混沌の中の秩序–素数列をめぐって

小木曽啓示

1 序

これは 2009 年 9 月に大阪大学で開催された日本数学会での市民講演会における講演の記録である. 本稿における内容はすべて既知事項であり, 筆者自身による数学的新貢献は皆無であることを最初にお断りしておく.

2 素数

2.1 素数の定義と素因数分解

定義 1 *(1)* 整数 m, n に対し, $n = mk$ である整数 k があるとき m は n の**約数**であるといい, 記号 $m|n$ で表す. また, 整数 m が整数 n の約数であることを m は n を割り切るともいう.
(2) 1 と自分自身以外に正の約数をもたない 2 以上の整数のことを**素数**という.
(3) 素数でない 2 以上の整数のことを**合成数**[1]という.

例 1 20 以下の正の整数のうち, 素数は

$$2, 3, 5, 7, 11, 13, 17, 19$$

の 8 個であり, それ以外の 12 個の数

$$1, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20$$

は素数ではない. 検証は各数毎に確かめればよく定義 *1(3)* の脚注を用いれば容易である. 定義により, 1 は素数ではないことに注意しておこう.

素数は, 0, 1 についで基本的な整数であり, 整数の考察における元素の役割をもつ:

[1]素数の定義により, 2 以上の整数 n に対し, n が素数でないことと n が $n = k \times \ell$ (k, ℓ はともに 2 以上のある整数) の形に書ける数であることは同値だからである.

定理 1 *(***Euclid***)*

2 以上の整数はすべて有限個の素数の積の形に書ける *(***素因数分解の存在***)*. 更に, 素数の積の形にするプロセスによらず, 書き表し方は次の意味で一通り*:*

与えられた整数 $n \geq 2$ に対し, n の素因数分解にあらわれる各素数 p の個数は n により一通りに決まる *(***素因数分解の一意性***)*.

2 以上の整数 n に対し, n の素因数分解に 1 回以上現れる素数 p のことを n の**素因数**という.

例 2 72 を素数の積に直してみよう. 小さい素数から順番に割り算してみることで直せるはずだと考えると

$$72 = 2 \cdot 36 = 2 \cdot 2 \cdot 18 = 2 \cdot 2 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^3 \cdot 3^2$$

と素因数分解できる. また, 九九の式 $8 \cdot 9 = 72$ 等を思い出せば

$$72 = 8 \cdot 9 = 2^3 \cdot 3^2$$

とより効率的に素因数分解できる. どちらの方法でも最終的な答は同じになっている. これが定理の後半の主張である. また, 計算結果から, 72 の素因数は 2 と 3 の 2 つである.

この定理 1 は約数・倍数の問題をはじめとし多彩な応用をもつ. 素因数分解の存在証明は次のように容易である. 2 以上の各整数 k に対して, 命題 P_k を「k は素数の積の形に書ける.」と定め, 命題 Q_k を「2 以上 k 以下のすべての整数 ℓ に対して命題 P_ℓ が真ならば, 命題 P_{k+1} も真である.」と定める. 示すべきことは 2 以上の任意の整数 k に対して命題 P_k が真であることである. それには, 数学的帰納法により, (i) 命題 P_2 は真, (ii)2 以上のすべての整数 k に対して命題 Q_k は真, の 2 つをいえばよい. 素数の定義から 2 は素数であり, 自明な等式 $2 = 2$ により, P_2 は真である. (ii) を確かめよう. $k+1$ が素数ならばよいから, $k+1$ が素数ではなかったとしよう. このとき, $k+1$ は 2 以上の整数であり, 素数ではないのだから, $k+1 = mn(m,\ n$ はともに 2 以上の整数) と書ける. このとき, $2 \leq m, n \leq k$ なので, 命題 Q_k の条件を $m,\ n$ にそれぞれ適用できて, $n,\ m$ はどちらも有限個の素数の積に書ける. 故に, その積である $k+1$ も有限個の素数の積に書ける. こうして命題 Q_k も真である.

一意性ははるかに深い性質であり, 次の問題の手順により証明できる:

問題 1 *(***H2***[2])*

(1) $a,\ b$ *を正の整数とし,* c *を* $a,\ b$ *をともに割り切る最大の正の整数 (*1 以上 a 以下の整数は有限個であり, 1 は a も b も割り切るから, このような正の整数 c は必ず存在する*)* とする. このとき整数全体の集合の部分集合として

$$\{ax + by \mid x, y \text{ は整数全体を動く } \} = \{cz \mid z \text{ は整数全体を動く } \}$$

であることを示せ.

(2) p *を素数,* $m,\ n$ *を整数とする. (1) を用いて,* $p | m \cdot n$ *ならば,* $p | n$ *または* $p | m$ *であることを示せ.*

(3) (2) を用いて, 素因数分解の一意性を示せ.

[2]以下, 問題についている記号 H2 は高校数 II・B までの知識と技法で解ける問題, H3 は高校数学 III・C までの知識と技法で解ける問題, D1 は理系大学 1 年までの知識と技法で解ける問題を表す. 論証力はある程度要求される.

本問の目的は, 素因数分解の一意性を (1),(2) に基づき証明することであり, (1), (2) の証明において素因数分解の一意性はまだ使えないことに注意しよう.

2.2 素数の見つけ方-Eratosthenes の篩法

100 以下の素数をすべて見つけることを考えよう. 1 は素数ではなかったことに注意して, まず候補である 2 以上 100 以下の整数を大きさの順に一列に並べよう.

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, \cdots, 95, 96, 97, 98, 99, 100\,.$$

ここで箱 P を用意して次の操作を考える:

(ステップ 1) まず, 最初の数 2 を箱 P に移し, $2 \times$ (2 以上の整数) の形の数 (定義から合成数である) をすべて列から消し去る. この時点で箱 P には数 2 が入っていて, 列の方は

$$3, 5, 7, 9, 11, 13, \cdots, 95, 97, 99\,.$$

に変わる.

(ステップ 2) 次に, 列に残った最初の数 3 を箱 P に移し, $3 \times$ (2 以上の整数) の形の数 (定義から合成数である) をすべて列から消し去る. この時点で箱 P には数 2, 3 が入っていて, 列の方は

$$5, 7, 11, 13, \cdots, 95, 97\,.$$

に変わる.

(ステップ 3) 次に, 列に残った最初の数 5 を箱 P に移し, $5 \times$ (2 以上の整数) の形の数 (定義から合成数である) はすべて列から消し去る. この時点で箱 P には数 2, 3, 5 が入っていて, 列の方は

$$7, 11, 13, \cdots, 97\,.$$

に変わる.

(ステップ 4) 次に, 列に残った最初の数 7 を箱 P に移し, $7 \times$ (2 以上の整数) の形の数 (定義から合成数である) をすべて列から消し去る. この時点で箱 P には数 2, 3, 5, 7 が入っていて, 列の方は

$$11, 13, \cdots, 97\,.$$

に変わる.

(ステップ 5) この時点で列に残った最初の数 11 は $\sqrt{100} = 10$ より真に大きな数であり, ステップ 1-4 の定め方から, ステップ 1-4 で箱 P に移されたどの数でも割り切れない. そこで, この列に残った数もすべて箱 P に入れる.

