$a \pmod p$ の剰余位数の分布について

第 4 回「代数学と計算」研究集会 (東京都立大学)
2001.11.8
知念 宏司 (大阪工業大学 工学部)
村田 玲音 (明治学院大学 経済学部)

1 問題とその背景

自然数 a ($a \neq 1$) をとり, p は奇素数, $p \nmid a$ とする. また $D_a(p)$ を a の $\bmod p$ での剰余位数, つまり $\mathbf{Z}/p\mathbf{Z}^\times$ において a が生成する部分群 $\langle a \rangle$ の位数, そして $I_a(p) := |\mathbf{Z}/p\mathbf{Z}^\times : \langle a \rangle|$ (a の $\bmod p$ での剰余指数) とする. 次の問題を考える:

問 題 1.1 集合

$$Q_a(x; k, l) := \{p \leq x \ ; \ D_a(p) \equiv l \pmod k\} \quad (0 \leq l < k)$$

の自然密度, i.e. $\Delta_a(k,l) := \lim_{x\to\infty} \sharp Q_a(x;k,l)/\pi(x)$ を求めよ ($\pi(x)$: x 以下の素数の個数).

まず, われわれがこのような問題を考えるに到った背景について説明する. 上記の D_a, I_a はともに奇素数全体の集合 P から自然数の集合 $\mathbf{N}$ への写像を与えているが, これらが全射であるか, という問題がある. これに対し, まず D_a は, $\mathbf{N}$ から高々有限個の元を除けば全射であること, すなわち, a によって決まる有限集合 $A(a) \subset \mathbf{N}$ ($A(a) = \emptyset$ もあり得る) が存在して,

$$D_a : P \longrightarrow \mathbf{N} - A(a)$$

が全射となることが多くの研究者によって示されている. I_a については, ある種の Kummer 拡大体 (無限個) に対する一般 Riemann 予想 (以下 GRH) の仮定のもとで, a の square-free part a_1 が $a_1 \not\equiv 1 \pmod 4$ なら

$$\sharp\{p \leq x \ ; \ I_a(p) = n\} \sim C_a^{(n)} \operatorname{li} x \quad (C_a^{(n)} > 0, x \to \infty) \tag{1.1}$$

となることが知られている (Lenstra [?], Murata [?]). とくに $n = 1$ の場合は, いわゆる「原始根に関する Artin の予想」で, Hooley [?] によって示されている. また $\operatorname{li} x = \int_2^x (1/\log t)dt$.

さて,「全射」とは定性的な性質であるが, 定量的性質はどうであろうか. I_a については上の結果 (??) が解答を与えている. しかし D_a の定量的性質はほとんど知られていないと思われる. D_a と I_a には

$$D_a(p)I_a(p) = p - 1 \tag{1.2}$$

という関係があるが, 言わば $\{p-1 \ ; \ p$ は素数 $\}$ の分布の不規則性をほとんど $D_a(p)$ の方が受け継いでいて, 挙動が不規則なため調べにくいという事情があると考えられる. そこでわれわれは, D_a の定量的性質を得るための一つの試みとして, $D_a(p)$ の値を $\bmod k$ で分類することを考えた. 以上が, われわれが問題 ?? を考えた背景である. もし D_a が $\mathbf{N}$ を「均等に」覆うのであれば, 上記 $Q_a(x;k,l)$ の密度はどれもだいたい $1/k$ になると期待される.

一方, 全く別の動機からこの問題を考察した研究者もいる. 1958 年, W. Sierpinski は [?] において次のような問題を考えている: まず 2 つの集合

$$\begin{aligned} A &:= \{p : \text{素数} \ ; \ p|2^n+1 \text{ for some } n \in \mathbf{N}\}, \\ B &:= \{p : \text{素数} \ ; \ p|2^{2n+1}-1 \text{ for some } n \in \mathbf{N}\} \end{aligned}$$

を考える. このとき彼は

$$\begin{aligned} A &= \{p \equiv \pm 3 \pmod 8 \text{ なるすべての素数 } p\} \\ &\quad \cup \{p \equiv 1 \pmod 8 \text{ なる無限個の素数 } p\}, \\ B &= \{p \equiv -1 \pmod 8 \text{ なるすべての素数 } p\} \\ &\quad \cup \{p \equiv 1 \pmod 8 \text{ なる, ある素数 } p\} \end{aligned}$$

となることを示した上で, 次の問題を提起した:

問 題 1.2 集合 B は $p \equiv 1 \pmod 8$ なる素数を無限個含むか.

