数理解析研究所講究録
第810巻 1992年 324-341

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 $k^\times$ の元, $\mathfrak{p}$ を k の有限素点とし, $(\alpha, \mathfrak{p}) = 1$ とすると「フェルマの小定理」により常に $\alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$ が成立ちますが, α ($\neq 1$ の巾根) を固定して $\mathfrak{p}$ を動かすとき

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

を満す $\mathfrak{p}$ はどの位あるか (有限個? 無限個?), 又そういう $\mathfrak{p}$ 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) のとき, 小さい自然数 $a > 1$ に対して $(1)_a$ (即ち $a^{p-1} \equiv 1 \pmod{p^2}$) を満す素数 p の例としては,

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

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

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

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

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「$n=4$の場合」との関係によってもよく知られています(§3)．さて§1で述べるように，合同式$(1)_\alpha$を満す素点pは"微分$d\alpha$"の零点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目ぬめた上で，

§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。残念乍ら，三つの可能性のどれが正しそうか(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 の各有限素点 $\mathfrak{p}$ に対して $k_\mathfrak{p}$ を k の $\mathfrak{p}$ 進完備化，$\mathrm{ord}_\mathfrak{p}$ をその指数加法付値，$\kappa_\mathfrak{p} = \mathbb{F}_q$ を剰余体 $(q = N\mathfrak{p})$，$\kappa_\mathfrak{p}$, $\kappa_\mathfrak{p}^\times$ の Teichmüller liftings を

$$\Delta_\mathfrak{p} = \{\zeta \in k_\mathfrak{p};\ \zeta^q = \zeta\}, \qquad \Delta_\mathfrak{p}^\times = \Delta_\mathfrak{p} - \{0\}$$

とおきます．

各 $\alpha \in k;\ \mathrm{ord}_\mathfrak{p}\alpha \geq 0$ に対して $\alpha \equiv \alpha(\mathfrak{p}) \pmod{\mathfrak{p}}$ となる $\alpha(\mathfrak{p}) \in \Delta_\mathfrak{p}$ が唯一つ存在するので，この $\alpha(\mathfrak{p})$ を(関数体との類似により)"関数" α が"点" $\mathfrak{p}$ 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) $\Delta_\mathfrak{p}$ が加法的には閉じていない (ii) 剰余標数の相異る $\mathfrak{p}$ に対する $\kappa_\mathfrak{p}$ は素体までもが相異る体である，という二点で，このように両者の間にはもともと大きな基本的相違がある事を(当たり前ではあるが)この際再確認しておきます．

さて $\alpha - \alpha(\mathfrak{p})$ の定める $\mathfrak{p}/\mathfrak{p}^2$ の元は α の $\mathfrak{p}$ に於る微分と見做せますから，

$$(d\alpha)_\mathfrak{p} := \alpha - \alpha(\mathfrak{p}) \pmod{\mathfrak{p}^2} \in \mathfrak{p}/\mathfrak{p}^2$$

と定めます．ただし $\mathrm{ord}_\mathfrak{p}\alpha < 0$ のときは(一応) $(d\alpha)_\mathfrak{p} = \infty$

とおく事にします。

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

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

と定めます。ただし, α が $\mathfrak{p}$ 整でないときは $\alpha(\mathfrak{p}) = 0$ とします (β も同様)。

$\Delta_{\mathfrak{p}}$ が乗法的に閉じている事より, $\mathrm{ord}_{\mathfrak{p}}\alpha, \mathrm{ord}_{\mathfrak{p}}\beta \geq 0$ なら

$$d(\alpha\beta)_{\mathfrak{p}} = \alpha(d\beta)_{\mathfrak{p}} + \beta(d\alpha)_{\mathfrak{p}} \qquad (\text{in } \mathfrak{p}/\mathfrak{p}^2)$$

が成立ちますが, 加法的には閉じていない事を反映して, 一般には

$$d(\alpha+\beta)_{\mathfrak{p}} \neq (d\alpha)_{\mathfrak{p}} + (d\beta)_{\mathfrak{p}}$$

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

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

$$(d\alpha)_{\mathfrak{p}} = 0 \iff \alpha^{N\mathfrak{p}-1} \equiv 1 \pmod{\mathfrak{p}^2}$$

