを素数分解

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots$$

に注意して、

$$\frac{1}{n^s} = \left(p_1^{-s}\right)^{\alpha_1} \left(p_2^{-s}\right)^{\alpha_2} \cdots$$

から、

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{\alpha_1=0}^{\infty} \sum_{\alpha_2=0}^{\infty} \cdots \left(p_1^{-s}\right)^{\alpha_1} \left(p_2^{-s}\right)^{\alpha_2} \cdots \tag{2.1}$$

と変形して、等比級数を計算すると

$$\zeta(s) = (1 + p_1^{-s} + p_1^{-2s} + \cdots) \times (1 + p_2^{-s} + p_2^{-2s} + \cdots) \times \cdots = \prod_p \frac{1}{\left(1 - p^{-s}\right)} \quad (2.2)$$

と書ける。これが、有名なオイラー積である。

3　整除および素因数分解

記号について。

以下でててくる文字は原則的に有理整数をあらわす。また、慣例に従い, ことわりのない限り, p は, 素数をあらわす.

3.1　整数に関する初等例

例 1: $2x+3y=1$ の整数解をすべて求めよ。

解：まず、これは解があることはメノコでわかる。$x=-1,\ \ y=1$ である。そこで、ひとつの解を (x_0,y_0) とすれば、$2x+3y=2x_0+3y_0$ となり,

$$2(x-x_0)=-3(y-y_0)$$

となり, 2 と 3 は互いに素であるから、

$$x-x_0=3t, y-y_0=-2t$$

とあらわせる。ただし、t は任意の整数である。これから、一般解として

$$x=x_0+3t,\ \ y=y_0-2t$$

と書ける。

例 2: $\sqrt{2}$ は無理数であることを証明せよ.

これは例 1 より複雑な思考例である。

証明：有理数であると仮定する。すなわち、$\sqrt{2}=\frac{p}{q}$ であるとせよ。ここで、p,q は互いに素なる整数である。もちろん正である。そこで、２乗すると,

$$p^2=2q^2$$

p は q と素であるから、p^2 は偶数である。さらに、こうなるためには、p 自身が２の倍数でなければならない；$p=2p'$ ゆえに、$q^2=2p'^2$ が成立する. おなじ論法で、$q=2q'$

ところが、これは、p, q が既約であると言う仮定と矛盾する。ゆえに、$\sqrt{2}$ は有理数ではない。

ある数が、別の数で割りきれるかということが、数について学校で数をならうときの出発点になる。 これをいいかえれば、ある数を分解するという考えにいきつく。

$$6 = 2 \times 3, \quad 15 = 3 \times 5, 60 \cdots$$

このようにながめると、すぐに気がつくことは、これ以上分解されないところまで到達する。この最終の分解が素因数分解で、その分解のなかの各要素が、素数になる。「素数とは、1 と自身以外に素因数をもたない数」と規定できる。

うえの２つの例でも、素数の特質が使われている。じつは、この定理は、昔昔のことであるが、高校一年生の数学で出てきたのであるが、これがさっぱりと理解できなかったと記憶する。普通の高校生がやるにはちょっと無理があったのだろう。

- 素数分解と一意生.

これは, つぎの原則からくる。

「2 整数 a, b の積 ab が c で割り切れると、a か b のいずれかが c でわりきれる. 」

整数 N を素数分解すると、ただひととおりの形で、$N = p_1^{\alpha} p_2^{\beta} \cdots p_n^{\omega}$ とあらわされる。ここで、『ただひとおりで』ということが重要である。

素数が無限個あるという事実は基本的である。これは証明を要することであるが、それほどむずかしいものではない。ここで、無限個というのは深刻である。宇宙が終わっても、これを汲み尽くす（全部列挙する）ことはできないのである！！

これを、実数が数直線で幾何学化できるのとは少しことなる。しかし、素数もある意味での幾何学化する試みはあるらしい。

さて、初等整数論とは**有理整数に関する現象**を扱う学問である。ここで、重要な観点は、２つの数のあいだの相対的関係である。

共通の因数をもつかもたないか。「もたない」とき、これら、2 数 (a, b としよう）は、「互いに素」とよばれ、(つまり、他人の関係)

$$(a, b) = 1$$

と表現する。

もしもつとすれば、それをいかに求めるか。

3.2　ユークリッド互除法

2 つの整数の最大公約数の求め方のアルゴリズムは次のようになる。

定義 a と b の最大公約数

$a > b$ のとき

$$(a, b) = (a \text{ と } b \text{ の最大公約数}) \tag{3.1}$$

$$(a, b) = 1 \Longrightarrow \text{“互いに素”} \tag{3.2}$$

原則:a が b で割り切れるときは

$$a = bq \Longrightarrow b \text{ は最大公約数} : (a, b) = b \tag{3.3}$$

である。一般に $a = bq + r,\ b > r(r \text{ は余り})$ と表すことが出来る。

定理

$$(a, b) = (b, r) \tag{3.4}$$

[証明]

$(a, b) = d$ とすると

$$\begin{aligned} a &= da' \\ b &= bb' \\ \therefore\ da' &= db'q + r \\ \therefore\ r &= d(a' - b'q) \end{aligned}$$

よって r は d で割り切れるので

$$(b, r) = d$$

[証明終]

例としては (126,86) を考えると

$$\begin{aligned} 126 &= 86 \times 1 + 40 \\ 86 &= 40 \times 2 + 6 \\ 40 &= 6 \times 6 + 4 \\ 6 &= 4 \times 1 + 2 \end{aligned}$$

となる。

$$\left.\begin{array}{l} a = bq_1 + r_2 \quad 0 < r_2 < b \\ b = r_2 q_2 + r_3 \quad 0 < r_3 < r_2 \\ r_2 = r_3 q_3 + r_4 \\ \cdots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n \quad 0 < r_n < r_{n-1} \\ r_{n-1} = r_n q_n \quad r_{n+1} = 0 \end{array}\right\} \tag{3.5}$$

ただし、$0 < r_n < r_{n-1} < \cdots < r_2 < b$ で、減少数列で b より多くの項を含まない。

$$\therefore r_n \text{が最大公約数} \tag{3.6}$$

3.3　連分数との関係

ユークリッド互除法は**連分数**に関連する。そこで、これについて述べる。

$$\sqrt{2} = 1 + (\sqrt{2} - 1), \quad \text{“第 1 項目の 1 は整数部分”} \tag{3.7}$$

一般に無理数：$\alpha = n + (\alpha - n),\ n = [\alpha] \leftarrow$ ガウス記号

$$\begin{aligned} x &= \frac{1}{1+x} \\ x_n &= \frac{1}{1+x_{n-1}}, \quad x_n = f(x_{n-1}) \end{aligned}$$

ここで $n \to \infty$ とすると

$$\begin{aligned} x_0 &= 1 \\ x_1 &= \frac{1}{1+1} \\ x_2 &= \frac{1}{1+\frac{1}{1+1}} \\ x_3 &= \frac{1}{1+\frac{1}{1+\frac{1}{1+1}}} \end{aligned}$$

ここで (3.5) に於いて

$$\left.\begin{array}{l} \frac{a}{b} = q_1 + \frac{r_2}{b} \\ \frac{b}{r_2} = q_2 + \frac{r_3}{r_2} \\ \frac{r_2}{r_3} = q_3 + \frac{r_4}{r_3} \\ \cdots \\ \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}} \\ \frac{r_{n-1}}{r_n} = q_n + 0 \end{array}\right\} \tag{3.8}$$

となるので

$$\begin{aligned} \therefore \frac{a}{b} &= q_1 + \frac{1}{q_2 + \frac{r_3}{r_2}} \\ &= q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{r_4}{r_3}}} \cdots \end{aligned} \tag{3.9}$$

となる。

有理数の連分数表示は有限項で終わる。

予測として

$$\frac{a}{b} = \frac{f(q_1, \cdots, q_n)}{g(q_1, \cdots, q_n)} \tag{3.10}$$

の形になる。

定義 用語

$$q_1, \cdots, q_i, \cdots : \text{部分商} \tag{3.11}$$

$$\delta_1 = q_1, \delta_2 = q_1 + \frac{1}{q_2}, \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}} \tag{3.12}$$

を**近似分数**と呼び、δ_s は q_{s-1} を $q_{s-1} + \frac{1}{q_s}$ に置き換えて得られる。

$$\delta_1 = \frac{q_1}{1}, \delta_2 = \frac{q_1 + \frac{1}{q_2}}{1} = \frac{q_1 q_2 + 1}{q_2 \cdot 1 + 0}$$

ここで $P_0 = 1, Q_0 = 0$ かつ $P_1 = q_1, Q_1 = 1$ とおくと

$$\delta_1 = \frac{P_1}{Q_1}, \delta_2 = \frac{q_2 \cdot P_1 + P_0}{q_2 \cdot Q_1 + Q_0} = \frac{P_2}{Q_2}$$

と表すことが出来る。

ここで s までの部分商は

$$\delta_s = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}} = \frac{P_s}{Q_s} \tag{3.13}$$

となる。

$$\begin{cases} P_s &= q_s P_{s-1} + P_{s-2} \\ Q_s &= q_s Q_{s-1} + Q_{s-2} \end{cases} \tag{3.14}$$

ただし初期条件は $P_0 = 1, P_1 = q_1, Q_0 = 0, Q_1 = 1$ である。

定理

$$\delta_s - \delta_{s-1} + \frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{h_s}{Q_s Q_{s-1}} \tag{3.15}$$

$$h_s = P_s Q_{s-1} - Q_s P_{s-1} \tag{3.16}$$

$$h_s = -h_{s-1} \tag{3.17}$$

(i)　$$P_s Q_{s-1} - P_{s-1} Q_s = (-1)^s \tag{3.18}$$

(ii)　$$\delta_s - \delta_{s-1} = \frac{(-1)^s}{Q_s Q_{s-1}} \tag{3.19}$$

$s = n$ が last なので

$$\frac{a}{b} = \frac{P_n}{Q_n} \tag{3.20}$$

4　剰余類とオイラーの関数

4.1　合同式

合同式の概念は, 整数論において決定的である. それは, 以下にみられる通り, おなじ余りを出す一連の数は, 「ひとつに」みなすというとく単純な考え方にもとづく. このように単純な見方が, 高等整数論においても引き継がれていく.

定義

$$a \equiv b \pmod{m} \Longleftrightarrow a - b = mt \tag{4.1}$$

これは剰余系 (あるいは類) をあたえる. つまり、m でわった余りが, その類を代表する. それを, バーをうえにつけて, $\bar{a}$ と記す. そうすると, 合同記号はふつうの等式になる.

$$\bar{a} = \bar{b} \Longleftrightarrow a \equiv b \pmod{m} \tag{4.2}$$

である。

例.$m = 7$ の場合、

$$\bar{a} = (0, 1, 2, 3, 4, 5, 6)$$

ですべての整数を分類できる. 類の中で計算 (和、積)

$$\bar{a} + \bar{b},\ \bar{a}\bar{b}$$

和の計算例.

$$\bar{3} + \bar{5} = \bar{1}$$

の計算は

$$\begin{cases} \bar{3} = 3 + 7t \\ \bar{5} = 5 + 7s \end{cases}$$

より、

$$\bar{3} + \bar{5} = (3 + 7t) + (5 + 7s) = 8 + 7(t + s) = 1 + 7 \times \cdots = \bar{1}$$

となる。

積の計算例.

$$\bar{3} \times \bar{5} = \bar{1}$$

の計算は

$$\bar{3} + \bar{5} = (3 + 7t) \times (5 + 7s) = 15 + 21s + 35t + 49ts = \bar{1}$$

となる。

以上の考えは、整数全体を m 個の類に分ける

- 類の代表

$$(0, 1, 2, \cdots, m-1) \tag{4.3}$$

- 既約類 (reduced)
  特に、m と素な数のみから成る類を既約類とよぶ。

4.2　類の考え方とオイラーの関数

定義 オイラーの関数

$1 \sim n$ までの数で n と素な数の個数 $\phi(n)$。

例 1. $n = 10$ の場合
1,2,3,4,5,6,7,8,9,10 の中で 10 と素な数は'1,3,7,9' なので

$$\phi(10) = 4$$

例 2. $n = 7$ の場合
1,2,3,4,5,6,7 の中で 7 と素な数は'1,2,3,4,5,6' なので

$$\phi(7) = 6$$

$n = p$: 素数 のとき

$$\phi(p) = p - 1 \tag{4.4}$$

$n = 70 = 7 \times 10$ なので

$$\phi(70) = 24 = \phi(7) \times \phi(10)$$

となる。一般に $(a,b)=1$ のとき

$$\phi(a,b)=\phi(a)\times\phi(b)$$

となる。これは**乗法関数**になっている。

定理 乗法関数

m,n が互いに素である場合、

$$\phi(m,n)=\phi(m)\times\phi(n) \tag{4.5}$$

m,n が互いに素 $\Longleftrightarrow (m,n)=1$ になる。このとき $mx+ny=1$ は必ず解をもつ。

$$(m,n)\neq 1\text{のとき } mx+ny=1 \text{ は解をもたない。} \tag{4.6}$$
$$(m.n)=d\text{のとき } mx+ny=d \text{ なら解をもつ。} \tag{4.7}$$

$\{mx+ny\}$ は任意の整数に対応。

$mx'+ny'=1$ なる x',y' に対して、$x=kx', y=ky',\ (k\in z)$ とおくと $mx+ny$ は 1 の k 倍、つまり全整数とれる。

[証明]

m,n が互いに素であるとき $(m,n)=1$ となる。このとき、$mx+ny=1$ は必ず解をもつ。[*1] [証明終]

4.3　乗法性の証明

合同式 $a\equiv b\pmod m$：$a=b+mt$ を満たす a,b (周期 m) $\to m$ を与えると m コの『類』が出来る。

既約類：m とお互いに素である数のみ含む類

$\{my+nx\}$ を考える。ここでは m と n を交換した x,y で類をつくることが重要。

$$x=1,2,\cdots,m \tag{4.8}$$
$$y=1,2,\cdots,n \tag{4.9}$$

[*1] $(m,n)\neq 1$ のとき $mx+ny=1$ は解をもたない
$(m,n)=d$ のとき $mx+ny=d$ なら解をもつ

(x, y) の組み合わせは mn コ存在する。m, n に対して mn コの類がつくられる。

> $\{my + nx\}$ と mn との既約数を考えると
>
> $\Leftrightarrow \{my + nx\}$ から mn と共通因数を持つものを除く
> $\Leftrightarrow x$ が m と共通因数をもつもの or y が n と共通因数をもつものを除く。

