剰余位数の分布の一性質について　Ⅱ

村田　玲音
石井　　坦

これは，産業経済研究所　共同研究 『整数論と暗号理論に関する共同研究』の報告記事である。研究期間は二年で，一年目終了時に中間報告を書いた（研究所年報18号，文献[10]）。本記事では，二年目の成果およびこの二年で得られた結果の概観をしたい。

今回の研究はあくまでも解析整数論的なものであるが，現在の『公開鍵暗号』特に『RSA 暗号』とよばれるものは，整数を法とする剰余位数と深いかかわりがある。そのため，我々は『代数学と計算』シンポジウム（2001年秋，於都立大学）―――この集会では計算量の理論や暗号に関する講演が多い―――などで結果を発表してきた。ただ，今回の結果が暗号に直接応用をもつといった状況ではないように思う。

１．はじめに

問題の背景については『中間報告』にかなり詳しく記したのでここでは省略する。

まず，引き続いて使う記号を再録しておきたい。

p は常に奇素数を表わすものとする。p で割れない自然数 a に対し，

$$I_a(p) = [(\mathbb{Z}/p\mathbb{Z})^* : <a(\mathrm{mod}\, p)>],$$

$$D_a(p) = \#\, <a(\mathrm{mod}\, p)>,$$

によって，a の剰余指数，剰余位数を定義する。我々の問題は，剰余位数 $D_a(p)$ を更に t を法とする剰余類によって分類し，その分布状態を調べようというものであった。つまり，任意の剰余類 $u\,(\mathrm{mod}\, t)$ をとって素数の部分集合

$$Q_a(x\,;u\,(\mathrm{mod}\, t)) = \{\, p \leq x;\, D_a(p) \equiv u\,(\mathrm{mod}\, t)\}$$

を考え，これの自然密度を求めるのが目的である。そして，前回の『中間報告』では，t として特に 4 をとったとき，かなり一般的な自然数 a に対してこの密度が求まることを報告した（定理４）。

今年度に得られた主な改良点は次の３点である。

① 法 t をかなり一般的にすることができた。

② a として，一般の有理数（負も許す）まで考察できるようになった。

③ $Q_a(x;u\,(\mathrm{mod}\,t))$ を更に細分化して考察した。

本研究は大阪工業大学の知念宏司氏との共同研究である。

これは報告記事なので，証明は載せていない。興味ある方は，準備中の本論文（[1][2]あるいは[3]，[4]）等を参照していただきたい。また，我々の結果はかなり一般的な t に対して得られているのだが，ここでは『中間報告』との比較の意味もあるので，$t=4$の場合を中心にして結果を略述していきたい。

2．今回の結果

今後は a として有理数を考えるので，$a=a_1/a_2$を a の既約分数表示とする。積 a_1a_2が p で割れなければ，上と同じく，a の剰余位数や剰余指数を定義することができる。そして a は完全 h 乗数であるとする（$a=a'^h$ と書ける最大の h のこと）。我々の結果は h についても一般化してあるのだが，結論がさらに煩雑になるので，この記事ではつねに h=1としておく。

$K_{r,s}$ によって，代数体$\mathbb{Q}(\zeta_r, a^{1/s})$ を表わす。$\zeta_r=\exp(1/2\,\pi r\sqrt{-1})$ の意味である。また，$[K:\mathbb{Q}]$によって体 K の拡大次数を表わす。

ここで新たに次の記号を導入する。これは上記の $Q_a(x;u\,(\mathrm{mod}\,t))$ を更に細分したものである。

$$R_a(x;l\,(\mathrm{mod}\,m);u\,(\mathrm{mod}\,t))=\{p\in Q_a(x;u\,(\mathrm{mod}\,t));p\equiv l\,(\mathrm{mod}\,m)\}$$

