



Title	数論に関する最近の話題
Author(s)	田中, 嘉浩
Citation	経済學研究, 63(2), 271-276
Issue Date	2014-01-24
Doc URL	https://hdl.handle.net/2115/54589
Type	departmental bulletin paper
File Information	ES_63(2)_271.pdf



<研究ノート>

数論に関する最近の話題

田 中 嘉 浩

1. はじめに

数学が後から多くの分野に於いて重要な应用を持つことは枚挙に暇がない。

随分前だが著者は [10] で、現代数学の計算量の理論で「簡単には解けない問題」となっている素因数分解の難易度を逆転の発想で応用した公開鍵暗号が考案・実用化され、それが情報通信技術の発展した現代に於いて、電子商取引 (EC) でのデータ送信や電子政府でのデジタル署名等、情報基盤で欠くことのできない技術になっていることを述べた。

計算量の理論自体は組合せ問題に不可欠な、 $P \neq NP$ 問題という重大な未解決問題を残して、その理論や実用的な解法の為に多くのアプローチが試みられている。

本稿では、組合せ問題のみならず他の数学の未解決問題とも深く関る数論に関するこの 20 年間、特に最近の発展について述べようと思う。

2. 整数と素数の関係

18 世紀の大数学者 Leonhard Euler (1707-1783) の業績にはガンマ関数の発見、グラフ理論、流体力学、多面体の公式等の多くの重要な結果が知られている [3] が、後に数世紀に渡る数学の難問に繋がる次のゼータ関数の導入は特に重要な結果である。

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

$$= \prod_p (1 - p^{-s})^{-1}$$

第 2 式は Euler が 1737 年に発見した式で、 $(1-x)^{-1} = 1 + x + \cdots$ から理解できるが、整数と素数を初めて関係付けたものである。

Euler 自身は、 $\zeta(0) = -\frac{1}{2}$, $\zeta(-1) = -\frac{1}{12}$, $\zeta(-2) = 0$, $\zeta(-3) = -\frac{1}{8}$, ... の値を無限級数の分数表示を用いて求め、別に求めている $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$, ... と合わせた値を得ている。また第 2 式を評価することにより、

$$\sum_p \frac{1}{p} \rightarrow \infty$$

という重要な結果を得ている。

19 世紀に G.F.B. Riemann は解析接続して $s \in \mathbb{C}$ の関数として $\zeta(s)$ を考え、次の展開形を示した ([6] 参照)。

$$\begin{aligned} \zeta(s) &= \frac{1}{s-1} \times \prod_{n=1}^{\infty} \left(1 + \frac{s}{2n}\right) e^{-\frac{s}{2n}} \\ &\times \prod_p \left(1 - \frac{s}{p}\right) e^{\frac{s}{p}} \times e^{As+B} \end{aligned}$$

