整数が持つ色々な性質

—— 素数と関連した問題

森田康夫

＜前書き＞

本稿は、東北地方の数学が好きな高校生を対象とし、1997年8月川井数理科学財団主催で行われた「仙台セミナー」での講演を、加筆しまとめたものです。

§1. 整数の定義と性質

数学基礎論を使う最も厳密な定義でも、自然数(正の整数)の定義は、数学的帰納法で行います。したがって、最初の数1から始め、1の次の数として2を作り、2の次の数として3を作り、以下同様にして n の次の数として $n+1$ を作り、このようにして作られる数の全体を**自然数**と呼び、$\mathbb{N}$ で表します。

自然数の全体 $\mathbb{N}$ には、帰納法を使って和と積が定義できます：

$$(m+1)+n=(m+n)+1,\ (m+1)\times n=(m\times n)+n.$$

また、小学校で習ったように、負の数を考えることにより、自然数から整数ができ、整数から**有理数**ができ、有理数から**実数**が構成できます。この場合、自然数から有理数を作るのは簡単ですが、有理数から実数を作るのは極限を考える必要があり、無限に関する公理[1]の取り方に自由度があります。この意味で、数学の中でも整数は最も基礎のしっかりした対象です。[2]

さて解析学や幾何学では、実数の上の関数や幾何学的対象を研究することになります。これに対して、整数論(数論)では、自然数、整数、有理数などの非連続的(離散的)な対象を研究します。非連続な対象は、ぐにゃぐにゃと変形する自由度がないので、非常に剛性が高く、その意味で結晶のような硬い感じがする数学的対象です。

[1] 選択公理や連続体仮説など。

[2] 数学は幾つかの公理を基にして築かれます。数学の基礎となるのは集合論ですが、自然数はその中でも一番基礎にあり、どの様な数学の体系にも共通に含まれます。

§2. 素因数分解の一意性

整数の全体を $\mathbb{Z}$ で表します。この上には、和と積と言う二つの演算が有ります。整数の和は、理論的にも非常に簡単なものですが、整数の積は、かなり高度なものを含みます。例えば a を自然数とし、変数 x, y についての方程式

$$x \times y = a \qquad x,\ y \geq 2$$

を考えます。これが整数の範囲で解を持つということは、a が合成数であることを意味し、かなり難しい性質です。[3]

一般に自然数 p が、1 ではなく、かつ 1 と p 以外の自然数で割り切れないとき、p は**素数**であると言います。[4] 素数は古代のインドやギリシャで発見され、整数の計算を効率化する手段として使われました。

さて、自然数に関する最も大切な性質は次の定理です。

定理 1 (素因数分解の存在と一意性). n を任意の自然数とすると、有限個の素数 $p_1, p_2, \cdots, p_t$ と自然数 $e_1, e_2, \cdots, e_t$ が存在し、

$$n \ = \ p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_t^{e_t}$$

と書ける。しかも、n を与えたとき、このような表し方は唯一つしか存在しない。

この定理を整数に拡張すると、任意の整数 n は、

$$n \ = \ \pm\, p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_t^{e_t} \qquad (p_1, p_2, \cdots, p_t \text{は素数}、e_1, e_2, \cdots, e_t \text{は自然数})$$

と一意的に書けることが分かります。

定理 1 では、このような表現が存在することも大切ですが、一意性の方がはるかに重要です。その例として、§4 で $x^2 + y^2 = z^2$ の整数解を求めます。

---

[3] 例えば現在の計算機の性能では、200 けたの自然数が合成数かどうかを判定するのは困難です。

[4] この定義は、小学校で教えられますが、小学生に正確な意味が分かるとは思えません。

§3. 素数分布と素数定理

素数の性質を研究することは、整数論の中でも最も重要なテーマです。

まず下にある2,000以下の素数の表を見てください。

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997, 1009, 1013, 1019, 1021, 1031, 1033, 1039, 1049, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1129, 1151, 1153, 1163, 1171, 1181, 1187, 1193, 1201, 1213, 1217, 1223, 1229, 1231, 1237, 1249, 1259, 1277, 1279, 1283, 1289, 1291, 1297, 1301, 1303, 1307, 1319, 1321, 1327, 1361, 1367, 1373, 1381, 1399, 1409, 1423, 1427, 1429, 1433, 1439, 1447, 1451, 1453, 1459, 1471, 1481, 1483, 1487, 1489, 1493, 1499, 1511, 1523, 1531, 1543, 1549, 1553, 1559, 1567, 1571, 1579, 1583, 1597, 1601, 1607, 1609, 1613, 1619, 1621, 1627, 1637, 1657, 1663, 1667, 1669, 1693, 1697, 1699, 1709, 1721, 1723, 1733, 1741, 1747, 1753, 1759, 1777, 1783, 1787, 1789, 1801, 1811, 1823, 1831, 1847, 1861, 1867, 1871, 1873, 1877, 1879, 1889, 1901, 1907, 1913, 1931, 1933, 1949, 1951, 1973, 1979, 1987, 1993, 1997, 1999