こうして最終的に箱 P に移された数全体

$$2, 3, 5, 7,$$

$$11, 13, 17, 19, 23, 29, 31, 37, 41, 43,$$

$$47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

の 25 個の数が 100 以下の素数全部になる. 実際, 消し去られた数はすべて合成数だから, 100 以下の素数はすべて箱 P に属している. 逆に, 次の問題の (2) ならば (1) をステップ 1-4 に順次用いることで, 箱 P に移された 10 以下の数 (ステップ 1-4 において箱 P に移された数) はすべて素数であることが順次従う. このとき, 次の問題の (3) ならば (1) により, 箱 P に属する 10 より大きい数 (ステップ 5 において箱 P に移された数) もすべて素数である. 故に, 箱 P に属する数はすべて素数である.

問題 2 *(***H2***)* m *を 2 以上の整数とする. 素因数分解の存在も用いて, 2 以上の整数* m *に対する次の命題 (1), (2), (3) は互いに同値であることを示せ.*
(1) m *は素数である.*
(2) m *は* m *未満のどの素数でも割り切れない.*
(3) m *は* $\sqrt{m}$ *以下のどの素数でも割り切れない.*

同じ考え方により, N 以下の素数をすべて見出すには, 2 以上 N 以下の整数をすべて一列にならべ, $\sqrt{N}$ 以下の素数 p すべてに対して, $p \times$ (2 以上の整数) の形の数をすべて列から取り除けばよいことになる. この方法によって, 与えられた整数以下の素数を (少なくとも原理的には) すべて書き下すことができる. この方法を **Eratosthenes の篩法**という.

Gauss(1777-1855) は, すでに 3000000(7 桁の数) までの素数が全部で 216745 個あることを知っていた.

現在 (2009 年 9 月) までに報告されている最大の素数は, 知る限り

$$2^{43112069} - 1 \, (12978189 \text{ 桁の数})$$

のようである[3]. また, 1 億桁以上の素数の最初の発見に対し 15 万ドルの懸賞金がかけられている:

http://www.ef.org/awards/coop

1 億桁の数を普通に書くには, 2 つの数字を 1 秒で書くとして 5000 万秒かかることになる. 頑張って毎日 12 時間づつ書き続けたとしても書ききるのには約 1157 日 (3 年 2ヶ月) かかることになる[4]. 現在, 最先端においては, このような想像を越えた大きな素数の発見が重要な問題 (の 1 つ) として問われているのである.

2.3 素数は無限個

では, 素数はいったいどの位あるのだろうか? Eratosthenes の篩法を繰り返していったとき, ある段階である数より大きな数がすべて消し去られてしまうことはないのだろうか?

定理 2 *(***Euclid***) 素数は無限個ある. 言いかえると, 正の整数* B *をどのように与えても, 必ず素数を* B *個以上見い出せる.*

今もって一億桁以上の素数が具体的に見出されていないにもかかわらず, この答は紀元前から知られていたのである. Euclid による原証明は背理法を用いた方法であり, その証明方法はしばしば大学

[3] 素数であることをどのように検証したのであろうか?
[4] この試算は渡部隆夫大阪大学教授から教わったものである.

入試問題のテーマにもなる有名なものである．ここでは 2006 年に Saidak[Sa] により発見された, 簡明かつ**背理法を用いない**証明[5]を紹介しよう．

証明.

(ステップ 1). n を 2 以上の整数とする．このとき, n と $n+1$ をともに割り切る正の整数は 1 のみ．

正の整数 m に対して $m|n$ かつ $m|(n+1)$ であれば, 引き算により, $m|1$ である．従って, $m=1$ である．

(ステップ 2). n を 2 以上の整数とする．n が異なる k 個以上の素数の積で割り切れるならば, $(n+1)\cdot n$ は異なる $k+1$ 個以上の素数の積で割り切れる．

条件により, $p_1 \cdot p_2 \cdots p_k | n (p_i$ は異なる k 個の素数) と書ける．$n+1 \geq 2$ だから, $p|n+1$ である素数 p が存在する (素因数分解の存在)．$p \neq 1$ だから, ステップ 1 により, p は n を割り切れない．他方, $p_i|n$ だから, $p \neq p_i$ である．こうして $p, p_1, p_2, \cdots, p_k$ は互いに異なる $k+1$ 個の素数である．しかも, これら $k+1$ 個の積は $(n+1)\cdot n$ を割り切る．$a|b$ かつ $c|d$ ならば, $a \cdot c | b \cdot d$ だからである．

(ステップ 3). 数列 $\{a_k\}$ を漸化式 $a_1 = 2$, $a_{k+1} = (a_k+1)\cdot a_k$($k$ は正の整数全体にわたる) により定義する．このとき, すべての正の整数 k に対して, a_k は異なる k 個の素数の積で割り切れる．特に, a_B は異なる B 個以上の素数の積で割り切れることになるから, 素数は確かに B 個以上存在するのである．

各正の整数 k に対して, 命題 P_k を「a_k は異なる k 個の素数の積で割り切れる.」と定め, 命題 Q_k を「命題 P_k が真であるならば命題 P_{k+1} も真である.」と定める．示したいことは P_k がすべての正の整数に対して真であるということである．そのためには, 数学的帰納法により, P_1 が真であること, 及び 任意の正の整数 k に対して命題 Q_k が真であること, の 2 つを示せばよい．a_1 が素数 2 で割り切れることから P_1 は真である．命題 Q_k における条件「P_k が真」は, ステップ 2 における条件を $n = a_k$ がみたすことを意味し, 命題 Q_k における帰結「P_{k+1} が真」は, a_{k+1} の定義 $a_{k+1} = (a_k+1)\cdot a_k$ により, ステップ 2 を $n = a_k$ に適用したときの帰結に他ならない．故に, ステップ 2 により, Q_k も真である．

こうして, 素数を小さいほうから順にならべた無限数列 (**素数列**):

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots, p_{25} = 97, \ldots, p_n, \ldots$$

ができる．n 番目の素数を n から明示的に与える公式は知られていない．

問題 3 *次の (1), (2) を示せ．*

*(1) (**H2**)* $p_n = f(n)$*(n はある正の整数以上のすべての整数) である整数を係数とする多項式* $f(x)$ *は存在しない．*

*(2) (**H3**)* $p_n = F(n)/G(n)$*(n はある正の整数以上のすべての整数) である有理数を係数とする多項式* $F(x)$, $G(x)$ *も存在しない．*

問題 4 $s > 1$ *を 1 より大きな実数とする．次の (1), (2) を示せ．*

*(1) (**H3**) 次を示せ．*

$$\sum_{n=0}^{\infty} \frac{1}{p_k^{sn}} = \frac{1}{1 - \frac{1}{p_k^s}}\,.$$

[5] この証明においては素因数分解の一意性も全く使われていないことにも注意しておく．

(2) *(***D1***)* 更に素因数分解の存在と一意性にも注意して, 次の両辺はともに収束して収束値は同じであることを示せ.