1859 年に Riemann は、

Riemann 予想

「 $\zeta(s)$ の非自明零点 ($s = -2n$, $n \geq 1$ 以外) の

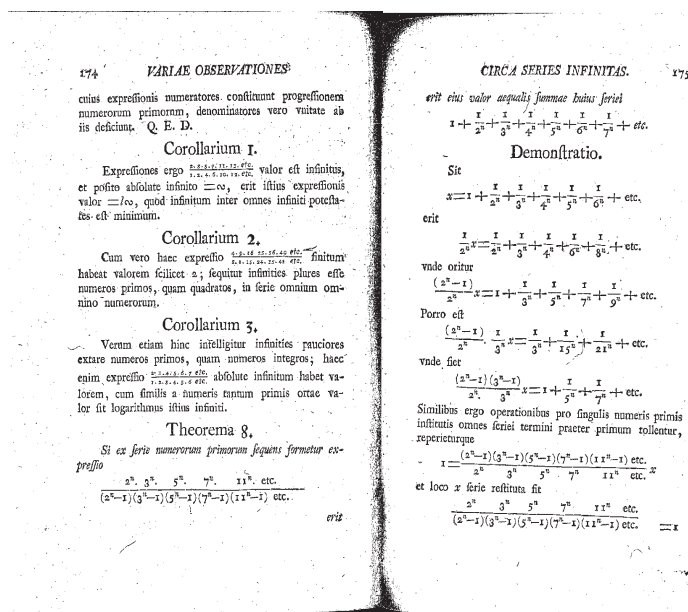


図1：Eulerの原論文

零点)は全て実部が $\frac{1}{2}$ となる」

という予想を残したが、長年に渡って解決されず、Hilbertの第8問題にもなっていたが、一世紀を得て「21世紀の数学7大未解決問題」(内Poincaré予想は2002年にG. Y. Perelmanに依って解決された)にも残っており、中でも難問とみなされている。

素数分布に関しては、

$\pi(x)$: x 以下の素数の個数

$$\text{Li}(x) = \int_2^x \frac{du}{\log u}$$

として、古くはde-la-Vallée-PoussinやJ.S. Hadamardに依り、素数定理

$$\pi(x) \sim \text{Li}(x) (= \frac{x}{\log x})$$

が知られていたが、H. von Kochに依り、リーマン予想が成立することと、

$$\pi(x) \sim \text{Li}(x) + O(x^{\frac{1}{2}} \log x)$$

が同値であることが示されている。

ところで、ゼータ関数には幾つかの変種が考えられており、次節に示す様に、特殊なゼータ関数に対するRiemann予想は20世紀中頃から解決し始めている。

3. 最近20年間の発展

Fermat予想の解決(1995)

1630年代後半にPierre de Fermat(弁護士且つ数学者)に依って書き残された

「不定方程式

$$x^n + y^n = z^n \quad (n \geq 3)$$

を満たす整数 x, y, z は存在しない」というFermatの最終定理とも言われる予想の解決である。

1993年にsci.mathか何かで「Andrew Wiles教授がFermatの最終定理の解決に成功した。Cambridge大学で講演を行う」というニュースが流れていたことは今では懐かしい。Wilesは、既にG. Freyに依るモジュラーでない楕円曲線の考案から谷山・志村予想の成立に帰着されていたFermat予想を谷山・志村予想を半安定の場合に証明したと述べた。後に若干の不備に気付かれたが、弟子のR. Taylorと共に岩澤理論を緩用し修正して2論文[13][11]に纏め、1995年2月に正しい認定が為された。予想の提示から350年以上掛けて証明されたことになる。

Goldbach 予想への前進 (1997)

1742年にC. GoldbachがEulerに宛てた書簡に由来するが、

「4以上の偶数は2つの素数の和で表せる」

という強いGoldbach予想を指すのが普通であり、既にRiemann予想や後述する双子素数予想と共にHilbertの第8問題に含まれているが、簡明な形の重要な未解決問題である。例えばGoldbach予想が成立する仮定の下ではBertrandの定理が簡単に導ける(Ricardo, 田中[9])他、双子素数予想との関係も示唆されている。

強いGoldbach予想からは、

「5を超えた奇数は3つの素数の和で表せる」

という弱いGoldbach予想を導ける。

1937年にI.M. Vinogradovは非常に大きな奇数(その後の改良でも約 10^{43000} 以上)に対しては弱いGoldbach予想が導けることを証明した。

1997年にJ. Deshouillers, G. Effinger, H. Te Riele, D. Zinoviev [2]により、一般化Riemann

予想が成立する仮定の下で弱いGoldbach予想が証明されている。

素数判定の多項式アルゴリズム (2002)

一般化Riemann予想が成立する仮定に依存した確率的アルゴリズムであるRabin-Miller法が知られていたが、2002年にM. Agrawal教授とN. Kayal, N. Saxenaが何の仮定にも依存しない決定的アルゴリズムであるAKS法を発見した([10]参照)。合成数の具体的な素因数を与えることは多項式ではできておらず、RSAの頑強性が脅かされた訳ではない。しかしながら、「PRIME is in P」であることが証明された理論的意義は大きい。

Catalan 予想の解決 (2002)