これに対し, Hasse [?] は, B の解析密度が $7/24$ であることを示した. ところで, 算術級数定理によって $\{p \ ; \ p \equiv s \pmod 8\}$ $(s = \pm 1, \pm 3)$ の密度は $1/4$ であるから, Sierpinski の結果は, B の密度が $1/4$ 以上であることを示している. 一方 $7/24 > 1/4$ より, Hasse の結果は, 集合 B は確かに $p \equiv 1 \pmod 8$ なる素数を無限個含むことを意味する. こうして問題 ?? は解決を見たが, 実は

$$\begin{aligned} A &= \{p \ ; \ D_2(p) \text{ は even}\}, \\ B &= \{p \ ; \ D_2(p) \text{ は odd}\} \end{aligned}$$

であることが初等的な計算によってわかるから (例えば Lagarias [?, p.452]), Sierpinski と Hasse は $Q_2(x; 2, 0)$ と $Q_2(x; 2, 1)$ を考察したことになる (主として解析密度の場合だが). この結果はのちに Hasse [?], Odoni [?] により一般化された. それは次の定理にまとめられる:

定 理 1.3 $a \in \mathbf{N}$, square-free, $a \geq 2$, q: 素数とすると,

$$\sharp Q_a(x; q, 0) = \Delta_a(q, 0) \operatorname{li} x + O\left(\operatorname{li} x \cdot \exp\left(-c\frac{\log\log x}{\log\log\log x}\right)\right) \quad (x \to \infty),$$

ただし, $\Delta_2(2, 0) = 17/24$, $\Delta_a(q, 0) = q/(q^2-1)$ $((a, q) \neq (2, 2))$.

このように, $Q_a(x; k, 0)$ は, 数列に現れる整数を割る素数の密度を調べる問題にも関連があり, 一般の代数体において類似の考察をする (i.e. a を適当な代数的整数とする) ことにより, Fibonacci 数列, Lucas 数列などに対する結果が得られている. この方向に関しては, Lagarias [?], [?], Kohno-Nakahara-Ok [?] およびそれらの文献表を参照.

これらの結果から, $Q_a(x; k, l)$ の密度が $1/k$ づつではないことはわかった.

ところで, ここに紹介した従来の結果は, いずれも $l = 0$ の場合を扱ったものである ($k = 2$ という自明な場合は除く). $l \neq 0$ の場合に $Q_a(x; k, l)$ の密度を求めることは可能だろうか. われわれはそのような場合に対して, 一定の結果を得た. つまり, $a \geq 2$, a は完全 b 乗数でないとする $(b \geq 2)$ とき, 現在までに次のような結果を得ている:

(1) $Q_a(x;4,l)$ の自然密度を決定した ($l=0,1,2,3$). ただし, $l=1,3$ のときは GRH を仮定することが必要 ($l=0,2$ は unconditional).

(2) 奇素数 q, $i\geq 1$ に対し, $Q_a(x;q^i,j)$ $(0\leq j<q^i)$ の自然密度が存在することを証明し, $q|j$ なる j に対して $Q_a(x;q^i,j)$ の自然密度を決定した. ただし, $j\neq 0$ の場合は GRH を仮定することが必要 ($j=0$ は unconditional).

GRH の仮定が必要とはいえ, $l\neq 0$ であるような $Q_a(x;k,l)$ の自然密度が求まったのは, 恐らく初めてのことと思われる.

本稿の目的は, 上記 (1) の結果とその証明の概略を紹介することである (なお, 講演申込時点でのアブストラクトには, (2) の結果を紹介すると書いたが, 当研究集会のシリーズでこの問題を報告するのは初めてであること, (1) はほぼ最終結果といえるところまで解決できていることなどから, (1) を紹介することにした). §2 で主結果を, §3 でその証明の概略を述べ, §4 では数値実験の結果を紹介する. また (2) の結果に関しては, §5 で簡単に触れることにする.

最後に, このあと登場する記号をまとめておく. 整数 k に対し, ζ_k は 1 の原始 k 乗根, $\varphi(k)$ と $\mu(k)$ はそれぞれ Euler の関数と Möbius の関数を表す. また, K を有限次代数体, $\mathfrak{p}$ を K の素イデアルとし, L/K を有限次 Galois 拡大とする. このとき Frobenius 記号 $(\mathfrak{p},L/K)$ を

$$(\mathfrak{p},L/K)=\left\{\sigma\in\mathrm{Gal}(L/K)\ ;\ \begin{array}{l}\mathfrak{p}\text{ の上の }L\text{ のある素イデアル }\mathfrak{q}\text{ に対して }\mathfrak{q}^\sigma=\mathfrak{q},\\ L\text{ の任意の整数 }\alpha\text{ に対して }\alpha^\sigma\equiv\alpha^{N\mathfrak{p}}\pmod{\mathfrak{q}}\end{array}\right\}$$

で定義する. ただし, $N\mathfrak{p}$ は $\mathfrak{p}$ の絶対ノルム. なお, この Frobenius 記号の記法は Lenstra [?] による.