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \Pi_{k=1}^{\infty} \frac{1}{1-\frac{1}{p_k^s}} \,.$$

この等式を **Euler の等式 (積公式)** という. また, この共通の収束値を $\zeta(s)(s>1)$ と書き, **ゼータ関数**という.

2.4 素数定理

では素数の現れ方にはまったく規則性がないのであろうか？

$$\pi(n) = (n\ \text{以下の素数の個数})$$

とおく. Gauss は 3000000 までの素数の表を 1000 毎にくぎり, 各区間に現れる素数の個数と桁数の逆数である $1/\log x$ の間にある種の比例関係がみられることに気づいた. より正確には, 桁数は自然対数の底 e に関する "桁数" $\log x = \log_e x$ のことであり, "桁数の逆数"を 2 から n まで連続的に足し合わせた数

$$\int_2^n \frac{dx}{\log x} = \int_2^n \frac{dx}{\log_e x}$$

(の近似値) と $\pi(n)$ を計算し, その比が 1 に近いことに気づいたのである. Gauss は, 具体的に

$$n = 500000\ \text{のとき}, \ \pi(500000) = 41556\,,\ \text{積分値} = 41606.4$$

$$n = 1000000\ \text{のとき}, \ \pi(1000000) = 78501\,,\ \text{積分値} = 79627.5$$

$$n = 1500000\ \text{のとき}, \ \pi(1500000) = 114112\,,\ \text{積分値} = 114263.1$$

$$n = 2000000\ \text{のとき}, \ \pi(2000000) = 148883\,,\ \text{積分値} = 149054.8$$

$$n = 2500000\ \text{のとき}, \ \pi(2500000) = 183016\,,\ \text{積分値} = 183245.0$$

$$n = 3000000\ \text{のとき}, \ \pi(3000000) = 216745\,,\ \text{積分値} = 216970.6\,.$$

であることを確かめ,

$$\lim_{n\to\infty} \frac{\pi(n)}{\int_2^n dx/\log x} = 1$$

であろうと予想したのである. この予想は Gauss が 72 歳のクリスマスイヴの日に友人にあてた手紙に書かれている ([Go], Appendix B, Gauss が Enke にあてた手紙). Gauss 自身はこの予想を示すことはできなかったが, 先立つ Euler の仕事 (問題 4), Gauss の貢献, その後の Dirichlet, Chebychev, Riemann らの貢献を経た後, 1896 年に Hadamard と de la Vallée Poussin により, 独立に証明された:

定理 3 *(***素数定理***)*

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\log n} = 1\ .$$

次の問により, 素数定理の式と Gauss の予想した式は同値であることに注意しよう.

問題 5 *(**H3**) 部分積分法等を用いて, 次を示せ.*

$$\lim_{n\to\infty}\frac{\int_2^n dx/\log x}{n/\log n}=1\,.$$

素数定理の証明においては, ゼータ関数 $\zeta(s)$ を複素数変数の関数にまで拡張して考えること (**複素関数論**) が本質的である ([Ka]). [Ka] にある素数定理の証明はかなり込み入ったものであるが, 1997 年の論文 [Za] で, D.Zagier は J. Newman の方法に基づいた, 2 ページの自己完結的[6] かつ非常に明快な証明を与えた.

素数定理は n 以下の素数の個数が比の意味で $n/\log n$ 個と大体同じであることを示す式であるが, これから n 番目の素数 p_n はやはり比の意味で $n\log n$ と大体同じであることがわかる. その理由は問題としておこう:

問題 6 *(1) (**H2**) $\pi(p_n)$ を n を用いて表せ.*

*(2) (**H3**) 素数定理を既知として, 次を示せ.*

$$\lim_{n\to\infty}\frac{p_n}{n\log n}=1\,.$$

*(3) (**D1**) (2) にも注意して, $p_n=F(n)/G(n)$(n はある正の整数以上のすべての整数) である実数を係数とする多項式 $F(x)$, $G(x)$ も存在しないことを示せ.*

3 Green-Tao の等差数列定理

3.1 Green-Tao の等差数列定理とは

Green と Tao は素数列 p_n に潜む驚くべき秩序を発見した:

定理 4 *(**Green-Tao の等差数列定理** [GT]) 素数列*

$$p_1,p_2,p_3,p_4,\ldots,p_n,\ldots$$

*には, いくらでも長い等差数列が含まれる. つまり, 任意に与えられた正の整数 k に対し, 素数列の中からうまく k 個の項を取り出して, k **個の素数からなる等差数列***

$$p_{\ell_1},p_{\ell_2},\ldots,p_{\ell_k}\ (\ell_1<\ell_2<\ldots<\ell_k)$$

ができる.

ここで, **等差数列**とは

$$4,7,10,13,\ldots$$

[6] 大学 2 年生程度の複素関数論の知識とステルチェス積分及びそれらの理解に必要な微分積分の基礎知識があれば後はなんの知識もいらないという意味である. 大学 2 年生以上の人にお勧めである.

のようにある数 (この例では 4) から始めて, 同じ数 (この例では 3) を次々とたしてできる数列のことである. より正確に述べると

$$a, a+d, a+2d, a+3d\ \ldots, a+(k-1)d, a+kd, \ldots$$

の形の数列が等差数列である. ここで最初の項 a のことを**初項**といい, 次々とたされる一定の数 d のことを**公差**という. この数列においては, 第 k 番目の項 a_k は初項 a に d を $k-1$ 回たすことで得られるから, $a_k = a+(k-1)d$ である. k 個の項からなる等差数列

$$a, a+d, a+2d, \ldots, a+(k-1)d$$

のことを**長さ k の等差数列**という.

この定理とその証明は数学界における "Nature" に相当する専門誌 **Annals of Mathematics** から出版された. また, この業績を主業績の一つとして Tao は 2006 年にスペインのマドリードで開催された国際数学者会議において, 数学界における "Nobel 賞" に相当する **Fields 賞**を受賞した[7].

定理に戻ろう. 2 項以下からなる数列はすべて等差数列だから, 定理が非自明なのは長さ k が 3 以上の整数の場合である.

例 3 *(1)* 3, 5, 7 は素数列に含まれる長さ 3 の等差数列 (公差 2) である. また, 5, 11, 17 も素数列に含まれる長さ 3 の等差数列 (公差 6) である. 2 番目の例では, 5 と 11 の間にある素数 7 は数列に現れていない. このように等差数列を作るときに素数はとびとびに選んでもよいことに注意しよう.

(2) 5, 11, 17, 23 は素数列に含まれる長さ 4 の等差数列 (公差 6) である. また, 43, 61, 79, 97 も素数列に含まれる長さ 4 の等差数列 (公差 18) である.

(3) 5, 11, 17, 23, 29 は素数列に含まれる長さ 5 の等差数列 (公差 6) である.

このように長さが小さいときには一見すると簡単である. (1), (2), (3) いずれの例においても, 素数列に含まれ, 5 を初項とする等差数列が見出された. では, 素数列に含まれる等差数列で, 5 を初項とし (次の長さである) 長さが 6 のものは作れるであろうか? 残念ながら決して作れないことがわかる. 第 6 項 $5+5\cdot d (d \geq 1)$ は, 5 より真に大きくかつ 5 で割り切れるため, 公差 d をどのような正の整数に選んでも, 第 6 項は必ず合成数になってしまうからである.