これについて，次の定理が成り立つ。s は任意の自然数である。

定理 1　（$p\equiv1\,(\mathrm{mod}\,4)$ なる素数に対する定理）

(1)　$j=0$ または 2 のとき，

$$R_a(x;1\,(\mathrm{mod}\,2^s);j\,(\mathrm{mod}\,4))=\delta_a(1,2^s;j,4)\frac{x}{\log x}+O\left(\frac{x\log\log x}{\log^2 x}\right)$$

ここで

$$\delta_a(1,2^s;0,4)=2^{1-s}-\sum_{r\geq S}\left\{\frac{1}{[K_{2^r,\,2^{r-1}}:\mathbb{Q}]}-\frac{1}{[K_{2^{r+1},\,2^{r-1}}:\mathbb{Q}]}\right\},$$

$$\delta_a(1,2^s;2,4)=\sum_{r\geq S}\left\{\frac{1}{[K_{2^r,\,2^{r-1}}:\mathbb{Q}]}-\frac{1}{[K_{2^{r+1},\,2^{r-1}}:\mathbb{Q}]}-\frac{1}{[K_{2^r,\,2^r}:\mathbb{Q}]}+\frac{1}{[K_{2^{r+1},\,2^r}:\mathbb{Q}]}\right\}$$

(2)　$j=1$ または 3 のとき。一般リーマン予想を仮定する。

$$R_a(x;1\,(\mathrm{mod}\,2^s);j\,(\mathrm{mod}\,4))=\frac{1}{2}\delta_a(1,2^s;1,2)\frac{x}{\log x}+O\left(\log|a_1a_2|\frac{x}{(\log x)^{3/2}}\right)$$

ここで

$$\delta_a(1,2^s;1,2)=\sum_{r\geq S}\left\{\frac{1}{[K_{2^r},{}_{2^r}:\mathbb{Q}]}-\frac{1}{[K_{2^{r+1}},{}_{2^r}:\mathbb{Q}]}\right\}.$$

$p\equiv 3\pmod 4$ なる素数に対しても同様な結果が得られるが，それには次の記号が必要である。法 4 の乗法群の Dirichlet 指標のうち，principal でない方を ψ とし，これを用いて次の数論的関数を定義する。μ は Möbius の関数である。

$$h_\psi(v)=\sum_{d|v}\mu(d)\psi\left(\frac{v}{d}\right)$$

定理２　（$p\equiv 3\pmod 4$ なる素数に対する定理――詳細は文献[12]を参照）

(1)　$R_a(x;3\pmod 4;0\pmod 4)=0$

$R_a(x;3\pmod 4;2\pmod 4)=\#\{p\leqslant x;p\equiv 3\pmod 4,\ \psi(p)=-1\}$

(2)　$j=1$ または 3 のとき。一般リーマン予想を仮定する。

$$R_a(x;3\pmod 4;j\pmod 4)=\frac{1}{2}\#\{p\leqslant x;p\equiv 3\pmod 4,\ \psi(p)=1\}$$

$$+(-1)^{\frac{j-1}{2}}\frac{1}{4}\Delta_a\frac{x}{\log x}+O\left(\log|a_1a_2|\frac{x}{(\log x)^{3/2}}\right)$$

ただし

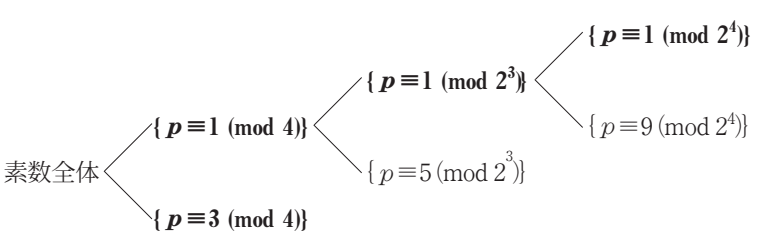
$$\Delta_a=\sum_{\substack{\sqrt{-2}\in K_{2v,2v}\\ v:\text{odd}}}\frac{h_\psi(v)}{[K_{2v},{}_{2v}:\mathbb{Q}]}-\sum_{\substack{\sqrt{2}\in K_{2v,2v}\\ v:\text{odd}}}\frac{h_\psi(v)}{[K_{2v},{}_{2v}:\mathbb{Q}]}$$