このような表は、自然数全体の表から、2以外の2の倍数、3以外の3の倍数と、2以上の自然数の真の倍数全体を消してゆくことにより得られます。[5] 素数表を作るには、これが現在でも最も効率的な方法で、10万程度までの素数表を作ることな

[5] エラトステネス (Eratostenes,275–194BC) のふるい、素数の真の倍数のみを除く作業にすると、もう少し効率的になります。

ら、少し時間をかけると手作業でもできます。計算機を使うと、100万 (10^8) までの素数表が1秒もかからず作れます。

この表から何が読み取れるでしょうか? ある与えられた数が素数かどうかは、この表から分かるとおり、非常に難しい問題で、暗号理論の基礎となっています。ある数が与えられたとき、それが素数であるかどうかは計算機を使って判定できますが、現在の計算機の能力では、100けたの整数が素数かどうかを判定するのが大体の限界となっています。[6]

個々の数が素数であるかどうかは非常に判定が難しいのですが、「素数がどれ位たくさん有るか」と言う問題はもう少し易しくなります。実際このような素数表から、ガウス (C. F. Gauss, 1777–1855) は、「x を正の数とすると、x 以下の素数の個数 $\pi(x)$ は、$x \to \infty$ としたとき、漸近的に $x/\log_e(x)$ で与えられる (**素数定理**)」ことを予想しましたが、この予想は J. H. Hadamard と C. de la Vallée-Poussin により証明されました (1896年)。

ここに出てきた $x/\log_e(x)$ と言う関数は、漸近的には

$$\mathrm{Li}(x) = \int_0^x \frac{du}{\log_e(u)}$$

に等しく、こちらの方が $\pi(x)$ のより良い近似を与えます。[7] この関数を使うと素数定理は

$$\pi(x) \;=\; \mathrm{Li}(x) \;+\; \mathrm{O}(\sqrt{x}\log_e(x))$$

---

[6]素数であるかの判定と、素因数分解の双方のプログラムが有りますが、ふるいの理論や楕円曲線の理論など、高度な整数論が使われます。

[7]数値例をあげると、

$\pi(10,000) = 1,229,$	$10,000/\log_e(10,000) = 1,085.74,$	$\mathrm{Li}(10,000) = 1,246.14$
$\pi(20,000) = 2,262,$	$20,000/\log_e(20,000) = 2,019.49,$	$\mathrm{Li}(20,000) = 2,288.61$
$\pi(30,000) = 3,245,$	$30,000/\log_e(30,000) = 2,910.09,$	$\mathrm{Li}(30,000) = 3,276.9$
$\pi(40,000) = 4,203,$	$40,000/\log_e(40,000) = 3,774.78,$	$\mathrm{Li}(40,000) = 4,233.01$
$\pi(50,000) = 5,133,$	$50,000/\log_e(50,000) = 4,621.17,$	$\mathrm{Li}(50,000) = 5,166.55$

のようになります。この範囲では $\pi(x)$ より $x/\log_e(x)$ の方が10% 程度小さくなっていますが、x をもっと大きくすると、その比は1に近づきます。

と言う予想に精密化できます。[8] [9] [10]

§4. ピタゴラス数の決定とフェルマの問題への応用

素因数分解の応用としてピタゴラスの等式

$$(\mathrm{P}) \ : \ x^2 \ + \ y^2 \ = \ z^2$$

の自然数解 $x, y, z \in \mathbb{N}$ を求めます。

(x, y, z) を (P) の自然数解とし、k を x, y, z の最大公約数とすると整数解 $x = kx_1, y = ky_1, z = kz_1$ と書け、x_1, y_1, z_1 は互いに素で (P) をみたします。そこで必要なら x, y, z の代わりに x_1, y_1, z_1 を取ることにより、(x, y, z) は (P) の自然数解で、互いに素であるとします。

x, y の 2 つとも偶数なら、z も偶数となり、x, y, z は互いに素にはなりません。したがって、少なくとも 1 つは奇数となります。

偶数の 2 乗は 4 で割り切れ、奇数の 2 乗は 4 で割ると 1 が余ります。[11] したがって x, y の双方が共に奇数なら、$x^2 + y^2$ は 4 で割ると 2 余り、$z^2 = x^2 + y^2$ が平方数にはなりませんから、x, y のうちちょうど一つが偶数となります。そこで必要なら x, y を入れ換え x が偶数であるとします。このとき、y, z は共に奇数となります。

$$(\frac{x}{2})^2 \ = \ \frac{z-y}{2} \ \frac{z+y}{2}$$

と (P) を変形します。y と z は互いに素だから、$(z-y)/2$ と $(z+y)/2$ も互いに素な自然数となります。そこで上式の左辺を素因数に分解すると、幾つかの素数が

[8] この式は、$(\pi(x) - \mathrm{Li}(x))/\sqrt{x}\log_e(x)$ の大きさが、$x \to \infty$ としたとき、ある定数より大きくならないことを意味します。

[9] この予想はリーマン予想と呼ばれ、現在の数学における最大の未解決問題です。なおリーマン予想は通常は、「ゼータ関数 $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ の複素平面 $\mathbb{C}$ における零点 s で、$s \neq -1, -3, -5, \cdots$ であるものは、実部 $\mathrm{Re}(s)$ が $1/2$ になる」と言う形で表現されます。§5 参照。

