

Fermat 商と「数の微分」について

京都大学 数理解析研究所

伊原 康隆
Yasutaka Ihara

k を代数体, α を k^x の元, p を k の有限素点とし,
 $(\alpha, p) = 1$ とすると「フェルマの小定理」により 常に
 $\alpha^{N(p)-1} \equiv 1 \pmod{p}$ が成立しますが, α ($\neq 1$ の中根) を 固定
して p を動かすとき

$$(1)_\alpha \quad \alpha^{N(p)-1} \equiv 1 \pmod{p^2}$$

を満たす p はどの位あるか (有限個? 無限個?), 又 这样的 p
全体の集合は如何なる構造をもつのか, という古くからの
問題に関しては, いまだに部分的解答すら与えられていない
ようです. $k = \mathbb{Q}$ (有理数体) a のとき, 小さな自然数 $a > 1$
に対して $(1)_a$ (即ち $a^{p-1} \equiv 1 \pmod{p^2}$) を満たす素数 p の列
としては,

$$a=2 \text{ では } p=1093, 3511 \text{ の } 2 \text{ つが } p < 3 \times 10^9 \text{ の範囲で,}$$

$$a=3: \quad p=11, 1006003 \quad (p < 2^{30} \sim 1.07 \times 10^9)$$

$$a=5: \quad p=20771, 40487, 53471161 \quad (p < 2^{29})$$

$$a=6: \quad p=66161, 534851, 3152573 \quad (p < 2^{28})$$

などが知られています ([BTW] など).

この問題は古く Abel も注目しており、又 Fermat の問題の「 $n=1$ の場合」との関係によってもよく知られています (β3)。さて §1 で述べるように、合同式 $(1)_\alpha$ を満たす素数 p は“微分 $d\alpha$ ”の零素と見做すことが出来るので、この問題はそれ程人工的なものではなく、代数体と関数体との類似がどこ迄「成立つ」のか、という整数論の永遠の主題の一つであるとも考えられます。しかし現代数学の既成理論の中にその解答を示唆してくれそうなものは (私には) 見当りません。そこで「 $(1)_\alpha$ を満たす p の全体は何らかのよい構造を有するであろう」という事は信じた上で、その構造を調べる為に (たとえ荒唐無稽であっても) いくつかの仮説を立てては数値実験を試みるという事が大いに望まれるのではないかと思います。ここでは

§1 数の微分 $d\alpha$ 、微分商 $\frac{d\beta}{d\alpha}$ の (仮の) 定義を与えて上の問題をその言葉に翻訳して眺めた上で;

§2 それらに関する三通りの可能性について論じ;

§3 問題の周辺への言及と

§4 他の方々による数値計算の結果の一部の紹介

をさせていただきます。残念ながら、三つの可能性のどれが正しいか (或は、どれも正しくないか) は今迄の計算では判断できません。

まとまりのない話ですが、この主題に興味を持たれる
きっかけにでもなれば幸いです。

§1 $d\alpha, \frac{d\beta}{d\alpha}$ の (仮の) 定義.

代数体 k の各有限素数 p に対して k_p を k の p 進完備
化, ord_p をその標準加法付値, $k_p = \mathbb{F}_q$ を剰余体 ($q = Np$),
 k_p, k_p^\times の Teichmüller liftings を

$$\Delta_p = \{\eta \in k_p; \eta^q = \eta\}, \quad \Delta_p^\times = \Delta_p - \{0\}$$

とおきます。

各 $\alpha \in k$; $\text{ord}_p \alpha \geq 0$ に対して $\alpha \equiv \alpha(p) \pmod{p}$ とする
 $\alpha(p) \in \Delta_p$ が唯一存在するので、この $\alpha(p)$ を (関数体との
類似により) “南数” α が “素” p でとる値と見ます。

ただ、関数体の場合との基本的相違点は (i) Δ_p が
加法的には閉じていない (ii) 剰余標数の異なる p に対する
 k_p は素体までもが異なる体である、という二点で、このように
両者の間にはもっと大きな基本的相違がある事を (当たり前
前ではあるが) この際再確認しておきます。