2 主 結 果

今回の主結果は次の通り:

定 理 2.1 $a\in\mathbf{N}$, $a\geq 2$ とし, a は完全 b 乗数 ($b\geq 2$) ではないとする. $a=a_1a_2^2$ (a_1: square free) とおく. すると GRH のもと,

$$\sharp Q_a(x;4,l)=\Delta_a(4,l)\,\mathrm{li}\,x+O\left(\frac{x}{\log x\log\log x}\right)\quad(x\to\infty)$$

が成立し, 自然密度 $\Delta_a(4,l)$ $(l=1,3)$ は次の式で与えられる:

(I) $a_1\equiv 1,3\pmod 4$ ならば

$$\Delta_a(4,1)=\Delta_a(4,3)=\frac{1}{6}.$$

(II) $a_1\equiv 2\pmod 4$ のとき, まず定数 C を次のように定義する:

$$C:=\prod_{\substack{p\equiv 3\pmod 4\\ p:\text{prime}}}\left(1-\frac{2p}{(p^2+1)(p-1)}\right)\quad(\approx 0.64365).$$

(i) $a_1 = 2$ のとき,

$$\Delta_a(4,1) = \frac{7}{48} - \frac{C}{8}, \quad \Delta_a(4,3) = \frac{7}{48} + \frac{C}{8}.$$

(ii) $a_1 > 2$ のとき, $a_1 = 2a_1'$ (a_1': odd) とおくと, a_1' の少なくとも 1 つの素因数 p が $p \equiv 1 \pmod 4$ を満たすなら

$$\Delta_a(4,1) = \Delta_a(4,3) = \frac{1}{6},$$

a_1' のすべての素因数 p が $p \equiv 3 \pmod 4$ を満たすなら

$$\begin{aligned} \Delta_a(4,1) &= \frac{1}{6} \pm \frac{C}{8} \prod_{p|a_1'} \frac{-2p}{p^3 - p^2 - p - 1}, \\ \Delta_a(4,3) &= \frac{1}{6} \mp \frac{C}{8} \prod_{p|a_1'} \frac{-2p}{p^3 - p^2 - p - 1}, \end{aligned}$$

ただし $\Delta_a(4,1)$ における複号は, $a_1' \equiv 3 \pmod 4$ のとき $+$, $a_1' \equiv 1 \pmod 4$ のとき $-$, $\Delta_a(4,3)$ における複号はこれと同順とする.

注 意. (1) $\Delta_a(4,0)$, $\Delta_a(4,2)$ は unconditional に求めることができ, 証明もいくぶん易しい. その場合の密度は,

$$\begin{aligned} a_1 = 2 &\implies \Delta_a(4,0) = \frac{5}{12}, \ \Delta_a(4,2) = \frac{7}{24}, \\ a_1 \neq 2 &\implies \Delta_a(4,0) = \Delta_a(4,2) = \frac{1}{3}. \end{aligned}$$

(2) この定理により, 密度 $\Delta_a(4,1)$, $\Delta_a(4,3)$ についてつねに

$$\Delta_a(4,1) \leq \Delta_a(4,3)$$

が成立していることがわかる. これは興味深い現象である.

(3) この定理の特別な場合 ($a \geq 3$, a は square-free, $a \equiv 1 \pmod 4$ としたときの $Q_a(x;4,l)$, $l = 1, 3$ の密度を求めること) については [?] で発表した.

3 証明の概略

この節では, 定理 ?? の証明を述べる.

一般に, a を固定して p を動かしたときの $D_a(p)$ の動きはきわめて不規則であるが, これを $I_a(p)$ の言葉で書き換えると, 代数体に関する量を用いて, ある程度挙動を知ることができる. D_a から I_a への移行は, 一種の sieve method による. まず, $n, s, t \in \mathbf{N}$ に対して素数集合 $N_a(x; n; s \pmod t)$ を

$$N_a(x; n; s \pmod t) = \{p \leq x \ ; \ I_a(p) = n, \ p \equiv s \pmod t\} \tag{3.1}$$

によって定義する. すると, 次が成り立つ:

補 題 3.1 (i)

$$\begin{aligned}\sharp Q_a(x;4,1) &= \sum_{f\geq 1}\sum_{l\geq 0}\sharp N_a(x;(4l+1)\cdot 2^f;1+2^f \pmod{2^{f+2}}) \\ &+ \sum_{f\geq 1}\sum_{l\geq 0}\sharp N_a(x;(4l+3)\cdot 2^f;1+3\cdot 2^f \pmod{2^{f+2}}),\end{aligned} \tag{3.2}$$