[10] 素数表から読み取れることをこれ以外にあげると次のようなものが見つかります。まず N を自然数とし、a を N と素な整数とする。このとき、$p \equiv a \pmod{N}$ となる素数が無限個存在することが分かります。このことは**算術級数の素数定理**と呼ばれ、P. G. L. Dirichlet(1805-59) により証明されました。同様に、素数の組 (p, q) で、$q = p + 2$ となるものが無限個有りそうに見えます。これは**双子素数の問題**と呼ばれますが、現在まで未解決です。

[11] 偶数の 2 乗は $\equiv 0 \pmod{4}$、奇数の 2 乗は $\equiv 1 \pmod{4}$ となります。§7 参照。

偶数乗の形で現れます。これを右辺の二つの互いに素な数の積に分け直すのですから、左辺に出てくるある素数のべきは、$(z-y)/2$ と $(z+y)/2$ の一方にのみ現れます。ここで $(z-y)/2>0, (z+y)/2>0$ ですから、これらの数の素因数分解には -1 をつける必要はありません。よって

$$(z-y)/2=m^2, \quad (z+y)/2=n^2$$

と書けます。符号に注意して以上の結果をまとめると、次の定理が証明できました。

定理 2 . x,y,z が $x^2+y^2=z^2$ の整数解であるとする。このとき、必要なら x と y を入れ換えると、

$$x=k2mn,\ y=k(m^2-n^2),\ z=k(m^2+n^2) \qquad (k,m,n \text{ は整数})$$

と書ける。

これを使って、フェルマの方程式 $x^4+y^4=z^4$ の整数解を調べます。少し一般化して、

$$x^4+y^4=z^2$$

と言う方程式の整数解を調べます。

x,y,z の最大公約数が k ですと、整数解 $x=kx_1, y=ky_1, z=k^2z_1$ と書け、x_1,y_1,z_1 は互いに素で、x_1,y_1,z_1 は $x_1^4+y_1^4=z_1^2$ をみたします。そこで必要なら x,y,z の代わりに x_1,y_1,z_1 を取ることにより、x,y,z は $x^4+y^4=z^2$ の整数解で、互いに素だとします。

もし、x が 0 なら方程式は $y^4=z^2$ となりますから、解は $y^2=\pm z$ となります。そこでこのような形の自明な解しか存在しないことを背理法で示すため、x,y,z は互いに素な自然数で、$x^4+y^4=z^2$ をみたし、しかも z が最小のものを取ります。さらに、必要なら x と y を入れ換えることにより、x が偶数であると仮定します。

そこで問題の方程式を $(x^2)^2+(y^2)^2=(z)^2$ と変形し、定理 2 を使うと、

$$x^2=2mn, \quad y^2=m^2-n^2, \quad z=m^2+n^2 \quad (m,n \text{ は自然数},\ m>n)$$

と書けます。

ここで y と z は互いに素だから、m と n も互いに素となります。しかも $m^2-n^2=y^2$ は奇数の 2 乗ですから、m^2-n^2 は 4 で割ると 1 余ります。これより m は奇数で n が偶数となることが分かります。ところが、$2mn=x^2$ は平方数ですから、

$$m=u^2,\quad n=2v^2\quad (u,v\text{は自然数})$$

と書けることが分かります。

他方 $y^2+n^2=m^2$ となりますから、定理 2 より

$$n=2st,\quad y=s^2-t^2,\quad m=s^2+t^2$$

と書けます。ここで s,t も互いに素となりますから、$st=n/2=v^2$ より、

$$s=a^2,\quad t=b^2\ (a,b\text{は互いに素な自然数})$$

と書けます。よって、

$$u^2=m=s^2+t^2=a^4+b^4$$

となります。これは最初の形の方程式の解で、a,b は互いに素な自然数で、しかも $z=m^2+n^2>m^2=u^4\geq u$ となります。これは仮定した z の最小性に矛盾しますから、$x^4+y^4=z^2$ の任意の整数解は、$xyz=0$ をみたします。[12]

§5. リーマンのゼータ関数

§4 の議論からも分かるように、素因数分解の一意性は、整数の持つ性質の中で最も重要な性質でしたが、そのことを解析的に表現することを考えます。

前の注に出てきた

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

[12]以上では、最小の解からより小さな解を作ることにより矛盾を導き、$xyz\neq 0$ となる自然数解が存在しないことを証明しました。このような証明法を**無限降下法**と呼び、不定方程式の解の研究では最近でも使われています。

と言う関数を考えます。これを**リーマンのゼータ関数**と呼びます。[13]

n を 2 以上の整数、σ を 1 より大きい実数とします。このとき、$x^{-\sigma}$ は単調減少関数ですから、

$$\frac{1}{n^\sigma} = \int_{n-1}^{n} \frac{1}{n^\sigma}\,dx < \int_{n-1}^{n} \frac{1}{x^\sigma}\,dx$$