さて $\alpha - \alpha(p)$ の定める \mathbb{F}/p^2 の元は α の p に於る微分と
見做せまゝから、

$$(d\alpha)_p := \alpha - \alpha(p) \pmod{p^2} \in \mathbb{F}/p^2$$

と定めます。ただし $\text{ord}_p \alpha < 0$ のときは (-応) $(d\alpha)_p = \infty$

と置く事にします。

また、2つの元 $\alpha, \beta \in k$ ($\alpha \neq 0, \neq 1$ の中根) に対して \mathcal{P} に於る微分商 $(\frac{d\beta}{d\alpha})_{\mathcal{P}} \in k_{\mathcal{P}} \cup (\infty)$ を、

$$\left(\frac{d\beta}{d\alpha}\right)_{\mathcal{P}} := \frac{\beta - \beta(\mathcal{P})}{\alpha - \alpha(\mathcal{P})} \pmod{\mathcal{P}}$$

と定めます。ただし、 α が \mathcal{P} 整でないときは $\alpha(\mathcal{P}) = 0$ としす (β も同様)。

$\Delta_{\mathcal{P}}$ が乗法的に閉じている事より、 $\text{ord}_{\mathcal{P}} \alpha, \text{ord}_{\mathcal{P}} \beta \geq 0$ なら

$$d(\alpha\beta)_{\mathcal{P}} = \alpha(d\beta)_{\mathcal{P}} + \beta(d\alpha)_{\mathcal{P}} \quad (\text{in } \mathcal{P}/\mathcal{P}^2)$$

が成立しますが、加法的には閉じていない事を反映して、一般には

$$d(\alpha + \beta)_{\mathcal{P}} \neq (d\alpha)_{\mathcal{P}} + (d\beta)_{\mathcal{P}}$$

(例えは $(d2)_{\mathcal{P}} \neq 0$)。特に、この意味の微分は、 k/\mathbb{Q} の分岐の情報のみを伝えている小体の微分加群 $\Omega_{\mathbb{Q}/\mathbb{Z}}^1, \Omega_{\mathcal{O}_{\mathcal{P}}/\mathbb{Z}_p}^1$ とは別種のもので、 $(\mathcal{O}, \mathcal{O}_{\mathcal{P}}$ は $k, k_{\mathcal{P}}$ の整数環; $\Omega_{\mathbb{Q}/\mathbb{Z}}^1$ (resp. $\Omega_{\mathcal{O}_{\mathcal{P}}/\mathbb{Z}_p}^1$) は \mathbb{Q} (resp. $\mathcal{O}_{\mathcal{P}}$)-加群として $\simeq \mathbb{Q}/\mathbb{Z}$ (resp. $\mathcal{O}_{\mathcal{P}}/\mathbb{Z}_p$) であつた。ただし $\delta, \delta_{\mathcal{P}}$ は $k/\mathbb{Q}, k_{\mathcal{P}}/\mathbb{Q}_p$ の共役差積イデアル)。

上記の定義は、 $k_{\mathcal{P}}/\mathbb{Q}_p$ の分岐の状況によって、多少の修正を要する可能性は十分あります。尚 $\text{ord}_{\mathcal{P}} \alpha = 0$ なら明らかに

$$(d\alpha)_{\mathcal{P}} = 0 \iff \alpha^{N_{\mathcal{P}}-1} \equiv 1 \pmod{\mathcal{P}^2}$$

で、 n によって $(1)_{\alpha}$ を添う \mathcal{P} と $d\alpha$ の零兵が結びついています。

さて 各 $\alpha \in k$ に対して その微分 $d\alpha \in \Omega$, 各 p に対して $(d\alpha)_p \in \mathbb{F}_p \cup (\infty)$ を対応させる関数, と定義します。
 (一般に, 有限-次元結合 $\sum_i \gamma_i d\alpha_i$ ($\alpha_i, \gamma_i \in k$) を, 各 p で $\text{ord}_p \alpha_i, \text{ord}_p \gamma_i \geq 0$ なるものに対して \mathbb{F}_p に値をとる関数として定義する=とも(定義だけなら)出来るわけです。) 又, 2つの元 $\alpha, \beta \in k$ ($\alpha \neq 0, \neq 1$ の中核) に対して $\frac{d\beta}{d\alpha} \in \Omega$, 各 p に対して $(\frac{d\beta}{d\alpha})_p \in k_p \cup (\infty)$ を対応させる関数と定義します。では この意味の微分商 $\frac{d\beta}{d\alpha}$ (或いは, 一般に $\sum_i \gamma_i \frac{d\beta_i}{d\alpha_i}$) は, 加同値な性質をもつのでしょうか? それは k の各元 γ の与える関数 $p \rightarrow \gamma \pmod{p} \in k_p \cup (\infty)$ たちとは, どの位近い性質をもつ関数なのでしょうか? 各 $d\alpha$ の零点 p は有限個でしょうか, 無限個でしょうか。それらについて今のところ, どの一つの α ($\neq 0, \neq 1$ の中核) についてでも, 全く何もわかっていません。

次のような可能性 (P1)(P2), ... が考えられます。

(P = Possibility の略)

§2 可能性のいくつか; (P1)(P2)(P3)

(P1) 各 $\alpha \in k^x \setminus \{1\}$ の中程に対して $(d\alpha)_p = 0$ とする
 p は どれだけ有限個.