こうして得られた既約数 $\{\bar{m}, \bar{n}\}$ に対して、

$$\begin{cases} x & : m \text{ と共通因数をもたない数} \\ y & : n \text{ と共通因数をもたない数} \end{cases} \tag{4.10}$$

を用いて $\{\bar{m}y + \bar{n}x\}$ を考えると、この集合の要素は mn と共通因数[*2] をもたない。このような集合の要素数は $\phi(m) \times \phi(n)$ コである。ゆえに、

$$\phi(mn) = \phi(m)\phi(n) \tag{4.11}$$

である。

「x に m と既約なもの」と「y に n と既約したもの」を代入したとき、$my + nx$ が mn と既約になる。

[証明] !!! 説明が必要? !!!

$$(x, m) = 1,\ (y, n) = 1$$
$$(my + nx, m) = (nx, m) = 1$$
$$(my + nx, n) = (my, n) = 1$$

以上から

$$(my + nx, mn) = 1 \tag{4.12}$$

[証明終]

[*2] 集合の要素は $\phi(mn)$

5　整数論的関数の演算子手法

整数論的関数には**オイラーの関数**と**メビウスの関数**がある。

5.1　メビウスの関数

定義

以下の性質をもつ関数をメビウス関数という:
$n = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdots$: 素因数分解 とすると、

- $n = 1$ ならば $\mu(1) = 1$
- n が素数の平方で割り切れるとき、$\mu(n) = 0$
- n が相異なる素数の k 個の積ならば、$\mu(n) = (-1)^k$

5.2　たたみ込み積 (convolution)

$f(n), g(n)$ について $n \in \boldsymbol{Z}$ とする。

定義 たたみ込み積

$$(f \otimes g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \Leftrightarrow (f * g)(x) = \int_0^x f(y) g(x-y) dy \qquad (5.1)$$

ここで $d|n = d$ は n の約数、$\sum_{d|n}$: n の約数である d のすべての和 である。

有用性：$f \otimes g = h$ となると、f が解ける.

$$\begin{aligned} f &= h \otimes g^{-1} \\ f(n) &= (h \otimes g^{-1})(n) \\ &= \sum_{d|n} h(d) g^{-1}\left(\frac{n}{d}\right) \end{aligned}$$

例としてオイラー関数 $\phi(n)$ を挙げると

$$\sum_{d|n} \phi(d) = \sum_{d|n} 1 \cdot \phi(d) = n$$

という性質がある。

$$\phi(n) = (\epsilon^{-1} \otimes \nu)(n) \leftarrow \nu と \epsilon は可換 \tag{5.2}$$

$$\therefore \phi(n) = \sum_{d|n} \mu(d)\nu(\frac{n}{d}) \tag{5.3}$$

$$もしくは、\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} \tag{5.4}$$

5.3　$f \otimes g$ の性質

まず一つ目の性質として、

可換律

$$f \otimes g = g \otimes f \tag{5.5}$$

がある。

[証明] $f \otimes g = g \otimes f$ の証明

$$\begin{aligned}(f \otimes g)(n) &= \sum_{d|n} f(d)g(\frac{n}{d}) \\ &= \sum_{d,d'=n} f(d)g(d') \\ &= \sum_{d',d=n} f(d')g(d) \\ &= \sum_{d|n} g(d)f(\frac{n}{d}) \\ &= (g \otimes f)(n)\end{aligned}$$

$$\therefore\ f \otimes g = g \otimes f\ \ (可換) \tag{5.6}$$

[証明終]

次の性質として、

結合律

$$(f \otimes g) \otimes h = f \otimes (g \otimes h) \tag{5.7}$$

がある。

[証明] $(f \otimes g) \otimes h = f \otimes (g \otimes h)$ の証明

$$\begin{aligned}
[(f \otimes g) \otimes h](n) &= \sum_{ld''=n} (f \otimes g)(l) h(d'') \\
&= \sum_{ld''=n} \left[\sum_{dd'=l} f(d) g(d') \right] h(d'') \\
&= \sum_{dd'd''=n} f(d) g(d') h(d'') \\
&= \sum_{dm=n} f(d) \sum_{d'd''=m} g(d') h(d'') \\
&= f \otimes (g \otimes h)
\end{aligned} \tag{5.8}$$

[証明終]

5.4　逆元 f^{-1}

逆元は $f \otimes f^{-1} = e$ となる f^{-1} である。

定義 e の定義

$$e(1) = 1, e(n) = 0 \quad (n \geq 2) \tag{5.9}$$

これはクロネッカー δ の類似、または δ 関数の類似となる。

定義

$$\begin{cases} \epsilon\text{関数} & \cdots \epsilon(n) = 1, \quad \text{for all } n \\ \nu\text{関数} & \cdots \nu(n) = n, \quad \text{for all } n \end{cases} \tag{5.10}$$

また ϵ, ν は乗法的である。

定理

e を積 $\otimes$ に関する単位元とすると、

$$e \otimes f = f \tag{5.11}$$

[証明]

$$(e \otimes f)(n) = \sum_{d|n} e(d) f(\frac{n}{d}) = f(n) \tag{5.12}$$

[証明終]

定理 f に対して f^{-1} が存在するための条件

整数論的関数 f に対して、整数論的関数 f^{-1} が存在するための必要十分条件は $f(1) \neq 0$

- **定理の証明**:

まず証明すべき事実は、$f \otimes f^{-1} = e$ となる f^{-1} が定義できる必要十分条件は、$f(1) \neq 0$ となることである。

[証明]

必要なことは $\otimes$ の定義に従って

$$(f \otimes f^{-1})(n) = \sum_{d/n} f(d) f^{-1}\left(\frac{n}{d}\right) = e(n) \tag{5.13}$$

と表される。ここで、$n = 1$ を代入すると、$f(1)f^{-1}(1) = e(1) = 1$ となることから明らかである。

逆に、$f(1) \neq 0$ として、f^{-1} を次のように定義する。まず、

$$f^{-1}(1) = \frac{1}{f(1)} \tag{5.14}$$

とおき、次に、$m < n$ である自然数に対して、$f^{-1}(m)$ が定義されたとして、$f^{-1}(n)$ を

以下のように定義する

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{d>1:d/n} f(d) f^{-1}\left(\frac{n}{d}\right) \tag{5.15}$$

となる。これから、

$$-\frac{1}{f(1)} \sum_{d/n} f(d) f^{-1}\left(\frac{n}{d}\right) = -\frac{f(1)}{f(1)} f^{-1}(n) - \frac{1}{f(1)} \sum_{d>1:d/n} f(d) f^{-1}\left(\frac{n}{d}\right) \tag{5.16}$$

となる。これは、$-f^{-1}(n) + f^{-1}(n) = 0$ すなわち

$$\sum_{d/n} f(d) f^{-1}\left(\frac{n}{d}\right) \tag{5.17}$$

つまり、

$$(f \otimes f^{-1})(n) = e(n) \tag{5.18}$$

が成り立ち、これですべての自然数 n に関して f^{-1} が定義されて $f \otimes f^{-1} = e$ となる。
[証明終]

定理

乗法的整数論的関数全体は $\otimes$ 積に関して閉じている。
$\Longrightarrow$ $\otimes$ **積に関して閉じている**とは、一般の整数論的関数全体 G(G は群) の部分集合となる。

この定理の証明するべき点は次の点である。

- f, g が乗法的

$$f(m,n) = f(m)f(n) \tag{5.19}$$
$$g(m,n) = g(m)g(n) \tag{5.20}$$

とすれば (但し、$(m,n) = 1$ で m, n は互いに素)、

$$(f \otimes g)(m,n) = f \otimes g(m),\ f \otimes g(n) \tag{5.21}$$

となる。

[証明]

$$
\begin{aligned}
(f\otimes g)(m,n) &= \sum_{d|(mn)} f(d)g\left(\frac{mn}{d}\right) \\
&= \sum_{m'|m,n'|n} f(m'n')g\left(\frac{mn}{m'n'}\right) \\
&= \sum f(m')f(n')g\left(\frac{m}{m'}\right)g\left(\frac{n}{n'}\right) \\
&= \sum_{m'|m} f(m')g\left(\frac{m}{m'}\right) \times \sum_{n'n} f(n)g\left(\frac{m}{n'}\right) \\
&= (f\otimes g)(m)\cdot(f\otimes g)(n) \\
\therefore\ (f\otimes g)(mn) &= f\otimes g(m)\cdot f\otimes g(n) \qquad (5.22)
\end{aligned}
$$

となり、$f\otimes g$ も乗法関数である。[証明終]

- f^{-1} も乗法的である。[*3]

$$f^{-1}(mn) = f^{-1}(m)\cdot f^{-1}(n) \qquad (5.23)$$

定理

$$\epsilon^{-1} = \mu \quad (\mu:\text{メビウス関数}) \qquad (5.24)$$

証明の方針は、$\epsilon\otimes\mu = \mu\otimes\epsilon = e$ となることを示せば良い。書き換えると、

$$
\begin{aligned}
(\mu\otimes\epsilon)(n) &= \sum_{d|n}\mu(d)\epsilon(\frac{n}{d}) \\
&= \sum_{d|n}\mu(d) = e(n) \qquad (5.25)
\end{aligned}
$$

を示せば良いことになる。

$$\sum_{d|n}\mu(d) = \begin{cases} 1 & (n=1) \\ 0 & (n>1) \end{cases} \qquad (5.26)$$

を示す。

[証明] (5.26) の証明

[*3] 証明は別途掲載

$n = p_1^{\alpha_1} p_2^{\alpha_2}$ は素因数分解できるとする。k を素数の数とすると

$$\begin{aligned}\sum_{d|n} \mu(d) &= 1 + \sum \mu(p_i) + \sum \mu(p_i, p_j) + \sum \mu(p_i, p_j, p_k) + \cdots \\ &= 1 - k + \binom{k}{2} - \binom{k}{3} + \binom{k}{4} \\ &= (1-1)^k = 0 \end{aligned} \tag{5.27}$$

$$0 = (1-1)^k \sum_{i=0}^{k} {}_kC_i (-1)^i \tag{5.28}$$

による。[証明終]

- **Dedenkind の反転公式**

公式 Dedenkind の反転公式

$$\sum_{d|n} f(d) = g(n) \text{ の時、}$$
$$f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}) \tag{5.29}$$

たたみ込みの積の形

$$\epsilon \otimes f = g \tag{5.30}$$

但し、$\epsilon(n) = 1$ for all n である。形式的に $f = \epsilon^{-1} \otimes g$ とする。$\epsilon^{-1} \equiv \mu$: メビウス関数から

$$f = \mu \otimes g$$
$$\therefore \ f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$$

なので $\epsilon \otimes \mu = e$ となることが証明できれば良いことになる。[*4]

$$\begin{aligned}(\epsilon \otimes \mu)(n) &= \sum_{d|n} \epsilon(d)\mu\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu\left(\frac{n}{d}\right)\end{aligned}$$

ここで定理

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) = \begin{cases} 1 & (n=1) \\ 0 & (n>1) \end{cases}$$

から、

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) = e(n) \tag{5.32}$$

$$\therefore\ (\epsilon \otimes \mu)(n) = e(n) \tag{5.33}$$

$$\therefore\ \epsilon \otimes \mu = e \tag{5.34}$$

となる。

定理

$$\sum_{d|n} \phi(d) = n \tag{5.35}$$

[証明]

$\phi(ab) = \phi(a)\phi(b)$ をもとにする。準備定理: 乗法関数 θ の一般公式

$$\theta(ab) = \theta(a)\theta(b) \tag{5.36}$$

[*4]

$$e(n) = \begin{cases} 1 & (n=1) \\ 0 & (n>1) \end{cases} \tag{5.31}$$

を思い出すこと

$a = P_1^{\alpha_1} + P_2^{\alpha_2} + \cdots + P_k^{\alpha_k}$ と素因数分解できるとする。

$$\begin{aligned}\sum_{d|n} \theta(d) &= \sum_{\beta_1=0}^{\alpha_1} \cdots \sum_{\beta_k}^{\alpha_k} \theta(P_1^{\beta_1} P_2^{\beta_2} \cdots P_k^{\beta_k}) \\ &= \left(\sum_{\beta_1=0}^{\alpha_1} \theta(P_1^{\beta_1}) \cdots \sum_{\beta_k=0}^{\alpha_1} \theta(P_k^{\beta_k}) \right) \\ &= (1 + \theta(P_1)\theta(P_1^2) + \cdots \theta(P_1^{\alpha_1})) \times (\cdots) \\ &\quad \times \cdots \times (1 + \theta(P_k)\theta(P_k^2) + \cdots \theta(P_k^{\alpha_k}))\end{aligned}$$

$\theta = \phi$ に適応する。

$$\phi(P^\alpha) = P^\alpha - P^{\alpha-1}$$

を使うと、

$$\begin{aligned}&1 + \phi(P_1) + \phi(P_1^2) + \cdots + \phi(P_1^{\alpha_1}) \\ =&1 + P_1 - 1 + P_1^2 - P_1 + \cdots + P_1^{\alpha_1} - P_1^{\alpha_1 - 1} \\ =&P_1^{\alpha_1}\end{aligned}$$

$$\therefore \sum_{d|n} \phi(d) = P_1^{\alpha_1} P_2^{\alpha_2} \cdots P_k^{\alpha_k} = n \tag{5.37}$$

[証明終]

定理

$$\sum_{d|n} \phi(d) = n \text{ のとき}$$

$$\phi(n) = \sum_{d|n} \mu(d)(\frac{n}{d}) \tag{5.38}$$

[証明]

Dedenkind 反転公式を適用すると

$$\sum_{d|n} \phi(d) = n \Longrightarrow (\epsilon \otimes \phi)(n) = \nu(n)$$

ただし、定義 $\nu(n) = n$ for all n とする。$\epsilon \otimes \phi = \nu$ より

$$\begin{aligned} \phi &= \epsilon^{-1} \otimes \nu = \mu \otimes \nu \\ \therefore\ \phi(n) &= \sum_{d|n} \mu(d)(\frac{n}{d}) \end{aligned} \tag{5.39}$$

[証明終]

問題

$\phi(a) = \sum_{d|n} \mu(d)\frac{a}{d}$ を用いて

$$\phi(ab) = \phi(a)\phi(b) \tag{5.40}$$

を証明せよ。
また、このために $a = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ として、

$$\phi(a) = a\left(1 - \frac{1}{P_1}\right)\left(1 - \frac{1}{P_2}\right)\cdots\left(1 - \frac{1}{P_k}\right) \tag{5.41}$$

を示せ。

5.5　ディリクレ級数への応用

整数論的関数 $f(n)$ に対して、つぎで定義される級数を考える：

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

を考える。 とくに, $f(n) = \epsilon(s)$ $(\epsilon(n) = 1 \ \ (\text{for} \ \ \text{all} \ n)$ のときは,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{\epsilon(n)}{n^s} \equiv \sum_{n=1}^{\infty} \frac{1}{n^s}$$

すなわち、リーマンのゼータ関数になる。

ここで、このような整数論的関数を係数とするディリクレ級数の通常の積を考える：

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \sum_{m=1}^{\infty} \frac{g(s)}{m^s}$$

これは、

$$F(s)G(s) = \sum_{n,m=1}^{\infty} \frac{f(n)g(m)}{(nm)^s} = \sum_{N=1}^{\infty} N^{-s} \sum_{nm=N} f(n)g(m) = \sum_{N} \frac{[f \times g](N)}{N^s}$$

とかける。つまり、ちょうど、$\otimes$ 積が、ディリクレ級数の係数としてあらわれることになり、いろいろなところで便利な関係式である。

いくつかの例をあげよう。

例 1: オイラーの関数 $\phi(s)$ に対して

$$\sum_{n=1} \frac{\phi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$$

[証明] 整数論的関数の性質：$[\phi \times \epsilon](s) = \nu(s)$, かつ $\nu(n) = n$ $(\text{for} \ \ \text{all} \ n)$ をつかうと

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s} = \sum_{n=1}^{\infty} \frac{[\epsilon \times \phi](n)}{n^s} \sum_{n=1}^{\infty} \frac{\nu(s)}{n^s} = \sum_{n=1} \frac{1}{n^{s-1}} = \zeta(s-1)$$

[証明終]

例 2:

$$\prod_p (1-p^{-s}) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

ただし、 p は素数をあらわす. $\prod_p$ はすべての素数にわたる無限積をあらわす.