と言う不等式が成り立ちます。したがって、

$$\zeta(\sigma) = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} < 1 + \int_{1}^{\infty} \frac{1}{x^\sigma}\,dx = 1 + \frac{1}{\sigma - 1} < \infty$$

となります。

複素数 s の実部を $\mathrm{Re}(s) = \sigma$ とおくと、n^{-s} の絶対値は $n^{-\sigma}$ になります。したがって s の実部 σ が 1 より大なら

$$|\zeta(s)| = |\sum_{n=1}^{\infty} \frac{1}{n^s}| \leq \sum_{n=1}^{\infty} |\frac{1}{n^s}| = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} < \infty$$

となり、$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ は収束します。このことより、$\zeta(s)$ は領域 $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1\}$ 上の関数を定めることが分かります。

ここで §3 で述べた素因数分解の一意性を思い出します。そうすると、任意の自然数は $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ の形に一意的に分解されますから、ゼータ関数の定義にこれを代入すると、

$$\zeta(s) = \sum (p_1^{-s})^{e_1} (p_2^{-s})^{e_2} \cdots (p_t^{-s})^{e_t} = \prod_{p:\text{素数}} (1 + (p^{-s}) + (p^{-s})^2 + (p^{-s})^3 + \cdots)$$ [14]

と変形されます。そこで等比級数の和の公式を使うと、ゼータ関数は

$$\zeta(s) = \prod_{p:\text{素数}} \frac{1}{1 - p^{-s}} \qquad (p \text{ は素数全体を動く})$$

と無限個の関数の積の形に表されます。これをゼータ関数の**オイラー積**と呼びます。

ここで注意すべきことは、ゼータ関数のオイラー積表示が有れば、

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \sum \frac{1}{(p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t})^s}$$

[13] この関数を最初に考えたのはオイラー (L. Euler, 1707–83) ですが、リーマン (G. F. B. Riemann, 1826–66) はこの関数を s が複素数を動く関数として考察し、関数等式などの証明に成功しました。

[14] $\sum$ が和を表すのに対して、$\prod$ は積を表します。

(右辺の $p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$ は素数のべきの有限個の積全体を動く) と言う等式が成り立ちますから、両辺を比較すると、任意の整数 n が $n = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$ の形に一意的に表現されることが分かります。つまり、ゼータ関数のオイラー積表示は、「素因数分解の一意性が成り立つ」と言う事実を解析的に表現していると言えます。ここにゼータ関数の重要性が有ります。実際ゼータ関数の解析的性質を詳しく調べることにより、実数の中での素数の分布の持つ性質が調べられます。

結果のみ述べますと、$(s-1)\zeta(s)$ は複素数平面の上の関数に拡張され、(修正因子を付け加えると) $s \mapsto 1-s$ と言う変換で不変になります (**関数等式**)。また $\zeta(s)$ は $s \to 1$ とすると ∞ に近付き、このことが素数が無限個存在すると言うことを解析的に表現しています。さらに $\zeta(s)$ は $s = -1, -3, -5, \cdots$ と言う負の整数で 0 となりますが、$0 < \mathrm{Re}(s) < 1$ と言う範囲を除くとそれ以外に 0 となる点は無く、しかも「$0 < \mathrm{Re}(s) < 1$ と言う範囲で $\zeta(s) = 0$ となる点 s は、すべて $\mathrm{Re}(s) = 1/2$ と言う直線上に有る」ことが予想されています (**リーマン予想**)。[15]

ゼータ関数は、これ以外にも整数論の色々な分野で定義され、それぞれの場合の整数論的内容を解析的に表現する関数となっています。上の リーマン予想は、現在の数学における最大の未解決の問題ですが、本来の リーマン予想ではなく、その類似となるゼータ関数に対しては、リーマン予想が証明されている場合が有ります。

§6. 二つの自然数の二乗の和 x^2+y^2 の形をした素数

素数の表を使って、いつ素数 p が平方数の和

$$p = x^2 + y^2 \quad (x, y \text{ は自然数})$$

の形になるかを調べます。小さい方から見てみますと、$2 = 1^2 + 1^2$ から始まり、$5 = 1^2+2^2$, $13 = 2^2+3^2$, $17 = 1^2+4^2$, $29 = 2^2+5^2$, $37 = 1^2+6^2$, $41 = 4^2+5^2$, $53 = 2^2+7^2$, $61 = 5^2+6^2$, $73 = 3^2+8^2$, $89 = 5^2+8^2$, $97 = 4^2+9^2, \cdots$ となります。これを良く見てみると、最初の $2 = 1^2+1^2$ を除き、素数 p は、p を 4 で割ったとき 1 余るとき、そのときに限り $p = x^2+y^2$ の形にかけることが分かります。[16]