(ii)

$$\begin{aligned}\sharp Q_a(x;4,3) &= \sum_{f\geq 1}\sum_{l\geq 0}\sharp N_a(x;(4l+3)\cdot 2^f;1+2^f \pmod{2^{f+2}}) \\ &+ \sum_{f\geq 1}\sum_{l\geq 0}\sharp N_a(x;(4l+1)\cdot 2^f;1+3\cdot 2^f \pmod{2^{f+2}}).\end{aligned} \tag{3.3}$$

これは全く初等的な計算により証明できる. 最初の目標は, この補題に現れる (??) の形の素数集合の自然密度を剰余項付きで求めることである. この素数集合は, (??) 左辺の

$$N_a(x;n) := \{p \leq x \ ; \ I_a(p) = n\}$$

に条件 $p \equiv s \pmod t$ を付け加えたものである. §1 で述べた通り, $N_a(x;n)$ の自然密度は Murata [?] で計算されている. 一方, 条件 $p \equiv s \pmod t$ は円分体 $\mathbf{Q}(\zeta_t)$ での p の分解を考えることにより扱うことができる:

補 題 3.2 $(s,t)=1$ とし, $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_t)/\mathbf{Q})$ を $\sigma : \zeta_t \mapsto \zeta_t^s$ で定まるものとすると,

$$p \equiv s \pmod t \ \Leftrightarrow \ (p, \mathbf{Q}(\zeta_t)/\mathbf{Q}) = \{\sigma\}.$$

したがって, $N_a(x;n;s \pmod t)$ の密度は基本的に [?] と同様の議論で求まる ([?] で key となる代数体の円分拡大を考える) が, 異なる点は, 上の体で完全分解しない素数を数えるために Chebotarev の密度定理を使うことである. そして, GRH を仮定する必要があるのは, Chebotarev の密度定理においてである:

定 理 3.3 (Chebotarev density theorem) L/K: Galois 拡大, C を $G = \mathrm{Gal}(L/K)$ の共役類, d_L : L の判別式, $n_L = [L:\mathbf{Q}]$ とし,

$$\pi_C(x, L/K) := \{\mathfrak{p} : K \text{ の素イデアル}, L \text{ で不分岐}, (\mathfrak{p}, L/K) = C, N\mathfrak{p} \leq x\}$$

とすると, GRH のもとで

$$\pi_C(x, L/K) = \frac{\sharp C}{\sharp G}\operatorname{li} x + O\left(\frac{\sharp C}{\sharp G}\sqrt{x}\log(d_L x^{n_L}) + \log d_L\right) \quad (x \to \infty).$$

証 明. Lagarias-Odlyzko [?, Theorem 1.1]. ∎

これらを用いると, GRH のもとで $N_a(x;n;s \pmod t)$ の評価ができる. その結果を述べるために, いくつかの記号を準備する. $r = 1, 3$, $l \geq 0$, $f \geq 1$ に対して

$$k = (4l+r)\cdot 2^f, \quad k_0 = \prod_{\substack{p\mid k \\ p:\text{prime}}} p \quad (k \text{ の core と呼ばれる}),$$

$$G_{k,n,d} = \mathbf{Q}(a^{1/kn}, \zeta_{kd}, \zeta_n), \quad \tilde{G}_{k,n,d} = G_{k,n,d}(\zeta_{2^{f+2}}),$$

そして, $c_r(k,n,d)$ を次のように定める. まず $\sigma_r \in \mathrm{Gal}(\mathbf{Q}(\zeta_{2^{f+2}})/\mathbf{Q})$ を $\sigma_r : \zeta_{2^{f+2}} \mapsto \zeta_{2^{f+2}}^{1+r\cdot 2^f}$ で定まるものとし, $\sigma_r^*|_{\mathbf{Q}(\zeta_{2^{f+2}})} = \sigma_r$ を満たす $\sigma_r^* \in \mathrm{Gal}(\tilde{G}_{k,n,d}/G_{k,n,d})$ を考える. このような σ_r^* はつねに存在するとは限らないが, 存在すればただ 1 つであることが証明できる. そこで $c_r(k,n,d)$ を

$$c_r(k,n,d) = \begin{cases} 1, & \sigma_r^* \text{ が存在するとき,} \\ 0, & \sigma_r^* \text{ が存在しないとき} \end{cases}$$

によって定める. すると

命 題 3.4 GRH の仮定のもとで

$$\sharp N_a(x;k;1+r\cdot 2^f \pmod{2^{f+2}}) = \delta_{f,l,r} \operatorname{li} x + O\left(\frac{x}{\log^2 x}(\log\log x)^4\right),$$

$$\delta_{f,l,r} = \frac{k_0}{\varphi(k_0)} \sum_{d|k_0} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n) c_r(k,n,d)}{[\tilde{G}_{n,k,d} : \mathbf{Q}]} \tag{3.4}$$

が成立する. n に関する和は絶対収束する.

