『経済研究』（明治学院大学）第 145 号　2012 年

剰余位数の分布について

経済学部　村　田　玲　音

§１　剰余位数・剰余指数

p を奇素数とする。p を法とする既約剰余類群（$Z/pZ)^*$ は $p-1$ 次の巡回群である。a を p で割れない自然数とすれば，剰余類 $a(\mathrm{mod}\ p)$ は（$Z/pZ)^*$ の元となり，この中で巡回部分群を生成する。この群を $\langle a(\mathrm{mod}\ p)\rangle$ によって表わすことにする。すると次の重要な分解が得られる。なお，［　：　］は部分群の指数，集合 G の元の個数を $|G|$ によって表わす（以下同様）：

$$p-1=[(Z/pZ)^*:\langle a(\mathrm{mod}\ p)\rangle]\times|\langle a(\mathrm{mod}\ p)\rangle|$$

右辺の第一項を剰余指数（residual index）とよび，第二項を剰余位数（residual order あるいは multiplicative order）という。

$p-1$ をこのように分解して考察してみたのは有名なガウスである。$a=10$ ととれば，a の剰余位数は分数 $1/p$ を循環小数に展開したときの循環節の長さに他ならない。ガウスは循環小数との関連で剰余位数や剰余指数に注目したようである。彼は p を色々動かしてみて，「p が大きくなると剰余位数の方は大きく変化するのに，剰余指数の方はあまり変化しない」ことに気づいた。天才的な計算能力から研究の糸口を発見したといわれるガウスならではの観察である。高木貞治の『近世数学史談』に「計算家ガウスに於いて著しい特徴は彼が数字的の計算に整数論を応用する点である。（中略）ガウスは幼児期に 200 以下の素数および素数冪の逆数を循環小数に化する表を作成し，後年それを 1000 以下まで継続している。」との文章が見えるので，案外早い時期の発見かもしれない。

ここで幾つかの p に対して，その剰余指数と剰余位数を例示してみよう。a の値はガウスに習って 10 ととってある。

（**表 1**）

① 素数（100 を超えた直後の 10 個）

	101	103	107	109	113	127	131	137	139	149
剰余指数	25	3	2	1	1	3	1	17	3	1
剰余位数	4	34	53	108	112	42	130	8	46	148

② 素数（1000 を超えた直後の 10 個）

	1009	1013	1019	1021	1031	1033	1039	1049	1051	1061
剰余指数	4	4	1	1	10	1	2	2	1	5
剰余位数	252	253	1018	1020	103	1032	519	524	1050	212

③ 素数（100000 を超えた直後の 10 個）

	100003	100019	100043	100049	100057	100069	100103	100109	100129	100151
剰余指数	2	1	2	2	1	1	1	29	4	2
剰余位数	50001	100018	50021	50024	100056	100068	100102	3452	25032	50075

印象的なのは，素数の大きさが変わっても中段の剰余指数の部分はほとんど変化していない点である。つまり，素数が大きくなった分は，ほとんど全部剰余位数の方に回っていることになる。従って剰余位数の動きは激しい。これがガウスの見つけた現象であった。

ここで一つ定義を置こう。

定義

剰余指数［$(Z/pZ)^*$：$\langle a(\mathrm{mod}\ p)\rangle$］が n で割りきれるとき「a は mod p で n 乗剰余（n-th power residue）である」という。特に剰余指数＝1 のとき，「a は mod p で原始根（primitive root）である」という。

a が mod p で n 乗剰余であるとは，別の剰余類の n 乗になっていることである。なお，原始根であることは“他の剰余類の冪乗で書けない”ことを意味しているわけではない。他の剰余類 $b(\mathrm{mod}\ p)$ によって $b(\mathrm{mod}\ p)^r = a(\mathrm{mod}\ p)$ としたとき，指数の r が $p-1$ と互いに素になっていればよい。

上記のガウスの観察から，次の予想は自然に出てくる。

原始根に関する Artin の予想

a が完全平方数でないなら，a が mod p で原始根になるような素数 p は無限個存在するだろう。

つまり上の表 1 のようなものをすべての素数 p に対して作れば、剰余指数の行に 1 が無限回出てくるだろうという予想である。これが Artin の予想と呼ばれているのは，20 世紀になって，E. Artin や Heibronn 等によってガウスの予想が再発見され，精密化されたからである。ガウスの観察以来 200 年以上経過したにもかかわらず，未だに完全解決をみていない難問である。ただし，一般リーマン予想