[15] §3 の素数分布と素数定理の項参照。

[16] 必要性は、次の § の mod 4 での計算を使うと容易に得られますが、十分性の証明は簡単ではあ

このことを発見したのは、フェルマ (P. de Fermat, 1601–1665) で、フェルマはこれ以外にも、任意の正の整数が平方数 4 個の和 $x_1^2+x_2^2+x_3^2+x_4^2$ $(x_1,x_2,x_3,x_4\in\mathbb{Z})$ の形にあらわされることや、8 で割って 3 余る数は 3 個の平方数の和 $x_1^2+x_2^2+x_3^2$ $(x_1,x_2,x_3\in\mathbb{Z})$ の形にあらわされることも見つけました。しかしフェルマは、これらの結果の証明を発表しませんでした。現在に伝わる証明を与えたのは、オイラーとラグランジェ(J. L. Lagrange,1736–1813) で、さらに後にはガウスの二元二次形式の理論として一般化され、今日の整数論の基礎となりました。

$p = x^2 + y^2$ (x,y は自然数) に戻ります。この方程式を詳しく調べるには、自然数の範囲で調べるより、整数の全体 $\mathbb{Z}$ と複素数 $\sqrt{-1}$ とから作られる集合

$$\mathbb{Z}[\sqrt{-1}] = \{\, a+b\sqrt{-1} \mid a,b\in\mathbb{Z} \,\}$$

の中で調べる方が調べやすく、一般化しやすくなります。$\mathbb{Z}[\sqrt{-1}]$ では上の方程式は、

$$p=(x+y\sqrt{-1})(x-y\sqrt{-1})$$

と積の形に書けます。これは、素数 p が $\mathbb{Z}[\sqrt{-1}]$ と言う範囲では、二つの複素数の積になることを意味します。

$\mathbb{Z}[\sqrt{-1}]$ と言う集合はどう言う性質を持つかを考えます。[17] 定義より容易に、この集合の元の和と積はまたこの集合に入ることが分かります。つまりこの集合は和と積で閉じています。さらに、「素因数分解の一意性が成り立つと言う証明が、$\mathbb{Z}$ において割り算ができると言うこと基づく」ことを思い出し、同じことをガウスの整数環 $\mathbb{Z}[\sqrt{-1}]$ で行うと、$\mathbb{Z}[\sqrt{-1}]$ でも素因数分解の一意性が成り立つことが分かります。[18] そうすると、前の方程式 $p=x^2+y^2$ (x,y は自然数) が解を持つことは、素数 p が $\mathbb{Z}[\sqrt{-1}]$ において二つの素数の積に分解することと同値なことが分かります。そこで、その様になるための条件を求めますと、p が 4 で割って 1 余ることが必要かつ十分であることが証明できます (§8 参照)。

りません。§8 参照。

[17] この集合には、ガウスが詳しく調べたので、ガウスの整数環と言う名がついています。

[18] $\mathbb{Z}[\sqrt{-1}]$ において $0,\pm1,\pm\sqrt{-1}$ ではなく、しかもそれ自身と $\pm1,\pm\sqrt{-1}$ 以外では割り切れない数を素数とします。そうすると、$\mathbb{Z}[\sqrt{-1}]$ の 0 以外の任意の数は、$\sqrt{-1}^a\pi_1^{e_1}\pi_2^{e_2}\cdots\pi_t^{e_t}$ ($a=0,1,2,3$, $\pi_1,\pi_2,\cdots\pi_t$ は $\mathbb{Z}[\sqrt{-1}]$ の素数、$e_1,e_2,\cdots,e_t$ は自然数) と言う形に一意的に表されることが分かります。

任意の正の正数が平方数4個の和 $x_1^2+x_2^2+x_3^2+x_4^2$ $(x_1,x_2,x_3,x_4\in\mathbb{Z})$ の形にあらわされることや、8で割って3余る数は3個の平方数の和 $x_1^2+x_2^2+x_3^2$ $(x_1,x_2,x_3\in\mathbb{Z})$ の形にあらわされることは、このことを使って証明できます。[19]

一般の整数係数の多項式 $f(X_1,X_2,\cdots,X_n)\in\mathbb{Z}[X_1,X_2,\cdots,X_n]$ を与えたとき、$p=f(x_1,x_2,\cdots,x_n)$ $(x_1,x_2,\cdots,x_n\in\mathbb{Z})$ と書ける素数 p を特徴づけることは非常に難しく、現在でもほとんど分かっていません。[20]

§7. 有限体

N を自然数とします。2つの整数 a,b は、差 $a-b$ が N で割り切れるとき、

$$a\equiv b \pmod N$$

と書き、a と b は N を法として**合同**であると言います。また整数の全体 $\mathbb{Z}$ をこの合同という関係で類別した集合を、

$$\mathbb{Z}/N\mathbb{Z} = \{\, a \pmod N \mid a\in\mathbb{Z}\,\}$$

と表します。以下 N が何かが明らかなときには、$a \pmod N$ を $\bar{a}$ と表します。

さてこの集合は

$$\mathbb{Z}/N\mathbb{Z} = \{\, a \pmod N \mid a=0,1,2,\cdots,N-1\,\}$$

と表され、N 個の元からなることが分かります。また

$$a_1\equiv b_1 \pmod N \qquad \text{かつ} \qquad a_2\equiv b_2 \pmod N$$

なら、

$$a_1+b_1\equiv a_2+b_2 \pmod N \qquad \text{かつ} \qquad a_1\times b_1\equiv a_2\times b_2 \pmod N$$

