福井工業大学研究紀要　第28号　1998

循環小数と素数分布

古田孝臣*・雪本義人**

Recurring Decimals and Prime Distribution

Yoshiomi Furuta and Yoshito Yukimoto

The purpose of this paper is to characterize prime numbers p by means of recurring decimals of their inverse fractional numbers $1/p$. This problem is equivalent to characterize p by means of solvability of Diophantine equation $x^n + py = 10$, where $n = (p-1)/\lambda$, λ being the length of recurring part of the decimal $1/p$. The problem is trivial in the case of $n = 1$, and is easy in the case of $n = 2$ by using the quadartic reciprocity law. However it is difficult in the case of $n > 2$, especially of $n > 4$, because of no sufficient theory such as class field theory for non-abelian extensions related to the above Diophantine equation. The present paper mainly deals with the case of $n = 2$, 3 and $n = 4$.

序.　素数 p の逆数 $1/p$ を小数表示したときの循環部分に現れる数の個数，即ち循環節の長さを基にして，素数を分類し，その類に属する素数の構造を調べたい．$1/p$ の循環節の長さを λ とするとき，λ は $p-1$ の約数であり，$n=(p-1)/\lambda$ とおくとき，この問題は，例えば１０進小数の場合なら，指定された自然数 n にたいして $x^n+py=10$ が整数解 x, y を持つような素数 p を分類せよという問題と同値である．$n=1$ の場合は自明であり，$n=2$ の場合は平方剰余の相互法則を用いることによって，該当する素数は 40 で割ったら余りが $1,3,9,13,27,31,37,39$ のいずれかになる素数であることが判る．しかし，n が 3 以上の場合にはこのように簡明な結果は得られない．このことは代数的整数論によれば，上の不定方程式の可解性は有理数体に 10 の n 乗根を添加して出来る代数体で素数 p がどのように素イデアル分解されるかという問題と同等であるが，n が 3 以上の場合には出てくる代数体が有理数体上アーベル拡大ではなく，従って類体論のみで単純には解決出来ないということによる．１９２０年に高木貞治によって類体論が完成されてから，アーベル拡大でない場合に類体論を拡張することが試みられているが，その過程において３５０年来の懸案であったフェルマー問題が近年その解決を見たとはいえ，類体論の拡張の道は未だ遠しの感がある．

上のような不定方程式の可解性は古くから興味を持たれており，非アーベル拡大の問題という意味で現在でも関心の深い問題である．不定方程式の可解性と循環小数との関わりも古くから関心が持たれていたのであろうが，上のような形での関わりを少なくとも著者達は知らなかった．著者達がこのような形での関心を持ったのは，数学愛好家である平間年雄氏が素数の逆数の循環小数について多くの計算をされて，その観察からいくつかの規則を見いだされ，それが著者達に伝えられたことが発端である．平間年雄氏はかつて戦時中に金子曽政元金沢大学長と共に外地で過ごされたことがあり，そのつながりから，さらに木戸睦彦元金沢大学数学教授を経て著者達にその計算結果が伝えられた．このようにして，上の形の不定方程式の研究に新たな刺激を与えられたことに感謝したい．

＊機械工学科　＊＊電気工学科

§1. 循環節の長さ

循環小数に関して次の定理が知られている.

定理 1.1([7,Theorem 10.6])

b を正の整数とする. α は互いに素な正の整数 r と s によって $\alpha=\frac{r}{s}$ と書かれ $0<\alpha<1$ であるものとする. ここで, s を b の素因数のみの積からなる整数 T と b と素な整数 U によって, その積に $s=TU$ と分解する. そして, ν を $b^\nu-1$ が U で割り切れるような最小の べき とし, N を b^N が T で割り切れるような最小の べき とする.

すると, α を b-進小数に表すとき, $0.00...a_Na_{N-1}...a_1$ の形の後 $c_1c_2...c_\nu$ の形で循環する.

この定理の証明については, 先ず次のことに注意する. N は b^N が T で割り切れるような最小の べき ということから, $b^N=aT$ となる整数 a があり,

$$b^N\alpha=b^N\frac{r}{TU}=\frac{ar}{U}=A+\frac{C}{U}$$

となる整数 A と C が

$$0\le A<b^N,\qquad 0<C<U$$

となるようにとれ, この A を b−進展開して, $0.00...a_Na_{N-1}...a_1$ の部分が得られる. 循環部分の証明については, 循環節に現れる数の組の型の個数に関する主張の追加を含めて, 以下で法 s の既約剰余類群による簡易化した証明を与える. この追加部分の主張は, 通常の１０進小数の場合に s が素数のとき平間年雄氏が多くの実例計算によって実験的に発見したものである.