（Dedekind のζ関数に関するリーマン予想）を仮定すれば，上の予想より更に精密な結果を証明することができ，それは計算機等による実際の姿をかなり正確に説明するということを，1967 年にイギリスの解析数論学者 C. Hooley が証明した。以下本稿では，一般リーマン予想（Generalized Riemann Hypothesis）のことを GRH と略記する。

まず特殊な定数 C を用意する。定義は $C=\prod_{q:\text{素数}}\left(1-\frac{1}{q(q-1)}\right)\fallingdotseq 0.37395\cdots$

定理A（Hooley, 1967［7］） GRH を仮定する。次の漸近式が成り立つ：

$$\|\, p\leqq x\,;\, a \text{ が mod } p \text{ で原始根} \,\| \sim C_a\,\pi(x)+O\left(\pi(x)\frac{\log\log x}{\log x}\right),$$

ただし C_a とは a のみによって定まる正定数で，a が特別な条件（本稿では省略する）を満たさない場合，$C_a=C$ になる。

ここで $\pi(x)$ とは正数 x 以下の素数の個数である。また〜は，左辺を右辺で割ったものの極限（$x\to\infty$）が 1 であることを意味する。上の定数 C は原始根を扱った問題にしばしば現れる定数で，“Artin の定数”と呼ばれることがある。

この定理によれば，通常の a の場合，a を原始根にもつ素数は素数全体の約 37.4%であることが分かる。例えば上の表 1 についてみれば，30 個の素数中 12 個について $a=10$ が原始根になっているので（40%），この程度のサンプルでも定理の主張と現状が良く一致していることが分かる。

上の Hooley の定理は，一般の剰余指数 n の場合へ拡張されており，GRH の仮定の下に，どのような頻度で「剰余指数＝ n」が起きるかも分かっている（［8］［10］）。

原始根は次のような基本的な性格をもっている：

(1) 既約剰余類群 $(Z/pZ)^*$ の生成元である。

(2) 既約剰余類群 $(Z/pZ)^*$ で，どんな q 乗剰余にもなっていない類である。

(3) 色々な角度から見て，分布にまったく規則性はなさそうである。

原始根というのは，案外色々なところに出てくる重要な数である。最近では，公開鍵暗号の世界でも生成元という名称で使われている。その重要性が(1)の「$(Z/pZ)^*$ の生成元」から来ていることは疑いない。整数の問題を mod p に reduction すると必然的に $(Z/pZ)^*$ が出てくるが，その元は原始根によって記述できるのであるから，登場する機会が多いのも頷ける。ところがそうした重要な数の分布を調べようとすると，性格の(3)に行き当たる。規則性がないのでシステマティックな研究がしにくく，まずは原始根を取り出して分布等の特徴を見ようとするとき，性格(1)の「生成元」というのは非常に使いにくい条件なのである。そこで我々は仕方なく，性格(2)を活用して原始根を調べていくことになる。たとえば先ほどの Artin 予想の場合のように「x 以下の素数の中から，a が原始根になっている p」を選り出そうとすると，

求める個数 ＝ $\pi(x)-\|\, a \text{ が 2 乗剰余になっている } p \,\|-\|\, a \text{ が 3 乗剰余になっている } p \,\|+$

$$|\{a \text{ が } 6 \text{ 乗剰余になっている } p\}| - |\{a \text{ が } 5 \text{ 乗剰余になっている } p\}| - \cdots$$

と，たいへん面倒な手続きが必要になる。所謂，篩法を使わざるをえない。

この辺の事情は「素数分布」と似通っている。素数は「素数の自由積が Q^* の元全部になる」という意味で有理数体 Q の生成元であるが，これを調べようとすると分布の複雑さに行き当たる。そして素数を選り出そうとすると「有理数体の生成元」という条件は使いにくく，結局「x 以下の素数」を選り出すには

$$x \text{ 以下の自然数} - |\{2 \text{ の倍数}\}| - |\{3 \text{ の倍数}\}| + |\{6 \text{ の倍数}\}| - |\{5 \text{ の倍数}\}| + \cdots$$