---

[19] これらのことの証明には、上記のような証明のほかにも、二次形式を使う証明や保型形式を使う証明など、色々なものが有ります。

[20] 整数係数の多項式 $f(X_1,X_2,\cdots,X_n)$ で、任意の素数 p が $p=f(x_1,x_2,\ldots,x_n)$ $((x_1,x_2,\ldots,x_n)\in\mathbf{N})$ と書けるものは存在します。

となりますから、整数の和と積は、この集合 $\mathbb{Z}/N\mathbb{Z}$ の上の和と積を定めます。とくに $\mathbb{Z}/N\mathbb{Z}$ の任意の元 $\overline{a}$ に対して、$\overline{a}+\overline{0}=\overline{a}$, $\overline{a}\times\overline{0}=\overline{0}$, $\overline{a}\times\overline{1}=\overline{a}$ となっています。

(例) $\mathbb{Z}/4\mathbb{Z}$ における和 $a+b \pmod 4$ と積 $a\times b \pmod 4$ を計算して表にすると、次の様になります：

和

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

積

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

これよりとくに

$$0^2\equiv 0 \pmod 4,\quad 1^2\equiv 1 \pmod 4,\quad 2^2\equiv 0 \pmod 4,\quad 3^2\equiv 1 \pmod 4$$

となりますから、$x^2\equiv a \pmod 4$ が整数解 $x\in\mathbb{Z}$ を持つためには、$a\equiv 0,1 \pmod 4$ となることが必要十分となります。§4 ではこのことを使いました。

N として素数 p を取ります。このとき、$\mathbb{Z}/p\mathbb{Z}$ は p 個の元からなります。これを p 個の元からなる**有限体**と呼び、$\mathbb{F}_p$ と表します。

$\overline{a}$ を $\mathbb{F}_p$ の $\overline{0}=0 \pmod p$ 以外の元とします。このとき a は p で割れませんから、p と互いに素となります。したがって、$ba+cp=1$ となる整数 b と c が存在します。そこでこの式の $\pmod p$ を取りますと、$b\times a\equiv 1 \pmod p$ となり、$\overline{b}\times\overline{a}\equiv\overline{1}$ となります。したがって、$\mathbb{F}_p$ の $\overline{0}$ でない元 $\overline{a}$ に対しては、乗法に関して**逆元** (その元に掛けると $\overline{1}$ となる元) $\overline{a}^{-1}$ が存在します。以下有限体 $\mathbb{F}_p$ の $\overline{0}$ でない元の全体を $\mathbb{F}_p^\times$ で表します。

$\mathbb{F}_p^\times$ の 2 つの元 $\overline{a}$ と $\overline{b}$ の積 $\overline{ab}$ は、逆元 $\overline{a}^{-1}\times\overline{b}^{-1}$ が有るから $\overline{0}$ ではなく、$\mathbb{F}_p^\times$ に属します。そこで $\overline{a}\in\mathbb{F}_p^\times$ を取り、そのべき $\overline{a}^m\,(m\in\mathbb{Z})$ の形に書ける元の全体 $<a>$ を考えます。このような元はすべて有限集合 $\mathbb{F}_p^\times$ に属しますから、$\overline{a}^m=\overline{a}^n$ となる $m,n\in\mathbb{Z}$, $m>n$ が存在します。これを $\overline{a}^n$ で割ると $\overline{a}^{m-n}=\overline{1}$ となります。そこで l を $\overline{a}^l=\overline{1}$ となる最小の自然数とすると、$<a>$ は l 個の元 $\overline{1},\overline{a},\overline{a}^2,\ldots,\overline{a}^{l-1}$ からなることが分かります。

$\mathbb{F}_p^\times$ の元全体を、比が $\overline{c}/\overline{b}$ が $< a >$ に入るとき同じ類に入るとして分類します。このときこの関係で分類された各類は、$\{\overline{a}^m\overline{b}\,|\,m=0,1,2,\ldots,l-1\}$ と書け、l 個の元からなります。したがって、$\mathbb{F}_p^\times$ は l 個の元からなる部分集合の幾つかの和集合となり、その元の個数を考えると、l は $p-1$ の約数となることが分かります。そこで l の定義に戻ると、$\overline{a}^{p-1}=(\overline{a}^l)^{(p-1)/l}=\overline{1}^{(p-1)/l}=\overline{1}$ となります。言い直すと、p で割り切れない任意の整数 a は、

$$a^{p-1}\equiv 1\ (\mathrm{mod}\ p)$$

をみたすことが分かります。これを**フェルマの小定理**と呼びます。[21]