定理 1.2　s と b は互いに素な正の整数とする. このとき, 1 以下の既約分数 $\frac{r}{s}$ の b−進小数表示に現れる循環節の長さは分子 r によらず一定であり, その長さを λ とすると, λ は $b^\nu\equiv 1 \mod s$ となる最小値 ν に一致し, 循環節に現れる数の組の型の個数を γ とするとき, 同じ型を持つ分子は同数個あって, $\lambda\gamma=\phi(s)$ となる.

(証明)　有理整数環 $\mathbf{Z}$ の法 s による既約剰余類群を G とする. G は位数 $\phi(s)$ の群であるが, その中で b で生成される部分群を B とおき, B の位数を m とすると, m は $\phi(s)$ の約数である. 分数 $\frac{1}{s}$ の b−進小数の長さは, b を s で割った剰余を r_1, r_1b を s で割った剰余を r_2, 以下同様に r_ib を s で割った剰余を r_{i+1} とするとき, 同じ剰余が再び現れる区間の長さの最小値に一致する. $r_i\equiv b^i \mod s$ だから, これら剰余の全体は b で生成される部分群 B に一致する. $r_i\equiv r_j \mod s$ とすれば $b^i\equiv b^j \mod s$, 従って $b^{i-j}\equiv 1 \mod s$ であり, $i-j$ は b の位数 m の倍数となる. 一方 $b^m\equiv 1 \mod s$ より $r_m=1$ となるから, $\frac{1}{s}$ の b−進小数の長さは b で生成される部分群 B の位数 m に一致する.

r が s と素のとき, 既約分数 $\frac{r}{s}$ の b−進小数を求めるときの剰余も $rb^i \mod s$ で表されるから, それらは剰余類別 G/B において r を含む類に一致する. これより定理の主張が得られる. 即ち $\lambda=m$ で, γ は剰余類群 G/B の位数に等しく $\lambda\gamma=\phi(s)$ となる. (証明終わり)

この定理から次のことが得られる ([1,10.1,Problem 22]).

系 1.3　素数 p にたいして $\frac{1}{p}$ の b−進小数の循環節の長さが偶数 $k=2t$ で循環節が $c_1c_2...c_k$ なら $j=1,2,...,t$ に対して $c_j+c_{j+t}=b-1$ である.

（証明）　$\dfrac{1}{p}$ の循環節の長さが $2t$ とすると $p|(b^{2t}-1)$ かつ $p\nmid(b^t-1)$ であり，$b^{2t}-1=(b^t+1)(b^t-1)$ だから $p|(b^t+1)$ である．よって $a=\dfrac{1}{p}(b^t+1)$ とおけば a は整数であり，a の循環節は c_j+c_{j+t} $(j=1\cdots t)$ であるが，

$$1=\frac{b-1}{b-1}=(b-1)\frac{\frac{1}{b}}{1-\frac{1}{b}}=(b-1)(\frac{1}{b}+\frac{1}{b^2}+\cdots)$$

だから $a=(a-1)+1$ の循環節は $c_j+c_{j+t}=b-1$ $(j=1\cdots t)$ となる．

§2．循環節の長さと拡大体

正の整数 b を 1 つ固定する．素数 p に対して，p を分母とする有理数の $b-$進小数展開における循環節の長さ λ は上の定理により，

$$b^{\nu}\equiv 1 \mod p \tag{2.1}$$

を満たす最小自然数 ν として与えられる．

以下，式 (2.1) を満たす ν の最小値 λ を $\lambda_b(p)$ で表し，$\gamma_b(p)=\dfrac{p-1}{\lambda_b(p)}$ と置くことにする．$\gamma_b(p)$ は定理 1.2 により，p と互いに素な正の整数 r にたいして，$\dfrac{r}{p}$ の b 進小数表示に現れる循環節の異なる組の型の個数である．これを底 b にたいする p の 循環節類数 と呼ぼう．

