

等差数列における最小素数について

三河寛 / 筑波大

MIKAWA Hiroshi

志

q, a が互いに素ならば 等差数列 $\{ql+a\}_{l=0,1,2,\dots}$ は素数を無限に含む。そこで、素数がはじめて現れるのはいつか、を考える。つまり $p \equiv a \pmod{q}$ をみたす素数 p のうち最小のもの、 $P(q, a)$ 、を q によって上から押えることを問題とする⁽¹⁾。リーマン予想を仮定すれば

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} \log p = \frac{x}{\phi(q)} + O(x^{\frac{1}{2}} (\log x)^2)$$

となり、 $x = x(q) = q^{2+\varepsilon}$ とすれば右辺は正ゆえ $P(q, a) \ll q^{2+\varepsilon}$ である。また Barban の定理⁽²⁾

$$(1) \quad \sum_{q \leq Q} \sum_{a \pmod{q}}^* \left| \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} \log p - \frac{x}{\phi(q)} \right|^2 \ll Q x (\log x) + \frac{x^2}{(\log x)^A}$$

において $x = x(Q) = Q^{1+\varepsilon}$ とすれば q, a を制限すると

$$\#\{(q, a) : \frac{Q}{2} < q \leq Q, (a, q) = 1, P(q, a) > x(Q)\} \ll Q^2 (\log Q)^{-A}$$

つまり $P(q, a) > x(Q) \gg q^{1+\varepsilon}$ なる頻度は 0 ゆえ $P(q, a) \ll q^{1+\varepsilon}$ と予測できる。

(1) K. Prachar: Primzahlverteilung, Springer-Verlag, 1957. Kap. X.
E. Bombieri: La grande crible dans la théorie analytique des nombres, Astérisque 18 (1974). §6.

g, a について一様に $P(g, a)$ を押える問題に関しては充分な仕事はなされている。⁽ⁱ⁾ ここで大きく譲歩して、(1) のごとく $P(g, a)$ を平均的に云々する。パラメーター g, a を共に動かすことは (1) で終っているから片方を止めてもう片方を動かす。

Bombieri-Vinogradov の定理⁽⁼⁾ から $a \neq 0$ が与えられたとき

$$(2) \quad \sum_{g \leq Q}^* \left| \sum_{\substack{p \leq x \\ p \equiv a(g)}} \log p - \frac{x}{\phi(g)} \right| \ll Q x^{\frac{1}{2}} (\log x)^5 + \frac{x}{(\log x)^A}$$

が従う。 $x = x(Q) = Q^{2+\varepsilon}$ とすれば $P(g, a) > x(Q)$ なる頻度は 0 と分る。ゆえ殆どの g について $P(g, a) \ll x^{2+\varepsilon}$ である。(2) はリーマン予想と同等の力をもつと言えるが、驚くことに、これはさらに強くなり^(ホ)、その結果、 g の指数は 2 を越える。^(ハ)

(ロ) ただし $Q < x$. 文字 A, ε で任意の正定数を表す。暗黙裡に A は大きく ε は小さい。また $(\text{mod } g)$ を単に (g) とかき、 $(a, g) = 1$ を $*$ で表す。

H.L. Montgomery: Topics in Multiplicative Number Theory, Springer Lecture Notes 227 (1971). chap. 17.

(i) D.R. Heath-Brown: Zero-free regions for L-functions and the least prime in an arithmetic progression, Proc. London Math. Soc. 64 (1992) 263-338.

(=) H. Davenport, H.L. Montgomery: Multiplicative Number Theory, 2nd. ed., Springer-Verlag, 1980. § 28.

(ホ) E. Fouvry: Autor du théorème de Bombieri-Vinogradov, Acta Math. 152 (1984) 219-244.; (II), Ann. Sci. Éc. Norm. sup. 20 (1987) 617-640.

E. Bombieri, J.B. Friedlander, H. Iwaniec: Primes in arithmetic progressions to large moduli, Acta Math. 156 (1986) 203-251.; (II), Math. Ann. 227 (1987) 361-393.; (III), J. American Math. Soc. 2 (1989) 215-224.

一方、(2)に相当するものは

$$\sum_{a(q)}^* \left| \sum_{\substack{p \leq x \\ p \equiv a(q)}} \log p - \frac{x}{\varphi(q)} \right|^2 \ll x (\log x)^4 + \frac{x^2}{\varphi(q) (\log x)^A}$$

と期待できる。^(b) もしこれが成立するなら 殆どの a について $P(q, a) \ll q^{1+\varepsilon}$ と言える。奇妙なことに (3) の型の不等式はさほど注目されていない様子である。これらふたつの問題について考えたことなど書残しておきたい。

(A) B. Rousselet: Inegalités de type Brun-Titchmarsh en moyenne, Publ. Math. d'Orsay, 88-01 (1988) 91-123.