上の二つの定理の要点は，

①　すべての場合に自然密度の存在が証明されている。ただし場合によっては一般リーマン予想が必要になる。なお，文献［７］も参照。

②　定理１では，$j=1,3$ の場合の式が共通であり，その自然密度を表わす式には拡大次数しか出てきていない。つまり j による特殊性がないのである。これに対して，定理２の $j=1,3$ の場合，Δ_a を含む部分が j によって変化するため，密度が違っていることが読み取れる。$Q_a(x;u\pmod t)$ を更に細分して $R_a(x;l\pmod m,u\pmod t)$ を考察したのは，こうした現象が明らかになるからである（モレー氏の注意による）。

なお，定理１，定理２では素数全体を次のように分割して結果が述べてある：



そして太文字にした集合の密度だけが定理では述べられていた。しかし差をとってやれば，他の様々な集合の密度も求めることができる。たとえば，

$$R_a(x;9\pmod{2^4};j\pmod 4)$$
$$=R_a(x;1\pmod{2^3};j\pmod 4)-(R_a(x;1\pmod{2^4};j\pmod 4))$$

など。

さて，上の二つの定理は自然密度を体の拡大次数などによって書き表しているだけなので，実際に密度がどのくらいなのか知ろうと思ったら，級数に現われた拡大次数などを正確に求めておかなくてはならない。一般的に言って，拡大体の次数計算はそんなに難しくはない（$j=0,2$ の場合は拡大次数の計算だけで済むので，その点でも幾分易しい）。これに対し，$p\equiv 3\pmod 4$ の場合に現われた Δ_a の計算はかなり厄介である。

途中の計算は省略して，結果のみ述べると次のようになる。

なお，以下では D は二次体 $\mathbb{Q}(\sqrt{a_0})$ の判別式を表わすものとする（a_0 は a の square free part）。また $\mathrm{sgn}(a)$ は単に a の符号を表す。

定理３　一般リーマン予想を仮定する。s は今まで通り，任意の自然数である。

D が２のべき乗でない場合，われわれの求めていた密度は次のようになる。

$$\delta_a(1,2^s;j,4)=\begin{cases}2^{1-s}-\dfrac{2}{3}4^{1-s} & j=0\\ \dfrac{1}{6}4^{1-s} & j=1\\ \dfrac{1}{3}4^{1-s} & j=2\\ \dfrac{1}{6}4^{1-s} & j=3\end{cases}$$

$p\equiv 3\pmod 4$ なる素数に対する結果は，少し複雑である。

定理４　一般リーマン予想を仮定する。

(1)　$8\mid D$ かつ D が $q\equiv 1\pmod 4$ なる素因子 q を持たない場合，

$$\delta_a(3,4;j,4)=\frac{1}{8}+\frac{1}{8}\,C\,\mathrm{sgn}(a)(-1)^{\frac{j+1}{2}}B_a$$

ただし
$$C=\prod_{p\equiv 3\pmod 4}\left(1-\frac{2p}{(p^2+1)(p-1)}\right)\fallingdotseq 0.643650\ldots$$

$$B_a=\prod_{\substack{p\mid D\\ p\equiv 3\pmod 4}}\frac{2p}{p^3-p^2-p-1}$$

(2)　$8\nmid D$，または D が $q\equiv 1\pmod 4$ なる素因子 q を持っている場合，

$$\delta_a(3,4;1,4)=\delta_a(3,4;3,4)=\frac{1}{8}$$

定理４に現われた定数 C, B_a は『中間報告』にも既にあらわれた定数である。このうち，C は絶対定数，そして B_a は有限積なので有理数になることに注意しておく。定理３，４により，$Q_a(x;u\pmod t)$ の密度は必ず

$$\alpha+\beta C,\ \alpha,\ \beta\in\mathbb{Q}$$

の形に書けることが分かる。

さて，ここで定理１～４を使って得られる結論を幾つか列挙してみたい。

上述したように，今回考察した $R_a(x;l\pmod m;u\pmod t)$ は，$Q_a(x;u\pmod t)$ を細分化したものであるから，$Q_a(x;j\pmod 4)$ を求めようと思ったら，$R_a(x;l\pmod m;j\pmod 4)$ を足し合わせてやればよい。