自然数 λ や $\gamma=\dfrac{p-1}{\lambda}$ が与えられたとき，それらが $\dfrac{1}{p}$ の $b-$進循環節の長さや $\dfrac{r}{p}$ の相異なる循環節の型の個数となるような素数 p はどのようなものであるかという問題が考えられる．

p を法とする既約剰余類は位数 $p-1$ の巡回群であり，その生成元の代表となる整数，即ち法 p の原始根の 1 つを g とすると，$\gamma_b(p)=m$ であることは $b\equiv g^m \mod p$ と同値である．従って，$\gamma_b(p)$ が m の倍数であることは

$$x^m\equiv b \mod p \tag{2.2}$$

が整数解 x を持つことと同値である．

さらに体論的には，Frobenius 置換の性質より次の定理が示される．

定理 2.1　$\gamma_b(p)$ が m の倍数であることは，ζ_m を 1 の原始 m 乗根とするとき，有理数体 $\mathbf{Q}$ 上のガロア拡大 $\mathbf{Q}(\zeta_m, \sqrt[m]{b})$ において p が完全分解することと同値である．

（証明）　$\gamma_b(p)$ が m の倍数とすると，$p\equiv 1 \mod m$ が必要であり，従って p は $\mathbf{Q}$ 上の m 分体 $\mathbf{Q}(\zeta_m)$ で完全分解する．従って $\mathbf{Q}(\zeta_m)$ における p の素因子を $\mathfrak{p}$ とすれば，その $\mathbf{Q}$ へのノルムは $N\mathfrak{p}=p$ である．$\mathfrak{P}$ を $\mathbf{Q}(\zeta_m, \sqrt[m]{b})$ における $\mathfrak{p}$ の素因子とすれば (2.2) より $\sqrt[m]{b}^{N\mathfrak{p}}=\sqrt[m]{b}^{p}\equiv\sqrt[m]{b} \mod \mathfrak{P}$ となるから，Frobenius 置換の性質より $\mathfrak{p}$ 従って p は $\mathbf{Q}(\zeta_m, \sqrt[m]{b})$ において完全分解する．よって定理の必要性が示されたが，逆をたどれば充分性も従う．（証明終わり）

さらに，Galois 拡大で分解する素イデアルの密度に関する Tschebotareff の定理より次の定理が得られる．

定理 2.2 $\gamma_b(p)$ が m の倍数であるような素数 p の密度は拡大 $\mathbf{Q}(\zeta_m,\ \sqrt[m]{b})$ の拡大次数の逆数に等しい．

§3. 循環節類数と素イデアル分解 1

m が 3 以上のとき，ガロア拡大 $\mathbf{Q}(\zeta_m,\ \sqrt[m]{b})$ は一般に非アーベル拡大である．そこで完全分解する素数の密度は前節の定理 2.2 のように与えられるが，それらの素数を簡明な式で類別するというようなことは一般には類体論を越える問題であって，現在の代数的整数論の核心的問題にもつながるものである．それだけに，指定された循環節類数を持つ素数の具体的分類に興味がある．

$m=2,3,4$ の場合には $\mathbf{Q}(\zeta_m)$ が有理数体や 2 次体であり，そこにおける m 乗剰余を扱うことが可能であり，それによって循環節類数が m の倍数であるような素数を知ることが出来る．

［$\gamma_b(p)=1$ のとき，従って $\lambda_b(p)=p-1$ とき］　これは b が法 p の原始根となるような素数 p はどのようなものであるかという問題であり，円分論で言えば，法 p の剰余類において b を含む剰余類に属する素数が素に留まるような p 円分体はどのようなものであるかという問題である．これは一般的には難しい問題であるが，特殊な場合については，次のようなことが知られている．

p が Fermat 型素数，即ち $p=2^n+1$ と表せる素数のとき，(このときは必然的に n が 2 の べき 即ち $n=2^m$ と表せて)，$p=5$ のときを除けば 5 が Fermat 型素数 p の原始根であり，$p=3$ のときを除けば 7 が Fermat 素数 p の原始根である．(Cf. [5,p.51])

これより，次のことが従う．

定理 3.1 p が Fermat 型素数のときは，$\dfrac{1}{p}$ の 5−進小数表示や 7−進小数表示では，その循環節の長さは恒に $p-1$ である．