問題 7 *(H2)*

(1) 素数列に含まれる長さ n の等差数列の初項は, 必ず n 以上の (素) 数であることを示せ. ただし, 公差は正とする.

(2) 素数列に含まれる無限等差数列 (長さが有限ではない等差数列) は存在しないことを示せ.

この帰結として素数列に含まれる等差数列はつねに長さが有限であり, 長さを長くするためには初項を大きくしていかなければならないことがわかる.

[7] Green, Tao 両氏はまだ 30 代であるが, ともに 20 代で超名門大学 (Cambridge 大学, UCLA) の正教授になっている. 特に, Tao 氏は 10 才で数学オリンピック銅メダル, 11 才で数学オリンピック銀メダル, 13 才で数学オリンピック金メダルに輝いている, これらはいずれも最年少記録である. また, 2009 年 9 月時点で, 170 本以上の論文があり, それらの論文は 979 人以上の数学者から 2344 回以上引用されていたが, その数は 2010 年 2 月現在 1070 人以上の数学者から 2553 回以上に増えている. これだけでもまさに数学界におけるイチローみたいな超スーパースターといえよう.

2009年9月現在に確認されている, 素数列に含まれる最長の等差数列は, 初項$a = 6171054912832631$(約6000兆), 公差$d = 81737658082080$(約80兆) の25項からなる等差数列

$$a, a+d, a+2d, \ldots, a+24d$$

である. この数列の各項が素数であることは, 例えば, Mathematica により検証できる. また, このa, dに対し

$$a - d = 31 \times 571 \times 344009787851$$

$$a + 25d = 1741 \times 470178945961$$

であり, この数列は素数列の中ではより長い等差数列には伸ばせないこともわかる.

Green-Tao が定理を見出したと思われる2004年頃に知られていた, 素数列に含まれる等差数列の最長の長さは23であった. このように, 素数列の中に実際に確認されている等差数列の長さは意外と短いのである.

では, Green-Tao はどうのようにして定理が正しいとの確信に至ったのだろうか? 論文からわかるのは次の3つである:

(I) Heuristic (発見的方法) (II) 他の有名な予想からの帰結 (III) 既知の定理とその拡張可能性.

以下, 本章では (I), (II), (III) について見ていき, 次章への橋渡しとする.

3.2 Heuristic (発見的方法)

実際にはそうでない "理想的な状況" を仮想することにより (多くの場合) 問題を定量的に計算可能な問題にして "結論に至る" という日常生活においてはしばしば行われる方法である. 数学においては, 行われた計算や推論が仮想なしに正当化できない限りナンセンスであるが, 定理の正しさがなんとなく "納得" できるといった心理的効果はあると思われる[8].

等差数列の長さ$k \geq 3$を固定する. また, Nを (kに比べて) 非常に大きな整数とする (例えば25に対しては6000兆をはるかに越える数). まず, すべての項が素数であるという条件をひとまず忘れて, N以下のk個の正の整数からなる等差数列

$$1 \leq a_1 < a_2 < \ldots < a_k \leq N$$

が何個位あるか考えてみよう. これは容易である. $a_k = a_1 + (k-1)d \leq N$により, 与えられた初項$a_1$に対して可能な公差$d$は

$$1 \leq d \leq [\frac{N - a_1}{k-1}]$$

($[x]$はx以下の最大の整数を表す) をみたす整数となる. 故に, 求める個数Sは

$$S = \sum_{a_1=1}^{N} [\frac{N - a_1}{k-1}]$$

[8]例えば, 無理数$\sqrt{2}$の存在を,「1辺の長さが2の正方形を描き, 各辺の中点を4頂点とする正方形を新たに作ると, 面積は半分の2になるので, その1辺の長さとして$\sqrt{2}$が存在する.」と "説明" するのがこれにあたる. ただし, この説明は, 辺の長さや面積の概念をきちんと定義すれば正当化できる.

$$\geq \sum_{a_1=1}^{N}(\frac{N-a_1}{k-1}-1)=\frac{N(N-1)}{2(k-1)}-N\geq \frac{N^2}{3(k-1)}$$

とわかる．では, この中ですべての項が素数であるものがどの位あると期待できるだろうか？素数定理によれば, N が非常に大きな数であれば, $\pi(N)/(N/\log N)$ はほとんど 1 である．故に, N 以下の正の整数 a を無作為に選んだ時に素数が選ばれる確率は, ほぼ $(N/\log N)/N = 1/\log N$ である．従って, **もし素数が十分に一様に分布していれば**, 先に求めた S 個の中にすべての項が素数であるものが

$$S\cdot(1/\log N)^k \geq \frac{N^2}{3(k-1)(\log N)^k} > 0$$

個以上あることになり，　定理は正し**そうに見える**のである．

一方, この論法を数学的に正当化することは無理である．現実には, 素数の分布は "一様" からは程遠いからである．例えば, 奇数からなる等差数列 1, 3, 5, ... には無限に素数があるが, 偶数からなる等差数列 2, 4, 6, ... に現れる素数は 2 のみである．より一般に, 与えられた整数 $d\geq 2$ に対し, 正の整数全体を d でわった余り 0, 1, ... $d-1$ により, d 組にわけたとき, 余りと d の最大公約数が 2 以上の組に含まれる素数はあったとしても初項だけであるが, **余りと d の最大公約数が 1 の組には素数はそれぞれ無限個含まれる (Dirichlet の定理)**．このように, 分布はいかなる意味においても一様からはほど遠いのである．

次の問からも素数の分布は一様からはほど遠いことがわかる:

問題 8 *(*H2*)*

(1) $10!+2,\ 10!+3,\ \ldots,\ 10!+10$ はすべて合成数であることを示せ.

(2) 与えられた正の整数 k に対して, k 個の続いた整数

$$a+1, a+2, \ldots, a+k$$

がすべて合成数であるような正の整数 a があることを示せ．.

3.3　他の有名な予想からの帰結

予想 1 *(***Erdös-Turán** *(1936))*

$$\sum_{n=1}^{\infty}\frac{1}{a_n}=\infty$$

である正の整数からなる数列

$$0 < a_1 < a_2 < \ldots < a_n < \ldots$$

にはいくらでも長い等差数列が含まれる.*(***この予想は現在未解決である.***)*

予想中の条件がある意味で必要であることは次の問からわかる:

問題 9 *(1) (***H3***)* 次を求めよ*:*

$$\sum_{n=1}^{\infty}\frac{1}{n(n+1)}\,.$$

*(2) (***H2***)* 数列 $a_n = n(n+1)(n=1,\ 2,\ \ldots)$ には長さ 3 以上の等差数列は含まれないことを示せ.

問題 10 *(**D1**) Euler* の等式 *(*問題 *4)* を用いて*,* 素数列は *Erdös-Turán* の予想 *(*予想 *1)* の条件

$$\sum_{n=1}^{\infty} \frac{1}{p_n} = \infty$$

をみたすことを示せ*.*

従って, Erdös-Turán 予想が正しければ Green-Tao の等差数列定理 (定理 4) も正しいはずなのである.