注 意. ただし, $N_a(x;k;s \pmod t)$ の密度そのもの, つまり漸近式の主要項係数のみであれば, Lenstra によってすでに求められていた ([?] の (2.15) 式および p.217 参照). しかし Lenstra [?] では基本的に解析密度の形で議論が進められており, 自然密度の場合の剰余項を与えることは本質的に不可能な証明となっている. したがって, われわれの命題 ?? は決して Lenstra の自明な corollary ではない.

以上の結果を用いて, 少々複雑な剰余項の処理を経ると, 次の結果を得る:

定 理 3.5 $k = (4l+1)\cdot 2^f$, $k' = (4l+3)\cdot 2^f$, k, k' の core をそれぞれ k_0, k_0' とする. GRH のもとで, $r = 1, 3$ に対し,

$$Q_a(x;4,r) = \Delta_a(4,r) \operatorname{li} x + O\left(\frac{x}{\log x \log\log x}\right),$$

$$\begin{aligned} \Delta_a(4,1) &= \sum_{f\geq 1}\sum_{l\geq 0} \frac{k_0}{\varphi(k_0)} \sum_{d|k_0} \frac{\mu(d)}{d} \sum_n{}' \frac{\mu(n) c_1(k,n,d)}{[\tilde{G}_{k,n,d} : \mathbf{Q}]} \\ &+ \sum_{f\geq 1}\sum_{l\geq 0} \frac{k_0'}{\varphi(k_0')} \sum_{d|k_0'} \frac{\mu(d)}{d} \sum_n{}' \frac{\mu(n) c_3(k',n,d)}{[\tilde{G}_{k',n,d} : \mathbf{Q}]}, \end{aligned} \tag{3.5}$$

$$\begin{aligned} \Delta_a(4,3) &= \sum_{f\geq 1}\sum_{l\geq 0} \frac{k_0}{\varphi(k_0)} \sum_{d|k_0} \frac{\mu(d)}{d} \sum_n{}' \frac{\mu(n) c_3(k,n,d)}{[\tilde{G}_{k,n,d} : \mathbf{Q}]} \\ &+ \sum_{f\geq 1}\sum_{l\geq 0} \frac{k_0'}{\varphi(k_0')} \sum_{d|k_0'} \frac{\mu(d)}{d} \sum_n{}' \frac{\mu(n) c_1(k',n,d)}{[\tilde{G}_{k',n,d} : \mathbf{Q}]}. \end{aligned} \tag{3.6}$$

ただし, $\sum_n{}' = \sum_{n\geq 1, n:\text{square free}}$ とする.

ここまでの結果について, より詳しいことは, [?] をご参照いただきたい.

主結果である定理 ?? を得るには, 係数 $c_r(k,n,d)$ を決定し, 級数 (??), (??) を計算しなければならない. 基本的には無限和を無限積 (Euler 積) に変形していくのだが, かなり複雑なので詳細は省略する.

4 数値実験

自然数 a $(a \neq 1)$ を固定し, $Q_a(x;4,l)$ $(l=0,1,2,3)$ の密度, すなわち $\sharp Q_a(x;4,l)/\pi(x)$ を計算した . x としては 10^7 まで取り, 10^3 から始めて 10 倍ごとに密度を出してある.

計算機環境

プログラムは C 言語で書き, OS は Linux (Kernel 2.0.36), コンパイラは GCC, CPU は Pentium 233MHz. 10^7 以下の素数は 664579 個あり, それらに対する位数 $D_a(p)$ の計算に要した時間は各 a につき約 7 時間 10 分 ~ 30 分であった.

現在のところ, a, p が与えられたときに $D_a(p)$ を高速に計算するアルゴリズムは知られていないと思われる. そこで数値実験では, $p-1$ を素因数分解してその約数をすべて求め, 小さい約数から順に, それが $D_a(p)$ であるかどうかを調べる, という方法を取っている. 一連の計算のうち最も時間を要するのはこの素因数分解であるため, $p-1$ の約数の一覧表を作っておけば劇的に速くできるであろう. ただその場合, 一覧表のファイルは相当大きくなることが予想されるため, まだ試していない. かわりに, $p-1$ がどのような素因数分解のパターンを持つかを, ある程度記録した補助ファイルを作って利用しており, それによって若干速くなることが観察されている. 例えば, $p-1 = 2 \times$ (素数) となっている p に印をつける, といったファイルを用意すると, 計算時間は約 5%速くなる. 一方, $p-1$ がそのような素因数分解をもつ素数 p は, 10^7 までの素数のうち, やはり約 5%である. このような補助ファイルの作り方はさまざま考えられるはずで, ファイルサイズを抑えつつ効率のよい補助ファイルを作ることも興味深い問題であろう. また, a を変えるたびに $p-1$ の素因数分解を新たにやり直すのでは効率が悪い. そこで, 新しい a に対する計算を行なうごとに, よりよい補助ファイルに書きかえるような「学習型」プログラムを作るのもおもしろいだろう.