［γ が 2 の倍数のとき］　このときは式 (2.2) は

$$x^2 \equiv b \mod p \tag{3.1}$$

であり，平方剰余記号を用いれば

$$\left(\frac{b}{p}\right)=1$$

ということである．平方剰余相互法則

$$\left(\frac{b}{p}\right)\left(\frac{p}{b}\right)=(-1)^{\frac{p-1}{2}\frac{b-1}{2}}$$

より，特に b が奇素数のとき，次のことが従う．

定理 3.2 b 及び p が奇素数のときは，p が $4n+1$ の形か $4n-1$ の形かに従って $p^*=p$ または $p^*=-p$ とおくとき，p^* が法 b の平方類に属することが $\gamma_b(p)$ が偶数であるために必要十分である．

b が奇素数と限らぬとき，例えば通常の $b=10$ のときは平方剰余記号の乗法性と平方剰余相互法則の補充法則も用いて

$$\left(\frac{10}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{5}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{p}{5}\right)$$

である．この値が 1 であるためには p が $8n\pm1$ の型なら，さらに $p=5n\pm1$ の型であることが必要充分であり，p が $8n\pm3$ の型なら，さらに $p=5n\pm3$ の型であることが必要充分である．この条件をまとめて，

定理 3.3 奇素数 p の逆数 $1/p$ の 10 進小数表示における循環節類数が偶数であるためには

$$p\equiv 1,3,9,13,27,31,37,39 \mod 40$$

であることが必要十分である．

次に，素数 p の循環節類数が 3 や 4 の倍数であるための条件は，円分体 $\mathbf{Q}(\zeta_3)$ や $\mathbf{Q}(\zeta_4)$ が類数 1 の 2 次体なので，そこにおける p の素因数についての 3 乗剰余や 4 乗剰余の相互法則（文献 [3]，[6]）を用いて $\mathbf{Q}(\zeta_m,\sqrt[m]{b})$ での分解の様子を見ればよい．

［γ が 3 の倍数のとき］ 円分体 $\mathbf{Q}(\zeta_3)$ は 2 次体 $\mathbf{Q}(\sqrt{-3})$ に等しく，そこでの 3 乗剰余の相互法則を用いる．$\gamma_{10}(p)$ が 3 の倍数となるような素数 p を知るには p の $\mathbf{Q}(\sqrt{-3})$ における素因数を π とするとき 3 乗剰余記号 $\left(\frac{10}{\pi}\right)_3=1$ となる p を求めればよい．$\pi=a+b\zeta_3$ となる有理整数 a,b 従って $p=a^2+ab+b^2$ である a,b を $\pi\equiv-1 \mod 3$ となるようにとることができるが，この π について 3 乗剰余の相互法則を用いれば

$$\left(\frac{10}{\pi}\right)_3=\left(\frac{2}{\pi}\right)_3\left(\frac{5}{\pi}\right)_3=\left(\frac{\pi}{2}\right)_3\left(\frac{\pi}{5}\right)_3$$

となる．さらに

$$\left(\frac{\pi}{2}\right)_3=\zeta_3^t \iff \pi\equiv\zeta_3^t \mod 2$$

$$\left(\frac{\pi}{5}\right)_3=\zeta_3^t \iff \pi^8\equiv\zeta_3^t \mod 5$$

によって $\left(\frac{10}{\pi}\right)_3$ の値が求められる．

［γ が 4 の倍数のとき］ 円分体 $\mathbf{Q}(\zeta_4)$ は 2 次体 $\mathbf{Q}(i)$ に等しく，そこでの 4 乗剰余の相互法則を用いる．$\gamma_{10}(p)$ が 4 の倍数となるような素数 p を知るには p の $\mathbf{Q}(i)$ における素因数を π とするとき $\left(\frac{10}{\pi}\right)_4=1$ となる p を求めればよい．$\pi=a+bi$ となる有理整数 a,b 従って $p=a^2+b^2$ である a,b を $\pi\equiv1 \mod (1+i)^3$ となるようにとることができるが，この π について 4 乗剰余の相互法則を用いる．$5=(-1+2i)(-1-2i)$ であるから

$$\left(\frac{10}{\pi}\right)_4=\left(\frac{2}{\pi}\right)_4\left(\frac{-1+2i}{\pi}\right)_4\left(\frac{-1-2i}{\pi}\right)_4$$