予想 2 *(***Hardy-Littlewood** *(1920* 年代*))*
$a_i x + b_i (i = 1, 2, \ldots, k)$ を正の整数 $a_i > 0$ と整数 b_i を係数とする k 個の 1 次式とする. これら k 個の多項式をすべてかけてできる k 次多項式

$$F(x) = \Pi_{i=1}^{k}(a_i x + b_i)$$

が以下に述べる条件 *(C)* をみたすならば*,* k 個の数

$$a_1 n + b_1, a_2 n + b_2, \ldots, a_k n + b_k$$

がすべて素数であるような正の整数 n が無限個ある*.*
条件 *(C):* 「各素数 p に対し*,* $F(m)$ が p でわりきれないような整数 m が必ずある*.*」
*(***この予想も現在未解決である.***)*

例 4 *(1)* x*,* $x+2$ に対して $F(x) = x(x+2)$ である. $F(-1) = -1$ だから*,* $F(x)$ は *Hardy-Littlewood* 予想 *(*予想 *2)* にある条件 *(C)* をみたす. 従って*,* もし *Hardy-Littlewood* 予想が正しければ*,* n*,* $n+2$ がともに素数である正の整数 n が無限個あることになる. つまり*,* **双子素数問題**が解けることになる.
(2) k を 3 以上の整数とする. k 個の 1 次式

$$x + 1, 2x + 1, \ldots, kx + 1$$

を考える. $F(x) = (x+1)(2x+1)\cdots(kx+1)$ であり*,* $F(0) = 1$ だから*,* $F(x)$ は *Hardy-Littlewood* 予想の条件 *(C)* をみたす. 従って*,* もし *Hardy-Littlewood* 予想が正しければ*,* 適当な正の整数 n に対して*,* k 個の数

$$n + 1, 2n + 1, \cdots kn + 1$$

はすべて素数となり*,* 素数列の中に k 項からなる公差 n の等差数列となる. つまり*, Green-Tao* の等差数列定理 *(*定理 *4)* が従うのである*.*

このように, Green-Tao の定理は有名な 2 つの未解決問題の特別な場合なのである. 通常, 予想 (特に歴史のある有名な予想) は正しいものと信じたいから, その特別な場合として導かれることは当然正しいものであってほしいのである.

3.4 既知の定理とその拡張可能性の追求

これは定理の証明にも関係する最も本質的部分である. Green-Tao の等差数列定理 (定理 4) は
(i) 素数を考える. (ii) 与えられた集合に等差数列を見出す.
という 2 つの部分からなっている. 今までは主に (i) について述べてきたが, 実際には, Green-Tao の等差数列定理の証明において素数が本質的になるのは最後の最後であって, 筆者が理解した限りでは, 証明の本質は**素数列への応用を念頭において (ii) の方法をある意味で極限まで強化すること**であると思われるのである.

例えば, 次の問題の (2) は (ii) に関する問題である ((1) は (2) へのヒント):

問題 11 *(***H2***)*
(1) 任意の実数 α と任意の正の整数 m に対して, $|\alpha x - y| < 1/m$ である *(*α と m に依存した*)* 整数 $x,\ y$ が存在することを示せ *(***Dirichlet の部屋割り論法***)*.
(2) $0 < a < a + \delta < 1$ である実数 $a,\ \delta$ を固定して考える. 整数全体の部分集合 $A_N,\ B_N$ を次で定める:

$$A_N = \{n \,|\, n \text{ は } -N \le n \le N\,,\ a < \{\sqrt{2}n\} < a + \delta \text{ をともにみたす整数}\,\},$$

$$B_N = \{n \,|\, n \text{ は } -N \le n \le N\,,\ a < \{1.41 \cdot n\} < a + \delta \text{ をともにみたす整数}\,\}\,.$$

任意に与えられた正の整数 k に対して, k に応じて正の整数 N を十分大きくとれば, A_N は長さ k の等差数列を含むことを示せ. 同様なことは B_N についても成り立つか? ここで, 実数 x に対し, $\{x\}$ は x の分数部分 $x - [x]$ *(*例えば, $\{\sqrt{2}\} = \sqrt{2} - [\sqrt{2}] = \sqrt{2} - 1$*)* である.

問題 (ii) に関しては, 次の Van der Waerden の定理を源泉とする一連の深い研究がある:

定理 5 *(***Van der Waerden** *(1927* 年*))*
1 以上 N 以下の N 個の正の整数を m 色で色分けする[9]ことを考える. このとき, 与えられた 2 つの整数 $m \ge 1,\ k \ge 3$ に対し, m と k に依存した正の整数 $N(m,k)$ があって次をみたす:
$N \ge N(m,k)$ ならば, 問題としている色分けにおいて, *(*N^m 個あるどの色分けにおいても*)*, 同じ色からなる長さ k の等差数列が必ず存在する.

この定理の証明は, 高校 2 年までの数学の知識があれば理解できるという意味では初等的である. ただし, 数学的帰納法を二重に組み込んだ論証を要するなどかなり込み入ったものである. 読みやすい (既存の) 証明が Tao の論文 [T06](Section 11) にある.

例 5 整数 $k \ge 3$ を固定し, $N \ge 2$ を整数とする. N 以下の正の整数を考え, 素数は緑色, 素数でない数は赤色で書くことで, N 以下の正の整数を色分けすることができる. このとき, *Van der Waerden* の定理によれば, 定理の意味で N を十分に大きくとれば, 赤色の数または緑色の数の少なくとも一方には長さ k の等差数列が見つかることになる. 実際には, 赤色の数の中に

$$4, 6, 8, 10, \ldots 2[N/2]$$

[9]正確には, N 以下の正の整数全体をどの 2 つも共通部分を持たない m 個の部分集合の和集合にするということである. また, 2 つの整数の色が同じであるとは, 同じ部分集合に属するということである.

という長さ k をはるかに越える長さの等差数列がある. 残念ながら, この考察だけからは, 緑色の数 (N 以下の素数) の中に長さが k 以上の等差数列があるかどうかについてはなにも言えないのである.

このように, Van der Waerden の定理は非常に美しい定理ではあるが, どの色の中に等差数列が見つけられるかについての積極的な情報が取り込まれていないところが弱点であった. Erdös と Turán はこの弱点を補強する形の定理を予想した (1936 年). その予想は Szemerédi により, 1975 年に次のように解決された:

定義 2 以下, 正の整数 N に対して, 集合 $[N]$ を

$$[N] = \{1, 2, \ldots, N-1, N\}$$

(1 以上 N 以下の整数全体の集合) と定める. $[N]$ の部分集合 A_N に対して

$$|A_N| = (A \text{ に属する整数の個数})$$

と書き, A_N の**元の個数**という. 例えば, $|[N]| = N$ である. A_N と $[N]$ の元の個数の比 $|A_N|/N$ を, $[N]$ の部分集合 A_N の**密度**という.