といった手続きが必要であった（エラトステネスの篩）。

原始根の分布が素数分布と違ってくるのはここからで，「a が n 乗剰余になっている素数 p」は「拡大体 $Q(a^{1/q}, \zeta_q)/Q$ で完全分解する素 ideal(p)」と，代数体の ideal の分解で記述される点である（ζ_q は 1 の原始 q-乗根，すなわち $\exp(2\pi i/q)$ の意味）。こうした p の個数を計算するには素 ideal 定理を使わなくてはならない。素 ideal 定理では主要項の後にかなり大きな剰余項がついてくる。この処理が原始根を調べる場合一番の障害になるのである。先ほどの“篩”を先まで進めないうちに，剰余項の総和が主要項を凌駕してしまい，意味のある結果が得られなくなってしまう。

GRH の役割はここにある。これを仮定すると素 ideal 定理の剰余項を低く抑えることができて，篩をかなり先まで実行することができ，場合によってはとてもシャープな結果が得られる。上述の Hooley の定理がその好例である。こうしたわけで，剰余指数や剰余位数の分野ではしばしば GRH の仮定が必要になる。なお，上の篩の実行で剰余項を抑えることができれば，その主要項は

$$\pi(x) \times \prod_{q:\text{素数}} \left(1 - \frac{1}{[Q(a^{1/q}, \zeta_q): Q]}\right)$$

となり，拡大次数 $[Q(a^{1/q}, \zeta_q) : Q]$ は通常 $q(q-1)$ になる。これが Artin 定数の出てくる所以である。

原始根・剰余位数といったものは，a と p との組み合わせで決まる性質である。このため，こうしたものの研究には次の 3 つの方向が考えられてきた（p を固定し a を動かして剰余位数を研究する方向は，まだ問題にされたことがないようである）。

- 剰余指数の研究
  - a を固定して素数 p を動かす方向
  - p を固定して a の方を動かす方向
- 剰余位数の研究 ——— a を固定して素数 p を動かす方向

このうち一番上の「a を固定し p を動かして剰余指数を調べる」方向の代表選手は Artin 予想である。これがあるため，この方向の研究は先行していて，優れた結果も多い。これ以外の方向は比較的成果も少なく，特に剰余位数の方はほとんど研究がなされていない。

この小論では，§2 で「a を固定し p を動かして剰余位数を調べる」方向について解説したい。§3 では，§2 の一つの発展形として mod pq の場合について述べる。いずれも私がこれまでに行ってきた研究を中心に述べる。

§ 2　剰余位数の分布—mod p の場合

上で例を見たが，剰余位数というのは解析数論の立場からは非常に調べにくい対象である。動きが非常に激しいことに加えて，剰余位数のように代数的整数論の結果と直接結びついてもいない。これまで，あまり研究されておらず，知られている結果も少ない。かなり有効な方法としては，次の二つが知られている。

① $a^n \equiv 1 \pmod{p}$ という条件を，円分多項式 $X^n - 1$ の X に a を代入した特殊値の，p での可除性の考察に置き換える。

② $p - 1 =$ 剰余位数 × 剰余指数　の関係式を用いる。

このうち②については上でも触れたが，長所は剰余指数の部分が代数的整数論と相性が良い点であろう。

以下，自然数 a を固定し，素数 p を動かす。素数集合 P から自然数集合 N への，二つの写像を考えよう。

写像 Φ：　$P \ni p \mapsto [(Z/pZ)^* : \langle a \pmod{p} \rangle] \ni N$

写像 Ψ：　$P \ni p \mapsto |\langle a \pmod{p} \rangle| \ni N$

Φ は，素数 p に対して剰余指数を対応させるもの，Ψ は剰余位数を対応させる写像である。Φ と Ψ の間には，非常に大きな共通点がある。それは両方とも「P から N への全射である」という点である。これは両方ともかなり深い結果で，Φ の全射性をいうには，まず GRH を仮定して Artin 予想を証明し，これを指数が一般の場合に拡張しなくてはならない。一方 Ψ の全射性は unconditional に得られる。証明は難しくないのだが，結果自体は非常に優れた結果であろうと思われる。

ところが同じ全射でも，Φ と Ψ の間には大きな相違点がある。

自然数 n の Φ による逆像は，GRH を仮定すれば，素数全体の或るパーセンテイジを占めるくらい大きな集合になる。一方，n の Ψ による逆像は，必ず有限集合になる。つまり，同じ全射であっても，N の覆い方がまるで違うのである。解析数論では，あまり小さな集合は巧く理論に乗せることができないわけで，このくらい写像の性質が違えば，研究方法も変えないといけないのではないかと思う。そこで我々は剰余位数を調べるにあたって，Ψ の値域集合を大きくとることにする。