となるが $-1\pm 2i\equiv 1 \mod (1+i)^3$ なので 4 乗剰余の相互法則より

$$\left(\frac{2}{\pi}\right)_4 = i^{-b/2}, \quad \left(\frac{-1\pm 2i}{\pi}\right)_4 = (-1)^{(a-1)/2}\left(\frac{\pi}{-1\pm 2i}\right)_4$$

である．さらに，第 2 式は π を法 5 で簡約し，補充法則より

$$\left(\frac{i}{-1\pm 2i}\right)_4 = i, \quad \left(\frac{1-i}{-1+2i}\right)_4 = i, \quad \left(\frac{1-i}{-1-2i}\right)_4 = -1$$

であることを用いて $\left(\frac{10}{\pi}\right)_4$ の値が求められる．

§4. 循環節類数と素イデアル分解 2

γ が 4 の倍数のとき，$\mathbf{Q}(\zeta_4, \sqrt[4]{b})$ における素イデアル分解法則を得るためには，前節末にふれたように，ガウス数体 $\mathbf{Q}(i)$ での 4 乗剰余法則の具体的形を知ればよいが，そのことがさらに一般な中心拡大における素イデアル分解法則の発展につながることが期待される．次のことが文献 [2] より導かれる．

$K=\mathbf{Q}(\sqrt{d_1}, \sqrt{d_2})$ を (2,2) 型アーベル体とし，$K_0=\mathbf{Q}(\sqrt{d_1d_2})$ とおく．m を $K/\mathbf{Q}$ に対して **abundant conductor** とし，M を K 上 mod m ray class field とする．K^* 及び $\widehat{K}$ を M における $K/\mathbf{Q}$ の種拡大及び（最大）中心拡大とする．即ち，M_0 を $M/\mathbf{Q}$ の中間体で $\mathbf{Q}$ 上最大のアーベル拡大とするとき，$K^*=KM_0$ であり，$\widehat{K}$ は $M/\mathbf{Q}$ の中間体で $\mathrm{Gal}(\widehat{K}/K)$ が $\mathrm{Gal}(\widehat{K}/\mathbf{Q})$ の中心な含まれるような最大の体である．m が $K/\mathbf{Q}$ に対して **abundant conductor** であるということは，今の場合 $\widehat{K}/K^*$ が 2 次拡大ということと同値である．

D を 2 次体 $K_0=\mathbf{Q}(\sqrt{d_1d_2})$ の判別式とする．　m と素な K_0 の整イデアルのノルムとなっているような有理整数 a にたいして

$$H(D,m,a)=\left\{\frac{ax^2+bxy+cy^2}{a}\in\mathbf{Z}\,;\,b,c,x,y\in\mathbf{Z},\right. \qquad (4.1)$$
$$\left. b^2-4ac=D,\ x\equiv 1, y\equiv 0 \mod m\right\}$$

とおく．

定理 4.1([2, Theorem 2.1]).　有理素数 p が種拡大 K^* で完全分解するためには，ある a によって $p\in H(D,m,a)$ であることが必要十分であり，p がさらに中心拡大 $\widehat{K}$ でも完全分解するためには a が $\left(\frac{d_1}{a}\right)=1$ を満たすことが必要十分である．

この定理を，$b=10$ のときに適用しよう．$\mathbf{Q}(\zeta_4, \sqrt[4]{10})$ を含むような拡大 M としては $d_1=-1, d_2=10$ とし $m=-40$ ととればよいことが [1, Proposition 3.4] より導かれる．このとき，K^* で完全分解する素数 p については，p が $\widehat{K}$ で完全分解することと $\mathbf{Q}(\zeta_4, \sqrt[4]{10})$ で完全分解することとは同値である．

一方，種拡大 K^* は $\mathbf{Q}$ 上の法 m の ray class field となるから，素数 p が K^* で完全分解するための条件は $p \equiv 1 \mod 40$ である．さらに $\mathbf{Q}(\sqrt{10})$ の判別式は -40 である．よって，$p \equiv 1 \mod 40$ を満たす素数 p にたいしては，p が $\mathbf{Q}(\zeta_4, \sqrt[4]{10})$ で完全分解するための条件は $-10 = b^2 - 4ac$ かつ $\left(\dfrac{-1}{a}\right) = 1$ 従って $a \equiv 1 \mod 4$ を満たす整数 a, b, c の組について p が $x \equiv 1, y \equiv 0 \mod m$ を満たす $x, y \in \mathbf{Z}$ によって