で, これによって $(1)_{\alpha}$ を添す $\mathfrak{p}$ と $d\alpha$ の零点が結びついています。

さて 各 $\alpha \in k$ に対してその微分 $d\alpha$ を，各 $\mathfrak{p}$ に対して $(d\alpha)_{\mathfrak{p}} \in \mathfrak{p}/\mathfrak{p}^2 \cup (\infty)$ を対応させる関数，と定義します。（一般に，有限一次結合 $\sum_i \gamma_i d\alpha_i$ $(\alpha_i, \gamma_i \in k)$ を，各 $\mathfrak{p}$ で $\mathrm{ord}_{\mathfrak{p}} \alpha_i, \mathrm{ord}_{\mathfrak{p}} \gamma_i \geq 0$ なるものに対して $\mathfrak{p}/\mathfrak{p}^2$ に値をとる関数として定義することも（定義だけなら）出来るわけです。）又，2つの元 $\alpha, \beta \in k$ $(\alpha \neq 0, \neq 1$ の冪根$)$ に対して $\frac{d\beta}{d\alpha}$ を，各 $\mathfrak{p}$ に対して $\left(\frac{d\beta}{d\alpha}\right)_{\mathfrak{p}} \in k_{\mathfrak{p}} \cup (\infty)$ 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，より一般に $\sum_i \gamma_i \frac{d\beta_i}{d\alpha_i}$）は，如何なる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 $\mathfrak{p} \longrightarrow \gamma \pmod{\mathfrak{p}} \in k_{\mathfrak{p}} \cup (\infty)$ 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 $\mathfrak{p}$ 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1つの $\alpha (\neq 0, 1$ の冪根$)$ についても，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 $\alpha \in k^\times \setminus \{1の冪根\}$ に対して $(d\alpha)_\mathfrak{p} = 0$ となる $\mathfrak{p}$ はタカダカ有限個.

関数体の微分 ($\neq 0$) の零点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のか?」という問題とも考えられます。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 $\log |d_k|$ はあるが) $d\alpha$ 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。

$\mathrm{ord}_\mathfrak{p}(d\alpha)_\mathfrak{p}$ が各 $\mathfrak{p}$ に対して定義できればよいわけですが,

☆ $k_\mathfrak{p}$ を有限次拡大 $K_\mathfrak{P}$ でおきかえたときの望ましい(?)関係

$$\mathrm{ord}_\mathfrak{P}(d\alpha)_\mathfrak{P} = e \cdot \mathrm{ord}_\mathfrak{p}(d\alpha)_\mathfrak{p} + \mathrm{ord}_\mathfrak{P}\delta \quad \begin{pmatrix} e: 分岐指数 \\ \delta: 相対差積 \end{pmatrix}$$

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

$$\mathrm{ord}_\mathfrak{p}\, d(\alpha^n) = \mathrm{ord}_\mathfrak{p}(n\alpha^{n-1}) + \mathrm{ord}_\mathfrak{p}\, d\alpha,$$

の両方を満す定義を与えることは出来ますが, それが自然なものであるか, 又そもそも自然な $\mathrm{ord}_\mathfrak{p}(d\alpha)_\mathfrak{p}$ が存在し得るかどうかさえも, 疑問です。又, $k_\mathfrak{p}$ が Archimedean のときにも $\mathrm{ord}_\mathfrak{p}(d\alpha)_\mathfrak{p}$ を定義しようとすると, $|\alpha|_\mathfrak{p} = 1$ なる α に対しては, $\mathrm{ord}_\mathfrak{p}(d\alpha)_\mathfrak{p} = +\infty$ とせざるを得ないようです.