[証明] まず、無限積は、ゼータ関数のオイラー積表示

$$\prod_p \frac{1}{1-p^{-s}} = \sum \frac{1}{n^s}$$

から、左辺は $\frac{1}{\zeta(s)}$ となることに注意する。かつ、

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{\epsilon(n)}{n^s}$$

から、整数論的関数の積公式： $[\epsilon \times \mu] = e$ を用いると

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{n=1}^{\infty} \frac{[\epsilon \times \mu](n)}{n^s} = 1$$

[証明終]

このように、一見手がでないような関数等式が、畳み込み積という技を使うと手もなくでてくるというのは、整数論の不思議にあるかもしれない。

[コメント] ：ゼータ関数は物理でもあらわれる不思議な関数である。典型的なものとして、黒体輻射の統計力学の分配関数の計算にでてくる積分

$$Z = \int_0^{\infty} \frac{x dx}{\exp[x] - 1}$$

を例示する。これは次のように計算される：

$$\sum_{n=1} \int_0^{\infty} x \exp[-nx] dx = \sum_{n=1} \frac{1}{n^2} \int_0^{\infty} t \exp[-t] dt = \zeta(2)\Gamma(2)$$

ここで、

$$\zeta(2) = \frac{\pi^2}{6}$$

に注意すると,

$$\sum \frac{1}{n^2} = \prod_p \frac{1}{1-p^{-2}} = \frac{\pi^2}{6}$$

この式から素数が無限個あるという事実がでてくる。なぜなら、有限個であれば、有限の積は、無理数にならないからである。これは、ゼータ関数というものが素数の情報を内包しているという事実の極々ささやかな兆候であるといえよう。

5.6　オイラー関数の整数論的等式の証明

定義

$$\sum_{d/n} \phi(d) = n \tag{5.42}$$

ここでは乗法性 $\phi(ab) = \phi(a)\phi(b)$ for $(a, b) = 1$ をつかった式変形による証明でなく、直接証明するものを二つ挙げます。

これは高木貞治の原則である「定義式から強引に圧出しないで、意味を十分練ってかかるとおのずと答えが出てくる」の典型的なものとなっています。

その 1. 高木初等整数論にもとづく証明

準備: 方針は n の約数 (n と 1 自身を含める) を n との最大公約数にもつ数によって分割するというところにある。そこで準備として以下のことを示しておく。

“余” 約数: 約数 d_1 に関して、$d\tilde{d} = n$ となる $\tilde{d}$ なるものをいう。これは行列式の余因子と少々似ている。これから

定理 余約数

$$\sum_{\tilde{d}/n} \phi(\tilde{d}) = \sum_{d/n} \phi(d) \tag{5.43}$$

つまり、約数の全体に関する和と余約数の全体に関する和は一致するということができる。これは直感的に納得できると思う。

以下の証明の鍵はこの余約数に関する等式を証明するところにある。

[**証明**] 高木初等整数論にもとづく証明

$x = (1, 2, \cdots, n)$ とならべて、これらの n 個の数 x を、それが約数 d を n と最大公約数をもつものでソートしてみる。そのような x の数は、x のなかで $x = dx'$ かつ $n = dn'$ とおいたときに、x' と n' が互いに素、記号で書けば、$(x', n') = 1$ となる x' の個数と

行っても良い。ここで x' がきまると x がただひとつ決まることに注意しよう。「この事実が約数 d に対して重複がないことを保証する」ことになる。つまり、$1 \sim n$ までのどれかひとつの x が対応するのである。つまり、1 対 1 の原則である。ここで、だめ押しの注意がある。それは x' は当然のことながら $x' = 1 \sim n'$ となる。それゆえに、この個数は $\phi(n') = \phi(\frac{n}{d})$ となる。そこで、すべての約数: $d_1 \equiv 1, d_2, \cdots d_k \equiv n$ に対して、$\phi(\frac{n}{d_i}) \equiv \phi(\tilde{d_i})$ をつくって和をとると、

$$n = \sum_{d/n} \phi(\frac{n}{d}) \equiv \sum_{\tilde{d}/n} \phi(\tilde{d}) \tag{5.44}$$

となる。

これは、いいかえれば、n この数を上のような最大公約数で分離したことの定義から従うのである。そして、最後に約数に関する $\phi(d)$ の和は余約数に関わる $\phi(\tilde{d})$ の和となることを用いると、

$$\sum_{d/n} \phi(d) = n \tag{5.45}$$

が帰結する。[証明終]

そのために、$n = 24$ で実験してみる。約数は

$$1, 2, 3, 6, 8, 12, 24 \tag{5.46}$$

である。それぞれに対して

$$\phi(1) = 1, \phi(2) = 1, \phi(3) = 2, \phi(4) = 2, \phi(6) = 2, \phi(8) = 4, \phi(12) = 4, \phi(24) = 8 \tag{5.47}$$

となり、

$$\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(8) + \phi(12) + \phi(24) \tag{5.48}$$

$$= 1 + 1 + 2 + 2 + 2 + 4 + 4 + 8 = 24 \tag{5.49}$$

で勘定が合うことが分かる。

しかし、正直な所 $\phi(n)$ なる関数自体が飲み込みにくい関数であることは確かである。例えば、$\phi(1000)$ で確認するのは手計算では無理でしょう。Mathematica で計算させれば一発でできますが。

その 2. その 1 を少し変形させたかたちの証明 (ヴィノグラードフ整数論の付録に基づく) を挙げる。

[**証明**] ヴィノグラードフ整数論の付録に基づく証明

まず、$\phi(d)$ の意味にたちもどることにする。意味は「$1 \sim d$ のなかで d と互いに素なもの a の個数をあらわす」ということであった。これを次のように言い換えよう。

$$\frac{a}{d} = \text{既約分数} \quad (1 \leq a \leq d) \tag{5.50}$$

となるものの個数が $\phi(d)$ となる。

この事実をもとに、つぎのことを考えよう。n 個の整数を

$$\frac{x}{n} = \frac{a}{d} \tag{5.51}$$

を満たすような x を考えてみる。具体的に並べると

$$\frac{1}{n}, \frac{2}{n}, \cdots, \frac{x}{n}, \cdots, \frac{n}{n}, \tag{5.52}$$

約数 d に対して、上のように既約となるような a をひとつ与えると、この a に対して、$1 \leq x \leq n$ の中に、ただひとつの x が定まる。

このことから、n のひとつの約数 d をあたえると、それから既約分数 $\frac{a}{d} = \frac{x}{n}$ となる n 個のなかの x の個数は $\phi(d)$ となる。d を変えていくと、互いに重なることなく、n が $\phi(d)$ 個ずつに配分される。つまり、$\sum_{d/n} \phi(d) = n$ となる。[証明終]

このように、やっていることは約数と互いに素という初歩的な概念だけしか用いていないのに関わらず、なんともイライラさせられるが、要は、「n 個の x が 1 対 1 対応で約数 d の既約な類 (つまり a) に振り分けられる」ということの操作自身のなかに鍵になる。如何ですかな? 最後は、1 対 1 の原則で乗り切ろう。

6　原始根とベキ剰余

6.1　合同式の基本

$a \equiv a' \pmod{m}, b \equiv b' \pmod{m}$ ならば

$$a \pm b \equiv a' \pm b' \tag{6.1}$$
$$ab \equiv a'b' \tag{6.2}$$

である。

一般に $a \equiv a', b \equiv b', \cdots \pmod{m}$ で $f(x, y, z, \cdots)$ を $x, y, z, \cdots$ の多項式とすると

$$f(a, b, c, \cdots) \equiv f(a', b', c', \cdots) \pmod{m}$$

となる。これを類の代表 $\bar{a}, \bar{b}, \bar{c}, \cdots$ を使うと

$$f(\bar{a}, \bar{b}, \bar{c}, \cdots)$$

となる。

$ac \equiv bc \pmod{m}$ かつ $(c, m) = 1$ であれば割れて

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

となる。

[証明]

$ac \equiv bc \pmod{m}$ より

$$ac - bc = mt$$
$$\therefore\ (a - b)c = mt\ (m \text{ の倍数})$$

となる。また $(c, m) = 1$ より $(a - b)$ は m の倍数となり

$$(a - b) = mt$$
$$\therefore\ a \equiv b \pmod{m} \tag{6.3}$$

[証明終]

6.2　合同方程式

定義 合同方程式

$$f(x) \equiv 0 \pmod{m} \tag{6.4}$$

で表される x を未知数とする方程式

この方程式は、x に 0 から $m-1$ の値を代入して、m の倍数に成るものが解となる (今、剰余類を考えるので $0 \sim m-1$ で問題ない)。

ひとつの解 $x_1 = x_0 \pmod{m}$ とすると、

$$f(x_1) \equiv f(x_0) \equiv 0 \pmod{m} \tag{6.5}$$

である。特に 1 次合同式:$ax \equiv b \pmod{m}$ の場合、

定理

1 次合同式:$ax \equiv b \pmod{m}$ の場合、$(a, m) = 1$ のとき $ax \equiv b \pmod{m}$ は 1 つの解をもつ。
$(a, m) = d$ $(d > 1)$ のとき b が d の倍数のときのみ解をもち、解の個数は d 個となる。

[証明]

$(a, m) = 1$ のとき剰余系 $(x_1, \cdots, x_m)$ としておくと $(ax_1, ax_2, \cdots, ax_m)$ も剰余系となる。なぜならば

$$\begin{aligned} ax_i &\equiv ax_j \pmod{m} \\ \therefore\ a(x_i - x_j) &\text{は } m \text{ の倍数} \\ \therefore\ (x_i - x_j) &\text{が } m \text{ の倍数} \\ \therefore\ x_i &\equiv x_j \pmod{m} \end{aligned}$$

ゆえに任意の b に対して $ax \equiv b \pmod{m}$ となる x が $(x_1, \cdots, x_m)$ の中にただひとつ決まる。

(別記)

$$\begin{aligned} ax &= b \pmod m \\ ax - b &= my \\ \therefore\ ax - my &= b \end{aligned} \tag{6.6}$$

一次不定方程式 (6.6) 式の整数解を求める問題と同値である。$(a, m) = 1$ のとき (6.6) 式は整数解。

$$\begin{cases} x = & x_0 + mt \\ y = & y_0 + as \end{cases} \Longrightarrow \begin{cases} x \equiv & x_0 \pmod m \\ y \equiv & y_0 \pmod a \end{cases} \tag{6.7}$$

(x_0, y_0) はひとつの解となっている。$x \equiv x_0 \pmod m$ の表記は、唯一の解 x_0 を代表とする。[証明終]

注意: $(a, m) = 1, \quad x, y \in \boldsymbol{Z}$

$ax + my$ は任意の整数を表す。

$$\Longleftrightarrow ax + my = c \text{ は必ず解をもつ} \tag{6.8}$$

$$\Longleftrightarrow ax + my = 1 \text{ は解をもつ} \tag{6.9}$$

既約剰余系:$\phi(m)$ 個 $(x_1, x_2, \cdots, x_{\phi(m)})$
$\pmod m$ の類の代入

定理

$(a, m) = 1$ のとき、

$$(ax_1, \cdots, ax_{\phi(m)}) = (x_1, \cdots, x_{\phi(m)}) \tag{6.10}$$

である。ただしこの等号の意味は「イコールではないが同じ剰余系として等しい」である。$(x_1, \cdots, x_{\phi(m)})$ を順番を入れ替えたもの。

[証明]

もし $ax_i \equiv ax_j \pmod{m}$ とすると $a(x_i - x_j)$ は m の倍数になる。

$$\therefore\ x_i - x_j \text{は } m \text{ の倍数} \tag{6.11}$$

$$\therefore\ x_i \equiv x_j \pmod{m} \tag{6.12}$$

これは仮定 $ax_i \equiv ax_j$ に反する。$\therefore\ x_i \neq x_j \pmod{m}$。ゆえに $(ax_i, \cdots, ax_{\phi(m)})$ も既約剰余系となる。[証明終]

$$ax_1 ax_2 \cdots ax_{\phi(m)} = a^{\phi(m)} x_1 x_2 \cdots x_{\phi(m)}$$

$$a^{\phi(m)} x - 1 \cdots x_{\phi(m)} \equiv x_1 \cdots x_{\phi(m)} \pmod{m}$$

$$\therefore\ a^{\phi(m)} \equiv 1 \pmod{m},\ \text{(Euler の定理)}$$

$m = p$(素数) のとき $\phi(p) = p - 1$ より

$$a^{p-1} \equiv 1 \pmod{p} \tag{6.13}$$

となる。

以上で、つぎの定理にまとめられる.