1844年にE. C. Catalanに依って提出された「不定方程式

$$x^m - y^n = 1, \quad x, y, m, n > 1$$

を満たす整数解は $x=3, y=2, m=2, n=3$, だけである」

という予想が、2002年にP. Mihăilescuに依って初等的に解決された。

右辺を $k>0$ と自然数に拡張したPillai予想の整数解が有限個であることが、abc予想が解決すれば解決されることが知られている。

Green-Tao の定理 (2004)

1770年代からLagrange and Waringにより k 個の素数からなる等差数列の公差はどれ程大きくなるかが研究されていたが、任意個数の素数からなる等差数列が存在するかどうか分っていなかった。

1936年にErdős and Turánは、

「整数列 $a_1 < a_2 < \dots$ が $\sum_i \frac{1}{a_i} = \infty$ を満たす無限数列ならば、任意の長さの等差数列を含む」

という予想を残している。

2004 年に B. Green and T. Tao [5] がその予想の系とも言える

「素数の中には任意の長さの等差数列が存在する」

という驚くべき結果を Szemerédi の定理の証明を改良するエルゴード理論のアプローチで証明した。

Tao は波動写像方程式の可解性、非線形 Schrödinger 方程式の散乱問題の解決、調和解析、組合せ論等多岐の分野に渡る気鋭の研究者であり、2006 年にフィールズ賞を受賞している。

佐藤-Tate 予想の解決 (2011)

1916 年に S. Ramanujan はモジュラー群 $SL(2, \mathbb{Z})$ に対する保型形式

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$$

に対するゼータ関数

$$L(s, \Delta) = \prod_q (1 - \tau(p) p^{-s} + p^{11-2s})^{-1}$$

を構成した。

Ramanujan は $1 - \tau(p) p^{-s} + p^{11-2s} = 0$ となる複素数 s が、 $\text{Re}(s) = \frac{11}{2}$ を満たす予想から、

$$|\tau(p)| \leq 2 p^{\frac{11}{2}}, \quad p \text{ は素数}$$

という Ramanujan 予想を残したが、後に P.R. Deligne によって証明された。

一方、

$$\tau(p) = 2 p^{\frac{11}{2}} \cos \theta_p, \quad 0 \leq \theta_p \leq \pi$$

に対して、1964 年に佐藤-Tate により、

「 $\{\theta_p\}$ の分布は、 $\forall [\alpha, \beta] \subset [0, \pi]$ に対して、 $\pi_\Delta(x; [\alpha, \beta]) = \{p \leq x \mid \theta_p \in [\alpha, \beta]\}$ とすると、 p によらず、

$$\lim_{x \rightarrow \infty} \frac{(\pi \Delta(x; [\alpha, \beta]))}{\pi(x)} = \frac{2}{\pi} \int_{[\alpha, \beta]} \sin^2 \theta \, d\theta$$

を満たす」

という予想が提出されていた。

Taylor 等 [1] は、

$$L_0(s, \Delta, \text{Sym}^m) = \prod_p \left(\left(1 - \frac{e^{im\theta_p}}{p^s}\right) \left(1 - \frac{e^{i(m-2)\theta_p}}{p^s}\right) \cdots \left(1 - \frac{e^{-i(m-2)\theta_p}}{p^s}\right) \left(1 - \frac{e^{-im\theta_p}}{p^s}\right) \right)^{-1}$$

が $s \in \mathbb{C}$ されることを用いて、佐藤-Tate 予想の完全解決に成功した [6]。

abc 予想の解決!?! (2012)

1985 年に J. Oesterle と D. Masser に依って提示された

「 a, b, c を $a + b = c$ を満たす互いに素な整数とすると、 $\forall \varepsilon > 0, \exists K(\varepsilon) \geq 1$ に対して、

$$\max\{|a|, |b|, |c|\} < K(\varepsilon) (\text{rad}(abc))^{1+\varepsilon}$$

但し、 $\text{rad}(abc) = \prod_{p|abc} p$ である」

という問題である。 $\varepsilon = 1$ に対して abc 予想が証明されれば Fermat 予想が不成立の時には $n < 6$ になる ($n = 3, 4, 5$ の場合は Fermat 予想は昔から個々に証明されているので Fermat