以下, 定理 ?? に沿って具体的な数値計算例を見ていこう. 記号を復習すると, a_1 は a の square-free part, a_1 が偶数かつ $a_1 > 2$ の場合は a_1 の奇数部分を a_1' とする (i.e. $a_1 = 2a_1'$).

(I) $a_1 \equiv 1, 3 \pmod 4$ のとき

このときの密度の理論値は, $\Delta_a(4,1) = \Delta_a(4,3) = 1/6$ (GRH のもと), $\Delta_a(4,0) = \Delta_a(4,2) = 1/3$ (unconditional) である. 例として $a = 5$, $33(= 3 \cdot 11)$, $45(= 5 \cdot 3^2)$, 11, $55(= 5 \cdot 11)$, $75(= 3 \cdot 5^2)$ を取った:

$a = 5$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.319277	0.156627	0.349398	0.174699
10^4	0.327628	0.167074	0.340668	0.164629
10^5	0.334619	0.167049	0.333055	0.165276
10^6	0.333227	0.167155	0.332934	0.166684
10^7	0.333320	0.166771	0.333099	0.166810

$a = 33$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.309091	0.151515	0.369697	0.169697
10^4	0.336868	0.154160	0.336052	0.172920
10^5	0.332569	0.165815	0.336219	0.165398
10^6	0.333015	0.166890	0.332900	0.167195
10^7	0.333170	0.166991	0.333565	0.166274

$a = 45$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.321212	0.127273	0.363636	0.187879
10^4	0.331974	0.168842	0.328711	0.170473
10^5	0.333299	0.169778	0.332986	0.163938
10^6	0.333473	0.166749	0.333231	0.166546
10^7	0.333322	0.167141	0.333212	0.166324

$a = 11$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.355422	0.138554	0.349398	0.156627
10^4	0.327628	0.172779	0.327628	0.171964
10^5	0.333472	0.166006	0.333681	0.166840
10^6	0.333253	0.166289	0.333749	0.166709
10^7	0.333316	0.166531	0.333386	0.166766

$a = 55$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.315152	0.169697	0.369697	0.145455
10^4	0.335237	0.172104	0.339315	0.153344
10^5	0.330900	0.169882	0.332881	0.166336
10^6	0.331868	0.166571	0.334658	0.166902
10^7	0.333175	0.166875	0.333259	0.166691

$a = 75$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.327273	0.169697	0.321212	0.181818
10^4	0.335237	0.163132	0.339315	0.162316
10^5	0.335280	0.168944	0.332777	0.162999
10^6	0.332938	0.166826	0.333321	0.166915
10^7	0.333337	0.166372	0.333395	0.166896

(II) $a_1 \equiv 2 \pmod 4$ **のとき**

(i) $a_1 = 2$ **のとき**

このときの密度の理論値は,

$$\Delta_a(4,1) = \frac{7}{48} - \frac{C}{8} \approx 0.06538,$$

(GRH **のもと**)

$$\Delta_a(4,3) = \frac{7}{48} + \frac{C}{8} \approx 0.22629,$$

$$\Delta_a(4,0) = \frac{5}{12} \approx 0.41667,$$

(unconditional)

$$\Delta_a(4,2) = \frac{7}{24} \approx 0.29167$$

である. **例として**, $a = 2,\ 50(= 2 \cdot 5^2)$ **を取った**:

$a = 2$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.425150	0.065868	0.275449	0.233533
10^4	0.418567	0.064332	0.296417	0.220684
10^5	0.417266	0.066208	0.291106	0.225420
10^6	0.416118	0.065506	0.291553	0.226824
10^7	0.416687	0.065425	0.291481	0.226407

$a = 50$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.415663	0.036145	0.295181	0.253012
10^4	0.409943	0.068460	0.290139	0.231459
10^5	0.416684	0.065172	0.292284	0.225860
10^6	0.416569	0.065889	0.291633	0.225910
10^7	0.416719	0.065351	0.291584	0.226345