定理 Euler の定理

$$a^{\phi(m)} \equiv 1 \pmod{m},\ \text{但し、} (a, m) = 1 \tag{6.14}$$

とくに $m = p$(素数) のとき $\phi(m) = p - 1$ より**フェルマーの小定理**が得られる。

定理 フェルマーの定理

$$a^{p-1} \equiv 1 \pmod{p} \text{ または } a^p \equiv a(p) \tag{6.15}$$

6.3　原始根

定義 M 次方程式 (合同方程式)

$$x^M \equiv 1 \pmod{p} \tag{6.16}$$

一般には $e < p-1$ で $a^e \equiv 1 \pmod{p}$ である。

a が $p-1$ より小さい正指数で $a^e \equiv 1 \pmod{p}$ を満たすものは存在する。例:$p = 13$ のとき $3^3 \equiv 1 \pmod{13}$

定義

$$a^q \equiv 1 \pmod{p} \tag{6.17}$$

となるような指数 q のうち最小のものを e とする。この e を a に対応する指数という。故に

$$a^e \equiv 1 \pmod{p} \tag{6.18}$$

定義 原始根

a が $(p-1)$ 以下で $a^q \equiv 1 \pmod{p}$ を満たす q が存在しないとき、すなわち $e = p-1$ の時[a] 、a を「p を法とする原始根」とよぶ。

[a] すなわち a に対応する指数が $p-1$ のとき

定理 準備定理

a のべきが m 乗してはじめて $a^m \equiv 1 \pmod{p}$ となるとき、つまり、m を a に対応する指数 $(1, a, a^2, \cdots, a^{m-1})$ は $x^m \equiv 1 \pmod{p}$ の互いに不合同な (異なる)m 個の解となる。

[証明]

a^k について $0 \leq k \leq m-1$ では

$$(a^k)^m = (a^m)^k \equiv 1 \pmod{p}$$

なので

$$\therefore\ a^k \text{は } x^m \equiv 1 \pmod{p} \text{ の解} \tag{6.19}$$

[証明終]

定理

p を法とする原始根は存在する。[a]

[a] 証明は省略

ひとつの原始根を r とすると、$r^{p-1} \equiv 1 \pmod{p}$ となる。準備定理より $(1, r, r^2, \cdots, r^{p-2})$ は互いに不合同である。すなわち $\bmod p$ に関する既約類の 1 つとなる。任意の数 b は $\bmod p$ の既約類となる

$$b \equiv r^k \pmod{p} \tag{6.20}$$

となるべき k が唯一 $(0 \leq k \leq p-1)$ に存在する。

定義

r を 1 つ与えると

$$r^\alpha \equiv a \pmod{p}, \quad (a, p) = 1 \tag{6.21}$$
$$\Longleftrightarrow \alpha = \mathrm{Ind}_r(a) \tag{6.22}$$

となる。これを「r **を底とする指数**」と呼ぶ。[a]
あるいは

$$r^\alpha \equiv a \pmod{p} \tag{6.23}$$

で $s \equiv \alpha \pmod{p-1}$ より

$$\alpha = \mathrm{Ind}_r(a) \tag{6.24}$$

[a] α は $\bmod (p-1)$ として $s \equiv \alpha \pmod{p-1}$

対数の類似

$$x = y, \quad y = x^n \tag{6.25}$$
$$\log_a x = \log_a y \quad \log y = n \log x \tag{6.26}$$

定理

$$a \equiv b \pmod{p} \tag{6.27}$$

$$\mathrm{Ind}(a) \equiv \mathrm{Ind}(b) \pmod{p-1} \tag{6.28}$$

[証明]

$$r^{\alpha} \equiv r^{\beta} \pmod{p}$$

$$\alpha = \mathrm{Ind}_r a,\ \beta = \mathrm{Ind}_r b$$

$$\alpha \equiv \beta \pmod{p-1}$$

$$\mathrm{Ind}(a) \equiv \mathrm{Ind}_r(b) \pmod{p-1}$$

[証明終]

定理

$$\mathrm{Ind}(ab) = \mathrm{Ind}(a) + \mathrm{Ind}(b) \tag{6.29}$$

$$\mathrm{Ind}(a)^n = n\mathrm{Ind}(a) \tag{6.30}$$

6.4　ベキ剰余

定理

$$x^n \equiv a \pmod{p} \tag{6.31}$$

n 次合同式の解が存在するための条件は

$$a^f \equiv 1 \pmod{p} \tag{6.32}$$

但し

$$f = \frac{p-1}{(n, p-1)} \tag{6.33}$$

定義

$x^n \equiv a(p)$ の解があるとき a **を** p **の** n **ベキ剰余**という。
とくに $n = 2$ のとき

$$x^2 \equiv a \pmod{p} \tag{6.34}$$

a を平方剰余 or 非剰余

γ を 1 つの原始根とすると

$$\gamma^x \equiv a \pmod{p} \quad (r^y = x \longrightarrow y = \log_r x \text{ の類似})$$
$$x \equiv \mathrm{Ind}(a) \pmod{p-1}$$

合同方程式 $f(x) \equiv 0 \pmod{p}$

$$x^n \equiv a \pmod{p} \tag{6.35}$$

定理

$x^n \equiv a \pmod{p}$, $(a, b) = 1$ が解をもつための必要十分条件は

$$a^f \equiv 1 \pmod{p} \tag{6.36}$$
$$f = \frac{p-1}{(n, p-1)} \left(= \frac{p-1}{e} \right) \tag{6.37}$$

[証明]

両辺の Ind_r をとる (適当な r に対する)

$$n\mathrm{Ind}\, x \equiv \mathrm{Ind}\, a \pmod{p-1} \tag{6.38}$$

$y = \mathrm{Ind}\, x, b = \mathrm{Ind}\, a$ としたとき 1 次合同式

$$ny \equiv b \pmod{p-1} \tag{6.39}$$

となる。ここで $(n, p-1) = e$ とする。解をもつためには b も e で割り切れる。このとき (6.38) 式は e 個の解がある。[*5] [証明終]

[*5] $n = 2, e = (2, p-1) = 2$ となり 2 個の解が存在する。

1 次合同式の復習

$ax \equiv b \pmod{m}$ のとき

- $(a, m) = 1 \Longrightarrow$ 1 個の解が存在する。
- $(a, m) = d \Longrightarrow b$ が a で割り切れるとき d 個の解がある。[*6]

$$\begin{cases} a = a'd \\ m = m'd \\ b = m'b' \end{cases} \tag{6.40}$$

$(a', m') = 1$ 故に、1 個の解がある。

[**証明**] 必要の証明

$\mathrm{Ind}_r a = b$ とする。かつ $b = eq$(e で b は割り切れる) とおく。

$$a \equiv r^b = r^{eq} \pmod{p} \tag{6.41}$$
$$a \equiv r^{eq} \pmod{p} \tag{6.42}$$
$$a^f \equiv r^{eqf} \pmod{p} \tag{6.43}$$

ここで $ef = p - 1$ ゆえにフェルマーの小定理から

$$a^f = r^{(p-1)q} \equiv 1 \pmod{p} \tag{6.44}$$

となることから

$$a^f \equiv 1 \pmod{p} \tag{6.45}$$

[証明終]

[**証明**] 十分の証明

$a^f \equiv 1 \pmod{p}$ とすると

$$a^f \equiv r^{bf} \equiv 1 \pmod{p} \tag{6.46}$$

となる。故に bf は $p-1$ で割り切れる。すなわち bf は fe で割り切れる。このことから、

$$b \equiv \mathrm{Ind}\, a \text{ は } e \text{ で割り切れる} \tag{6.47}$$
$$x^n \equiv a \pmod{p} \text{ は解をもつ} \tag{6.48}$$

[*6] $a'x \equiv b' \pmod{m'}$

[証明終]

この a を**ベキ剰余**とよぶ。

定義

$x^n \equiv a \pmod{p}$ が解をもつとき、a **を** n **ベキ剰余**とよぶ。解が無いとき非剰余とよぶ。とくに $n=2$ のとき平方剰余とよぶ。

$(n, p-1) = e > 1$ のとき $\mathrm{Ind}\, a$ が e の倍数になる a が n 巾剰余となる。

$$\mathrm{Ind}\, a = 0, e, 2e, 3e, \cdots, (f-1)e \tag{6.49}$$

なお $f = (p-1)/e$ である。すなわち $(p-1)$ 個の既約類のうち $1/e$ が n 巾剰余となる。とくに $n = 2$(平方剰余)$e = (2, p-1) = 2$。$(p-1)$ の既約類のうち $1/2$(半分) が平方剰余となる。例. $p = 19$。

$x = 1, 2, 3, \cdots, 17, 18$. x^2 を計算。$\frac{18}{2} = 9$ 個が平方剰余。

$$1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16, 5^2 = 25 \equiv 6 \pmod{19} \tag{6.50}$$

$$6^2 = 36 \equiv 17, 7^2 = 49 \equiv 11, 8^2 = 64 \equiv 7, \quad 9^2 = 81 \equiv 5 \pmod{19}, \cdots \tag{6.51}$$

結果、

$$\begin{cases} \text{平方剰余} & :1,4,5,6,7,8,11,16,17\text{の } 9 \text{ 個} \\ \text{非平方剰余} & : \text{残り} \end{cases} \tag{6.52}$$

これらは計算機の数値計算で確認できる。

7　平方剰余と相互法則

定義 Legendre の記号

$x^2 \equiv a \pmod{p}$, a が平方剰余のとき、

$$\lambda_p(a) = \left(\frac{a}{p}\right) = \begin{cases} (a \text{ が} \pmod{p} \text{ で平方剰余のとき}) & 1 \\ (a \text{ が} \pmod{p} \text{ で非剰余のとき}) & -1 \end{cases} \tag{7.1}$$

これは巡回群の指標の特別な場合である。[a]

[a] 1 種の指標、群の表現論での指標、character のようなもの、$\chi(g)$

定理 基本定理 その 1

$$\left(\frac{a}{p}\right) = (-1)^{\mathrm{Ind} a} \tag{7.2}$$

[証明]

$\mathrm{Ind}\, a$ が 2 の倍数 (偶数) のとき平方剰余。$\mathrm{Ind}\, a$ が奇数のとき非剰余であることから従う。[*7] [証明終]

[*7] ベキ剰余...$x^n \equiv a \pmod{p}$, $n\mathrm{Ind}\, x \equiv \mathrm{Ind}\, a \pmod{p-1}$, $(n, p-1) = e$ とする $(e > 1)$。$\mathrm{Ind}\, a$ が e の倍数のとき e 個の解あり。

定義 基本定理 その 2

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \cdots \text{オイラーの規準} \tag{7.3}$$

a

---

[a] $x^2 \equiv a \pmod{p}$ が解をもつための条件は

$$a^f \equiv 1 \pmod{1} \tag{7.4}$$

$$f = \frac{p-1}{(2, p-1)} = \frac{p-1}{2} \tag{7.5}$$

[証明]

- $\left(\frac{a}{p}\right) = 1$ のとき (剰余)
  $x^2 \equiv a \pmod{p}$ が解をもつ $\Longrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$
- $\frac{a}{p} = -1$ のとき (非剰余)
  $x^2 \equiv a \pmod{p}$ 解無し $\Longrightarrow a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$

一方、$a^{p-1} \equiv 1 \pmod{p}$ であるから (フェルマーの小定理)、

$$(a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \equiv 0 \pmod{p}$$

$$a^{\frac{p-1}{2}} - 1 \not\equiv 0 \pmod{p}$$
$$\therefore\ a^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$$
$$\therefore\ a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

以上を項目をまとめると

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \tag{7.6}$$

[証明終]

定理 平方剰余の相互法則

- 定理：$p, q(\neq 2)$ 素数
- 主定理：

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{7.7}$$

定理 (補充定理 1)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \tag{7.8}$$

[証明]

オイラーの規準より

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

$$\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}} \equiv \pmod{p}$$

これが成立するのは

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

のときだけ [証明終]

定理 (補充定理 2)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \tag{7.9}$$

[証明]

$2=\frac{(1+i)^2}{i}$ より

$$\begin{aligned}\left(\frac{2}{p}\right) &\equiv 2^{\frac{p-1}{2}} \text{ (オイラーの規準より)}\\ &\equiv \frac{(1+i)^{p-1}}{i^{\frac{p-1}{2}}}\\ &\equiv \frac{(1+i)^p}{i^{\frac{p-1}{2}}(1+i)}\\ &\equiv \frac{1+i^p}{i^{\frac{p-1}{2}}(1+i)} \pmod p\end{aligned}$$

[*8] ここで

$$\frac{1+i^p}{i^{\frac{p-1}{2}}}=i^{\frac{p+1}{2}}+i^{-\frac{p-1}{2}}=i^{\frac{1}{2}}\left[i^{\frac{p}{2}}+i^{-\frac{p}{2}}\right]$$

ここで $e^{\frac{\pi i}{2}}=i$ より

$$\frac{(1+i)^p}{i^{\frac{p-1}{2}}}=e^{\frac{\pi i}{4}}\left(e^{\frac{p\pi i}{4}}+e^{-\frac{p\pi i}{4}}\right)$$

となることから

$$\begin{aligned}\frac{1}{1+i}e^{\frac{\pi i}{4}}\left(e^{\frac{p\pi i}{4}}+e^{-\frac{p\pi i}{4}}\right) &= \frac{1}{\sqrt{2}e^{\frac{\pi i}{4}}}e^{\frac{\pi i}{4}}\left(e^{\frac{p\pi i}{4}}+e^{-\frac{p\pi i}{4}}\right)\\ &= \frac{1}{\sqrt{2}}2\cos\frac{\pi}{4}\\ &= \sqrt{2}\cos\frac{p\pi}{4}\\ &= \frac{\cos\frac{p\pi}{4}}{\cos\frac{\pi}{4}}=\begin{cases}1 & p\equiv\pm1 \pmod 8\\ -1 & p\equiv\pm3 \pmod 8\end{cases}\end{aligned}$$

[証明終]

[*8] $(a+b)^p\equiv a^p+b^p \pmod p$

8　平方剰余の相互法則の証明

平方剰余の相互作用の証明で、初等整数論のクライマックスに来ました。これをガウスの和をつかうやりかたでやろうとしていますが、それよりも、剰余系の概念の意味を練ることにより初等的証明をやるのが、やはり本来の整数論の精神の叶っていることになるかと思います。もちろん機会仕掛けのオレンジ宜しく、ガウスの和を巧みにつかう近代的手法は非常に重要であるということは言うまでもありません。