剰余位数の性質について，こうした考え方に立って具体的に結果が得られているのは次の二つである。

1）値域を N 内の剰余類ととる（私と知念宏司氏との共同研究，2004 年～，［1］［2］［3］[11]）

2）値域を素数集合 P ととる（私と Carl Pomerance 氏との共同研究［12]）

このうち 2）については既に［13］に記事を書いたので，本稿では省略する。

1）について

N 内に任意の剰余類 $v \pmod{k}$ をとって，集合

$$Q_a(x\,;\,k, v) = \{\, p \leqq x\,;\, a \pmod{p} \text{ の剰余位数} \equiv v \pmod{k} \}$$

を考察する。まず取り組まなくてはならない問題は次の二つである。

1　$Q_a(x\,;k,\nu)$ に自然密度は存在するか？

2　密度が存在する場合には，その密度は k や ν を変化させたときどんな分布をしているのか？

この問題には先駆者がいる。$\nu=0$ の場合には $Q_a(x\,;k,0)$ に密度の存在することが示されており，その密度も具体的に計算されている（Hasse, 1965［5］［6］，並びに Odoni, 1981［14］）。こうした先行結果があるため，我々の研究では ν を任意にしておくことが重要であった。

この問題について我々の得た結果は次の通りである。

定理の内容を分かりやすく説明するため，一番単純な場合をあげる。

$k=4$ ととる。a を $a=a_0\times a_1$（a_1 は square-free）と分解する。

定理 1［1］　$a_1\equiv 1, 3 \pmod 4$ なら

Ⅰ）　$Q_a(x\,;k,\nu)$ は $\nu=0, 1, 2, 3$ で自然密度をもつ。ただし，$\nu=0, 2$ の場合，自然密度の存在は unconditional に得られ，$\nu=1, 3$ の場合は GRH の仮定が必要である。

Ⅱ）　その密度は，次で与えられる：

$$\pi(x)\begin{cases} |Q_a(x\,;4,0)| \sim \dfrac{1}{3}\pi(x) \\ |Q_a(x\,;4,1)| \sim \dfrac{1}{6}\pi(x) \\ |Q_a(x\,;4,2)| \sim \dfrac{1}{3}\pi(x) \\ |Q_a(x\,;4,3)| \sim \dfrac{1}{6}\pi(x) \end{cases}$$

本稿では証明は一切省略する。興味ある方は full-paper［1］［2］を参照してください。

以下，$Q_a(x\,;k,\nu)$ の自然密度のことを $\Delta_a(k,\nu)$ と書くことにしよう。

上でも述べたように，この定理の紹介にあたっては，一番単純な場合を示した。この結果は一般の剰余類 $\nu \pmod k$ の場合に拡張できている。ただ，k が複雑になると「密度の存在」と「密度計算のアルゴリズム」までは分っているが，密度の具体形は難しくなる。より詳しく言うと，k が素数べきまでなら，一応密度の具体形が求まっている。k が二つ以上の素因子を含む合成数になると，密度はある連立一次方程式の解として得られるが，その方程式を具体的に解くのは相当困難である。

この結果は自然密度の理論値を求めたものであるが，それがどの程度まで実測値と合っているか，少し例をあげてみたい。以下の数値例では $x=10^7$ とした。この問題の場合は 10^7 までの素数を使うと，かなり信憑性のあるデータになるようである。

$a=5$ の場合の，理論値（上）と実測値（下）

$v=0$	$v=1$	$v=2$	$v=3$
$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{6}$
0.333320	0.166771	0.333099	0.166810

$a=21$ の場合の，理論値（上）と実測値（下）—— a は合成数

$v=0$	$v=1$	$v=2$	$v=3$
$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{6}$
0.332836	0.166527	0.333917	0.166720

上の結果ですぐに目を惹く点は，密度が 1/3 や 1/6 といったきれいな有理数で書けている点であろう。ただ，これは a の値によって大きく変化し，密度が有理数にならない場合もしばしば起こりうる。参考に $a=2$ の場合を挙げておこう。まず，特殊な数 δ を導入しなくてはならない。

$$\delta=\prod_{\substack{q\equiv 3 \pmod 4\\ q:\text{素数}}}\left(1-\frac{2q}{(q^2+1)(q-1)}\right)\fallingdotseq 0.64365$$