前出 Bombieri-Friedlander-Iwaniec (III).

R.C. Baker, G. Harman: The Brun-Titchmarsh theorem on average, Analytic Number Theory. Progress in Math. 138 (1996) 39-103.

H. Mikawa: On primes in arithmetic progressions, Tsukuba J. Math. (submitted).

(b) 前出 Montgomery の I-II. Chap. 17 参照。

ちなみに 根元素数 (高々 21 個の素因数をもつもの) についてのアナロジーは

D.R. Heath-Brown: Almost-primes in arithmetic progressions and short intervals, Math. Proc. Cambridge Phil. Soc. 83 (1978) 353-375.

H. Iwaniec: On the Brun-Titchmarsh theorem, J. Math. Soc. Japan 34 (1982) 95-123.

H. Mikawa: Almost-primes in arithmetic progressions and short intervals, Tsukuba J. Math. 13 (1989) 387-401.

H. Mikawa: On almost-primes in arithmetic progressions, Tsukuba J. Math. 14 (1990) 167-184.

(c) 前出 Davenport-Montgomery の教科書. §24.

分角群の手法は他にも種々ある。読み応えあるのは、

G. Harman: Eratosthenes, Legendre, Vinogradov and beyond, The hidden power of the simplest sieve, London Math. Soc. Lecture Notes Series 237 (1997) 161-173.

(d) $m \sim M$ の $\sum_{m \leq x} \frac{1}{m}$ は $M < m \leq 2M$ を表す。

また $x = \log x$ と略記する。

式

g に関する平均を考える。まず篩を用いて素数を自然数の積として表示する。すると (2) の左辺は

$$[I] \sum_{g \sim Q}^* \left| \sum_{\substack{m \sim M \\ mn \equiv a(g)}} \sum_{n \sim N} a_m - \frac{1}{\varphi(g)} \sum_{\substack{m \sim M \\ (mn, g)=1}} \sum_{n \sim N} a_m \right| ; \begin{array}{l} x \ll MN \ll x \\ 1 \ll M \ll x^{\frac{2}{3}} \\ a_m \ll \log m \end{array}$$

$$[II] \sum_{g \sim Q}^* \left| \sum_{\substack{m \sim M \\ mn \equiv a(g)}} \sum_{n \sim N} a_{\wedge(n)} - \frac{1}{\varphi(g)} \sum_{\substack{m \sim M \\ (mn, g)=1}} \sum_{n \sim N} a_{\wedge(n)} \right| ; \begin{array}{l} x \ll MN \ll x \\ x^{\frac{1}{3}} \ll M \ll x^{\frac{2}{3}} \\ a_m \ll \tau(m) \end{array}$$

に分解する。⁽¹⁾ n の係数が [I] では 1、[II] では $\wedge$ となることが肝要である。パラ x -タ- M の範囲を分解区間と呼ぶ。

[I] の分解区間は $[1, x^{\frac{2}{3}}]$ である。絶対値の内側は

$$\sum_{\substack{m \sim M \\ (m, g) \neq 1}} a_m \left(\sum_{\substack{n \sim N \\ mn \equiv a(g)}} 1 - \frac{1}{\varphi(g)} \sum_{\substack{n \sim N \\ (n, g) \neq 1}} 1 \right) \ll Mx$$

だから [I] は $\ll QMx$ でこれが $\ll x^A$ となっていれば $M \ll x^{1-\varepsilon} Q^{-1}$ であればよい。そこで $[1, x^{\frac{1-\varepsilon}{Q}}]$ を許容区間と呼ぶ。当然 $\langle \text{分解} \rangle \subset \langle \text{許容} \rangle$ でなくてはならないから条件 $Q \ll x^{\frac{1}{3}-\varepsilon}$ を置く。

[II] の許容区間を調べる。[II] の 2 乗は

$$\begin{aligned} & \ll Mx^3 \sum_{g \sim Q}^* g \sum_{\substack{m \sim M \\ (m, g) \neq 1 \\ mn \equiv a(g)}} \left| \sum_{n \sim N} \wedge(n) - \frac{1}{\varphi(g)} \sum_{\substack{n \sim N \\ (n, g) \neq 1}} \wedge(n) \right|^2 \\ & = Mx^3 (W - 2V + U) \end{aligned}$$