定理 6 (**Szemerédi**) $0 < \delta < 1$ である実数 δ を任意に選んで固定する. 密度が δ 以上である $[N]$ の部分集合について考える. このとき, δ と与えられた整数 $k \geq 3$ に対し, δ と k に応じて定まる正の整数 $N(\delta, k)$ があって, 次が成り立つ:

$N \geq N(k, \delta)$ ならば, 密度が δ 以上である $[N]$ の部分集合には, 長さ k の等差数列が必ず含まれる.

例 6 $N \geq N(k, \delta)$ のとき, $[N]$ の色分けで生じた部分集合 A, B の密度がどちらも δ 以上であったならば, A にも B にも長さが k の等差数列が見つかることになる. このように, *Szemerédi* の定理は *Van der Waerden* の定理よりかなり強力になっているのである.

問題 12 (**H2**) $\delta = 1/m$ と定めることにより, *Semerédi* の定理から, *Van der Waerden* の定理を復元せよ.

例 7 A_N を N 以下の素数全体の集合とする. $A_N \subset [N]$ に *Szemerédi* の定理が適用できるであろうか? 適用できるためには, ある実数 δ (ただし, $0 < \delta < 1$) が存在して, 十分大きなすべての整数 N に対して $|A_N|/N \geq \delta$ でなければならない. しかしながら, 素数定理により, $N \to \infty$ において

$$\frac{|A_N|}{N} = \frac{\pi(N)}{N} = \frac{\pi(n)}{\frac{N}{\log N}} \cdot \frac{1}{\log N} \to 1 \cdot 0 = 0$$

なので, このような δ は存在しない. 従って, *Szemerédi* の定理をもってしても, *Green-Tao* の等差数列定理を直接導くにはまだ不十分なのである.

Green-Tao の等差数列定理を得るためには, Szemerédi の定理をもう 2 段階拡張することが必要となった. 以下, その拡張について述べる.

Szemerédi の定理は非常に美しい上に強力な定理であり, 多くの数学者に刺激を与えた. 中でも Furstenberg(エルゴード理論)[10] と Gowers(関数解析と組合わせ論)[11] はそれぞれの分野あるいは立場から, Szemerédi の定理の拡張あるいは別証明を与えることに成功した. その中では, 集合とその部分集合のみではなく, **集合上の関数と期待値も考える**ことが重要になった. 関数では足し算引き算掛け算定数倍ができる (**関数全体は環構造と線形空間の構造をもつ**) ため, 使える道具や自由度が格段に増すという利点がある. Furstenberg と Gowers の仕事の詳細はここでは省略[12] し, 期待値の定義と, 期待値と等差数列の関係の原型を問題として述べるにとどめる:

定義 3 以下, N を素数とする.

$$[N] = \{1, 2, \ldots, N-1, N\}$$

の元 a, b 対し, 整数としての和 $a+b$ と N でわった余りが等しくなる $[N]$ の元 c のことを a, b の $[N]$ における和 $(+)$ と定める. また, 整数としての積 $a \cdot b$ と N でわった余りが等しくなる $[N]$ の元 d を a, b の $[N]$ における積 $(\cdot)$ と定める. $[N]$ に和と積をこのように定めた対 $([N], +, \cdot)$ ことを記号で $\mathbf{Z}_N$ と書く[13].

$f(x)$ を $[N] = \mathbf{Z}_N$ を定義域とする実数値関数とする. このとき, $f(x)$ の**期待値** $\mathbf{E}(f(x)|x \in [N])$ を

$$\mathbf{E}(f(x)|x \in [N]) = \frac{1}{N} \sum_{x \in [N]} f(x)$$

と定める. ここで右辺の和は N 個の項の和の平均であることに注意する.

また, $f(x)$ の**長さ k の等差数列上の値の積の期待値**

$$\mathbf{E}(f(x)f(x+r)\cdots f(x+(k-1)r) \,|\, x \in \mathbf{Z}_N, r \in \mathbf{Z}_N)$$

を

$$\mathbf{E}(f(x)f(x+r)\cdots f(x+(k-1)r) \,|\, x \in \mathbf{Z}_N, r \in \mathbf{Z}_N) = \frac{1}{N^2} \sum_{x, r \in \mathbf{Z}_N} f(x)f(x+r)\cdots f(x+(k-1)r)$$

と定める. ここで右辺の和は N^2 個の項の和の平均であることに注意する.

問題 13 *(***H2***)* 次を示せ:

$$|\mathbf{E}(f(x)|x \in [N])|^2 = \mathbf{E}(f(x)f(x+r)|x, r \in \mathbf{Z}_N) \ .$$

このような歴史を経て, 2006 年の論文 ([T06]) において, Tao は, Szemerédi の定理の異なる定式化と別証明を与えることに成功した:

---

[10] 2007 年に数学における権威ある賞である Wolf 賞を受賞している. また, ICM2010 の Plenary Speaker でもある.

[11] ICM1998 において Fields 賞を受賞している.

[12] 興味のある方は優れた解説 [Kr] 等を参照されたい.

[13] $\mathbf{Z}_N$ は代数学で学ぶ剰余環 $\mathbf{Z}/(N)$ に他ならない. N は $\mathbf{Z}_N$ における和と積に関して 0 の役割をするので, $\mathbf{Z}_N$ においては N は 0 と同一視する. 集合としては $[N] = \mathbf{Z}_N$ であり, $[N]$ と $\mathbf{Z}_N$ の違いは, $\mathbf{Z}_N$ においては和と積が指定されているということだけである. また, N を素数に選んだのは, $\mathbf{Z}_N$ の 0 以外の元が積に関する逆数をもつようにするためである.

定理 7 *(***Tao; Semerédi の定理の変形版***)* $0<\delta<1$ である実数 δ と 3 以上の整数 k を任意に選んで固定する．$[N]=\mathbf{Z}_N$ 上

(1) すべての $x\in[N]$ に対し，$0\le f(x)\le 1=\nu_{\mathrm{const}}(x)$ *;*

(2) $\mathbf{E}(f(x)|x\in[N])>\delta$

の *2* 条件をともにみたす関数 $f(x)$ について考える．このとき，δ と k に依存して決まる整数 $N(\delta,k)$ と正の実数 $c(\delta,k)>0$ があって，次をみたす*:*

N が $N(\delta,k)$ 以上の素数であるならば，*(1), (2)* をみたすどの関数 $f(x)$ に対しても

$$\mathbf{E}(f(x)f(x+r)\cdots f(x+(k-1)r)|x,r\in\mathbf{Z}_N)>c(\delta,k)\ .$$

Tao の定理 ([T06]) の証明は，　実質約 20 ページでありやや長いが，必要になる知識は，Bertrand の公準「2 以上の整数 x に対して $x<p<2x$ である素数 p が存在する.」([Ka], Chebychev の定理) と Weierstrass の多項式近似定理 ([Su]) を除けば，Landau の記号とその使い方，有限次元抽象線形空間とその上の抽象内積の定義，数列に対する Cauchy-Schwarz の不等式といった，理系であれば大学 2 年次までに履修することだけである．また，Van der Waerden の定理 (定理 5) は用いられるが，その証明は付録に付けられている．