関数体の微分 ($\neq 0$) の 零兵の個数は有限ですから、「それ
 との類似性がここでも成立つか?」という問題も考えられます。
 尚、関数体の場合は微分因子の次数 = $2g-2$ ですが、
 代数体の場合には ($2g-2$ の類似 $\log |d_E|$ はあるか) $d\alpha$ の
 因子が自然に定義され得るものかどうかすら不明です。

$\text{ord}_p (d\alpha)_p$ が 各 p に対して定義できればよいわけですが、

★ k_p を有限次拡大 K_p でおまかえたときの望ましい(?) 関係

$$\text{ord}_p (d\alpha)_{K_p} = e \cdot \text{ord}_p (d\alpha)_p + \text{ord}_p \delta \quad \left(\begin{array}{l} e: \text{分岐指数} \\ \delta: \text{相対差積} \end{array} \right)$$

★★ α を α^n ($n \in \mathbb{Z}, n \neq 0$) でおまかえたときの望ましい(?) 関係

$$\text{ord}_p d(\alpha^n) = \text{ord}_p (n\alpha^{n-1}) + \text{ord}_p d\alpha,$$

の両方を満たす定義を与えることは出来ず、それが「自然な
 ものであるか、又 それも自然な $\text{ord}_p (d\alpha)_p$ が存在し得るかどうか
 などは、疑問です。又、 k_p が Archimedean のときには $\text{ord}_p (d\alpha)_p$
 を定義しようとする、 $|\alpha|_p = 1$ なる α に対しては、 $\text{ord}_p (d\alpha)_p =$
 $+\infty$ とせざるを得ないようです。

以下の「可能性2」は、 $(d\alpha)_f = 0$ とする f は無限個あったとしても α は以下の意味で「Abel的に ∞ に収束」して、各 α, β に対して関数 $f \mapsto \left(\frac{d\beta}{d\alpha}\right)_f$ は、 $\frac{d\beta}{d\alpha}$ の極と零点を併せて Weierstrass 因数分解が出来るのではなにか? という、これも一つの空想です。

まず、 k の有限素点の (一般には) 無限集合 P が「Galois 的 (resp. Abel 的) に ∞ に収束する」とは、 k の任意の有限次 Galois (resp. Abel) 拡大 K/k に対して P の有限部分集合 S_K が存在して、 $f \in P \setminus S_K$ なら f は K/k で完全分解すること、と定義します。類体論によって、 P が Abel 的に ∞ に収束するなら、 P に属する素イデアルは有限個を除いては単項でしか任意に与えられた k の modulus m に対してある有限集合 $S_m \subset P$ が存在して、 $f \in P \setminus S_m$ なら $f = (\pi)$; $\pi \equiv 1 \pmod{m}$ となります。

ついでに、(与えられた、 k の素イデアルからなる) 集合 P が Galois 的に ∞ に収束する為の必要十分条件が十分 explicit に書けるかどうかは「非-アベル類体論」に与った一つの試金石である、と云えるかもしれません。

[用語 (... ∞ に収束) について] 無限素点は K/k で殆んど完全分解することからつけた一時的なもの。

(P2) 任意の $\alpha \in k^x \setminus \{1\}$ に対して α を固定するとき,

(i) $(d\alpha)_p = 0$ とする p 全体の集合は Abel 的に ∞ に収束する.

(ii) 各 p に対して $\text{ord}_p(d\alpha)_p$ が有効に定義され, 特に $(d\alpha)_p = 0 \iff \text{ord}_p(d\alpha)_p > 0$.

(iii) (i) による形式積 $(d\alpha) = \prod_{p \text{ (有限素点)}} \text{ord}_p(d\alpha)_p$

は k の 1 つのイデアル類を定めるが, これは k の共役差積イデアル δ_k の属する類.