となる。 W, V, U は 2 乗を直にひいた結果である。まず、

$$W = \sum_{g \sim Q}^* g \sum_{\substack{n, n' \sim N \\ (nn', g) \neq 1}} \Lambda(n) \Lambda(n') \sum_{\substack{m \sim M \\ mn \equiv a(g) \\ mn' \equiv a(g)}} 1$$

$n \equiv n'(g)$ でなくとも m の合同式は解けない。解けるなら、 m の個数は自明に $Mg^{-1} + O(1)$ であるから

$$\begin{aligned} W &= M \sum_{g \sim Q}^* \sum_{\substack{n, n' \sim N \\ (nn', g) \neq 1 \\ n \equiv n'(g)}} \Lambda(n) \Lambda(n') + O\left(\sum_g g \sum_n \Lambda(n)^2 \left(\frac{N}{g} + 1\right)\right) \\ &= M \sum_{g \sim Q}^* \sum_{\substack{b(g) \\ (b, g) \neq 1}} \left(\sum_{\substack{n \sim N \\ n \equiv b(g)}} \Lambda(n) \right)^2 + O(Q(N+Q)N\mathfrak{L}^2). \end{aligned}$$

同様に

$$V, U = M \sum_{g \sim Q}^* \varphi(g) \left(\frac{1}{\varphi(g)} \sum_{\substack{n \sim N \\ (n, g) \neq 1}} \Lambda(n) \right)^2 + O(QN^2\mathfrak{L}).$$

すると

$$W - 2V + U = M \sum_{g \sim Q}^* \sum_{\substack{b(g) \\ (b, g) \neq 1}} \left(\sum_{\substack{n \sim N \\ n \equiv b(g)}} \Lambda(n) - \frac{1}{\varphi(g)} \sum_{\substack{n \sim N \\ (n, g) \neq 1}} \Lambda(n) \right)^2 + O(Q(N+Q)N\mathfrak{L}^2).$$

$Q < N$ なら (1) を用いて上の和を押えられる。結局 [II] は

$$\ll M^2 \mathfrak{L}^3 (QN\mathfrak{L} + N^2 \mathfrak{L}^{-A}) + Q(N+Q)MN\mathfrak{L}^5$$

$$\ll Q(M+N+Q) \times \mathfrak{L}^5 + \mathfrak{L}^2 \mathfrak{L}^{3-A}.$$

ゆえ $Q \ll x^{\frac{1}{2}-\varepsilon}$ のとき許容区間は $[Qx^{-\varepsilon}, x^{1-\varepsilon}Q^{-1}]$ である。

分解区間 $[x^{\frac{1}{3}}, x^{\frac{2}{3}}]$ を含んでいなくてはならないから $Q \ll x^{\frac{1}{3}-\varepsilon}$

とする。これは $Q < N$ と [I] にも適っている。

さて $Q = x^{\frac{1}{2}-\varepsilon}$ での許容区間はつぶれてしまう。上では誤差を $O(1)$ とした。これをフーリエ展開し、その結果とし

て出現する Kloosterman 和の平均値を押えることにより
 $Q = x^{\frac{1}{2}}$ のときでも許容区間が生き残るようにできる。実際、
 $Q \gg x^{\frac{1}{2}}$ のとき [II] の許容区間は

$$\left[Q^2 x^{\varepsilon-1}, x^{\frac{5}{6}-\varepsilon} Q^{-\frac{4}{3}} \right]$$

となる⁽⁷⁾。これが $[\alpha, \beta], \alpha^2 \leq \beta$ の形であってほしい。なぜなら
 $1 < M_j < \alpha \ (1 \leq j \leq n)$ について $M_1 M_2 \cdots M_n > \beta$ ならば $[\alpha, \beta]$ に
 落ちるある部分積 $M_{(1)} M_{(2)} \cdots M_{(r)}$ が存在する、という事実が
 あれば篩を制御し易いからである。これを要請するなら、
 $Q = x^{\frac{17}{32}-\varepsilon}$ が限界となり、このとき許容区間は $[x^{\frac{1}{16}-\varepsilon}, x^{\frac{1}{8}}]$ で
 ある。そしてこの中に [II] の分解区間が含まれるように篩を
 操作する。しかし、しわよせとして [I] に手に負えない項が
 現れる。そこで、これら何処にも引受け手が無い項の符号を
 正にコントロールして無視する。すなわち素数の個数をその
 まま扱うのを諦めて lower bound を考えるのである。 $P(g, \alpha)$
 を云々するには十分である。もちろん無視する項の寄与は小
 さくなくてはならない。幸いにも、以上の気楽な要求をすべ
 てみたす lower bound sieve を組み立てられる。かくして
 $\alpha \neq 0$ を固定したとき 殆どの g について $P(g, \alpha) \ll g^{\frac{32}{17}+\varepsilon}$
 である。