という訳で、以下の証明は高木とヴィノグラードフをまぜたものでやります。

ここでまずいくつかの準備定理を準備する。

8.1　準備定理その 1

ガウスの記号:$[x] = x$ を超えない整数:を使うことにする。

定理

2 つの奇数 p, q に対して、

$$\sum_{0<x<q/2} [\frac{p}{q}x] + \sum_{0<y<p/2} [\frac{q}{p}y] = \frac{p-1}{2} \cdot \frac{q-1}{2} \tag{8.1}$$

この意味は、幾何学的には、座標のうえで原点を頂点にした長方形の中の格子点 (座標が整数になる点) の数を勘定することで直感的に理解できると思います。ここでは証明を省くが、Vinog の第 2 章の問題として出ていますのでぜひみてください。

8.2　準備定理その 2

奇素数 p の絶対最小既約数系

$$-\frac{p-1}{2}(\equiv p_1), \cdots, -2, -1, 1, 2, \cdots, \frac{p-1}{2} \tag{8.2}$$

をまず思い出すことにしよう。その正の部分

$$1, 2, \cdots, \frac{p-1}{2}(\equiv p_1)$$

に、p と素な任意の整数の整数 a をかけると

$$a, 2a, 3a, \cdots, p_1 a$$

ができるが、これは

$$a \equiv \epsilon_1 r_1(p), 2a \equiv \epsilon_2 r_2(p), \cdots, p_1 a \equiv \epsilon_{p_1} r_{p_1}(p) \tag{8.3}$$

と表せることに注目する。ここで、$r_1, \cdots, r_{p_1}$ は、もとの正の絶対最小剰余と同じになる。すなわち、順番を並べ替えただけになる (この事実は、剰余系の意味を考えると了解できるであろう)。また、$\epsilon_x = \pm 1$ で、mod p での剰余とみたときに、$x < \frac{p}{2}$ であれば、$\epsilon_x = 1, x > \frac{p}{2}$ であれば $\epsilon_x = -1$ をとるいわば「パリティ」を表す。要するに、絶対最小剰余が、符号に変えて出てきて、それがすべて異なることである。以下で実験をするので、各自確認してください。

この準備のもと、(??← 不明) を掛け合わせて、$1 \cdots 2 \cdots p_1 = r_1 \cdot r_2 \cdots r_{p_1}$ で両辺を約することにより

$$a^{(p-1)/2} \equiv \epsilon_1 \cdot \epsilon_2 \cdots \epsilon_{p_1} \pmod{p} \tag{8.4}$$

が得られる。

さらに、オイラーの規準

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

に注意すると、つぎの定理が得られる。

定義

$$\left(\frac{a}{p}\right) = \epsilon_1 \cdot \epsilon_2 \cdots \epsilon_{p_1} \tag{8.5}$$

これは、言い換えれば、ルジャンドルの記号が上で定義されたパリティの積で表示できることを意味している。

実験例: $p = 17, a = 6$ の場合。この例では、$p_1 = \frac{17-1}{2} = 8$。平方剰余は $1 \sim 8$ の平方をつくることにより

$$1, 2, 4, 8, 9, 13, 15, 16$$

となることがわかる。ゆえに、$a = 6$ は剰余ではないから、$(\frac{a}{p}) = -1$ となる。これをパリティで確かめる。$a, 2a, 3a, \cdots, p_1 a$ の $\pmod{17}$ をつくると

$$6 \equiv 6, 12 \equiv -5, 18 \equiv 1, 24 \equiv 7, 30(\equiv 13) \equiv -4, 42 \equiv 8, 48(\equiv 14) \equiv -3$$

となり、$p/2$ が 8 を超える (ϵ がマイナスになる) のは 3 個になるので、$(q/p) = (-1)^3 = -1$ になり非剰余となる。同じく、$a = 8$ の場合に実行して平方剰余となることを確かめられよ。

さて、うえのパリティ積をさらに変形しよう。このために、ガウスの記号を利用する。天下り的ではあるが

$$\left[\frac{ax}{(p/2)}\right] = \left[\frac{2ax}{p}\right]$$

なるものを考える。$ax = \alpha + tp$ と表すと、

$$\frac{ax}{(p/2)} = 2t + \frac{2\alpha}{p}, (\alpha < p)$$

に注意すると、$a < \frac{p}{2}$ あるいは、$\alpha > \frac{p}{2}$ にしたがい、$\frac{2\alpha}{p} = 0$ あるいは、$\frac{2\alpha}{p} = 1$ ゆえ、$[\frac{2ax}{p}]$ = 偶数、奇数となる。これと符号定数 ϵ の意味を考えて、

$$\epsilon_x = (-1)^{(2ax/p)} \tag{8.6}$$

と表せることがわかる。これから、

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1}\left[\frac{2ax}{p}\right]} \tag{8.7}$$

うえの式をさらに変形する [このために、剰余記号の性質を列挙しておこう。これらの証明は練習問題として残しておこう]

1. $\left(\frac{abc\cdots}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots$
2. $\left(\frac{a^2}{p}\right) = 1$
3. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ (if $a \equiv b \pmod p$)

さて、$\frac{a}{p}$ のかわりに $\left(\frac{2a}{p}\right)$ を考える。a が奇数の場合を考えよう。相互法則の証明の為にはそれで十分である。まず、$a \equiv b \pmod p$ のとにきは、うえの (iii) から

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right)$$

さらに、(i),(ii) より $\left(\frac{b^2a}{p}\right) = \left(\frac{a}{p}\right)$。これから

$$\left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right)$$

これに、(??← 不明) を適用すると、

$$\left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{\sum_{x=1}^{p_1}\left[\frac{(a+p)x}{p}\right]}$$

指数の肩は、

$$\left(\frac{\frac{a+p}{2}}{p}\right) = (-1)\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right] + \sum_{x=1}^{p_1} x \tag{8.8}$$

かつ、$\sum_{x=1}^{p_1} x = (p^2-1)/8$。ゆえに、

$$\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right] + \frac{p^2-1}{8} \tag{8.9}$$

これから、$a=1$ とおくと、$(1/p)=1$ に注意すると、

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

すなわち、第 2 補充法則が同時に導かれる。

8.3　証明の完結

ここまでくると、相互法則は一息である。(8.9) において、$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ をつかうと、

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1}} \tag{8.10}$$

(結局、因子 2 がなくなっただけ!!)

ここで、$a = q$(奇素数) とおくと、

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{x=1}^{p_1}\left[\frac{qy}{p}\right]} \tag{8.11}$$

および、p と q をいれかえたもの

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{y=1}^{q_1}\left[\frac{py}{q}\right]} \tag{8.12}$$

を掛け合わせて定理 1:

$$\sum_{x=1}^{p_1}\left[\frac{qx}{p}\right] + \sum_{y=1}^{q_1}\left[\frac{py}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}$$

をつかうと、相互法則

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

が導かれる。

追記: 以上の証明仮定はどうだったでしょうか。ガウスの記号とパリティの考えを巧妙に使っている所が、整数論独特の隠れた技であるという記がします。

ちなみに、相互法則の重要性は単に整数論だけに閉じたものではないようで、ある種の相反性あるいは双対性を表しているものとして捉えられているもののようです。たとえば物理では電荷と磁荷の双対性を表明しているディラックの量子化。

相互作用を、空間曲線が絡むときにでてくる、いわゆるガウスの絡み数 (linking number) が相互法則と対応していると主張している学者がいます。たとえば小野孝氏 (彼のテキスト:数論序説に述べられている)。最近の研究者はもっと真剣に、その類似を追求しているようです。数論幾何学という分野があるそうです。「素数と結び目」(シュプリンガージャパン) という本はそのようなことを書いています。専門用語が錯綜してなかなか読めませんが、結び目のトポロジーを整数論の類似で追求しようということらしく、最近のゲージ理論と経路積分をつかって、整数論的現象 (とくに非可換類体論) を解明できるのではないかという夢 (Langlands program というらしい) をかがげているようで、ここで、場の理論をやろうとする諸君の中に、物理の再度から、攻め込んでいくという人が $\cdots$。どうでしょうか?

9 Gauss の和

9.1 定義

以下では、Legendre 記号 (q/p) を, $\lambda_p(q)$ なる記号を併用することにする。

定義 Gauss の和

$$\tau = \sum_{x \in F_p^*} \lambda_p(x) \exp\left[\frac{2\pi i x}{p}\right] \tag{9.1}$$

[a] これを拡張すると

$$\tau_a = \sum_{x \in F_p^*} \lambda_p(x) \exp\left[\frac{2\pi a i x}{p}\right] \ (\tau = \tau_1) \tag{9.4}$$

---

[a]

$$F_p = (0, 1, \cdots, p-1) \tag{9.2}$$
$$F_p^* = (1, 2, \cdots, p-1) \tag{9.3}$$

τ_a(or τ) の等式

定理

$$S = \begin{cases} \sqrt{P}, & P \equiv 1 \pmod 4 \\ i\sqrt{P}, & P \equiv 2 \text{ or } 3 \pmod 4 \end{cases} \tag{9.5}$$

[a]

---

[a] $p = 3$ の時、手計算で check できる

$p=3$,$x \in F_p^*(1,2)$

$$\begin{aligned} S &= \sum_{x=1,2} \left(\frac{x}{p}\right) \exp\left(\frac{2\pi i x}{p}\right) \\ &= \left(\frac{1}{3}\right) \exp\left(\frac{2\pi i \cdot 1}{3}\right) + \left(\frac{2}{3}\right) \exp\left(\frac{2\pi i \cdot 2}{3}\right) \\ &= 1 \cdot \exp\left(\frac{i2\pi}{3}\right) - \exp\left(\frac{4\pi i}{3}\right) \\ &= -\frac{1}{2} - i\frac{\sqrt{3}}{2} + \frac{1}{2} + \frac{\sqrt{3}}{2}i \end{aligned}$$

$p=3$ のとき $x=1,2$ で x^2 を計算する。$1^2=1, 2^2=4\equiv 1 \pmod 3$ となり、平方剰余:1, 非剰余:2

9.2 いくつかの補題

補題 1:

$$\tau_a = \lambda_p(a)\tau \tag{9.6}$$

[証明]

$a=0$ のとき

$$\tau_0 = \lambda_p(0)\tau = 0$$

$$\sum_{x\in F_p^*} \lambda_p(x)\exp(2\pi i \times 0) = \sum_{x\in F_p^*} \lambda_p(x) = 0$$

$a \neq 0$ のとき

$$\begin{aligned} \lambda_p(a)\tau_a &= \sum_{x\in F_p^*} \lambda_p(a)\lambda_p(x)\exp\left[\frac{2\pi i x a}{p}\right] \quad (a,p)=1 \\ &= \sum_{x\in F_p^*} \lambda_p(ax)\exp\left[\frac{2\pi i x a}{p}\right] \\ (ax\equiv y) \text{ と書き改める} \ &= \sum_{x\in F_p^*} \lambda_p(y)\exp\left[\frac{2\pi i y}{p}\right] = \tau \end{aligned}$$

さらに, 両辺に $\lambda_p(a)$ をかけると $\lambda_p^2(a)=1$ をつかうと、

$$\tau_a = \lambda_p(a)\tau$$

[証明終]

補題 2:

$$\tau_a^2 = p^*,\ (a,p) = 1 \tag{9.7}$$

但し、$p^* = (-1)^{\frac{p-1}{2}} p$

[証明]

$$S = \sum_{a \in F_p} \tau_a \cdot \tau_{-a}$$

を用意する。[*9]

$a \neq 0$ に対して

$$\begin{aligned}
\tau_a \tau_{-a} &= \lambda_p(a)\tau \lambda_p(-a)\tau \\
&= \lambda_p(-a^2)\tau^2 \\
&= \left(\frac{-1}{p}\right)\left(\frac{a^2}{p}\right)\tau^2 \\
&= \lambda_p(-1)\tau^2 \\
&= (-1)^{\frac{p-1}{2}}\tau^2
\end{aligned}$$

となり、

$$S = \sum_{a \in F_p} \tau_a \tau_{-a} = \sum_{a \in F_p^*} \tau_a \tau_{-a} = (p-1)(-1)^{\frac{p-1}{2}}\tau^2$$

一方、

$$\begin{aligned}
S &= \sum_{a \in F_p^*} \left(\sum_{x \in F_p^*} \lambda_p(x) \exp\left(\frac{2\pi i a x}{p}\right) \times \sum_{y \in F_p^*} \lambda_p(y) \exp\left(\frac{2\pi i a y}{p}\right) \right) \\
&= \sum_x \sum_y \lambda_p(xy) \sum_{a \in F_p^*} \exp\left[\frac{2\pi i}{p} a(x-y)\right] \\
&= \sum_x \sum_y \lambda_p(xy) p \delta_{x,y} \\
&= \sum_{x=1}^{p-1} \lambda_p(x^2) p = \left(\sum_{x=1}^{p-1} 1\right) p = p(p-1)
\end{aligned}$$

[*9] $\sum_{a \in F_p} = \sum_{a \in F_p^*}, \tau_0 = 0$

よって

$$\sum_{a\in F_p}\exp\left[\frac{2\pi i}{p}a(x-y)\right]=p\delta_{x,y}$$

つまり、

$$\sum_{a\in F_p}\exp\left[\frac{2\pi i}{p}a(x-y)\right]=\begin{cases}p & (x-y=0)\\ 0 & (x-y\neq 0)\end{cases} \tag{9.8}$$

なので

$$(p-1)(-1)^{\frac{p-1}{2}}\tau^2=p(p-1)$$
$$\therefore\ \tau^2=(-1)^{\frac{p-1}{2}}p\equiv p^*$$

もしくは

$$\tau_a^2=(\lambda_p(a))^2\tau^2=1\times\tau^2=p^*$$

[証明終]

9.3 Gauss の和を用いた相互法則の証明

$a=q$ のとき

$$\left(\frac{a}{p}\right)=\lambda_p(a)\longrightarrow\lambda_p(q)=\left(\frac{q}{p}\right)\Longleftrightarrow x^2\equiv q\pmod p \tag{9.9}$$

準備:

$$\begin{aligned}\tau^{q-1}&=(\tau^2)^{\frac{q-1}{2}}=(p^*)^{\frac{q-1}{2}}\\ &\equiv\lambda_q(p^*)\pmod q\end{aligned} \tag{9.10}$$

となる。但し、$\tau^2=p^*$ とオイラーの規律を用いた。

これから、

$$\tau^q\equiv\lambda_q(p^*)\tau \tag{9.11}$$

が得られる. さらに

$$\begin{aligned}\tau^q &\equiv \left(\sum_{x\in F_p}\lambda_p(x)\exp\left[\frac{2\pi ix}{p}\right]\right)^q \\ &\equiv \sum_{x\in F_p}\lambda_p^q(x)\exp\left[\frac{2\pi ixq}{p}\right] \quad (q \text{ は奇素数}) \\ &= \sum_{x\in F_p}\lambda_p(x)\exp\left[\frac{2\pi ixq}{p}\right] \\ &= \tau_q \pmod q\end{aligned}$$