(iv) $\alpha, \beta \in k^x \setminus \{1\}$ とし, $m \in (d\alpha), (d\beta)$ と

無縁な k の square-free なイデアルとする. (i) によって $(d\alpha), (d\beta)$ は $znz^{-1} \pmod{m}$ の Strahl 類を定め, znz^{-1} については (iii) による単項類中へ, 形式因子 $(d\beta)/(d\alpha)$ は $(\mathcal{O}_k/m)^x / (\mathcal{O}_k^x \text{ の像})$ の一つの元を定めるが, この商数 $\left(\left(\frac{d\beta}{d\alpha} \right)_k \right)_{k|m}$ の定める元と一致.

(P3) 各 $\alpha \in \mathbb{Z}^x \setminus \{1\}$ の中根} に対して

$$\#\{p; (d\alpha)_p = 0, N(p) \leq x\} \sim \log \log x \quad (x \rightarrow \infty)$$

(\sim は、さし当たり 比 $\rightarrow 1$ 程度の弱い意味にておく).

これは、 \mathbb{Z}/p^2 内で任意に選ばれた元が 0 になる確率が $N(p)^{-1}$ であるとき、 α が固定されて p が動く場合の $(d\alpha)_p$ の分布にも適用できると (勝手に) 考えると たちちに導かれます。よく知られているように、

$$\sum_{p; N(p) \leq x} N(p)^{-1} \sim \log \log x$$

(この場合の \sim は 差 $= O(1)$ 。尚 $\log \log x$ の頭に $[x: \mathbb{Q}]$ はつかない)

ここで注意しなくてはならないのは、関数体の場合でも、同じ議論を用いれば同じ推測が生ずる、 x にも拘らず関数体のときは $(d\alpha)_p = 0$ となる p は有限個しかなく、という事である。

つまり、代数体と関数体をこの真に於て区別する何らかの根拠がないと、この確率論的推測は説得力がない、という感じである。

(P4) その他の可能性

[関係] (P1)と(P3)はそれぞれ $d\alpha$ の零点の個数が有限個, 無限個と主張しているので, 明らかに相反しています.

又 (P2)と(P3)も両立しません. なぜなら, $\alpha \in k$, K/k : 有限次アーベルとするとき, (P2)によれば $d\alpha$ の k での零点はほとんどすべて K/k で完全分解するので,

$$\{K \text{ の素数 } p; (d\alpha)_p = 0, N(p) \leq x\}$$

$$\cong [K:k] \{k \text{ の素数 } p; (d\alpha)_p = 0, N(p) \leq x\}$$

となり, 又 $x \sim \log \log x$ である事を主張する (P3)とは反するわけでは.

(P1)と(P2)が両立するかはわかりませんが, もし (P1)が成立し, かつ $d(2)$ 及び $d(3)$ の零点が既に知られている2つづつしかないと仮定すると (P2)の(iv)は成立しません.

§3 問題の周辺 (復習, 別の見方など)

フェルマの問題との関係 p を任意の素数とする. このとき
 $x^p + y^p + z^p = 0$, $p \nmid xyz$ なる $x, y, z \in \mathbb{Z}$ が存在すれば,
 $a^{p-1} \equiv 1 \pmod{p^2}$ がすべての $a \in \mathbb{Z}$, $(a, p) = 1$, $2 \leq a \leq 43$ に
 対して成立つ (Wieferich, ...). 従って特に ($a=2, 3$ に適用して)
 $p > 3 \times 10^9$ にならなければならない.....

d_2, d_3, \dots それぞれの零因子はかりに無限個あつて, 共通
 零因子となるとたかだか有限個しかなさないので ($\sum \frac{1}{p} = \infty$ で
 $\sum \frac{1}{p^2} < \infty$) が, 果してどうだろうか.

合同式 (1)_a の類体論による“解釈例” \mathbb{Q} の唯一の
 \mathbb{Z}_p 拡大 $K_p = \bigcup_{n=1}^{\infty} K_p^{(n)}$ ($[K_p^{(n)} : \mathbb{Q}] = p^n$) とするとき, 各
 素数 $l \neq p$ に対して, $l^{p-1} \equiv 1 \pmod{p^{n+1}} \iff l$ は $K_p^{(n)}$ で
 完全分解, ($n=1, l=2$ のとき更に書き直すと: S_{p^2} : 1 の原始 p^2 乗根,
 $\theta_p = \sum_{\delta \in \Delta_p} (\zeta_{p^2})^\delta \in K_p^{(1)}$, $N_{K_p^{(1)}/\mathbb{Q}}(\theta_p) = t_p$ とおくと, $t_p \in \mathbb{Z}$,
 $t_p \equiv -1 \pmod{p^2}$. この t_p を用いて上記相互律を書換えると:
 $2^{p-1} \equiv 1 \pmod{p^2} \iff t_p \equiv 0 \pmod{2}$

となります.)