(ii-a) $a_1 > 2$**,** a_1' **の少なくとも 1 つの素因数が** $\equiv 1 \pmod 4$ **のとき**

このときの密度の理論値は, $\Delta_a(4,1) = \Delta_a(4,3) = 1/6$ (GRH **のもと**), $\Delta_a(4,0) = \Delta_a(4,2) = 1/3$ (unconditional) **である**. **例として** $a = 10(= 2 \cdot 5),\ 30(= 2 \cdot 3 \cdot 5),\ 210(= 2 \cdot 3 \cdot 5 \cdot 7)$ **を取った**:

$a = 10$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.325301	0.174699	0.331325	0.168675
10^4	0.329258	0.169519	0.338223	0.162999
10^5	0.334202	0.167675	0.332534	0.165589
10^6	0.332616	0.167588	0.333992	0.165805
10^7	0.333346	0.166644	0.333487	0.166522

$a = 30$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.327273	0.169697	0.296970	0.206061
10^4	0.336868	0.170473	0.327896	0.164763
10^5	0.331734	0.169256	0.336531	0.162478
10^6	0.333117	0.166227	0.333563	0.167093
10^7	0.333255	0.166354	0.333401	0.166991

$a = 210$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.286585	0.158537	0.384146	0.170732
10^4	0.320816	0.160816	0.341224	0.177143
10^5	0.330935	0.169691	0.331665	0.167710
10^6	0.333936	0.166013	0.333210	0.166841
10^7	0.333555	0.166878	0.333078	0.166490

(ii-b) $a_1 > 2$, a_1' のどの素因数も $\equiv 3 \pmod 4$ のとき

このときの密度の理論値は, a の値に応じて変化する. 例として $a = 6(= 2\cdot 3)$, $14(= 2\cdot 7)$, $42(= 2\cdot 3\cdot 7)$ を取る. $\Delta_a(4,1)$, $\Delta_a(4,3)$ を定理 ?? によって計算すると

$$\begin{aligned}
\Delta_6(4,1) &= \frac{1}{6} - \frac{3C}{56} \approx 0.13219,\\
\Delta_6(4,3) &= \frac{1}{6} + \frac{3C}{56} \approx 0.20115,\\
\Delta_{14}(4,1) &= \frac{1}{6} - \frac{7C}{1144} \approx 0.16273,\\
\Delta_{14}(4,3) &= \frac{1}{6} + \frac{7C}{1144} \approx 0.17061,\\
\Delta_{42}(4,1) &= \frac{1}{6} - \frac{3C}{1144} \approx 0.16498,\\
\Delta_{42}(4,3) &= \frac{1}{6} + \frac{3C}{1144} \approx 0.16835
\end{aligned}$$

(GRH のもと), また, いずれの場合も $\Delta_a(4,0) = \Delta_a(4,2) = 1/3$ (unconditional) である:

$a = 6$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.331325	0.126506	0.325301	0.216867
10^4	0.334963	0.133659	0.333333	0.198044
10^5	0.333785	0.133577	0.332847	0.199791
10^6	0.333151	0.132249	0.333507	0.201093
10^7	0.333331	0.132179	0.333019	0.201471

$a = 14$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.319277	0.168675	0.343373	0.168675
10^4	0.337408	0.163814	0.334963	0.163814
10^5	0.332951	0.164338	0.332325	0.170386
10^6	0.333278	0.163384	0.332157	0.171181
10^7	0.333266	0.162875	0.333570	0.170289

$a = 42$

x	$l=0$	$l=1$	$l=2$	$l=3$
10^3	0.309091	0.169697	0.327273	0.193939
10^4	0.327080	0.159869	0.338499	0.174551
10^5	0.332569	0.165189	0.335697	0.166545
10^6	0.333690	0.165870	0.334034	0.166406
10^7	0.333566	0.165129	0.333027	0.168277

5 附記 — $Q_a(x; q^i, j)$ の場合

最後に, q: 奇素数, $i \geq 1$ のときの $Q_a(x; q^i, j)$ について, 現在までにわかっていることを簡単に述べる. まずいくつかの記号を導入する. j は $1 \leq j \leq q^i - 1$ を満たすとし, これを $j = hq^e$ $(q \nmid h,\ 0 \leq e \leq i-1)$ と表す. この h に対し $h\overline{h} \equiv 1 \pmod{q^{i-e}}$ とし, $1 \leq r < q^i$, $(q,r) = 1$ なる r, $f \geq e$, $l \geq 0$ に対して

$$k = \{(\overline{h}r) \pmod{q^{i-e}} + l \cdot q^{i-e}\}q^{f-e}$$

とおく. この k に対して, k の core k_0, 体 $G_{k,n,d}$, $\tilde{G}_{k,n,d}$, 係数 $c_r(k,n,d)$ を §3 と同様に, 次のように定める:

$$G_{k,n,d} = \mathbf{Q}(a^{1/kn}, \zeta_{kd}, \zeta_n), \quad \tilde{G}_{k,n,d} = G_{k,n,d}(\zeta_{q^{f+2}}).$$