§8 多項式の mod p での分解

§6 で調べた $p=x^2+y^2$ (p は 2 でない素数、x,y は自然数) を考えます。

この不定方程式 $p=x^2+y^2$ に解が有るものとし、それを mod p で考えると、$x^2\equiv -y^2\ (\mathrm{mod}\ p)$ と言う合同式を得ます。ここで y は p より小ですから、p と素になり、$y\not\equiv 0\ (\mathrm{mod}\ p)$ となります。したがって前 §の結果により、$uy\equiv 1\ (\mathrm{mod}\ p)$ となる自然数 u が存在します。このとき $(ux)^2\equiv -(uy)^2\equiv -1\ \ (\mathrm{mod}\ p)$ となり、$z=ux$ は

$$z^2\equiv -1\ \ (\mathrm{mod}\ p)$$

の解となります。したがって、フェルマの小定理より $(-1)^{(p-1)/2}=z^{p-1}\equiv 1\ \ (\mathrm{mod}\ p)$ となりますから、$(p-1)/2$ は偶数となり、$p\equiv 1\ (\mathrm{mod}\ 4)$ となります。

逆に $p\equiv 1\ (\mathrm{mod}\ 4)$ だとします。このとき、$p-1$ は 4 で割り切れますから、$z=a^{(p-1)/4}$ とおくと、

$$a^{p-1}-1=z^4-1=(z-1)(z+1)(z^2+1)$$

と因数分解されます。ところがフェルマの小定理より、有限体 $\mathbb{F}_p$ における $p-1$ 次の方程式 $a^{p-1}-1\equiv 0\ (\mathrm{mod}\ p)$ はちょうど $p-1$ 個の解を持ちます。したがって、右辺の $z^2+1=a^{(p-1)/2}+1\equiv 0\ (\mathrm{mod}\ p)$ は $(p-1)/2$ 個の解を持ちます。

[21] 有限個の元からなる群 G の元 g は、G の元の個数 $|G|$ 乗すると単位元になります： $g^{|G|}=1$. 上では、$\mathbb{F}_p^\times$ が $p-1$ 個の元からなる群をなすことから、$\overline{a}^{p-1}=\overline{1}$ となることを示しました。

そこで z を絶対値が最小になる合同式 $z^2 \equiv -1 \pmod{p}$ の解とすると、$z^2+1^2 = pt$ (z, t は自然数、$|z| \leq (p-1)/2$) と書けます。そうすると、

$$1 \leq t < \frac{(p/2)^2+1}{p} = \frac{p}{4} + \frac{1}{p} < p$$

となり、t は p と素になり、$vp+wt=1$ となる整数 v, w が存在します。そこでガウスの整数環 $\mathbb{Z}[\sqrt{-1}]$ の中で、

$$(z+\sqrt{-1})(z-\sqrt{-1}) = z^2+1^2 = pt$$

の素因数分解を考えます。

右辺の p は $\pm 1, \pm\sqrt{-1}$ ではありませんから、何か $\mathbb{Z}[\sqrt{-1}]$ における素因数

$$\pi = x + y\sqrt{-1} \qquad (x, y \in \mathbb{Z},\ \pi \neq \pm 1, \pm\sqrt{-1})$$

が p を割り切ります。そこで必要なら π の代わりに $-\pi$ を取ることにより、π が左辺の $z+\sqrt{-1}$ を割り切るとします。このとき、複素共役を取ることにより、$\overline{z+\sqrt{-1}} = z-\sqrt{-1}$ の $\mathbb{Z}[\sqrt{-1}]$ における素因数である $\bar{\pi}$ は $\bar{p}=p$ を割り切ることが分かります。他方 p と t は互いに素で $vp+wt=1$ となりますから、π も $\bar{\pi}$ も t を割り切りません。したがって、左辺の因数分解に出てくる $\pi\bar{\pi} = (x+y\sqrt{-1})(x-y\sqrt{-1}) = x^2+y^2$ は、右辺の p を割り切ります。ところが p は素数だから、その約数 $x^2+y^2 \neq 1$ は p と一致します。したがって、

$$x^2+y^2 = (x+y\sqrt{-1})(x-y\sqrt{-1}) = p$$

となり、p は x^2+y^2 の形に書けます。

さて上では、合同式 $z^2 \equiv -1 \pmod{p}$ が解を持つかどうかが問題となりました。そこで一般に、$f(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 \in \mathbb{Z}[z]$ を整数係数の z の多項式とし、これをある素数 p に関する mod p で考えた

$$f(z) \equiv 0 \pmod{p}$$

が、有限体 $\mathbb{F}_p$ の中でいくつ解を持つかを考えます。

$f(z)=z^2+1$ については上で調べましたが、同様にして、$f(z)=z^2+z+1$ を考えますと、今度は $\mathbb{Z}[\sqrt{-1}]$ の代わりに

$$\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}] = \{ a+b\frac{-1+\sqrt{-3}}{2} \mid a,b\in\mathbb{Z} \}$$

が出てきて、その結果、$f(z)\equiv 0 \pmod p$ が有限体 $\mathbb{F}_p$ において相異なる解を持つための必要十分条件は、$p\equiv 1 \pmod 3$ であることが分かります。一般に、$f(z)$ が z の2次式であるときには、この問題は解け、「p がある合同式をみたすことが必要かつ十分である」と言う形で解が与えられます (**平方剰余の相互法則**)。