$$\frac{ax^2 + bxy + cy^2}{a} \in \mathbf{Z}$$

で表されることである．

$\gamma_{10}(p)$ が 4 の倍数となる素数 p についてはは $p \equiv 1 \mod 4$ が必要であるが，上で求めたのは $p \equiv 1 \mod 40$ を満たす場合であって，求めるべき素数の中で密度 1/10 に過ぎない．$p \equiv 1 \mod 40$ を満たさない場合についても，個々の素数 p については前節の方法で $\gamma_{10}(p)$ が 4 の倍数となるかどうかの判定が出来るが，それと中心拡大としての一般的方法との関連に興味がある．これはなお今後の課題であるが，次のことが言える．

命題 4.2 7 以上の素数 p が $\mathbf{Q}(\zeta_4, \sqrt[4]{10})$ で完全分解するためには p が $\mathbf{Q}(\zeta_4, \sqrt{10})$ で完全分解し，さらに $\mathbf{Q}(\zeta_4, \sqrt[4]{5})$ 及び $\mathbf{Q}(\zeta_4, \sqrt[4]{2})$ で共に完全分解するかまたは共に不分解であることが必要であり，p が $\mathbf{Q}(\sqrt{5})$ で分解するときはそれらが十分でもある．

これを循環節類数について述べれば，

命題 4.3 $\gamma_{10}(p)$ が 4 の倍数であるためには，

$$p \equiv 1, 9, 13, 37 \mod 40$$

であって，さらに $\gamma_5(p)$ と $\gamma_2(p)$ がともに 4 の倍数，またはともに 4 の倍数ではないことが必要であり，$p \equiv 1, 9 \mod 40$ のときにはこれが十分でもある．

$\gamma_5(p)$ や $\gamma_2(p)$ が 4 の倍数であるための条件としては，ガウス数体の 4 乗剰余の具体的形を調べることによって得られるが，ある合同条件を満たすような 1 部の素数については，その条件が $\gamma_{10}(p)$ の場合と同じようにして求められる．これら 2 つの方法の共通部分を分析することによって，素イデアル分解に基ずく素数の分類をさらに一般の中心拡大の場合に広げる可能性が期待される．このことに関連して b が素数である場合には次のことが数値的な実証とともに種々の状況からみて正しいと予想される．しかしながらその証明は未だ完成されていない．

［1］ $\gamma_5(p)$ が 4 の倍数である，従って p が $\mathbf{Q}(\zeta_4, \sqrt[4]{5})$ で完全分解するためには $p = \dfrac{29x^2 + 26xy + 6y^2}{29}$ が次の条件を満たすような整数 x, y で成立することが必要十分である．

$p \equiv 1 \mod 10$ で y は偶数

または

$p \equiv -1 \mod 10$ で y は奇数

［2］ $\gamma_2(p)$ が 4 の倍数である，従って p が $\mathbf{Q}(\zeta_4, \sqrt[4]{2})$ で完全分解するためには $p = \dfrac{17x^2 + 14xy + 3y^2}{17}$ が次の条件を満たすような素数 p と整数 x, y で成立することが必要十分である．

p mod 16	x mod 8	y mod 8
1	1	0
1	3	4
1	5	4
1	7	0
9	1	2
9	3	2
9	5	6
9	7	6

参 考 文 献

[1] Y. Furuta, A prime decomposition symbol for a non-abelian central extension which is abelian over a bicyclic biquadratic field, Nagoya Math. J.,79(1980),79-109.

[2] Y. Furuta and T. Kubota, Central extensions and rational quadratic forms, Nagoya Math. J.,130(1993),177-182.

[3] H. Hasse, Bericht Über Neuere Untersuchungen und Probleme aus der Theorie der Algebraishen Zahlkörper, Jahresberichit der Deutschen Mathematiker-Vereinigung, 1930.

[4] 木田祐司・牧野潔夫, UBASIC によるコンピュータ整数論, 日本評論社, 1994.

[5] N. Koblitz, A Couse in Number Theory and Cryptography, Springer-Verlag, 1994.

[6] 倉田令二郎, 平方剰余の相互法則, 日本評論社, 1992.

[7] K. H. Rosen, Elementary Number Theory and its Applications, Addison-Wesley Publ. Co., 1984.

(平成９年11月19日受理)