予想成立の証明になる)ことが初等的に証明されるので, Fermat 予想より難問である。

2012年8月に京都大学の望月新一教授がインターネットに公開した4部作で500頁にもなる論文に続く2013年2月の[8]では, $\forall \varepsilon > 0$ に対する abc 予想が Frey とは異なる楕円曲線を, 彼独自の F_1 理論で扱って証明されており検証が為されている。[8]では $\varepsilon=1$ として $K(\varepsilon) \geq 1$ の存在は証明されているが $K(\varepsilon)=1$ とは言われていない。しかしながら, 6以上ではないにせよ, $K(\varepsilon)$ の値に対する有界な値以上では Fermat 予想が成立することが証明される他, Wieferich 素数が無限に存在することが証明される等, 他に解決される問題も多い, より弱い予想の Szpiro 予想も証明されているので意義は大きい。

Mersenne 素数の更新 (2013)

1644年に M. Mersenne は $M_n = 2^n - 1, n \leq 257$ の素数性に関する予想 ($n=2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ の時素数)を出した。その予想は Pervouchine, Powers, Cole 等によって追加・修正され, $n \leq 257$ では, $n=2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$ となっている。より大きい n に対しては Lucas テストと共に長大な素数生成の方法となっており, その探索 (GIMPS) は分散コンピューティングの例として有名である。現在の最大素数の記録は $M_{57885161} = 2^{57885161} - 1$ (17425170桁; Cooper, Woltman, Kurowski, 2013)である。但し Mersenne 素数が無限個有るかどうかは, $2^{2^n} + 1$ の形の Fermat 素数が5個しかないかどうかと共に, 今でも未解決である。

Mersenne 素数の逆数の和が,

$$\sum_{M_{n,p}} \frac{1}{M_n} < \sum_{n=2}^{\infty} \frac{1}{2^n - 1} < \sum_{n=2}^{\infty} \frac{1}{2^{n-1}} = 1$$

と有限値に収束することからも難問であること

が分る。

双子素数予想への前進 (2013)

差が2である様な素数の対を双子素数といい,

「双子素数は無限に存在する」

という双子素数予想は Hardy-Littlewood による x 以下の対の数が $2C \int_2^x \frac{dx}{(\log x)^2}$, $C=0.66016\dots$, になるという予想はあるものの未解決である。但し, 双子素数の逆数の和が, $1.90216\dots$ に収束することは V. Brun によって証明されている。

2013年4月17日に会計士の経験もある Yitang Zhang 教授が,

$$\liminf_{n \rightarrow \infty} (p_{n+1} - p_n) < 7 \times 10^7$$

という形で,

「素数の差が 7×10^7 以内のペアが無限に存在する」

ことを証明した原稿[14]を *Annals of Mathematics* に送り, 改訂を経て5月21日に採択されている。

Goldston, Pintz and Yildirim [4] は, k_0 -tuple という異った k_0 組の整数

$$\mathcal{H} = (h_1, \dots, h_{k_0}), k_0 \geq 1$$

の概念を導入し, 許容 k_0 -tuple を各 p に対して $\text{mod } p$ の要素の全ては含まない k_0 -tuple と定義した。

次の予想を考える。

「(DHL) $\mathcal{H}$ を固定した許容 k_0 -tuple ($k_0 > 2$) とする。その時, $n + \mathcal{H}$ が少なくとも2つの素数を含む無限の n 移動が存在する」

Goldston, Pintz and Yildirim [4] は, Elliott-

Halberstam 予想が、素数分布に関する分布レベル $\exists \vartheta = \frac{1}{2} + \varpi$, $\varpi > 0$ で成立する仮定の下で, (DHL) が $\exists k_0$ に対して成立することを示し, ペアが有界になる結果を得た。