ここでは Tao による変形版 (定理 7) から Szemerédi の定理 (定理 6) が従うことを検証しておこう．

A_N を $[N]$ の部分集合で密度が δ より大きいとする．$[N]=\mathbf{Z}_N$ 上の関数 $f(x)$ を

$x\in A_N$ に対しては $f(x)=1$, $x\notin A_N$ に対しては $f(x)=0$

と定める．定め方により，

$$\mathbf{E}(f(x)|x\in\mathbf{Z}_N)=\ (A_N\text{ の密度})>\delta$$

である．故に，関数 $f(x)$ は，定理 7 における前提条件 (1), (2) をみたす．従って，定理 7 の帰結により，素数 N を十分に大きくとれば

$$\mathbf{E}(f(x)f(x+r)\cdots f(x+(k-1)r)|x,r\in\mathbf{Z}_N)>c(\delta,k)>0$$

である．特に，

$$f(x)f(x+r)\cdots f(x+(k-1)r)>0$$

である組

$$(x,x+r,\cdots,x+(k-1)r)$$

が $c(\delta,k)N^2$ 個以上ある．条件により，このような組 $(x,x+r,\cdots,x+(k-1)r)$ の各項 $x+\ell r$ に対し，$f(x+\ell r)\neq 0$ である．従って，$f(x)$ の定義により，$x+\ell r$ はすべて A_N 属する．故に，　このような組

$$(x,x+r,\cdots,x+(k-1)r)$$

は A_N に属する長さが k で公差が r の等差数列である[14].

[14] 厳密には次の 3 点に心配が残る．

(i) 求めた等差数列はすべて $r=0$ になってしまうことはないのか?

(ii) $\mathbf{Z}_N$ における足し算は N を法として考えているため，$2+(N-1)=1$ のように，求めた数列は実はすべて循環してしまっている (本当の等差数列ではない) といったことはおこらないのか？

(iii) 変形版では N を素数に限定しているが原版ではこのような制限はないためこの点で弱くなってしまっていたりしないのか？

(i) は，$r=0$ である列は N 個であり $c(\delta,k)N^2$ より (N が大きければ) はるかに小さいことから解消される．また，(ii), (iii) は変形版を $\delta=\delta/2k$, k に適用して，2 以上の自然数 N に対して $kN<N'<2kN$ である素数 N' があること (Bertrand の公準) を用いることで同時に解消される．

先と同様, $A_N = \{N$ 以下の素数 $\} \subset [N]$ と A 以外では 0 である関数 $0 \leq f(x) \leq 1$ と正の実数 $\delta > 0$ をどのように選んでも, 十分大きな素数 N すべてにわたり $\mathbf{E}(f(x)|x \in \mathbf{Z}_N) > \delta$ とすることは, 素数定理により不可能である.

Green-Tao が至った最後の拡張は

「変形版の条件 (1) における $1 = \nu_{\mathrm{const}}(x)$ を期待値がおよそ 1 であるような揺らぎを許した非負関数に拡張する.」

であった.

4 Green-Tao の準乱雑測度と Semerédi 型定理

4.1 Green-Tao の Semerédi 型定理

定義 4 十分大きなすべての素数 N に対して, $[N] = \mathbf{Z}_N$ 上の非負関数 $\nu_N(x)$ が与えられているとする.

$$\lim_{N\to\infty} \mathbf{E}(\nu_N(x)|x \in [N]) = 1$$

であるとき, $\nu_N(x)$ を $[N] = \mathbf{Z}_N$ 上の**測度**であるという. より正確には, 上の条件をみたす非負関数と定義域の組の集合 $\{(\nu_N(x), [N] = \mathbf{Z}_N)\}$ が測度である. 更に, 3 以上の整数 k が与えられたとする. 測度 $\{(\nu_N(x), \mathbf{Z}_N)\}$ が, 変数のアファイン変換に関して, $(k \cdot 2^{k-1}, 3k-4, k)$-線形条件と 2^{k-1} 相関条件と呼ばれる条件をみたすとき, この測度のことを k-**準乱雑測度**という[15].

定理 8 *(***Green-Tao の Semerédi 型定理***)* $0 < \delta < 1$ である実数 δ と 3 以上の整数 k を任意に選んで固定する. また, $\nu_N(x)$ を $[N] = \mathbf{Z}_N$ *(*N は十分大きなすべての素数にわたる*)* 上の k-準乱雑測度とする.

(1) すべての $x \in [N] = \mathbf{Z}_N$ に対し, $0 \leq f(x) \leq 1 = \nu_N(x)$;

(2) $\mathbf{E}(f(x)|x \in [N]) > \delta$

の *2* 条件をともにみたす $[N] = \mathbf{Z}_N$ 上の関数 $f(x)$ について考える. このとき, δ と k に依存して決まる整数 $N(\delta, k)$ と正の実数 $c(\delta, k) > 0$ があって, 次をみたす*:*

N が $N(\delta, k)$ 以上の素数であるならば, *(1), (2)* をみたすどの関数 $f(x)$ に対しても

$$\mathbf{E}(f(x)f(x+r)\cdots f(x+(k-1)r)|x, r \in \mathbf{Z}_N) > c(\delta, k) - \epsilon(\delta, k, N)$$

が成り立つ. ここで, $c(\delta, k)$ は定理 *7(Tao* による *Szemerédi* の定理の変形版*)* に登場した数 $c(\delta, k)$ と同じであり, $\epsilon(\delta, k, N)$ は δ, k, N にのみ依存し *(*$\nu_N(x)$ や $f_N(X)$ には依存しない*)* 非負実数で

$$\lim_{N\to\infty} N(\delta, k, N) = 0$$

をみたす数である.

[15] 大ざっぱには変数のアファイン変換に関して k からみて十分に一様なふるまいをする測度といった感じである. もちろん, $(k \cdot 2^{k-1}, 3k-4, k)$-線形条件と 2^{k-1} 相関条件を厳密に述べない限り数学的にきちんと定義したことにはならないが, ここでは省略する. 記述は複雑であり, 証明に立ち入ってその使われ方を見ない限りその意味はわからないからである. 正確な定義に興味のある方は原論文 [GT] を参照されたい.

論文 [GT] において, Green-Tao はこの定理 (定理 8) をまず証明 (Green-Tao の等差数列定理 (定理 4) とは全く独立である) し, 次に, この定理を等差数列定理 (定理 4) に応用することを考えたのである.

4.2 修正された von Mangoldt 関数と Green-Tao の準乱雑測度

定義 5 *(Green-Tao の k-準乱雑測度)*
N を非常に大きな素数, $w = w(N) = \log(\log N)$ とし, $W = W(N)$ を $w = w(N)$ 未満の素数すべての積とする. n を正の整数とする. $Wn + 1$ が素数であるとき,

$$\tilde{\Lambda}_N(n) = \frac{\varphi(W)}{W} \log{(Wn+1)}$$

と定め, それ以外の正の整数 n に対しては $\tilde{\Lambda}_N(n) = 0$ と定める. ここに $\varphi(N)$ は N 以下で N と互いに素である正の整数の個数 *(***Euler 関数***)* である. 関数 $\tilde{\Lambda}_N(n)$ のことを, **修正された von Mangoldt 関数**という.