例１　我々が今回の問題に注目するきっかけになった，$1/3$，$1/6$，$1/3$，$1/6$という綺麗な分布は，定理３，４で $s=2$ とおいてみれば得られる。例えば a が square-free で法４で１に合同な自然数の場合，

$$\delta_a(1,4;j,4)=\begin{cases}\dfrac{1}{3} & j=0\\ \dfrac{1}{24} & j=1\\ \dfrac{1}{12} & j=2\\ \dfrac{1}{24} & j=3\end{cases}$$

$$\delta_a(3,4;j,4)=\begin{cases}0 & j=0\\ \dfrac{1}{8} & j=1\\ \dfrac{1}{4} & j=2\\ \dfrac{1}{8} & j=3\end{cases}$$

が容易に計算できるので，この両者を足してやれば，確かに例の分布が得られている。

例２　$a=6$ ととって，$Q_6(x;1\pmod 4)$ を考えよう。『中間報告』の定理４で，この自然密度は

$$\frac{1}{6}-\frac{3}{56}C\fallingdotseq 0.13219\ldots,\ (C\text{ は定理４の }C\text{ と同じ})$$

になることが分かっていた。

今回の結果を使ってこれを再確認する。

$$Q_6(x;1\ (\mathrm{mod}\ 4)) = R_6(x;1\ (\mathrm{mod}\ 4);1\ (\mathrm{mod}\ 4)) + R_6(x;3\ (\mathrm{mod}\ 4);1\ (\mathrm{mod}\ 4))$$

そして

$$\delta_6(1,4;1,4) = \frac{1}{24} \qquad (\text{定理３，}s\text{=2の場合})$$

さらに　$\mathrm{sgn}(6) = +1$，$(-1)^{\frac{J+1}{2}} = -1$，$D = 24$より

$$\delta_6(3,4;1,4) = \frac{1}{8} + \frac{1}{8}\cdot 1\cdot(-1)\frac{3}{7}C = \frac{1}{8} - \frac{3}{56}C$$

$$\frac{1}{24} + \frac{1}{8} - \frac{3}{56}C = \frac{1}{6} - \frac{3}{56}C$$

以上の計算によって，同じ結論が得られた。

これ以外の例は，後で数値例を出すときに一緒に述べる。

３．４以外の法について

『中間報告』にも一部書いたことだが，我々の $Q_a(x;u\ (\mathrm{mod}\ t))$ に関する問題は，剰余 t を法とする加法群 $\mathbb{Z}/t\mathbb{Z}$ の構造と深い関わりがある。$t=4$ の場合，この加法群は次のような構造になっていて，２つの部分群をもっている：

$$\{0,1,2,3\} = \mathbb{Z}/4\mathbb{Z}$$
$$\cup$$
$$\{0,2\}$$
$$\cup$$
$$\{0\}$$

ここで，一番下の部分群を使って得られるのが $Q_a(x;0\ (\mathrm{mod}\ 4))$ に関する結果であり，これは仮定なしで得られる。中央の部分群を使って得られるのが $Q_a(x;0\ (\mathrm{mod}\ 2)) = Q_a(x;0\ (\mathrm{mod}\ 4)) + Q_a(x;2\ (\mathrm{mod}\ 4))$ に関する結果で，これにも仮定は不要である。両者を差し引くと，$Q_a(x;2\ (\mathrm{mod}\ 4))$ に関する結果が，やはり仮定なしで得られるのである。ところが部分群はこの二つしかないため，１の類と３の類を分離することができず，これを分離しようとしたら一般リーマン予想が必要になるということであろう。