以下の「可能性2」は，$(d\alpha)_{\mathfrak{p}} = 0$ となる $\mathfrak{p}$ は無限個あったとしても それは以下の意味で "Abel的に ∞ に収束"して，各 α, β に対して関数 $\mathfrak{p} \longmapsto \left(\frac{d\beta}{d\alpha}\right)_{\mathfrak{p}}$ は，$\frac{d\beta}{d\alpha}$ の極と零点を用いて Weierstrass 因数分解が出来るのではないか？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，$\mathfrak{p} \in P \setminus S_K$ なら $\mathfrak{p}$ 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 に属するモジュラルは有限個を除いては単項で，しかも任意に与えられた k の modulus m に対してある有限集合 $S_m \subset P$ が存在して，$\mathfrak{p} \in P \setminus S_m$ なら $\mathfrak{p} = (\pi)$; $\pi \equiv 1 \pmod{m}$ となります．

ついでに，(与えられた，k のモジュラルからなる) 集合 P が Galois的に ∞ に収束する為の必要十分条件が十分 explicit に表わされるかどうかが「非アーベル類体論」にとっての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 でほと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 $\alpha \in k^\times \setminus \{1の冪根\}$ を固定するとき,

(i) $(d\alpha)_\mathfrak{p} = 0$ となる $\mathfrak{p}$ 全体の集合は Abel 的に ∞ に収束する.

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

(iii) (i)により形式積 $(d\alpha) = \prod_{\mathfrak{p}(有限素点)} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(d\alpha)_\mathfrak{p}}$ は k の1つのイデアル類を定めるが, それは k の共役差積イデアル δ_k の属する類.

(iv) $\alpha, \beta \in k^\times \setminus \{1の冪根\}$ とし, $\mathfrak{m}$ を $(d\alpha), (d\beta)$ と無縁な k の square-free なイデアルとする. (i)によって $(d\alpha), (d\beta)$ はそれぞれ $\bmod \mathfrak{m}$ の Strahl 類を定め, それらの比は (iii) によって単項類ゆえ, 形式因子 $(d\beta)/(d\alpha)$ は $(\mathcal{O}/\mathfrak{m})^\times / (\mathcal{O}^\times の像)$ の一つの元を定めるが, これが関数 $\left(\left(\frac{d\beta}{d\alpha}\right)_\mathfrak{l}\right)_{\mathfrak{l}|\mathfrak{m}}$ の定める元と一致.

(P3) 各 $\alpha \in k^\times \setminus \{1\}$ の冪根 に対して

$$\#\{\mathfrak{p};\ (d\alpha)_\mathfrak{p}=0,\ N(\mathfrak{p})\leq x\} \sim \log\log x \qquad (x\to\infty)$$

($\sim$ は，さし当たり 比 $\to 1$ 程度の弱い意味にしておく)．

これは，$\mathfrak{p}/\mathfrak{p}^2$ 内で任意に選ばれた元が 0 になる確率が $N(\mathfrak{p})^{-1}$ であることを，α が固定されて $\mathfrak{p}$ が動く場合の $(d\alpha)_\mathfrak{p}$ の分布にも 適用できると (勝手に) 考えると ただちに 導びかれます。 よく知られているように，

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

(この場合の $\sim$ は 差 $=O(1)$. 尚 $\log\log x$ の頭に $[k:\mathbb{Q}]$ 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，それにも拘らず関数体のときは $(d\alpha)_\mathfrak{p}=0$ となる $\mathfrak{p}$ は有限個しかない，という事です。つまり，代数体と関数体を この点に於て区別する何らかの根拠が分かると，この確率論的推測は 説得力がない，という感じです。

(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，

$$\{K\text{の素点 } \mathfrak{P};\ (d\alpha)_{\mathfrak{P}}=0,\ N(\mathfrak{P})\leq x\}$$

$$\text{“}\geqq\text{”}\cdot[K:k]\{k\text{の素点 } \mathfrak{p};\ (d\alpha)_{\mathfrak{p}}=0,\ N(\mathfrak{p})\leq x\}$$

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

(P1)と(P2)が両立するかはわかりませんが，もし(P1)が成立ちしかも $d(2)$ 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)は成立ちません．

§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 $a\in\mathbb{Z}$, $(a,p)=1$, $2\le a\le 43$ に対して成立つ（Wieferich, …）．従って特に（$a=2,3$ に適用して）$p>3\times 10^9$ でなくてはならない……

$d2, d3, \cdots$ それぞれの零点はかりに無限個あっても，共通零点となるとタカダカ有限個しかなさそうです（$\sum\frac{1}{p}=\infty$ でも $\sum\frac{1}{p^2}<\infty$）が，果してどうでしょうか．

合同式 $(1)_\alpha$ の類体論による"翻訳例" $\mathbb{Q}$ の唯一の $\mathbb{Z}_p$ 拡大を $K_p=\bigcup_{n=1}^{\infty}K_p^{(n)}$ $([K_p^{(n)}:\mathbb{Q}]=p^n)$ 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：ζ_{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 とするとき,

$d(\ell)$ の零点が有限個 $\Longleftrightarrow$ $K/\mathbb{Q}$ に於る ℓ の延長は有限個.