Zhang [14] は Elliott-Halberstam 予想に代わる予想が $0 \leq \varpi \leq \frac{1}{1168}$ に対して成立することから (DHL) が $k_0 = 3.5 \times 10^6$ に対して成立することを示し, その時の $\mathcal{H}$ の要素の最小直径 $H(k_0)$ が 7×10^7 未満であることを示して冒頭の結果を得た。

現在, 共同研究目的に Polymath Wiki が作られているが, Polymath8 project: bounded gaps between primes が今 6 月から Zhang [14] の k_0 や H の値を (双子素数予想解決に向けて) 改良することを目標として開始された。現在 (9 月時点) で k_0 , H の両方の値が Zhang [14] より 4 桁程度改良されている様である。

4. おわりに

Riemann 予想に関連する問題としては, 最近 20 年間ではないが, 2 節の終わりに言及した様に, 20 世紀中頃から後半に, A. Selberg がセルバーグゼータ関数に対する Riemann 予想, R.R. Deligne が合同ゼータ関数に対する Riemann 予想 (Weil 予想) を解決し——Deligne はそれから Ramanujan 予想も解決している——, 各々がフィールズ賞の榮譽を受けていることにも言及されるべきである。更なる特殊や本来の Riemann 予想への進展が続いていくと思われる。

末筆ながら, E. Landau がいみじくも 1912 年に難攻不落の問題として挙げた, Goldbach 予想, 双子素数予想, $n^2 + 1$ の素数が無限にある予想, n^2 と $(n+1)^2$ の間に 1 つは素数が存在する予想の 4 つの問題 [12] は, その殆ど全てがそのままの形で未解決問題として残っていることには驚かされるばかりであり, 新たなブ

レークスルーが待望されるところである。

参考文献

- [1] T. Barnet-Lamb, D. Geraghty, M. Harris, R. Taylor, “A family of Calabi-Yau varieties and potential automorphy II,” *Publications of RIMS*, 47 (2011) 29–48.
- [2] J. -M. Deshouillers, G. Effinger, H. Te Riele, D. Zinoviev, “A complete Vinogradov 3-primes theorem under the Riemann hypothesis,” *Electronic Research Announcements of American Mathematical Society*, 3 (1997) 99–104.
- [3] W. Gauyschi, “Leonhard Euler: His life, the man, and his works,” *SIAM Review*, 50 (2008) 3–33.
- [4] D.A. Goldston, J. Pintz, and C.Y. Yildirim, “Primes in tuples I,” *Annals of Mathematics*, 170 (2009) 819–862.
- [5] B. Green and T. Tao, “The primes contain arbitrary long arithmetic progressions,” *arXiv preprint math*, 0404188, 2004.
- [6] 黒川信重, 『リーマン予想の先へ (深リーマン予想——DRH)』, 東京図書 (2013)。
- [7] P. Mihăilescu, “Primary cyclonic units and a proof of Catalan's conjecture,” *J. reine angew. Math.* 572 (2004) 167–195.
- [8] S. Mochizuki, “A panoramic overview of inter-universal Teichmüller theory,” RIMS-1774, 2013.
- [9] H.J. Ricardo and Y. Tanaka, “Goldbach's conjecture implies Bertrand's postulate,” submitted to *The American Mathematical Monthly*, 112 (2005) 492.
- [10] 田中嘉浩, 「現代暗号の数理」『経済学研究』(北海道大学) 第 54 巻第 3 号 (2004) 87–98。
- [11] R. Taylor and A. Wiles, “Ring-theoretic properties of certain Hecke algebras,” *Annals of Mathematics*, 141 (1995) 553–572.
- [12] D. Wells, Prime Numbers – The most mysterious figures in math, Wiley, 2005 (『プライムナンバーズ』, 伊地知監訳, オライリー・ジャパン, 2008)。
- [13] W. Wiles, “Modular elliptic curves and Fermat's last theorem,” *Annals of Mathematics*, 141 (1995) 443–551.
- [14] Y. Zhang, “Bounded gaps between primes,” *Annals of Mathematics*, to appear.