そこで、$f(z)$ が3次式の場合を考えます。このときには、同様に解ける場合と、まるで結果を統制する法則が分からない場合が生じます。同様に解ける場合は、「有理数の全体 $\mathbb{Q}$ と $f(z)=0$ のある解 θ から和、差、積で作られる複素数の全体を

$$\mathbb{Q}(\theta) = \{ c_0+c_1\theta+\cdots+c_{n-1}\theta^{n-1} \mid c_0,c_1,\cdots,c_{n-1}\in\mathbb{Q} \}$$

と置くと、$f(z)=0$ の他の2つの解もこの中に入る」ことが必要かつ十分であることが知られています (次ページ参照)。

例えば、$f(z)=x^3+x^2-2x-1$ の場合には、$\cos(2\pi/7)$、$\cos(4\pi/7)$、$\cos(6\pi/7)$ が解となり、この条件をみたします。このとき p と解の個数を書きますと、(2,0), (3,0), (5,0), (7,1), (11,0), (13,3), (17,0), (19,0), (23,0), (29,3), (31,0), (37,0), (41,3), (43,3), (47,0), (53,0), (59,0), (61,0), (67,0), (71,3), (73,0), (79,0), (83,3), (89,0), (97,3), $\cdots$ となり、素数 7 のときには解の個数は1個 (3重解) となりますが、それ以外の素数 p については、$p\equiv\pm 1 \pmod 7$ のとき、そのときに限り3つの解を持つことが分かります。

これに対し、$\mathbb{Q}(\sqrt[3]{a})=\mathbb{Q}+\mathbb{Q}\sqrt[3]{a}+\mathbb{Q}\sqrt[3]{a^2}$ (純3次体と呼ぶ) に対応する

$$f(z) = z^3 - a \qquad (a \text{ は3乗の形ではない整数})$$

で実験をしてみますと、結果はまるで規則が分からないものとなります。

例えば、$f(z)=z^3-5 \pmod p$ の p と解の個数を書きますと、(2,1), (3,1), (5,0), (7,0), (11,1), (13, 3), (17,1), (19,0), (23,1), (29,1), (31,0), (37,0), (41,1), (43,0), (47,1), (53,1), (59,1), (61,0), (67,3), (71,1), (73,0), (79,0), (83,1), (89,1), (97,0),

(101,1), (103,0), (107,1), (109,0), (113,1), (127,3), (131,1), (137,1), (139,0), (149,1), (151,0), (157,0), (163,3), (167,1), (173,1), (179,1), (181,3), (191,1), (193,0), (197,1), (199,3), (211,3), (223,0), (227,1), (229,0), (233,1), (239,1), (241,3), $\cdots$ となります。この表から、 $p \equiv 2 \pmod 3$ なら[22] 解の個数が 1 となることが分かります。[23] しかし、 $p \equiv 1 \pmod 3$ 場合には解の個数が 0 または 3 となりますが、そのうちのどちらかを決める規則を発見するのは困難です。

逆にこのようなことが良く分かる多項式としては、 q を素数としたとき、単位円の q 等分点 $z = \exp(2\pi\sqrt{-1}/q)$ を解とする多項式

$$f(z) = \frac{z^q - 1}{z - 1} = z^{q-1} + z^{q-2} + \cdots + z + 1$$

があります。これについては、 p が q 以外の素数なら、 f を $p^f \equiv 1 \pmod q$ となる最小の自然数とするとき、 $f(z) \pmod p$ は f 次の多項式 $(q-1)/f$ 個の積に分解されます。とくに $p \equiv 1 \pmod q$ のとき、そのときに限り、 $f(z) \equiv 0 \pmod p$ は $q-1$ 個の解を持ちます。これを円の q 等分点の体 $\mathbb{Q}(\exp(2\pi\sqrt{-1}/q))$ における**分解法則**と呼びます。[24]

一般に、整数係数の多項式 $f(z)$ を取り、 $f(z) \pmod p$ を有限体 $\mathbb{F}_p$ を係数とする多項式と見て既約多項式に分解することを考えます。 K で有理数と $f(z) = 0$ の解から和と積で作られる元全体のなす集合を表します。このとき、「 $f(z) \pmod p$ の既約多項式への分解の型が p に関する合同条件で決まるのは、 K が有理数体 $\mathbb{Q}$ のガロア拡大で、しかもそのガロア群がアーベル群になることが必要かつ十分で有る」と言うのが高木貞治 (1875-1960) の**類体論**の主定理で、そうならない多項式については、この問題は現在でも解けていません。

（もりた やすお，東北大学大学院理学研究科）

---

[22] $z^2 + z + 1 \equiv 0 \pmod p$ が解を持たないとき。

[23] きちんと証明することもできます。

[24] 例えば、 $q = 5$、 $f(z) = z^4 + z^3 + z^2 + z^1 + 1$ と置き、 p と $f(z) \equiv 0 \pmod p$ の解の個数を書くと、(2,0), (3,0), (5,1)(4 重解), (7,0), (11,4), (13,0), (17,0), (19,0), (23, 0), (29,0), (31,4), (37,0), (41,4), (43,0), (47,0), (53,0), (59,0), (61,4), (67,0), (71,4), (73,0), (79,0), (83,0), (89,0), (97,0), (101,4), (103,0) $\cdots$ となります。