また $\sigma_r \in \mathrm{Gal}(\mathbf{Q}(\zeta_{q^{f+2}})/\mathbf{Q})$ を $\sigma_r : \zeta_{q^{f+2}} \mapsto \zeta_{q^{f+2}}^{1+rq^f}$ で定まるものとし, $\sigma_r^*|_{\mathbf{Q}(\zeta_{q^{f+2}})} = \sigma_r$ を満たす $\sigma_r^* \in \mathrm{Gal}(\tilde{G}_{k,n,d}/G_{k,n,d})$ を考える. そして

$$c_r(k,n,d) = \begin{cases} 1, & \sigma_r^* \text{ が存在するとき}, \\ 0, & \sigma_r^* \text{ が存在しないとき} \end{cases}$$

とする. このような σ_r^* は, 存在すればただ 1 つであることは §3 と同様である. すると, 定理 ?? と同様にして, 次の定理が証明される:

定 理 5.1 $a \geq 2$, a は完全 b 乗数でないとする $(b \geq 2)$ と, GRH の仮定のもと,

$$\sharp Q_a(x; q^i, j) = \Delta_a(q^i, j) \operatorname{li} x + O\left(\frac{x}{\log x \log\log x}\right),$$

$$\Delta_a(q^i, j) = \sum_{\substack{1 \leq r < q^i \\ (q,r)=1}} \sum_{f \geq e} \sum_{l \geq 0} \frac{k_0}{\varphi(k_0)} \sum_{d|k_0} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n) c_r(k,n,d)}{[\tilde{G}_{k,n,d} : \mathbf{Q}]}.$$

この定理に現れる級数 $\Delta_a(q^i, j)$ を簡単な式で表すことはまだできていないが, 係数 $c_r(k,n,d)$ の決定はすべて終わっている. その計算にはかなり複雑な場合分けが必要なのでここでは述べないが, その結果を用いると, $q|j$ であるような $\Delta_a(q^i, j)$ は, すべて級数として等しいことが示される. これと unconditional にわかる $Q_a(x; q^i, 0)$ の密度

$$\Delta_a(q^i, 0) = \frac{1}{q^{i-2}(q^2-1)} \quad (i \geq 1)$$

を合せることで, 次のことが証明される:

定 理 5.2 GRH のもと, $i \geq 1$, $q|j$ ならば,

$$\Delta_a(q^i, j) = \frac{1}{q^{i-2}(q^2-1)} \quad (i \geq 1).$$

注 意. (1) 結局, 定理 ?? は $j = 0$ の場合も含んでいることになる (ただし, $j = 0$ のとき GRH は不要).
(2) 定理 ?? は, $q = 2$ の場合も成立することがわかっている. また $q = 2$ の場合の $c_r(k,n,d)$ もすべて決定できている.

参考文献

[1] 知念 宏司, 村田 玲音 : $a \pmod p$ の剰余位数の分布について, 数理解析研究所講究録 1219 『解析数論の展望と諸問題』(2001 年 7 月), 245-255.

[2] Hasse, H. : Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteibarer Ordnung mod p ist, Math. Ann. **162** (1965), 74-76.

[3] _____ : Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod p ist, Math. Ann. **166** (1966), 19-23.

[4] Hooley, C. : On Artin's conjecture, J. Reine Angew. Math. **225** (1967), 209-220.

[5] Kohno, Y., Nakahara, T. and Ok, B.-M.: On a density of primes dividing the generalized Fibonacci numbers, 数理解析研究所講究録 1060 『数論とその応用』(1998 年 8 月), 172-175.

[6] Lagarias, J. C. : The set of primes dividing the Lucas numbers has density 2/3, Pacific J. Math. **118** (1985), 449-461.

[7] _____: Errata to the set of primes dividing the Lucas numbers has density 2/3, ibid. **162-2** (1994), 393-396.

[8] Lagarias, J. C. and Odlyzko, A. M. : Effective versions of the Chebotarev density theorem, in *Algebraic Number Fields (Durham, 1975)*, 409-464, Academic Press, London, 1977.

[9] Lenstra Jr., H. W. : On Artin's conjecture and Euclid's algorithm in global fields, Invent. Math. **42** (1977), 201-224.

[10] Murata, L. : A problem analogous to Artin's conjecture for primitive roots and its applications, Arch. Math. **57** (1991), 555-565.

[11] Odoni, R. W. K. : A conjecture of Krishnamurthy on decimal periods and some allied problems, J. Number Theory **13** (1981), 303-319.

[12] Sierpinski, W. : Sur une décomposition des nombre premiers en deux classes, Collect. Math. **10** (1958), 81-83.