従って すべての p に対する K_p の合成体を K とすると,
 $d(\ell)$ の零因子が有限個 $\iff K/\mathbb{Q}$ に於ける ℓ の延長は有限個.

また, ℓ が 類数 1 の実 2 次体で ε が ℓ の基本単数 のとき,
 ℓ の素イデアル \mathfrak{p} に対し,

$$\varepsilon^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}^2} \iff \ell \text{ は } \mathfrak{p} \text{ のみで分岐する } p\text{-} \text{ 次巡回拡大をもつ}$$

S. Hahn [H] は $K_p^{(1)}(\sqrt{-1})$ 上の ある 無限次不分岐 pro-2 拡大体を用いて, $\varepsilon^{p-1} \not\equiv 1 \pmod{p^2}$ 且つ $c(\log p)^2$ に比べて小さな ℓ の存在を (一般リーマン予想の仮定のもとで) 示している (c は絶対定数).

$\Delta_p \pmod{p^2}$ について: これについては §4 参照.

$|\Phi_n(\alpha)|$ の下からの評価: $d\alpha$ の零因子の問題はむしろ,

$\mu_\infty = \{\bar{\mathbb{Q}} \text{ 上の } 1 \text{ の中根全体}\}$ と α との間 の “距離” の評価の問題と捉える方が (少くともある意味では) 自然かも知れません. 云いかえると, 1 の原始 n 等分方程式 $\Phi_n(x)$ に対する $|\Phi_n(\alpha)|_v$ を種々の v と n に対して上下から評価する問題です.

例えば, 既に知られていることもかもしれませんが, $\ell = \mathbb{Q}$, $a \in \mathbb{Q}^\times - \{\pm 1\}$, d : a の分母 とするとき, \mathbb{R} の $|\cdot|_\infty$ についての $|\Phi_n(a)|_\infty$ の下からの評価 (初等的に証明できる)

$$\frac{d^{\varphi(n)}}{n} |\Phi_n(a)|_{\infty} > 1 \quad (n: \text{十分大})$$

と積公式を用いて次の事が示せます。 a を固定し $p \in \mathbb{N}$ が動かし

$$\{\text{素数}\} \ni p \longrightarrow a \pmod{p} \text{ の群 } (\mathbb{Z}/p)^{\times} \in \{\text{自然数}\} \text{ に於る位数}$$

は殆んど surjective (image の補集合は有限). この方法を refine して da の零点の研究にも使えるようになるば... というのも一つの課題です.

$$\underline{(p\text{-進 } \log)_{p \leq \infty}: \text{Idèles} \rightarrow \text{Adèles.}} \quad k \text{ の各有限素数 } p$$

に対して p -進対数関数 $\lambda_p: 1+p \rightarrow k_p$ は, $\lambda_p(\Delta_p^{\times})=0$ とおけるように $\mathcal{O}_p^{\times} \rightarrow k_p$ (準同型写像) に拡張せよ, $\alpha \in \mathcal{O}_p^{\times}$ なら

$$\begin{aligned} \lambda_p(\alpha) \equiv 0 \pmod{p} &\iff \lambda_p(\alpha^{N_p-1}) \equiv 0 \pmod{p} \\ &\iff \alpha^{N_p-1} \equiv 1 \pmod{p^2} \end{aligned}$$

(\iff は "大体". 例えは $\text{ord}_p p < p-1$ から成立.)

そこで, 今 p を動かして archimedean とおいておいた p -進 \log を並べたものを考えれば, (λ_p は, $k_p^{\times} \rightarrow k_p$ の自然な拡張を持つ) ということになるので) それは k の idele 群から adèle 群への準同型は与えられる, それにやがて近づくことになる. これによる global idèles k^{\times} の像が global adèles k の元でどのように "近似" されるか, というのも我々の問題の一つの自然な捉え方と思われがちが, 今のところ, これを進める手がかりがほとんどない.