*10

補題 1: $\tau_q = \lambda_p(q)\tau$ を使うと

$$\lambda_q(p^*)\tau \equiv \lambda_p(q)\tau \pmod q$$

両辺に τ をかけると

$$\lambda_q(p^*)\tau^2 \equiv \lambda_p(q)\tau^2 \pmod q$$

$\tau^2 = p^*$ より

$$\begin{aligned}\lambda_q(p^*)p^* &\equiv \lambda_p(q)p^* \pmod q \\ \text{それゆえ } \lambda_q(p^*) &\equiv \lambda_p(q) \pmod q\end{aligned}$$

両辺が ± 1 より、

$$\lambda_q(p^*) = \lambda_p(q)$$

$$\begin{aligned}\lambda_q(p^*) &= \lambda_q\left[(-1)^{\frac{p-1}{2}}p\right] \\ &= \left[\frac{(-1)^{\frac{p-1}{2}}p}{q}\right] \\ &= \left(\frac{-1}{q}\right)^{\frac{p-1}{2}}\cdot\left(\frac{p}{q}\right) \\ &= (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{p}{q}\right)\end{aligned}$$

$$\therefore\ (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

$$\therefore\ \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}$$

*10 $(a+b+c+\cdots)^q \equiv a^q + b^q + c^q + \cdots$

10　Gauss の和の計算

定理

$$G(p)=\sum_{x\in F_p^*}\left(\frac{x}{p}\right)\exp\left[\frac{2\pi ix}{p}\right]=\begin{cases}\sqrt{p} & p\equiv 1 \pmod 4\\ i\sqrt{p} & p\equiv 3 \pmod 4\end{cases} \tag{10.1}$$

[証明]

証明の方針はフーリエ級数とガウス積分を使う。まず、

$$G(p)=\sum_{x=1}^{p-1}\exp\left[\frac{2\pi ix^2}{p}\right] \tag{10.2}$$

と変形する。さらに

$$G(p)=\sum_{x\in r}\exp\left[\frac{2\pi ix}{p}\right]-\sum_{y\in n}\exp\left[\frac{2\pi iy}{p}\right] \tag{10.3}$$

に注意する。ここで $X^p=1, X=e^{\frac{2\pi i}{p}}=\xi$ とする。

$$1+\xi+\xi^2+\cdots+\xi^{p-1}=0$$
$$1+\xi+\xi^2+\cdots+\xi^{p-1}=1+\sum_{x\in r}\xi^x+\sum_{y\in n}\xi^y=0$$

従って

$$\therefore\ G(p)=1+2\sum_{x\in r}\xi^x \tag{10.4}$$

を得る。

この意味は:$X^2=x \pmod p$ に注意すると, 平方剰余は $\frac{p-1}{2}$ 個。それは 2 回ずつ出現する。そして 0 は 1 回出現する。というわけである：つまり

$$\therefore\ G(p)=\sum_{p=0}^{p-1}\exp\left[\frac{2\pi ix^2}{p}\right]$$

[証明終]

10.1 Gauss の和変形

定理 Gauss の和変形

$$G(p) = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \exp\left[\frac{2\pi i x}{p}\right] = \sum_{x=0}^{p-1} \exp\left[\frac{2\pi i x^2}{p}\right] \tag{10.5}$$

これは一般の m では

$$G(m) = \sum_{k=0}^{m-1} \exp\left[\frac{2\pi i x^2}{m}\right] \tag{10.6}$$

また $G(m)$ には次の性質がある。

$$G(m) = \begin{cases} (1+i)\sqrt{m} & m \equiv 0 \pmod 4 \\ \sqrt{m} & m \equiv 1 \pmod 4 \\ 0 & m \equiv 2 \pmod 4 \\ i\sqrt{m} & m \equiv 3 \pmod 4 \end{cases} \tag{10.7}$$

このように $G(m)$ の計算に帰着させるところが要になる．この計算に フーリエ級数を使い、ガウス積分に帰着させる。

[証明]

Step1.

$$f(t) = \sum_{k=0}^{m-1} \exp\left[\frac{2\pi i (k+t)^2}{m}\right] \tag{10.8}$$

を導入する。 ここで

$$G(m) = f(0) \tag{10.9}$$

であることをつかう。ただちにわかるように、$f(t) = f(t+1)$ となる。これは, $f(t)$ は周期 1 の周期関数である。

そこで、フーリエ展開をすると,

$$f(t) = \sum_{n=-\infty}^{\infty} a_n \exp\left[-2\pi i n t\right] \tag{10.10}$$

$$a_n = \int_0^1 \sum_{k=0}^{m-1} \exp\left[\frac{2\pi i(k+t)^2}{m}\right] \exp\left[2\pi i n t\right]\, dt$$

$$G(m) = f(0) = \sum_{n=-\infty}^{+\infty} a_n \quad \Longrightarrow \text{無限級数} \tag{10.11}$$

Step2. a_n の計算: $\int_0^1 \exp\left[\frac{2\pi i(k+t)^2}{m}\right] \exp\left[2\pi i n t\right]\, dt$ において, 完全平方より

$$\frac{(k+t)^2}{m} + nt = \frac{(k+t)^2 + mnt}{m}$$

ゆえに

$$(k+t)^2 + mnt = (k+t+\frac{mn}{2})^2 - (kmn + \frac{1}{4}m^2n^2)$$

かつ

$$\begin{aligned} \therefore\ a_n &= \sum_{k=1}^{m-1} \int_0^1 \exp\left[\frac{2\pi i(k+t)^2}{m}\right] \exp\left[2\pi i n t\right]\, dt \\ &= \exp\left[-\frac{2\pi i m n^2}{4}\right] \sum_{k=1}^{m-1} \int_0^1 \exp\left[2\pi i \frac{(k+t+\frac{1}{2}mn)^2}{m}\right]\, dt \end{aligned} \tag{10.12}$$

ここで $S = k + t + \frac{1}{2}mn$ とおくと (10.12) 式は

$$(10.12)\text{ 式} = \exp\left[-\frac{2\pi i m n^2}{4}\right] \times \sum_{k=0}^{m-1} \int_{k+\frac{1}{2}mn}^{k+1+\frac{1}{2}mn} \exp\left[2\pi i \frac{S^2}{m}\right]\, dS$$

さらに

$$\int_{\frac{1}{2}mn}^{1+\frac{1}{2}mn} + \int_{1+\frac{1}{2}mn}^{2+\frac{1}{2}mn} + \cdots + \int_{2+\frac{1}{2}mn}^{m+\frac{1}{2}mn} = \int_{\frac{1}{2}mn}^{m+\frac{1}{2}mn} \exp\left[\frac{2\pi i S^2}{m}\right]\, dS$$

これをまとめると

$$a_n = \exp\left[-\frac{2\pi i m n^2}{4}\right] \int_{\frac{1}{2}mn}^{m+\frac{1}{2}mn} \exp\left[\frac{2\pi i S^2}{m}\right]\, dS \tag{10.13}$$

従って

$$G(m) = \sum_{n=-\infty}^{+\infty} a_n$$
$$= \sum_{n=-\infty}^{\infty} \exp\left[-\frac{2\pi i m n^2}{4}\right] \int_{\frac{1}{2}mn}^{m+\frac{1}{2}mn} \exp\left[\frac{2\pi i S^2}{m}\right] dS \tag{10.14}$$

Step3.

$$\sum_{n=-\infty}^{+\infty} \longrightarrow \sum_{n:\text{even}} + \sum_{n:\text{odd}}$$

ここで n :even のとき、

$$\exp\left[-\frac{2\pi i m n^2}{4}\right] = 1 \tag{10.15}$$

n :odd$(2l+1)$ のとき、

$$\exp\left[-\frac{2\pi i m n^2}{4}\right] = \exp\left[-\frac{2\pi i m (2l+1)^2}{4}\right] \equiv \eta = \begin{cases} 1 & m \equiv 0 \pmod 4 \\ -i & m \equiv 1 \pmod 4 \\ -1 & m \equiv 2 \pmod 4 \\ +i & m \equiv 3 \pmod 4 \end{cases} \tag{10.16}$$

$$\therefore\ G(m) = \sum_{n:\text{even}} \int_{\frac{1}{2}mn}^{m+\frac{1}{2}mn} \exp\left[\frac{2\pi i S^2}{m}\right] dS + \sum_{n:\text{odd}} \eta \cdot \int_{\frac{1}{2}mn}^{m+\frac{1}{2}mn} \exp\left[\frac{2\pi i S^2}{m}\right] dS \tag{10.17}$$

ここで

$$\sum_{n:\text{even}} \int_{\frac{1}{2}mn}^{m+\frac{1}{2}mn} f(s)\, dS = \sum_{k=-\infty}^{+\infty} \int_{mk}^{m(k+1)} f(s)\, dS = \int_{-\infty}^{+\infty}$$

より $G(m)$ の第 1 項は

$$\sum_{n:\text{even}} \int_{\frac{1}{2}mn}^{m+\frac{1}{2}mn} \exp\left[\frac{2\pi i S^2}{m}\right] dS = \int_{-\infty}^{+\infty} \exp\left[\frac{2\pi i S^2}{m}\right] dS = \sqrt{m} \int_{-\infty}^{+\infty} \exp[2\pi i \xi^2]\, d\xi \tag{10.18}$$

また、

$$\sum_{n:\text{odd}} \int_{\frac{1}{2}mn}^{\frac{1}{2}mn+m} = \sum_{k\ (n=2k+1)} \int_{m(k+\frac{1}{2})}^{m(k+\frac{3}{2})} \longrightarrow n : \text{even のときの } k \text{ を } k \to k+\frac{1}{2} \text{と置き換えたもの} \tag{10.19}$$

$G(m)$ の第 2 項は

$$\sum_{n:\text{odd}} \int_{\frac{1}{2}mn}^{m+\frac{1}{2}mn} \exp\left[\frac{2\pi i S^2}{m}\right] dS = \int_{-\infty}^{\infty} \exp\left[\frac{2\pi i S^2}{m}\right] dS = \sqrt{m} \int_{-\infty}^{\infty} \exp[2\pi i \xi^2]\, d\xi \tag{10.20}$$

したがって、

$$G(m) = (1+\eta)\sqrt{m} \int_{-\infty}^{+\infty} \exp[2\pi i \xi^2]\, d\xi \tag{10.21}$$

となり、Gauss 積分に帰着できた。実行すると

$$\begin{aligned} \int_{-\infty}^{\infty} \exp[2\pi i \xi^2]\, d\xi &= \sqrt{\frac{\pi}{-2\pi i}} = \sqrt{\frac{i}{2}} = \frac{1}{\sqrt{2}}\sqrt{i} \\ &= \frac{1}{\sqrt{2}}\sqrt{e^{\frac{\pi}{2}i}} = \frac{1}{\sqrt{2}} e^{\frac{\pi}{4}i} = \frac{1}{\sqrt{2}}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) \\ &= \frac{1}{2}(1+i) \end{aligned} \tag{10.22}$$

$$G(m) = \frac{1}{2}(1+i)(1+\eta)\sqrt{m} \tag{10.23}$$

$$\eta = \begin{cases} 1 & m \equiv 0 \pmod 4 \\ -i & m \equiv 1 \pmod 4 \\ -1 & m \equiv 2 \pmod 4 \\ +i & m \equiv 3 \pmod 4 \end{cases}$$

$$G(m) = \begin{cases} (1+i)\sqrt{m} & m \equiv 0 \pmod 4 \\ \sqrt{m} & m \equiv 1 \pmod 4 \\ 0 & m \equiv 2 \pmod 4 \\ i\sqrt{m} & m \equiv 3 \pmod 4 \end{cases}$$

従って、とくに $m = p$(素数) のとき、$m \equiv 0, m \equiv 2$ は除外。

$$G(p) = \begin{cases} \sqrt{p} & p \equiv 1 \pmod 4 \\ i\sqrt{p} & p \equiv 3 \pmod 4 \end{cases}$$

[証明終]

11　代数的整数論序論

目標：平方剰余相互法則の真相をのべる．それは、それ自体閉じた定理であるが、ただそれだけならば、ありふれた数学の単なる定理と同様である．

その背後に、はるか未来を見通した秘密が隠されているのである。ガウスの偉大なところは、その事実を把握していたことであるらしい。

ずばり、結論をいうと、有理素数が,『２次体において因数分解される規則を平方剰余の相互法則が記述する』というのがその真の意味である。これが高木貞治をして、類体論のもっとも卑近な例をあたえているといわしめた所以である。

具体的な例をあげる。

例：素数 p に対して,

$$x^2+y^2=p$$

が整数解をもつような p はどのようなものか。

答えは、$p\equiv 1(\mod 4)$ なる素数。

[[真相]]:

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$$

となる．平方剰余（ルジャンドル）記号があらわれるのである。

もっと正確にいうと,

$$\left(\frac{-4}{p}\right)=(-1)^{\frac{p-1}{2}}$$

ここで、ルジャンドル記号の性質：

$$\left(\frac{-4}{p}\right)=(-1)^{\frac{p-1}{2}}=\left[\left(\frac{2}{p}\right)\right]^2\left(\frac{-1}{p}\right)=\left(\frac{-1}{p}\right)$$

かつ、平方が 1 になることをつかう。

うえの話しを、筋をつけるための理論を展開しよう。それがガウスの整数である。

11.1　ガウスの整数　K(i)

つぎのような複素数の集合を考える:

$$\{a+ib\}$$

ここで、a,b は有理数である。これを、ガウスの数体とよぶ。体をなすことは、加減乗除によって、この集合が閉じていることをいう。ただし除法に関しては, ゼロをのぞく。

ここで、有理数 a,b をとくに、整数（有理整数）に制限する。これは、割り算をのぞいて、加減と積に関して閉じている。この集合がガウスの整数である。これを, $\alpha=a+ib$ と記す. 以下、ギリシャ文字は、ガウスの整数をあらわす。

複素共役は、$\bar{\alpha}=a-ib$ で与えられるのは、通常のものと一致する。

$$\alpha=\beta\gamma\cdots$$

一般的事実を列挙しておく.

1: $\{a+ib\}$ の全部は, 和と積に関して閉じている.
2: $\alpha(\equiv a+ib)$ が, $\beta(\equiv a'+ib')$ で割り切れる. $\rightarrow \alpha=\beta\gamma$. β は, α の約数. これは、有理整数の場合と同様である.
3: ノルム (Norm) ：$N(\alpha)=\alpha\bar{\alpha}$ によって定義する. これは通常の複素数の大きさと同じである.