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

$$\varepsilon^{N\mathfrak{p}-1} \equiv 1 \pmod{\mathfrak{p}^2} \Longleftrightarrow \begin{array}{l} k \text{ は } \mathfrak{p} \text{ のみが分岐する} \\ p \text{ 次巡回拡大をもつ} \end{array}$$

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, $\ell^{p-1} \not\equiv 1 \pmod{p^2}$ 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) 示しています (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 : $d\alpha$ の零点の問題はむしろ,

$\mu_\infty = \{\overline{\mathbb{Q}}$ 上の 1 の冪根全体$\}$ 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 $|\Phi_n(\alpha)|_v$ を様々の $|\ |_v$ 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かもしれませんが, $k = \mathbb{Q}$, $a \in \mathbb{Q}^\times - \{\pm 1\}$, d: a の分母 とするとき, 既の $|\ |_\infty$ 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)

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

と積公式を用いて次の事が示せます。 a を固定し p を動かすとき

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

は殆んど surjective (image の補集合は有限). この方法を refine して $da \neq 0$ の研究にも使えるようになれば… というのも一つの課題です.

(p進 log)$_{p\leq\infty}$: Idèles $\to$ Adèles. k の各有限素点 $\mathfrak{p}$ に対して $\mathfrak{p}$進対数関数 $\lambda_\mathfrak{p} : 1+\mathfrak{p} \longrightarrow k_\mathfrak{p}$ は, $\lambda_\mathfrak{p}(\Delta_\mathfrak{p}^\times)=0$ とおく事により $O_\mathfrak{p}^\times \to k_\mathfrak{p}$ (準同型写像) に拡張され, $\alpha \in O_\mathfrak{p}^\times$ なら

$$\lambda_\mathfrak{p}(\alpha) \equiv 0 \pmod{\mathfrak{p}} \iff \lambda_\mathfrak{p}(\alpha^{N\mathfrak{p}-1}) \equiv 0 \pmod{\mathfrak{p}}$$
$$\iff \alpha^{N\mathfrak{p}-1} \equiv 1 \pmod{\mathfrak{p}^2}$$

($\overset{\cdot}{\iff}$ は"大体". 例えば $\mathrm{ord}_\mathfrak{p} p < p-1$ なら成立つ).

そこで, 今 $\mathfrak{p}$ を動かして archimedean もこめてすべての $\mathfrak{p}$進 log を並べたものを考えると, ($\lambda_\mathfrak{p}$ は, $k_\mathfrak{p}^\times \to k_\mathfrak{p}$ への自然な拡張は持しないと思われるので) それはそのままでは k の idèle 群から adèle 群への準同型は与えないが, それにやや近いものにはなる. 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ますが, 今のところ, これを進める手がかりらしきものが掴めません.

§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）当数理研の松本眞氏が計算された資料があります。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の零点について：まず[BTW]に，$a\in\mathbb{Z}$, $2\le a\le 99$, $\sqrt[m]{a}\notin\mathbb{Z}$ $(m=2,3,\cdots)$ 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に依存していますが，いずれの場合も $10^{7.5}<x<10^{9.5}$ $(2.85<\log\log x<3.09)$ 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

$a=19$ $(p=3, 7, 13, 43, 137, 6306149)$

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

（いずれも $x=2^{27}=10^{8.12\cdots}$）．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 2.5～3.0 という事で，[P3]と一応符合しています．(この範囲での $\sum_{p<x} p^{-1}$ と $\log\log x$ の差は一桁小さい order の筈)　それにしても，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すぎます．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ないといけないわけですが，これは技術的に困難かも知れません．(例えば $\log\log x = 12$ 位までやって，仮にその位の x に対する p が見つかっても，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も立たないでしょう)