§4 数値計算

関連した数値計算では、大分以前(1982-83年)日立CEの
 青山智夫氏が、又1992年4月(シンポジウム直後)当数理研の
 松本真氏が計算した資料があります。両氏に改めて
 感謝致します。前者を[A]後者を[M]で引用致します。

daの零乗について: まず[BTW]に、 $a \in \mathbb{Z}$, $2 \leq a \leq 99$,
 $\sqrt[m]{a} \notin \mathbb{Z}$ ($m=2, 3, \dots$) なる各aに対して $a^{p-1} \equiv 1 \pmod{p^2}$ を満
 す素数pを探索した結果の表が出ています。調べたpの
上限 $x = x(a)$ は a に依存してはいますが、いざの場合も
 $10^{7.5} < x < 10^{9.5}$ ($2.85 < \log \log x < 3.09$) となっています。
 各 a に対して ($a^{p-1} \equiv 1 \pmod{p^2}$, $p < x$ となる) p の個数は
 平均 2~3 個です。

p の個数の多い a の例としては

$$a=19 \quad (p=3, 7, 13, 43, 137, 63061489)$$

$$a=20 \quad (p=281, 46457, 9377747, 122959073)$$

(いざの場合 $x = 2^{27} = 10^{8.12\dots}$)。一方、 $a=21, 29, 34, 47, 61, 66, 72,$
 $88, 90$ では一つも p が見つかっていません(例えば $a=21, 34$ は
 $x = 2^{29}$, $a=29$ は $x = 2^{28}$ で)

この範囲の各 a に対する $\log \log x(a)$ の値と、 p の個数の平均は共に大体 $2.5 \sim 3.0$ という事で、[P3] と一応 対応しています。(この範囲での $\sum_{p < x} p^{-1}$ と $\log \log x$ の差は一行小さい order の筈) そんなにしても、 p の個数が 3 個程度の範囲では、[P1]? [P3]? 等の判断材料として弱まっています。これを進める為には a の範囲はあまり広げずに p の範囲をもっと広げたいといけなわけですが、これは技術的に困難かも知れません。(例えは $\log \log x = 12$ 位までやって、仮にその位の x に対する p が見つかったと、それは約 7 万桁の数ですから、それを印刷するには一冊の本が必要になる位で、その数値をプリントアウトしても何の役に立たないでしょう)

[P3] のもとになる "確率 $1/p$ の独立性" が正しいかどうかを推測するには、むしろ Δ_p の $\text{mod } p^2$ での分布をみる、等によって、 p に比べて小さい正整数 $a > 1$ で $a^{p-1} \equiv 1 \pmod{p^2}$ を満たすものがどの位あるか、それについて、同じ根拠 "... $1/p$..." をもとにして計算される期待値と合っているか、を見る方がよいかも知れません。例えは

$$\#\{(a, p); 1 < a < \log p, a^{p-1} \equiv 1 \pmod{p^2}, p < x\}$$

の期待値は $\sum_{p < x} \frac{\log p}{p} = \log x + O(1)$ ですが、 $x = 10^8$ とすると

実際の個数は 16, 期待値は 18.42. で、これはほぼ合っている

す. n について $x = 10^{10}$ 位迄は計算し ($\log x = 23.025\dots$)
 実際、 (R, p) の個数が n と 7 の位増えるかどうか、位は見た
 いものであす. 尚 [BTW] の表から (P2) に関する encouraging なデータ
 は読みとれません^(*)

代数体の例 実 2 次体 K の基本単数 ε に対する $d\varepsilon$
 の素因数を有する例としては、 $K = \mathbb{Q}(\sqrt{2})$, $\varepsilon = 1 + \sqrt{2}$ とすると、
 $N_p = 13, 31$ なる K の素イデアル \mathfrak{p} たち (計 4 個) は $d\varepsilon$ の素因数になって
 います. 一方、 $K = \mathbb{Q}(\sqrt{5})$, $\varepsilon = \frac{1}{2}(1 + \sqrt{5})$ に対しては、剰余
 標数 $p \leq 104729$ なる素イデアルの範囲で 一つも素因数が
 見つかりませんでした [A].