この数を用いると，

$$1\begin{cases}\Delta_2(4,0)=\dfrac{5}{12} & \fallingdotseq 0.41667\\ \Delta_2(4,1)=\dfrac{7}{48}-\dfrac{\delta}{8} & \fallingdotseq 0.06538\\ \Delta_2(4,2)=\dfrac{7}{24} & \fallingdotseq 0.29167\\ \Delta_2(4,3)=\dfrac{7}{48}+\dfrac{\delta}{8} & \fallingdotseq 0.22629\end{cases}$$

となる。δ は全く得体のしれない数であるから，従って $|Q_a(x;\,4,\,1)|$ の密度なども得体のしれない数になる。ついでに，この場合も理論値と実測値の比較をあげておく：

	$v=0$	$v=1$	$v=2$	$v=3$
理論値	0.416667	0.065377	0.291667	0.226289
実測値	0.416687	0.065425	0.291481	0.226407

もう一つ，密度の存在を言う際，とった剰余類によって GRH が要ったり要らなかったりするのもちょっと奇異に感じられることであるが，これについてはある程度理由が分っている。これはとった剰余類の法 k によって決まる加法群（Z/kZ）の構造によるらしい。再び $k=4$ の場合を例にとると，加法群（$Z/4Z$）は真の部分群を二つもっている。その二つからそれぞれ一つずつ，non-trivial な結果が得られるのである。

$$
\begin{array}{rcl}
(Z/4Z) = \{0, 1, 2, 3\} & & \\
\quad | & & \\
\{0, 3\} & \rightarrow & |Q_a(x; 2, 0)| \text{ の密度} \\
\quad | & & \\
\{0\} & \rightarrow & |Q_a(x; 4, 0)| \text{ の密度}
\end{array}
$$

そして $|Q_a(x; 2, 0)|$ から $|Q_a(x; 4, 0)|$ を引けば，$|Q_a(x; 4, 2)|$ が得られるわけである。またこれによって，Hasse-Sherpinski や Odoni の結果が得られた理由もわかる。彼らは（Z/kZ）に必ず存在する，一番易しい真部分群 $\{0\}$ に対応する結果を得ていたのである。

数論的関数としての密度関数 $\Delta_a(k, v)$ の挙動は，かなり複雑なようである。一番の問題は，適当な確率モデルがなく，密度 $\Delta_a(k, v)$ の値が全く予測できないことである。詳しい説明はしないが，実は $\Delta_a(2, 1) = 1/3$ になる理由は，比較的簡単な確率的解釈が可能である。ところがこれをどう精密化してみても，$\Delta_a(4, 1) = 1/6$ になる確率的解釈が出てこない。つまり，$\Delta_a(2, 1) = 1/3$ がなぜ $\Delta_a(4, 1) = \Delta_a(4, 3) = 1/6$ と半分ずつになるのか，その理由は解らないのである。これが当たり前でないことは，$a = 2$ の場合の例が示している。一般の $\Delta_a(k, v)$ では，その密度の存在を言うのに GRH が必要であったし，$a = 2$ の場合は 1/6 からかなり離れた値になってしまうなど，背景にはかなり複雑な理由が潜んでいるのかもしれない。

また，密度関数 $\Delta_a(k, v)$ は“乗法性”も持っていない。ここで言う乗法性とは，以下のような意味である。例に即して説明する。

$$
\begin{array}{ccccc}
Z/12Z & \cong & Z/4Z & \times & Z/3Z \\
j(\mathrm{mod}\ 12) & \longleftrightarrow & j_1(\mathrm{mod}\ 4) & , & j_2(\mathrm{mod}\ 3)
\end{array}
$$

の対応関係によって，

$$\Delta_a(12, j) = \Delta_a(4, j_1) \times \Delta_a(3, j_2)$$

が成立するかどうかを問題にするのである。これが成立すれば，一般の合成数 k を素因数分解することにより，k として素べきの場合だけを計算すればよくなる（これを乗法性と呼んだ）。しかしこれは成立しないことが実例によって分かっている。

反例　$a = 5$ ととる。$1(\mathrm{mod}\ 12) \longleftrightarrow 1\ (\mathrm{mod}\ 4), 1(\mathrm{mod}\ 3)$ であるが

$$\Delta_5(12, 1) = \frac{5}{96} - \frac{21}{940}D$$

$$\Delta_5(3, 1) \times \Delta_5(4, 1) = \frac{3}{8} \times \frac{1}{6} = \frac{1}{16}$$