定義：単数とは, 1 の約数あるいは, すべての整数の約数となるものである.

単数のノルムは 1 である. これは, $\epsilon\alpha=\alpha$ であるから, 両辺のノルムをとって, $N(\epsilon\alpha)=N(\epsilon)N(\alpha)=N(\alpha)$ より, $N(\epsilon)=1$.

有理整数の単数は, ±1 のみ.

ガウスの整数の場合は, $\epsilon=x+iy$ (x,y は有理整数) とおいて, $N(\epsilon)=x^2+y^2=1$ から, $x=\pm1, y=\pm1$ となるので, ガウスの整数の場合の単数は

$$\epsilon=\pm1,\pm i$$

の 4 個になる.

定義: $\alpha = \epsilon\beta$ のとき, α と β は同伴数と称する.

ガウスの整数において、(通常の) 有理整数と同様の素因数分解ができる。

●: $\alpha = a + ib$ の分解.

$\alpha = \beta\gamma$ とおくと, $N(\beta\gamma) = N(\beta)N(\gamma)$. 従って, $N(\alpha)$ が素数であれば, $N(\beta)$ あるいは, $N(\gamma)$

11.2　2 次体の一般理論

2次体というのは、$\sqrt{m}$ （m は平方数を含まない有理整数＝有理数での整数；2次の整数と区別するためにつかう）を、$x+y\sqrt{m}$ 、ここで,「(x,y) は有理数」となる全体をいう。

いか、いくつかの用語の定義をしておこう。

- $\alpha = x+y\sqrt{m}$ に対して, $\bar{\alpha} = x-y\sqrt{m}$ を α の共役とよぶ.（ノート：複素共役を一般の2次の数に拡張するのである。実の無理数に対しても適用するのである）
- トレース $\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha}$
- ノルム: $N(\alpha) = \alpha\bar{\alpha}$

2次体の数は、別の言い方をすると、有理係数の2次方程式の根のことである。

これを一般化すると、有理数係数の代数方程式の根を代数的数という。2次体というのは、つまり、2次の代数体のことにほかならない。2次の特殊性によって、それは、$x+y\sqrt{m}$ と平方根をつかって表せるのである。

そこで, 有理整数の考えを代数的数に拡張しようというのである. すぐに思い浮かぶのは、(x,y) を有理整数に制限したもの

$$x+y\sqrt{m}$$

を2次の整数と定義できそうである. しかし, それでは, 不足であるというのが問題のポイントである.

2次の係数が1である有理整数係数の2次方程式の根が2次の整数であるということであれば、たとえば、

$$x^2-3x+7=0$$

を考えよう. この根は

$$x=\frac{3\pm\sqrt{-19}}{2}$$

となり、うえの形にはならない。しかし、これを整数の定義としてもよいというのである。

どんな形のものが 2 次の整数となるべきかを確定しよう. 結果を定理の形でのべておこう。

定理 A

m を平方因数を有しない整数として, 2 次体 $K(\sqrt{m})$ における整数はつぎのように与えられる.

(i) $m \equiv 2, 3(\mathrm{mod}4)$ のときには, 整数は

$$x + y\sqrt{m} \quad (x, y) \text{ は有理整数}$$

(ii) $m \equiv 1(\mathrm{mod}4)$ のときには, 整数は

$$\frac{x + y\sqrt{m}}{2} \quad (x, y) \text{ は有理整数, かつ } x \equiv y \pmod 2$$

これは、定理というより、定義ではないかとも思われるのであるが、2 次の整数というものの性格を規定すると、導かれるという意味で定理になる。

さて、2 次の整数のもつべき性格とはなにか。以下、その集合を $\mathrm{Z}(\sqrt{m})$ と記す.

(i) $\alpha, \beta \in \mathrm{Z}(\sqrt{m})$ ならば、$\alpha \pm \beta \in \mathrm{Z}(\sqrt{m})$.

(ii) $\alpha \in \mathrm{Z}(\sqrt{m})$ ならば, 共役 $\bar{\alpha} \in \mathrm{Z}(\sqrt{m})$

(iii) 有理数で、かつ 2 次の整数であるものは, 有理整数である。

(iv) 以上の 3 つの条件を満たして整数の範囲をできるだけ広げる。

この (iv) は、要領を得ないが、以下の説明でその意図がうかびあがる。

うえの (i) - (iii) は、

$$a + b\sqrt{m} \quad (a, b \text{ 有理整数})$$

ととれば、自動的に充足されるが、この形以外の形の可能性はないかというのである.

以上のもとに、定理 A に示されたものが, 2 次の整数であることを示す.

[定理 A の証明]: まず、α をこのような整数としよう. すると, その共役 $\bar{\alpha}$ も整数で, $\alpha = x + y\sqrt{m}$ とおくと, $\bar{\alpha} = x - y\sqrt{m}$ と書け（ x, y は有理数であることに注意)：

$$\alpha + \bar{\alpha} = 2x, \quad \alpha\bar{\alpha} = x^2 - y^2 m$$

は、最初の規約により有理整数になる. $\alpha, \bar{\alpha}$ はしたがって, 有理整数係数の 2 次方程式

$$t^2 + at + b = 0$$

の根になる. さて, うえのことから、$(2x)^2-4(x^2-4y^2m)=4y^2m$ も有理整数となる。m は平方因数をもたないことから, $2y$ は有理整数となる. （何故なら, $2y=u/v$ なる規約分数とすると, $4y^2m=mu^2/v^2$ となり, m は平方因数をもたないことから $4y^2m=mu^2/v^2$ は, 有理整数になることはない. これは矛盾である.)

したがって, $2x=p, 2y=q$ とおくと, 整数となるべき数は、

$$\alpha=\frac{p+q\sqrt{m}}{2}$$

の形の数である. ただし、p,q　は有理整数である。

さて、$\alpha\bar{\alpha}$ が有理整数であることから、

$$\frac{p^2-mq^2}{4}=\text{整数}$$

つまり,

$$p^2\equiv mq^2 \pmod 4$$

となることを要する. これに適合する p,q の値がいかなる場合が生じるかを検討する. それには, mod 4 について場合分けを行えばよい.

(a): $m\equiv 2(\bmod 4)$: このときは, $m=$ 偶 ゆえ、p は偶数, かつ, q も偶数となるので、整数 $\alpha=\frac{p+q\sqrt{m}}{2}$ は, $x+y\sqrt{m}$ $(x,y$ は有理整数$)$ の形になる.

(b) $m\equiv 3(\bmod 4)$: この場合も、p,q ともに, 偶数であることがわかる. ゆえに, 整数 $\alpha=\frac{p+q\sqrt{m}}{2}$ は, $x+y\sqrt{m}$ $(x,y$ は有理整数$)$ の形をとる.

うえの (a),(b) をまとめると, 定理の (i) の場合が示された.

(c) $m\equiv 1(\bmod 4)$: このときは, p,q はともに偶数である場合が許容されることすぐにわかる. そのほかに, p,q がともに, 奇数の場合も適合する. なぜなら, $m=4k+1$ であるから, $p=2a+1, q=2b+1$ とすると, $p^2-(4k+1)q^2$ は, 4 の倍数がでてくる. 2 つの場合をまとめると, 整数は $\alpha=\frac{p+q\sqrt{m}}{2}$ で, $p\equiv q \pmod 2$ の形になる.

以上で, 2 次の整数の形が決まったが、これが、整数のもつべき性質をもつかどうかを確認しておく必要がある.

$m\equiv 2,3(\bmod 4)$ の場合は, ただちにでてくる（証明略) .

$m\equiv 1(\bmod 4)$ の場合にたしかめる.

$\alpha=\frac{p+q\sqrt{m}}{2}, p\equiv q \pmod 2$, および, $\beta=\frac{p'+q'\sqrt{m}}{2}, p'\equiv q' \pmod 2$ とおくと, 和 (差) に関して

$$\frac{p+q\sqrt{m}}{2}\pm\frac{p'+q'\sqrt{m}}{2}=\frac{(p+p')\pm(q+q')\sqrt{m}}{2}\quad p\pm p'\equiv q\pm q' \pmod 2$$

積に関しては

$$\frac{p+q\sqrt{m}}{2}\cdot\frac{p'+q'\sqrt{m}}{2}=$$

以上から定理 A の内容が確認された.

11.3　イデアル

２次体の整数においても整除の関係が決定的に重要になる. α を　β で割ると、商 γ と余り κ がでる：

$$\alpha = \beta\gamma + \kappa$$

ここで、κ は,

$$|\kappa| < |\beta|$$

を満たすことが肝要である。これによって互除法が可能になる。

割り切れる場合：$\alpha = \beta\gamma$ は、さらに、β, γ を分解していくという具合に連鎖がつづいて、最終的に素なる因数（素数）に分解されるところで終わる。

ここで、問題は、素因数分解が一通りに決まるかということである。つぎの例から明らかなように、ただちに、破綻するのである。

$K(\sqrt{-5})$ の整数を考えて、つぎに分解を考える：

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \tag{11.1}$$

また、

$$21 = 3 \times 7 = (4 + \sqrt{-5})(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) \tag{11.2}$$

のように、６は２通り、２１は３通りに分解される。そして、それぞれの因数は素数であることがわかる. なぜなら、

$$3 = \alpha\beta$$

として、両辺のノルムをとると、$N(3) = 9 = N(\alpha)N(\beta)$. $N(\alpha) > 1, N(\beta) > 1$ より、$N(\alpha) = N(\beta) = 3$　　となり、$\alpha = x + \sqrt{-5}$ とすれば (x, y は有理整数; $K(\sqrt{-5})$ の整数は、この形であることに注意）,$x^2 + 5y^2 = 3$ を満たす整数は存在しない。他の因数も同様である。

このように、２次体の整数では、素数分解の一意性が成り立たないのは、むしろありふれた現象であるといえる。たとえば、$K(\sqrt{-26})$ において

$$27 = 3^3 = (1 + \sqrt{-26})(1 - \sqrt{-26})$$

も他の例である。

一意性が成り立たたないと数の系としてこれ以上議論することは不可能になる。これを打開するために、イデアルの概念が導入された。これを定義するまえに、理想数の考えに

ついてふれておこう。うえの $K(\sqrt{-5})$ の場合に、Kummer は, $2, 1+\sqrt{-5}$ などの素数をさらに分解するような理想数をつぎのように導入した：

$$\begin{cases} 2 & = A^2, 3 = B\bar{B},\ \ 1+\sqrt{-5} = AB, 1-\sqrt{-5} = A\bar{B}, \\ 3 & = B\bar{B}, 1+2\sqrt{-5} = \bar{B}C, 1-2\sqrt{-5} = B\bar{C} \\ 7 & = C\bar{C}, 1+2\sqrt{-5} = \bar{B}C, 1-2\sqrt{-5} = \bar{B}\bar{C} \end{cases}$$

うえの式で、A, B, C は実際の数ではないが、仮にそのようなものを「理念的」な数として、Kummer は便宜的に導入したのである。

この理念的な数を、実際の２次体の整数の『集合』で置き換えようというのが、出出金人のイデアル論である。

イデアルの定義：整数全体 の集合を O とおく. （これもイデアルであることに注意) R を O の部分集合として, つぎの条件をみたすとき、 R をイデアルとよぶ。

(i): α, β が R の要素とすると, $\alpha \pm \beta$ も R にふくまれる.

(ii): R の要素 α に, O の要素 λ をかけたもの $\lambda\alpha$ は, R に含まれる

(i), (ii) をもとに, ２次の整数のイデアルの形を確定することができる:

イデアルの標準基底

$A = [a, b+c\omega]$、ただし、a は、A に含まれる最小の正の有理整数, かつ, c は, A の整数で, ω の係数が最小の正の有理整数. ω は、$m \equiv 2, 3 \pmod 4$ にたいして, $\omega = \sqrt{m}$, $m \equiv 1 \pmod 4$ にたいして, $\omega = \frac{1+\sqrt{m}}{2}$

まず、この意味ですが、なんで「最小」がでてくるかという疑念ですが、じつは、なんでもないことです。有理整数のつくるイデアルを考えると, たとえば、2 の倍数は、あきらかにイデアルをつくる。ここにふくまれる数の最小の正の整数は、2 そのもので、あとは、2 の倍数になるのは明らかです。２次の整数の場合は無理数がでてくるので、その部分の最小単位 c があると考えることができるということです。だから、有理整数の場合の自然な拡張にすぎないといえる。(どうでしょうか)

[証明] (a) まず, A が有理整数を含む. これはつぎのことからいえる. α を, A の数として, その共役 $\bar{\alpha}$ の積 $\alpha\bar{\alpha}$ をつくると,A に含まれる. (because; イデアルのもつ性質の (ii), つまり, 『α に整数全体 O の数 λ をかけたもの $\lambda\alpha$ も A に含まれる』ことから、$\lambda = \bar{\alpha}$ にとればよい). そこで、$\alpha\bar{\alpha}$ は有理整数となることがわかっている。すなわち、A は有理整数を含むことがわかる。

(b): A の任意の有理整数の整数倍はまた A に含まれる (これも (ii) の特別の場合としていえる)。さて 整数 t を考えると, これは、A に含まれる有理整数の『(正で) 最小のもの a』 の倍数でなければならない. これは以下のようにしていえる. 一般に, 有理整数の除法の原則から, $t = ka + a'$ とかけて, $a' \neq 0$ であったとしよう. すると $0 < a' < a$. ところで、$a' = a - ka$ はまた, A の要素（because; a, ka は A の要素であるから) で、かつ $a' < a$ であるから、最小であるとした a より小さい有理整数 a' が A の要素となることにより矛盾が生じる。故に, $a' = 0$, すなわち、$t = ka$.

(c) つぎに, A の整数は、２次の整数の一般論から, $x + y\omega$ の形でかける. ただし, x, y は有理整数である. ここで、A にふくまれる整数のうちで、ω の係数が最小の正の有理整数をもつものを, $b + c\omega$ としよう. すると、$x + y\omega$ にたいして、係数 y は, c の整数倍でなければならない. これは以下のようにいえる；$y = qc + r$ とすると, $x + y\omega - q(b + c\omega) = x - qb + r\omega$ は, A に含まれる。(コメント：なぜ, この数を考えるのかちょっと思いつきにくいところがあるが)。 もし $r \neq 0$ としてみると, $0 < r < c$ であるので, これは, ω の係数が最小の数 c より小さい A の整数があらたに生じて矛盾が生じる. ゆえに, $r = 0$ でなければならない; すなわち、$y = cq$.