では，$t=3$の場合はどうなるであろうか。この場合，法３の加法群は次のようになっている。

mod 3の加法群　　mod 5の加法群

$$\{0,1,2\}=\mathbb{Z}/3\mathbb{Z} \qquad \{0,1,2,3,4\}=\mathbb{Z}/5\mathbb{Z}$$
$$\cup \qquad\qquad \cup$$
$$\{0\} \qquad\qquad \{0\}$$

そこで期待できるのは，一番下の部分群を使って得られる $Q_a(x;0\ (\mathrm{mod}\ 3))$ は仮定なしで得られ，1の類と2の類の分離にはリーマン予想が必要になる，ということであろう。そして実際にその通りなのである。

これも結果のみを書くことにする（[12]）。

定理5　$j=0$ に対しては無条件，$j=1,2$ に対しては一般リーマン予想を仮定する。また s は任意の自然数。

(1)　$R_a(x;1\ (\mathrm{mod}\ 3^s);j\ (\mathrm{mod}\ 3))$ や $R_a(x;2\ (\mathrm{mod}\ 3));j\ (\mathrm{mod}\ 3)$ は自然密度をもつ。

(2)　$R_a(x;1\ (\mathrm{mod}\ 3^s);j\ (\mathrm{mod}\ 3))$ の自然密度を $\delta_a(1,3^s;j,3)$ とすれば，これは次で与えられる：

$$\delta_a(1,3^s;j,3)=\begin{cases}\dfrac{1}{2}\,3^{1-s}-\dfrac{1}{8}3^{2-2s} & j=0\\ \dfrac{1}{16}\,3^{2-2s} & j=1\\ \dfrac{1}{16}\,3^{2-2s} & j=2\end{cases}$$

(3)　$R_a(x;2\ (\mathrm{mod}\ 3);j\ (\mathrm{mod}\ 3))$ の自然密度を $\delta_a(2,3;j,3)$ とすれば，これは次のように与えられる。法3の Dirichlet 指標のうち，principal な方を χ_0，principal でない方を ψ とする。また絶対定数 C' を次で定義する：

$$C'=\prod_{p\equiv 2\ (\mathrm{mod}\ 3)}\left(1-\frac{2p}{(p^2+1)(p-1)}\right)\fallingdotseq 0.173977\ldots$$

すると，

D が $q\equiv 1\ (\mathrm{mod}\ 3)$ なる素因子 q を持つ場合，

$$\delta_a(2,3;j,3)=\frac{1}{4}\,\chi_0(j)+\frac{1}{4}\psi(j)C'$$

D が $q\equiv 1\ (\mathrm{mod}\ 3)$ なる素因子 q を持たない場合，$D=2^dD'$（D' は奇数）とすれば，

(i)　$d=0$ のとき，$\delta_a(2,3;j,3)=\dfrac{1}{4}\,\chi_0(j)+\dfrac{1}{4}\psi(j)C'\left\{1+(-1)^{\Omega(D')+1}2^2\prod_{\substack{p\mid D\\ p>3}}\dfrac{2p}{p^3-p^2-p-1}\right\}$

(ii)　$d>0$ のとき，$\delta_a(2,3;j,3)=\dfrac{1}{4}\,\chi_0(j)+\dfrac{1}{4}\psi(j)C'\left\{1+(-1)^{\Omega(D)}2^{4-2d}\prod_{\substack{p\mid D\\ p>3}}\dfrac{2p}{p^3-p^2-p-1}\right\}$

ただし，$\Omega(D')$はD'を割る素因子の個数（重複度もこめたもの）である。

この定理によれば，$t=4$のときに$1/3$，$1/6$，$1/3$，$1/6$が一番自然だったように，$t=3$の場合は$\frac{3}{8}$，$\frac{5}{16}+\frac{C'}{4}$，$\frac{5}{16}-\frac{C'}{4}$が一番自然な分布状態であることが分かる。