となって，この両者は一致していない。ここで D とは mod 6 の non-trivial character χ を用いて定義される次の数である：

$$D=\prod_{\substack{q:\text{素数}\\ q\neq 2,3}}\frac{q^3-q^2-q-x(q)}{(q-1)(q^2-x(q))}\fallingdotseq 0.86989$$

最後に，密度 $\Delta_a(k, v)$ はどのようにして決まるのか，それを与える式を簡単に見てみたい。何度か触れたように，これには関係式「$p-1=$剰余位数×剰余指数」を用いるのである。まず，次の集合を導入する：

$$N_a(x\,;n, s(\mathrm{mod}\ t))=\{p\leqq x\,;\ a\ \text{の剰余位数}=n,\ p\equiv s(\mathrm{mod}\ t)\}$$

これは一見して分かるように，“原始根に関する Artin 予想”で研究の対象になった集合である（Artin 予想が問題にした集合を上の形に習って書けば $\{p\leqq x\,;\ a\ \text{の剰余位数}=1\}$ となる）。そしてこの形の集合は，GRH を仮定すれば計算が可能になっていた。

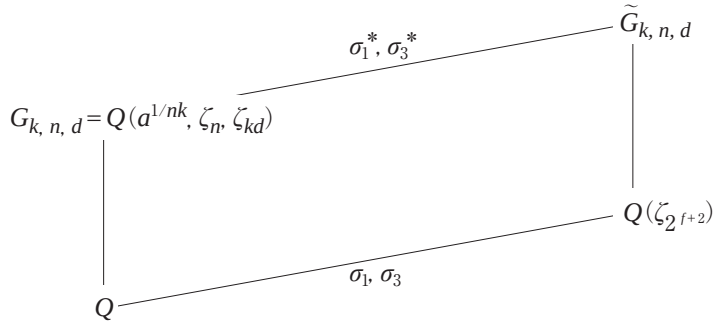
まず $|Q_a(x\,;4,\ 1)|$ を変形していって，次の式を証明する：

$$|Q_a(x\,;4,\ 1)|=\sum_{f\geqq 1}\sum_{\ell\geqq 0}|N_a(x\,;\ (4\ell+1)2^f,\ 1+2^f(\mathrm{mod}\ 2^{(f+2)})|\ +\ \text{（同じ形の無限級数）}$$

ここに Artin 予想で使われた Hooley の方法（篩法）を適用するのである。すると次のような式が得られる。上の式は素数の個数を分解した式であるのに対し，下の式は密度を分解した式になっている。この間に GRH を用いて，誤差項の処理を行なったのである。

$$\Delta_a(4,\ 1)=\sum_{f\geqq 1}\sum_{\ell\geqq 0}\frac{k_0}{\varphi(k_0)}\sum_{d|k_0}\frac{\mu(d)}{d}\sum_{n=1}^{\infty}\frac{\mu(n)c^{(1)}(k,\ n,\ d)}{[\tilde{G}_{k,\ n,\ d}:Q]}\ +\ \text{（同じ形の無限級数）}$$

ただし $k=(4\ell+1)2^f$, $k_0=\prod_{q|k,\ q:\text{素数}}q$ である。この式を使って密度を計算するのだが，その際重要なのは最後の項の分母分子に出てきている $[\tilde{G}_{k.n.d}:\ Q]$ や $c^{(1)}(k,\ n,\ d)$ といった数である。これは次のような代数体の量として定義される：



$\sigma_1,\ \sigma_3$ は，次の作用で定まる拡大体 $Q(\zeta_{2^{f+2}})/Q$ の自己同型群の元であり：

$$\sigma_1:\zeta_{2^{f+2}}\mapsto(\zeta_{2^{f+2}})^{1+2^f},$$
$$\sigma_3:\zeta_{2^{f+2}}\mapsto(\zeta_{2^{f+2}})^{1+3\cdot 2^f},$$

係数 $c^{(1)}(k, n, d)$ は，σ_1 が $\sigma_1^* \in Aut(\tilde{G}_{k,n,d}/G_{k,n,d})$ に拡張できるなら 1，そうでない場合は 0 と定義する。これらの数を代数体 $\tilde{G}_{k,n,d}$ ごとに決定し，上の $\Delta_a(4, 1)$ の式に代入して無限級数を計算すると前掲の定理 1 が得られる。

こうしたことを証明なしで長々と書いたのは，我々の目的とする密度が，いかに強く代数体の数量に依存しているかを述べたかったのが一つ，それと剰余指数を経由して剰余位数の結果を得ようとするといかに手間がかかるか，それを説明したかったからである。