より一般に $\alpha_\ell = 2 \cos \frac{2\pi}{\ell} \in \mathbb{Q}(\cos \frac{2\pi}{\ell}) = K$ については
 (上の例は $\ell = 5$) 素因数をもつ場合が沢山あります. 例えは
 $\ell = 29$ のとき $d\alpha_\ell$ は $p = 59$ の K に於ける 14 個の素因子のうち
 の 2 個を素因数としています. α が $2 \cos \frac{2\pi}{\ell} = \zeta_\ell + \zeta_\ell^{-1}$ のように
 2 つの 1 の ℓ 乗根の和のときに $d\alpha$ の素因数を見つける問題は、

Δ_p^x 内での合同式

$$(*) \quad a + b + c \equiv 0 \pmod{p^2}; \quad (a, b, c \in \Delta_p^x)$$

の解を求める問題と直接関係してゐます (理由は明らかと
 思ふます). $q \equiv 1 \pmod{3}$ のときは 1 の原 2 次乗根 $\omega \in \Delta_p^x$ は
 $1 + \omega + \omega^2 = 0$ を満たし、 $(*)$ の解を与えますが、 $(*)$ のそれ以外
 の解 (non-trivial な解とよぶ) が 各 q に対してどの位あるか

^{*} はじめ $a = 2$ のときの 2 つの p に対して $p-1 = 1092 = 2^2 \cdot 3 \cdot 7 \cdot 13$,
 $3510 = 2 \cdot 3^3 \cdot 5 \cdot 13$ と沢山の因子をもつ (Abelian に ∞ に近い!) のが印象的でしたか、
 これはそう一般的でたう!

も興味深い問題です。 $q = p$ のときでは, (*) が non-trivial な解をもつ最小の p が $p = 59$ で, これが上記 $d\alpha_{29}$ の零点を与えています。 $p < 100$ では 3 つの p は あと 79, 83 の計 3 つです。 [M] によると, $p < 10000$ なる 全 1236 個の素数 p のうちの 15% に当る 187 個の素数 p に対して (*) が non-trivial な解をもちます ($\rightarrow d\alpha_2$ たちの沢山の零点)。

$\Delta_p^x \pmod{p^2}$ の分布 [M]: $\Delta_p^x \setminus \{\pm 1\} \pmod{p^2}$ の元は各 i ($1 < i < p-1$) に対して $i + pc_i \pmod{p^2}$ ($0 \leq c_i < p$) 型の元が 1 つずつあるわけだが, $\frac{c_i}{p}$ たちの $(0, 1)$ 区間上での分布 (p と i と関係なく) は どうなっているでしょうか。 $\Delta_p^x \pmod{p^2}$ を小さい p に対して計算し $\frac{c_i}{p}$ の分布表を作ってみると, はじめのうちには グラフにいくつかの山や谷があり, 「何かある?」と思わせますが, [M] によって $p < 10000$ まで計算した結果, $(0, 1)$ 区間を 100 等分しても 各小区間での $\frac{c_i}{p}$ たち ($p < 10000, 1 < i < p-1$) のコスウのバラツキは 3% 以内に収まることが判明し, この分布は, 内違なく 平等分布 のようです。

従って, $c_i = 0$ となる (p, i) も 相応に少く,

$$\#\{1 < a < p, a^{p-1} \equiv 1 \pmod{p^2}, p \leq x\}$$

についても “期待値” と 実際の個数 の内にあまり開きはないうようです。 ($x = 1000$ では 期待値 ≈ 160 , 個数 144)

$(d2)_p, (d3)_p, (d5)_p, (\frac{d3}{d2})_p$ の表 [A]: これは、 $2n$ 以上
 かなり大きな p に対して迄計算されてはいますが、今のところ殆んど
 使途がありません。ただ、 $a = 2^m 3^n$ ($(m, n) = 1$) 型の有理
 数 a に対する da の零因子を調べるのには役立っています。
 例えば $d(\frac{2}{3})$ の零因子は $p < 27449$ では $p = 23$ の
 1つだけ、等。

[31 用]

[A] 日立 CE 青山智夫氏による 1982-83 年の計算

[M] 数理論研. 松本真氏による 1992 年の計算

[BTW]^(*) Brillhart-Tonascia-Weinberger, "On the
 Fermat quotient"; in "Computers in number theory"
 (A.O.L. Atkin, B.J. Birch, editors), Proc. Sci. Res. Council
 Atlas Symp 2, Oxford (1969), Academic Press, London 1971.

[H]. S. Hahn: "On Mirimanoff type congruences,"
 to appear in J. Number theory.

(*) これはかなり古いのですが、私はその後この種の計算が
 進められたという話を聞いておりません。行方知の方があったら
 どうか御一報下さい。