最後に$t=5$の場合について略述する。

法5の加法群は法3の場合とほとんど同じ構造を持っているので（前ページの図参照），$t=3$の場合と同様，$Q_a(x;0 \pmod 5)$は仮定なしで得られ，1の類から4の類までの四つの類の分離にはリーマン予想が必要になることが予想される。そしてそれはその通りなのだが，我々の計算によれば，ここに今ひとつ興味深い現象がある。結果のみ挙げてみよう。

定理6　aはsquare freeで$a\equiv 1 \pmod 4$とする（これが一番簡単な場合である）。

(1)　$\#Q_a(x;0,5)\sim\frac{5}{24}\pi(x)$

(2)　ここでは一般リーマン予想を仮定する。次の四つの定数を定義する：

$$E_0=\prod_p\left(1-\frac{1}{p(p-1)}\right)\fallingdotseq 0.37395\ldots \qquad (\text{Artin の定数})$$

$$E_1=E_0\prod_{p\equiv 2,3 \pmod 5}\left(1-\frac{2p}{(p^2+1)(p-1)}\right)\fallingdotseq 0.12931$$

$$E_2=E_0\prod_{p\equiv 2(5)}\left(1-\frac{(1-\sqrt{-1})p}{(p^2-\sqrt{-1})(p-1)}\right)\prod_{p\equiv 3(5)}\left(1-\frac{(1+\sqrt{-1})p}{(p^2+\sqrt{-1})(p-1)}\right)\prod_{p\equiv 4(5)}\left(1-\frac{2p}{(p^2+1)(p-1)}\right)$$

$$\fallingdotseq 0.36469+0.22404\sqrt{-1}$$

$E_3=E_2$の複素共役

すると次の漸近式が得られる：

$$\pi(x)^{-1}\ \#Q_a(x;j,5)\text{の主要部}\sim\begin{cases}\frac{19}{96}-\frac{1}{16}(E_1-E_2-E_3) & j=1\\ \frac{19}{96}-\frac{1}{16}(-E_1-\sqrt{-1}E_2+\sqrt{-1}E_3) & j=2\\ \frac{19}{96}-\frac{1}{16}(-E_1+\sqrt{-1}E_2-\sqrt{-1}E_3) & j=3\\ \frac{19}{96}-\frac{1}{16}(E_1-E_2-E_3) & j=4\end{cases}$$

ここで興味深いのは，定数E_2とE_3が複素数になっていることである。ところが密度を与える部分ではこの四つの複素定数が巧く虚部が消えるように組み合わさっているので，結果として実定数を与えている（ここでは話を簡単にするため，$\#Q_a(x;j,5)$の主要部について述べたが，

$Q_a(x;j,5)$ の正確な密度に対しても同じ現象がおきている)。我々の考えているのはある素数集合の密度なので，これが（存在するなら）実数値であることは明らかなのだが，それが複素定数の組み合わせによって与えられているところが大変興味深い。この $t=5$のときの現象を見ると，おそらく一般の t を法とした場合には，$\varphi(t)$ 個の複素定数が現われ（その定義式には t を法とする Dirichlet 指標が現れる)，その組み合わせによって，問題の素数集合の密度が与えられることになっているのだろう。ただ，その詳しい証明についてはまだ残っている部分がある。

4．数　値　例

最後に，理論値と実測値の比較のため，数値実験の結果をまとめておく。なお，こうした数値実験は，我々の場合，単に理論値の検証というだけでないと思っている。我々の結論は一般リーマン予想を仮定しているので，一般リーマン予想はこうした面でも実際と良く合うといった見方ができるのではないかと考える。