§ 3　剰余位数の分布—mod *pq* の場合

この章では，§2 で論じた問題を $(Z/pqZ)^*$ で考えたときの結果を略述する。p, q は互いに異なる素数である。前の $(Z/pZ)^*$ との一番の違いは，$(Z/pqZ)^*$ が巡回群にならない点である。原始根とは“既約剰余類群の生成元”であるところに重要な意味があった。今度は群が巡回群でないので，生成元はなくなってしまう。その意味では原始根に関する問題を剰余群 $(Z/pqZ)^*$ で考える場合，定義から大きく考え直さなくてはならない。例えば Pomerance 氏などは原始根の定義を拡げて，Artin 予想の類似等を考えている（[9]）。しかし剰余位数の方は群構造が変わっても意味はそのまま保たれる。更に我々の頭の中にあったのは，mod pq が公開鍵暗号 RSA 暗号の中で非常に重要な使われ方をしていることであった。

§2 で始めたのと同様，剰余類 $v \pmod k$ をとり，次を導入する：

$$R_a(x; k, v) = \{(p, q); p \leqq x, q \leqq x, a \pmod{pq} \text{の剰余位数} \equiv v \pmod k\}$$

そして $\lim_{x\to\infty} \pi(x)^{-2} |R_a(x; k, v)|$ を考察するのである。

得られた結果を下に挙げる。前回同様 $k=4$ ととってあるが，前回と違って mod pq では計算できているのが，まだこの場合だけなのである。

定理 2［ 4 ］　$a_1 \equiv 1, 3 \pmod 4$ なら

Ⅰ）　$R_a(x; k, v)$ は $v=0, 1, 2, 3$ で自然密度をもつ。ただし，$v=0, 2$ の場合，自然密度の存在は unconditional に得られ，$v=1, 3$ の場合は GRH の仮定が必要である。

Ⅱ）　その密度は，次で与えられる：

$$\pi(x)^2 \begin{cases} |R_a(x; 4, 0)| \sim \frac{5}{9}\,\pi(x)^2 \\ |R_a(x; 4, 1)| \sim \frac{1}{18}\,\pi(x)^2 \\ |R_a(x; 4, 2)| \sim \frac{1}{3}\,\pi(x)^2 \\ |R_a(x; 4, 3)| \sim \frac{1}{18}\,\pi(x)^2 \end{cases}$$

ここでも証明は一切省略する。詳しくは［ 4 ］を参照。

定理 1 でも，mod 4 の剰余類によって密度が $\frac{1}{3}$ や $\frac{1}{6}$ になり，“分布に大きな差――偏り”のあることが分ったが，mod pq の場合，この偏りはもっとひどくなった。$v=0$ の場合と $v=1, 3$ の場合は，分布密度に実に 10 倍の開きがあるのである。

$a \pmod{pq}$ の剰余位数は，$a \pmod{p}$ の剰余位数と $a \pmod{q}$ の剰余位数の最小公倍数になる。“最小公倍数”という乗法的に定まる量を“4 で割った余り”という加法的なものによって分類するところが，定理 2 の難しさと面白さである。

章末に数値例との比較を挙げておいた。理論値と実験値は非常に良い一致を示している。

上にも書いたが，mod pq の場合の計算はむつかしく，現在までにできているのは k が 4 で a にも“一番計算しやすい”仮定を置いた場合のみである。数値計算の方は $a=2$ の場合もできているので載せてみたが，この理論値がどんな形になるのかは分かっていない。

我々の与えた証明はかなり複雑であるが，要点は $|R_a(x\,;\,4,\,v)|$ の計算を $|Q_a(x\,;\,k,\,v)|$ に帰着できた点にある。鍵になった式は

$$|R_a(x\,;\,4,\,1)| = |Q_a(x\,;\,4,\,1)|^2 + |Q_a(x\,;\,4,\,3)|^2$$

$$+ \sum_{\substack{D<x \\ D\equiv 1 \pmod 4 \\ D_0=1,\ D_1>1}} 2^{\omega(D_1)-1}\,\|Q_a(x\,;\,4D,\,D)| - |Q_a(x\,;\,4D,\,3D)\|^2 + (\text{右辺第 3 項と同じ形の無限級数})$$

ただし，D は奇数で，D の素因子のうち mod 4 で 1 に合同な素因子のみの積が D_0，mod 4 で 3 に合同な素因子のみの積が D_1 である。また $\omega(n)$ とは n を割り切る異なる素数の個数を表す。