(d) そこで、A に属する有理整数であるので, うえの (b) でのべたことから $x - qb$ は a の倍数でなければならない. ゆえに, p を有理整数として, $x - qb = pa$ あるいは、$x = pa + qb$. 以上をまとめると；イデアル A の整数は、p, q を有理整数として

$$pa + q(b + c\omega)$$

と書けることがわかる。[証明終]

イデアルの形が２つの基底, $a, b + c\omega$ の有理整数の結合として形で書けることを明記するために、

$$A = [a, b + c\omega]$$

なる記法を用いる。つまり、A に属する整数は、$pa + q(b + c\omega)$ として表されるというのである。

11.4　イデアルの積

$$A = (\alpha_1, \cdots, \alpha_n), B = (\beta_1, \cdots, \beta_m)$$

を２つのイデアルとする. つぎのように定義する：

$$AB = (\alpha_1\beta_1, \cdots, \alpha_i\beta_j, \cdots, \alpha_n\beta_m)$$

のような nm 個の整数からなるイデアルである。これはイデアルを構成することはイデアルの定義にもどればたしかめられる：また、これは

$$\sum_{\mu\nu} \xi_{ij}\alpha_i\beta_j, \quad \xi_{ij}\epsilon O$$

で表される数の集合である。

命題：

$$AB = BA,\ (A+B)C = AB + AC,\ (AB)C = A(BC)$$

ここで、つぎの問を設定する。

$AB = AC$　なるとき, $B = C$ は成立するか

これを証明するために, 以下の手順を行う。
まず、共役イデアルを定義する：それは

$$\bar{A} = (\alpha_1^*, \cdots, \alpha_n^*)$$

命題
$J = AB$ のとき, $\bar{J} = \bar{A}\bar{B}$
証明： $AB = (\alpha_1\beta_1, \cdots, \alpha_i\beta_j, \cdots, \alpha_n\beta_m)$ より,

$$\bar{AB} = ((\alpha_1\beta_1)^*, \cdots, (\alpha_i\beta_j)^*, \cdots, (\alpha_n\beta_m)^*) = (\alpha_1^*\beta_1^*, \cdots, \alpha_n^*\beta_m^*) = \bar{A}\bar{B}$$

定理
$A\bar{A}$ は, 有理整数から生ずる単項イデアルになる.

証明：(i) 単項イデアルのときは, $A=(\alpha), \bar{A}=(\alpha^*)$, より $A\bar{A}=(\alpha\alpha^*)$, かつ $\alpha\alpha^*$ は有理整数となるので成立する.

(ii) $A=(\alpha,\beta), \bar{A}=(\alpha^*,\beta^*)$ より,

$$A\bar{A}=(\alpha\alpha^*,\alpha\beta^*,\alpha^*\beta,\beta\beta^*)$$

ここで,

$$a=\alpha\alpha^*, b=\alpha\beta^*+\alpha^*\beta, c=\beta\beta^*$$

とおくと, a,b,c は　$A\bar{A}$ に属する有理整数ゆえ, それらの最大公約数を n とすれば, $ax+by+cz=n$ を満たす (x,y,z) なる有理整数がとれる. 従って,　n は $A\bar{A}$ に属する有理整数である.

一方, $\alpha\beta^*, \alpha^*\beta$ は n で割り切れる. なぜなら,

$$\frac{\alpha\beta^*}{n}+\frac{\beta\alpha^*}{n}=\frac{b}{n}(\equiv p),\quad \frac{\alpha\beta^*}{n}\cdot\frac{\beta\alpha^*}{n}=\frac{c}{n}(\equiv q)$$

はともに有理整数で, $\frac{\alpha\beta^*}{n}, \frac{\alpha^*\beta}{n}$ は, $x^2-px+q=0$ の根であるから, 整数である. ゆえに, $\alpha\beta^*, \alpha^*\beta$ は, n で割り切れので, $A\bar{A}$ に含まれる. よって, n は $A\bar{A}$ に含まれる. すなわち, $A\bar{A}=(n)$.　[証明おわり]

うえの定義で出てきた n をイデアル A のノルムとよぶ: $N(A)=n$

これをつかうと次の定理がでてくる：

「定理」： $AB=AC$ なるとき, $B=C$.

証明：両辺に $\bar{A}$ をかければ, ノルムの定義から $nB=nC$ となり, これからでてくる.

つぎの定理が重要である

定理

$A=[a,b+c\omega]$ が標準基底で表されるとき,

$$N(A)=ac$$

証明：$A \equiv cA_0 = c[a_0, b_0 + \omega]$, ここで, $a = a_0, b = cb_0$. ゆえに,

$$N(A) = N(cA_0) = N(c)N(A_0) = c^2 N(A_0)$$

従って, $N(A_0) = a_0$ を示せばよい.

11.5　2 次体の素イデアル：素数の分解

まず、

$$\mathbf{P} = [p, b + c\omega] \tag{11.3}$$

を素イデアルとして, $\mathbf{P}$ にふくまれる最小の有理整数 p は, 有理素数であることに注意する。

『なぜならもしそうでなければ、$p = ab$ と分解できて、$1 < a < p$ (あるいは、$1 < b < p$) となる a, b が $\mathbf{P}$ のなかに存在することになり、p の最小性に反する』

さて、$p = \mathbf{PQ}$ と 2 次体の素イデアルで分解できたとしよう。ノルムをとることにより

$$N(p) = N(\mathbf{P})N(\mathbf{Q}) = p^2 \tag{11.4}$$

これから、$N(\mathbf{P})$ は, p で割り切れる。以下に 2 つの場合が生じる：

(i) $N(\mathbf{P}) = p, N(\mathbf{Q}) = p$

(ii) $N(\mathbf{P}) = p^2 N(\mathbf{Q}) = 1$

ここで、(i) の場合は、$\mathbf{Q} = \bar{\mathbf{P}}$ となり、(ii) の場合は,　$p = \mathbf{P}$ となる。つまり、p は、2 次のイデアルで分解されない。

まとめると、

$$N(\mathbf{P}) = p^f \quad (f = 1, 2) \tag{11.5}$$

さて、$\mathbf{P} = [p, b + c\omega]$ において、c は p の約数であったから、今の場合 2 つの場合に分けられる。

●: $c = p$, かつ b は、c の倍数であることから p の倍数 ($b = b_0 p$) ゆえ,

$$\mathbf{P} = [p, b_0 p + p\omega] = [p, p\omega] = p$$

ここで、$[a, na + x] = [a, x]$ をつかう。

●: $c = 1$ のとき、

$$\mathbf{P} = [p, b + \omega], \quad \text{かつ } N(\mathbf{P}) = p \tag{11.6}$$

従って、定理 X 系 b より、$N(b+\omega)$ が、p でわりきれる。

そこで、

(1): $m \equiv 2,3 \ (\mathrm{mod}4)$ のとき、$\omega = \sqrt{m}$ ゆえ,

$$N(b+\omega) = (b+\sqrt{m})(b-\sqrt{m}) = b^2 - m$$

が p で割り切れる。よって、$b^2 \equiv m \ (\mathrm{mod}p)$, あるいは、

$$(2b)^2 \equiv 4m \ (\mathrm{mod}p) \tag{11.7}$$

(2): $m \equiv 1 \ (\mathrm{mod}4)$ のとき, $\omega = \frac{1+\sqrt{m}}{2}$ ゆえ、

$$N(b + \frac{1+\sqrt{m}}{2}) \equiv 0 \ (\mathrm{mod}p)$$

ゆえ

$$(2b+1)^2 \equiv m \ (\mathrm{mod}p) \tag{11.8}$$

(11.7) と (11.8) をまとめると、$r = 2b, 2b+1$ として

$$r^2 \equiv d \ \ (\mathrm{mod}p) \tag{11.9}$$

となることが $p = \mathbf{P}\bar{\mathbf{P}}$ と分解されるために必要条件である。ただし、

$$d = 4m \ (m \equiv 2,3 \ (\mathrm{mod}4) \text{ のとき}, \ \ d = m \ (m \equiv 1 \ (\mathrm{mod}4) \text{ のとき} \tag{11.10}$$

定義：d を**判別式** という.

以上のことから、平方剰余記号をつかえば、$p = \mathbf{P}\bar{\mathbf{P}}$ と分解されるための必要条件として,

$$(\frac{d}{p}) = 1 \tag{11.11}$$

この関係式が、$p = \mathbf{P}\bar{\mathbf{P}}$ となるために十分なことの証明：

(I) p が m の約数でないとする。さらに、$p \neq 2$ の場合を考える。$p = 2$ のときは、別途あつかう。

$\mathbf{P} = [p, r+\sqrt{m}], \bar{\mathbf{P}} = [p, r-\sqrt{m}]$ とおくと,

$$\mathbf{P}\bar{\mathbf{P}} = (p^2, 2pr, r^2 - m) = p(p, 2r, k) \equiv (p)$$

ここで、$k = \frac{r^2-m}{p}$ = 有理整数. かつ、$(p, 2r, k) = (1)$ (単項イデアル) に注意。したがって、$p = \mathbf{P}\bar{\mathbf{P}}$ と分解されることがわかる。

さらに、$(\mathbf{P}, \bar{\mathbf{P}}) = (p, r + \sqrt{m}, r - \sqrt{m})$ は, $2r$ を含み、かつ $(p, 2r) = 1$ ゆえに、$(\mathbf{P}, \bar{\mathbf{P}}) = 1$ 従って、$\mathbf{P} \neq \bar{\mathbf{P}}$.

(II) p が m の約数なるとき,
$r = 0$ とおける；ゆえに

$$\mathbf{P} = (p, \sqrt{m}), \bar{\mathbf{P}} = (p, -\sqrt{m}) \tag{11.12}$$

ゆえに $\mathbf{P}\bar{\mathbf{P}} = p$, かつ, $\mathbf{P} = \bar{\mathbf{P}}$

したがって、$p(\neq 2)$ 判別式の約数であるときは、

$$p = \mathbf{P}^2 \tag{11.13}$$

すなわち、p は分岐する。

ここで、残されていた $p=2$ の場合を扱う。

まず、うえの (II) の場合とおなじく、2 が m の約数となる場合をかんがえると、

(a) $m \equiv 2, \pmod 4$ の場合, $r \equiv m \equiv 0 \pmod 2$ より、

$\mathbf{P} = [2, \sqrt{m}], \ \bar{\mathbf{P}} = [2, -\sqrt{m}]$ となり、$\mathbf{P} = \bar{\mathbf{P}}$ となる。従って、

$$2 = \mathbf{P}^2$$

となる。

(b) $m \equiv 3, \pmod 4$ の場合, $r \equiv m \equiv 1 \pmod 2$ より、$\mathbf{P} = [2, 1+\sqrt{m}], \ \bar{\mathbf{P}} = [2, 1-\sqrt{m}]$. この場合、(I) と同様に、

$$\mathbf{P}\bar{\mathbf{P}} = (4, 4, 1-m) = 2$$

かつ、$\mathbf{P} = \bar{\mathbf{P}}$ であるから、

$$2 = \mathbf{P}^2$$

となる。

(c) $m \equiv 1, \pmod 4$ の場合：

$$\mathbf{P} = [2, b + \frac{1+\sqrt{m}}{2}]$$

となる。ここで、$r^2 \equiv m \equiv 1 (\mathrm{mod}\ 2)$ ゆえ、$r = \pm 1$ これから、$b = 0$ あるいは、$b = -1$ がでてくる。(なぜなら、$r = 2b+1 = 1$ より、$b = 0$, また、$r = b = -1$ にしたがって、$\frac{1+\sqrt{m}}{2}$ または, $\frac{1+\sqrt{m}}{2} - 1$ が、$\mathbf{P}$ でわりきれる。そこで、その積; $\frac{m-1}{4}$ が有理整数でかつ 2 で割り切れなければならない。つまり、 $m-1 = 8k$: ゆえに、$m \equiv 1 (\mathrm{mod}\ 8)$. これが、$\mathbf{P}\bar{\mathbf{P}} = 2$ の必要条件である。またもし、$\frac{m-1}{4}$ が有理整数でかつ 2 で割り切れないとすると、$m-1 = 4(2l+1)$; $m = 8l+5$ となり, $\mathbf{P} = 2$ である。

逆に、$m \equiv 1 (\mathrm{mod}\ 8)$ であれば、

$$\mathbf{P} = [2, \frac{1+\sqrt{m}}{2}], \bar{\mathbf{P}} = [2, \frac{1-\sqrt{m}}{2}]$$

で、

$$\mathbf{P}\bar{\mathbf{P}}(4, 2, \frac{1-m}{4}) = 2$$

となり、かつ

$$(\mathbf{P}, \bar{\mathbf{P}}) = (2, \frac{1+\sqrt{m}}{2}, \frac{1-\sqrt{m}}{2}) = 1$$

となり、$\mathbf{P} \neq \bar{\mathbf{P}}$ である。

従って、

- : $m \equiv 1 \pmod 8$ ならば、$2 = \mathbf{P}\bar{\mathbf{P}}$; $\mathbf{P} \neq \bar{\mathbf{P}}$
- : $m \equiv 5 \pmod 8$ ならば、$2 = \mathbf{P}$

まとめると：

素数の 2 次体における分解定理：
◯: ($p \neq 2$) なる p が判別式 d の約数でないとき：

●: $\left(\frac{d}{p}\right) = 1$ ならば、$p = \mathbf{P}\bar{\mathbf{P}}$
●: $\left(\frac{d}{p}\right) = -1$ ならば、$p = \mathbf{P}$

$p = 2$ は例外である。
• $m \equiv 2, 3 \pmod 4, d \equiv 0$ のとき、$\mathbf{P}^2 = 2$.
• $m \equiv 1 \pmod 4$ $(d = m)$ のとき、$\mathbf{P}\bar{\mathbf{P}} = 2$
• $m \equiv 5 \pmod 8$ $(d = m)$ のとき、$2 = \mathbf{P}$ (分解せず)

分岐定理
$p = \mathbf{P}^2$ なる素数は、判別式 d の約数となるものである。

コメント：
アーベル体＝類体という言明が、高木貞治のよってたつ位置である。
アーベル体　＝　k 上の代数体のガロア群がアーベル群となる拡大体 K/k である。
この観点から一般のガロア群の具体的様相はほとんどわからないということのようである。アーベル体という特殊なものに限定すると少しわかるということである。
2 次体は、有理数体のアーベル体のごく手近な例を形成していて、その本質を垣間みせてくれる。2 次体の類数公式をゼータ関数で計算されるのはその頂点に位置するものとみられる。