例３　$t=4$ の場合の例。実測値では小さい方から10^7個の素数を使って計算してある（$x=179424673$である)。従って一番右の欄には$10^{-7}\#R_a(x;3\,(\mathrm{mod}\,4);1\,(\mathrm{mod}\,4))$ の値が記入してある。

a の値	$\delta_a(3,4;1,4)$ の理論値	その実測値
2	$\frac{1}{8}-\frac{1}{8}\,C\fallingdotseq 0.044544$	0.044580
−2	$\frac{1}{8}+\frac{1}{8}\,C\fallingdotseq 0.090519$	0.090605
10	$\frac{1}{8}=0.125$	0.124993
14	$\frac{1}{8}-\frac{7}{1144}\,C\fallingdotseq 0.121062$	0.121106

例４　$t=3$ の場合の例。一番右の欄は$10^{-7}\#R_a(x;2\,(\mathrm{mod}\,3);1\,(\mathrm{mod}\,3))$ である。

a の値	$\delta_a(2,3;1,3)$ の理論値	その実測値
3	$\frac{1}{4}=0.25$	0.250011
5	$\frac{1}{4}+\frac{67}{188}C'\fallingdotseq 0.304368$	0.304333
14	$\frac{1}{4}+\frac{1}{4}C'\fallingdotseq 0.293494$	0.293398

例５　$t=5$ の場合の例。ここでは上と異なり，$\pi(x)^{-1}\,\#Q_a(x;j,5)$ を比較してある。密度の理論値は定理６に挙げた近似値を使うと

a の値	$j=1$	$j=2$	$j=3$	$j=4$
13	0.235543	0.178356	0.234475	0.143292
21	0.235494	0.176925	0.233715	0.145532
42	0.235654	0.178146	0.233766	0.144101

となる。これを x として10^8をとって，比較のため実測値を計算してみたのが，次の表である。

a の値	$j=1$	$j=2$	$j=3$	$j=4$
13	0.235620	0.178355	0.234440	0.143273
21	0.235709	0.176875	0.233722	0.145379
42	0.235541	0.178005	0.234004	0.144144

参考文献

［1］ Chinen K., Murata L., On a distribution property of the residual order of $a\,(\mathrm{mod}\,p)$. e-print archive, http://xxx.lanl.gov/archive/math, article number math. NT/0211077

［2］ Murata L., Chinen K., On a distribution property of the residual order of $a\,(\mathrm{mod}\,p)$, II. e-print archive, http://xxx.lanl.gov/archive/math, article number math. NT/0211083

［3］ 知念宏司 - 村田玲音：“On a distribution property of the residual order of $a\,(\mathrm{mod}\,p)$. I, 京都大学数理解析研究所 講究録1219 (2001), 245 - 255.

［4］ 知念宏司 - 村田玲音：“On a distribution property of the residual order of $a\,(\mathrm{mod}\,p)$. II, 京都大学数理解析研究所 講究録1274 (2002), 62 - 69.

［5］ Hasse H.：Über die Dichte der primzahlen p, für die eine vorgegebene ganzrationale Zahl $a>0$ von gerader bzw. ungerader Ordnung mod p ist, Math. Ann. Bd.166 (1966) pp. 19 - 23.

［6］ Hooley C.：On Artin's Conjecture, J. Reine angew. Math. Bd 225 (1967) pp. 209 - 220.

［7］ Lenstra Jr. H.W.：On Artin's conjecture and Euclid's algorithm in global fields, Invent. Math. Vol.42

(1977) pp. 201 - 224.

[8] Moree P.：On the density of primes in arithmetic progression having a prescribed root, MpI-preprint 57, Bonn 1998.

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

[10] 村田玲音 - 石井坦：剰余位数の分布の一性質について，明治学院大学産業経済研究所　研究所年報第18号 (2001), 65 - 72.

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

[12] Moree P.：On the distribution of the order and index of $g \pmod p$ over residue classes.
e-print archive, http://xxx.lanl.gov/archive/math, archive number math NT/0211259.