この式の特徴は，左辺は $|R_a(x\,;\,4,\,1)|$ であるのに対し，右辺が $|Q_a(x\,;\,k,\,v)|$ の和で書けてしまっている点である。つまり，mod pq の問題が mod p の問題に書き換えられたことを意味する。しかしその計算に必要な $|Q_a(x\,;\,k,\,v)|$ の方の剰余類は $\equiv D \pmod{4D}$ 等と複雑になり，しかもその D がすべての奇数を動くという状況になった。

これを計算するにあたって問題になるのは，右辺第 3 項と 4 項の厄介な無限級数である。ところが a について定理 2 に置いた仮定を置くと，実は $|Q_a(x\,;\,4D,\,D)| = |Q_a(x\,;\,4D,\,3D)|$ となって，むつかしい項が消えてしまうのである。定理 2 が最初に得られたのはこうした事情による。a がもっと複雑になると第 3 項や第 4 項からも密度に寄与する部分が出てきて，計算は飛躍的に面倒になるだろう。

以上，剰余位数についてこれまで分かってきたことを略述してきた。こうして解説記事を書いてみても，まだ周辺的なことしか分かっておらず，本当に知りたい部分へはかなり距離がある感が強い。ただ，剰余類の位数というのは非常に魅力的でかつ重要なものであることは確信できる。今後もこの方向の研究を続けていきたい。

理論値と実験値との比較（mod pq の場合）

$a=5$ の場合の，理論値（上）と実測値（下）

$v=0$	$v=1$	$v=2$	$v=3$
$\frac{5}{9}$	$\frac{1}{18}$	$\frac{1}{3}$	$\frac{1}{18}$
0.555538	0.055638	0.333186	0.055638

$a=12=2^2\cdot 3$ の場合の，理論値（上）と実測値（下）

$v=0$	$v=1$	$v=2$	$v=3$
$\frac{5}{9}$	$\frac{1}{18}$	$\frac{1}{3}$	$\frac{1}{18}$
0.555667	0.055590	0.333154	0.055590

$a=2$ の場合の実測値（理論値はまだ計算できていない）

$v=0$	$v=1$	$v=2$	$v=3$
0.659746	0.050637	0.255088	0.034528

参考文献

［1］ Koji Chinen-Leo Murata, On a distribution property of the residual order of a(mod p), J. of Number Theory 105 (2004) 60–81.

［2］ Koji Chinen-Leo Murata, On a distribution property of the residual order of a(mod p) III, J. Math. Soc. Japan 58–3 (2006) 693–720.

［3］ Koji Chinen-Leo Murata, On a distribution property of the residual order of a(mod p) IV, "Number Theory-Tradition and Modernization" Springer Science, (2006) 11–22.

［4］ Koji Chinen-Leo Murata, On a distribution property of the residual order of a(mod pq), (pre-print).

［5］ H. Hasse, 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. Unteilbarer Ordnung mod p ist, Math. Ann. 162 (1965) 74–76.

［6］ H. Hasse, 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 (1967) 19–23.

［7］ C. Hooley, On Artin's conjecture, J. Reine Angew. Math., 225 (1967) 209–220.

［8］ H.W. Lenstra Jr., On Artin's conjecture and Euclid's algorithm in global fields, Inventiones Math. 43 (1977) 201–224.

［9］ S. Li-C. Pomerance, On generalizing Artin's conjecture on primitive roots to composite moduli, J. Reine Angew. Math., 556 (203), 205–224.

［10］ Leo Murata, A problem analogous to Artin's conjecture for primitive roots and its applications, Arch. Math., (1991) 555–565.

［11］ Leo Murata-Koji Chinen, On a distribution property of the residual order of a(mod p) II, J. of Number Theory 105 (2004) 82–100.

［12］ Leo Murata-Carl Pomerance, On the largest prime factor of a Mersenne number, CRM (Centre de Recherches Mathématiques) Proceedings and Lecture Notes, Vol. 36 (2004) 209–218.

［13］ 村田玲音，a(mod p) の剰余位数が素数になっているような素数 p の分布について，明治学院論叢　第 700 号　総合科学研究　第 70 号，2004 年 3 月，121–131。

［14］ R.W.K. Odoni, A conjecture of Krishnamurty on decimal periods and some allied problems, J. Number Theory 13 (1981) 303–319.