[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 $\bmod p^2$ 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 $a^{p-1}\equiv 1 \pmod{p^2}$ を満すものがどの位あるか，それについても，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．例えば

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

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ます

す. これについて $x=10^{10}$ 位迄は計算し ($\log x = 23.025..$) 実際の (k,p) の個数が あと7つ位増えるかどうか, 位は見たいものです. 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 $d\varepsilon$ で零点を有する例としては, $k=\mathbb{Q}(\sqrt{2})$, $\varepsilon=1+\sqrt{2}$ とすると, $Np=13, 31$ なる k の素イデアル p たち(計4ケ)は $d\varepsilon$ の零点になっています. 一方, $k=\mathbb{Q}(\sqrt{5})$, $\varepsilon=\frac{1}{2}(1+\sqrt{5})$ に対しては, 判定指数 $p \le 104729$ なる素イデアルの範囲で一つも零点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 $\ell=5$) 零点をもつ場合が沢山あります. 例えば $\ell=29$ のとき $d\alpha_\ell$ は $p=59$ の k に於る14ケの素因子のうちの2個を零点としています. α が $2\cos\frac{2\pi}{\ell} = \zeta_\ell + \zeta_\ell^{-1}$ のように2つの1の巾根の和のときに $d\alpha$ の零点を見つける問題は, $\Delta_p^\times$ 内での合同式

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

の解を求める問題と直接関係しています (理由は明らかと思います). $q \equiv 1 \pmod 3$ のときは1の原始3乗根 $\omega \in \Delta_p^\times$ は $1+\omega+\omega^2=0$ を満し, (*) 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 $p-1 = 1092 = 2^2\cdot 3\cdot 7\cdot 13$, $3510 = 2\cdot 3^3\cdot 5\cdot 13$ と沢山因子をもつ (Abelian に∞に近い!) のが印象的でしたが, これはそう一般的でない!

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。$p<100$ ではそういう p は あと 79, 83 の計3ケです。[M] によると，$p<10000$ なる全1236個の素数 p のうち 約15%に当る 187個の素数 p に対して (*) が non-trivial な解をもちます($\leftrightarrow d\alpha_\ell$ たちの沢山の零点)。

$\underline{\Delta_p^\times (\mathrm{mod}\, p^2)\text{の分布 [M]}}$： $\Delta_p^\times \sim \{\pm 1\}$ $\mathrm{mod}\, p^2$ の元は各 i $(1<i<p-1)$ に対して $i+pc_i$ $(\mathrm{mod}\, p^2)$ $(0\leq c_i<p)$ 型の元が1つづつあるわけですが，$\frac{c_i}{p}$ たちの $(0,1)$ 区間上での分布(pもそも粗かす)はどうなっているでしょうか。$\Delta_p^\times(\mathrm{mod}\, p^2)$ を小さい p に就て計算し $\frac{c_i}{p}$ 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 $p<10000$ まで計算された結果，$(0,1)$ 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，間違いなく $\underline{\text{平等分布}}$ のようです。

従って，$c_i=0$ となる (p,i) も相応に少く，

$$\#\{1<a<p,\ a^{p-1}\equiv 1\ (\mathrm{mod}\, p^2),\ p\leq x\}$$

についても"期待値"と実際の個数の内に あまり開きはないようです。($x=1000$ では 期待値 $\fallingdotseq 160$, 個数 144)

$(d2)_p$, $(d3)_p$, $(d5)_p$, $\left(\frac{d3}{d2}\right)_p$ の表 [A]: これは，それぞれかなり大きな p に対して迄計算されていますが，今のところ殆んど使途がありません．ただ，$a = 2^m 3^n$ $((m,n)=1)$ 形の有理数 a に対する da の零点を調べるのには役立っています．

例えば $d\left(\frac{2}{3}\right)$ の零点は $p < 27449$ では $p = 23$ の1つだけ，等．

[3] 用]

[A] 日立CE 青山智夫氏による 1982-83 年の計算

[M] 数理研．松本眞氏による 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．御存知の方があったらどうか御一報下さい．