修正された von Mangoldt 関数のもつ最も重要な性質は

$$\lim_{N\to\infty} \frac{\sum_{n=1}^{N} \tilde{\Lambda}_N(n)}{N} = 1$$

が成り立つことである[16].

Green-Tao の等差数列定理 (定理 4) に応用する上で重要になるのは, 定理 8 における k-準乱雑測度 $\nu_N(x)$ と関数 $f_N(x)$ の選択である. 先行する解析数論の結果にも助けられて, Green-Tao は次の定理の証明に成功した:

定理 9 *(Green-Tao の k-準乱雑測度)* 3 以上の整数 k を任意に選んで固定する.

$$\epsilon_k := \frac{1}{2^k \cdot (k+4)!}$$

と定める. また, N を *(*与えられた k に比べて*)* 十分大きな素数とする. このとき,

$$\epsilon_k \cdot N \leq n \leq 2\epsilon_k \cdot N$$

をみたすすべての整数 n に対して

$$\nu_N(n) \geq \frac{1}{k \cdot 2^{k+5}} \tilde{\Lambda}_N(n)$$

である $[N] = \mathbf{Z}_N$ 上の k-準乱雑測度 $\nu_N(x)$ がある. ここで, $\tilde{\Lambda}_N(x)$ は修正された *von Mangoldt* 関数である.

定理 9 の証明では最新の解析数論の結果が (証明付で) 使われる. [GT] を通して初等的と言えないのはこの部分だけであり, Green-Tao の等差数列定理 (定理 4) を導くのに必要な素数の性質はすべて定理 9 に内包されてしまっている.

[16] Dirichlet の定理の素数定理版から容易に従う.

4.3 定理 8 と定理 9 から定理 4 が従うことの証明

最後に, 定理 8,9 を使って, Green-Tao の等差数列定理 (定理 4) を導こう.

整数 $k \geq 3$ を任意に選んで固定する.ϵ_k を定理 9 で定めた実数とする. 定理 9 における $[N] = \mathbf{Z}_N$ の測度 $\mu_N(x)$ と, 次により定まる $[N] = \mathbf{Z}_N$ 上の関数 $f_N(x)$ について考える:

$$f_N(x) = \frac{1}{k \cdot 2^{k+5}} \cdot \tilde{\Lambda}_N(x) \ (\epsilon_k N \leq x \leq 2\epsilon_k N \text{ のとき})$$

$$f_N(x) = 0 \ (\text{それ以外の } x) \ .$$

定理 9 における $\nu_N(x)$ の定め方と, 修正された von Mangoldt 関数 $\tilde{\Lambda}_N(x)$ の定義により,

$$0 \leq f_N(x) \leq \nu_N(x)$$

であり, $f_N(x)$ が 0 以外の値をとるのは, $Wx + 1(W = W(N)$ は定義 6 で定めた数) が素数であり, かつ $\epsilon_k N \leq x \leq 2\epsilon_k N$ をみたす場合に限られる. 故に, N が十分に大きな素数であれば, 期待値 $\mathbf{E}(f_N(x)|x \in [N])$ は

$$\mathbf{E}(f_N(x)|x \in [N]) = \frac{1}{k \cdot 2^{k+5} \cdot N} \sum_{\epsilon_k N \leq x \leq 2\epsilon_k N} \tilde{\Lambda}_N(x)$$

$$= \frac{1}{k \cdot 2^{k+5} \cdot N} \cdot (2\epsilon_k N - \epsilon_k N)(1 + o(1)) > \frac{\epsilon_k}{k \cdot 2^{k+6}} > 0$$

をみたす[17]. こうして,

$$\delta = \frac{\epsilon_k}{k \cdot 2^{k+6}}$$

に対し, $\nu_N(x)$ と $f_N(x)$ は定理 8 の条件 (1), (2) をともにみたすことが確かめられた. 故に, 定理 8 の帰結により, 十分大きな素数 N に対して

$$\mathbf{E}(f_N(x)f_N(x+r)\cdots f_N(x+(k-1)r)|x, y \in \mathbf{Z}_N) > \frac{c(\delta, k)}{2} > 0$$

である. 左辺の和に対する $r = 0$ である項の寄与は (修正された von Mangoldt 関数の形を考えると) 高々

$$\frac{(\log N)^k \cdot N}{N^2} = \frac{(\log N)^k}{N} \to 0 \, (N \to 0)$$

のオーダーである, 従って, (今一度修正された von Mangoldt 関数の形と, f_N の値が 0 にならない x の範囲が $N/2\epsilon_k$ におさまっていることを考慮すると)

$$f_N(x)f_N(x+r)\cdots f_N(x+(k-1)r) > 0 \ , \ r \neq 0$$

である, 集合 $[N]$ に属する (循環しない) 本来の狭義増加等差数列

$$x, x+r, \ldots, x+(k-1)r$$

[17] ここで, 第 2 の等式における $o(1)$ は $N \to \infty$ で 0 に収束する N のある関数であり, この等式の成立は修正された von Mangoldt 関数の最も重要な性質と述べた性質による.

が $N^2/(\log N)^k \to \infty (N \to \infty)$ のオーダーで存在することが従う．この数列の各項における f_N の値は (すべての積が 0 でないことから) 決して 0 にはならない．故に, f_N の定義により,

$$W \cdot (x + \ell \cdot r) + 1 \ (0 \leq \ell \leq k-1 \text{ は整数})$$

はすべて集合 $[N]$ に属する**素数**である．故に新しい狭義増加数列

$$W \cdot x + 1, W \cdot (x + r) + 1, \ldots, W \cdot (x + (k-1)r) + 1$$

は長さ k の素数からなる等差数列 (公差 $W \cdot r$) である．こうして, 示したかった Green-Tao の等差数列定理 (定理 4) が示された.

参考文献

[GT] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics **167** (2008) 481–547 (ArXiv:math/0404188).

[Go] L. J. Goldstein, *A history of the prime number theorem*, American Math. Monthly **80** (1973) 599–615.

[Ka] 河田敬義, 数論 *I, II, III*, 岩波基礎数学講座.

[Kr] B. Kra, *Green-Tao theorem on arithmetic progressions in the primes: an ergodic point of view*, Bulletin of the American Mathematical Society **43** (2006) 3–23.

[Sa] F. Saidak, *A new proof of Euclid's theorem*, American Math. Monthly **113** (2006) 937–938.

[Su] 杉浦光夫, 解析入門 *I*, 東大出版会.

[T06] T. Tao, *A quantitative ergodic theory proof of Szemerédi' theorem*, The electronic Journal of Combinatorics **13** (2006) 49 pages (ArXiv:math/0405251).

[T07] T. Tao, *What is good mathematics?*, Bulletin of the American Mathematical Society **44** (2007) 623–634 (ArXiv:math/0702396).

[Za] D. Zagier, *Newman's short proof of the prime number theorem - dedicated to the Prime Number Theorem on the occasion of the 100th birthday*, American Math. Monthly **104** (1997) 705–708.

(おぎそけいじ・大阪大学大学院理学研究科)