(7) 前出 (ホ) 参照。(ル) そうであるなら Siegel zero は存在しないことを導びける。

参

a に関する平均を考える。(3)の左辺は指標 $\chi(\bmod q)$ を用いて表示できるけれども L 関数の zero-free region が狭いため全く手が出ない。もし広いなら 殆どの a について

$$(4) \quad P(q, a) \ll q^{\frac{6}{5} + \varepsilon}$$

と言えるのだが。また(3)の2乗を直接開くなら

$$= \sum_{\substack{p, p' \leq x \\ p \equiv p'(q)}} \log p \log p' - \frac{x^2}{\varphi(q)} (1 + O(x^{-A}))$$

となるから $p \equiv p'(q)$ をみたす p, p' をかきえることになるけれども、これもまた困難である。(1)

そこで $p - p' \equiv 0(q)$ を $p + p' \equiv k(q)$ に変更する。ふたつの素数の和として表せる偶数は Goldbach 数と呼ばれるから、 $q \equiv k(q)$ をみたす Goldbach 数 g のうち最小のもの、 $G(q, k)$ を考える。(7) もちろん q が偶数ならば k も偶数とする。こうして

(7) Ju. V. Linnik: Some conditional theorems concerning binary problems with prime numbers, Izv. Acad. Nauk SSSR, 16(1952) 503-520.

M. Jutila: On the least Goldbach's number in an arithmetical progression, Ann. Univ. Turku. Ser. A. I., 118 no. 5 (1968) 8p.

Z. Kh. Rakhmonov: The least Goldbach number in an arithmetic progression, (Zbl. 618.10046; MR. 89c:11142).

H. Mikawa: On Goldbach numbers in arithmetic progressions, Tsukuba J. Math. (to appear).

(7) I. M. Vinogradov: Selected Works, Springer-Verlag, 1985. p. 360.

Z. Kh. Rakhmonov: The distribution of values of Dirichlet characters and their applications, Trudy Mat. Inst. Steklov, 207(1994) 286-296.

$G(g, k)$ の問題点を 各台の α について $P(g, \alpha)$ を押えることの
アナロジーと見做す。

さて g を素数 $\neq 2$ に制限する。すると $g+g \equiv 0(g)$ だから
 $G(g, 0) = 2g$ である。これで $k=0$ の難所を避けたことになる。
以下 $1 \leq k \leq g-1$ とする。合同式を指標で表すと

$$\sum_{\substack{p, p' \leq x \\ p+p' \equiv k(g)}} \log p \log p' = \frac{1}{g-1} \sum_{\chi(g)} \left(\sum_{p \leq x} \bar{\chi}(p) \log p \right) \left(\sum_{p \leq x} \chi(k-p) \log p \right).$$

主指標 χ_0 の寄与は $\frac{x^2}{\phi(g)} (1 + O(x^{-A}))$ でこれが主項のはず
だから 目標は

$$\sum_{\substack{\chi(g) \\ \chi \neq \chi_0}} \left| \sum_{p \leq x} \chi(p) \log p \right| \left| \sum_{p \leq x} \chi(p-k) \log p \right| \ll x^2 x^{-A}$$

となる。 $\sum_{p \leq x} \chi(p) \log p$ と $\sum_{p \leq x} \chi(p-k) \log p$ とを比べてみると、前者
が L 関数の zero に言及せずには扱えないのに対して、後者は
 $x^{\frac{2}{3}+\varepsilon} \ll g \ll x$ なら篩を用いて $\ll (gx)^{\frac{1}{2}} x^4$ とできる。(7) これを
前者に求めるなら、準リーマン予想を仮定しなくてはならない。
かくして $k \neq 0$ とシフトしたことで L 関数の zero-free region が
十分広いことに相当するものを手に入れたことになる。すると
と $G(g, k)$ を (4) と同様に押えられる。さらに前章でのように
lower bound sieve を持込めば、すべての素数 $g \neq 2$ とすべての
の k に対して $G(g, k) \ll g^{\frac{14}{13}+\varepsilon}$ となる。