数理解析研究所講究録
1160巻 2000年 86-93

等差数列における最小素数について

三河寛／筑波大
MIKAWA Hiroshi

壱

q, a が互いに素ならば 等差数列 $\{ql+a\}_{l=0,1,2,\cdots}$ 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。(イ)

リーマン予想を仮定すれば

$$\sum_{\substack{p \le x \\ p \equiv a(q)}} \log p = \frac{x}{\varphi(q)} + O\left(x^{\frac{1}{2}} (\log x)^2\right)$$

となり、$x = x(q) = q^{2+\varepsilon}$ と撰ぶと右辺は正ゆえ $P(q,a) \ll q^{2+\varepsilon}$ である。また Barban の定理(ロ)

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

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

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

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。

(イ) K. Prachar: Primzahlverteilung, Springer-Verlag, 1957. Kap. X.
E. Bombieri: La grand 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厖大な仕事がなされている。(ハ) ここでは大きく譲歩して、(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

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

が従う。$x = x(Q) = Q^{2+\varepsilon}$ と撰べば $P(g,a) > x(Q)$ なる頻度は 0 と分る。ゆえ殆どの g について $P(g,a) \ll g^{2+\varepsilon}$ 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(ヘ)。

(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 $(\mathrm{mod}\ g)$ 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.

(ハ) 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. Sciet. 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

$$\sum_{a(g)}^{*}\Big|\sum_{\substack{p\le x\\ p\equiv a(g)}}\log p-\frac{x}{\varphi(g)}\Big|^2\ll x(\log x)^4+\frac{x^2}{\varphi(g)(\log x)^A}$$

と期待できる(ト)。もしこれが成立するなら 殆どのaについて $P(g,a)\ll g^{1+\varepsilon}$ 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。

(ヘ) B. Rousselet : Inegalités de type Brun-Titchmarsh en moyene, 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).

(ト) 前出 Montgomery の ノート. Chap. 17 参照。
ちなみに 概素数 (高々2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.

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

(リ) $m\sim M$ の記号 $\sim$ は、$M<m\le 2M$ を表す。
また $\mathcal{L}=\log x$ と略記する。

式

q に関する平均を考える。まず篩を用いて(千)素数を自然数の積として表示する。すると(2)の左辺は

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

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

に分解する。(リ) n の係数が[I]では1、[II]ではΛとなることが肝要である。パラメータ 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

$$\sum_{\substack{m\sim M\\ (m,q)=1}} a_m\left(\sum_{\substack{n\sim N\\ mn\equiv a(q)}} 1 - \frac{1}{\varphi(q)}\sum_{\substack{n\sim N\\ (n,q)=1}} 1\right)\ll M\mathscr{L}$$

だから[I]は $\ll QM\mathscr{L}$ でこれが $\ll x\mathscr{L}^{-A}$ となってほしいから $M\ll x^{1-\varepsilon}Q^{-1}$ であればよい。そこで $[1, x^{1-\varepsilon}Q^{-1}]$ を許容区間と呼ぶ。当然〈分解〉⊂〈許容〉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

$$\ll M\mathscr{L}^3\cdot\sum_{q\sim Q}^{*} q\sum_{\substack{m\sim M\\ (m,q)=1}}\left|\sum_{\substack{n\sim N\\ mn\equiv a(q)}}\Lambda(n) - \frac{1}{\varphi(q)}\sum_{\substack{n\sim N\\ (n,q)=1}}\Lambda(n)\right|^2$$

$$= M\mathscr{L}^3(W-2V+U)$$

となる。W, V, U は2乗を直にひらいた結果である。まず、

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

$n\equiv n'(q)$ でなくては m の合同式は解けない。解けるなら、m の個数は自明に $Mq^{-1}+O(1)$ だから

$$W=M\sum_{q\sim Q}^{*}\sum_{\substack{n,n'\sim N\\(nn',q)=1\\ n\equiv n'(q)}}\Lambda(n)\Lambda(n')+O\left(\sum_q q\sum_n \Lambda(n)^2\left(\frac{N}{q}+1\right)\right)$$

$$=M\sum_{q\sim Q}^{*}\sum_{\substack{b(q)\\(b,q)=1}}\left(\sum_{\substack{n\sim N\\ n\equiv b(q)}}\Lambda(n)\right)^2+O(Q(N+Q)N\mathcal{L}^2).$$

同様に

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

すると

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

$Q<N$ なら (1) を用いて上の和を押えられる。結局 [II] は

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

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

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 $Q=X^{\frac{1}{2}-\varepsilon}$ でこ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Kloostermann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

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

となる(ヌ)。これが $[\alpha,\beta]$、$\alpha^2 \leqq \beta$、の形であってほしい。なぜなら $1<M_j<\alpha\ (1\leqq j\leqq n)$ について $M_1M_2\cdots M_n>\beta$ ならば $[\alpha,\beta]$ に落ちるある部分積 $M_{(1)}M_{(2)}\cdots M_{(\ell)}$ 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。$P(g,a)$ 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 $a\neq 0$ を固定したとき 殆どの g について $P(g,a)\ll g^{\frac{32}{17}+\varepsilon}$ である。

(ヌ)前出(ホ)参照。(ル)そうできるなら 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 $\chi \pmod q$ 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

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

と言えるのだが。また(3)の2乗を直接開くなら

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

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

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 q のうち最小のもの、$G(q,k)$、を考える。(ヲ) もちろん q が偶数ならば k も偶数とする。こうして

(ヲ) 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. Turk. 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).

(ル) 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.

$G(g,k)$の問題を 殆どの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

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

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

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

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 $\ll (gx)^{\frac{1}{2}}e^4$ 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$G(g,k)$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kに対して $G(g,k)\ll g^{\frac{14}{13}+\varepsilon}$ となる。

三月三日