整数論 の極一部 における p 進的手法の紹介

加塩朋和 * (東京理科大学 理工学部 数学科)

ワークショップ「代数学の萌芽」

2022 年 3 月 4 日

*E-mail: kashio_tomokazu@ma.noda.tus.ac.jp

p 進数とは

Definition ($p = 2, 3, 5, 7, 11, \dots$)

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \qquad \text{(“逆” 極限)}$$

c.f. 順極限

$\{1\} \hookrightarrow \{1,2\} \hookrightarrow \{1,2,3\} \hookrightarrow \cdots\cdots$

$$\rightsquigarrow \varinjlim_n \{1,2,\dots,n\} = \bigcup_n \{1,2,\dots,n\} = \mathbb{N}$$

逆極限

$$\{0,\dots,p-1\} \overset{\bmod p}{\twoheadleftarrow} \{0,\dots,p^2-1\} \overset{\bmod p^2}{\twoheadleftarrow} \{0,\dots,p^3-1\} \overset{\bmod p^3}{\twoheadleftarrow} \cdots\cdots$$

$$\rightsquigarrow \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$$

p 進数とは

Definition

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_n)_n \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \;\middle|\; a_{n+1} \overset{\bmod p^n}{\longmapsto} a_n \right\}$$

$$= \left\{ \begin{array}{cccccccccc} & \{0 \sim p-1\} & \times & \{0 \sim p^2-1\} & \times & \{0 \sim p^3-1\} & \times & \cdots & \\ & \Cup & & \Cup & & \Cup & & & \\ (& a_1 & , & a_2 & , & a_3 & , & \cdots &) \\ \text{s.t.} & a_1 & \overset{\bmod p^1}{\longleftarrow\!\shortmid} & a_2 & \overset{\bmod p^2}{\longleftarrow\!\shortmid} & a_3 & \overset{\bmod p^4}{\longleftarrow\!\shortmid} & \cdots & \end{array} \right\}$$

p 進数とは

p 進数

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \left\{ (a_n)_n \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \;\middle|\; a_{n+1} \overset{\text{mod } p^n}{\longmapsto} a_n \right\}$$

Example. $\mathbb{Z}_5 \subset \mathbb{Z}/5^1\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z} \times \mathbb{Z}/5^3\mathbb{Z} \times \mathbb{Z}/5^4\mathbb{Z} \times \cdots$

$$\begin{array}{ccccccccc}
\{0 \sim 4\} & \times & \{0 \sim 24\} & \times & \{0 \sim 124\} & \times & \{0 \sim 624\} & \times & \cdots \\
\rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} & & \\
2 & \overset{\text{mod } 5^1}{\longleftarrow\!\shortmid} & 7 & \overset{\text{mod } 5^2}{\longleftarrow\!\shortmid} & 57 & \overset{\text{mod } 5^3}{\longleftarrow\!\shortmid} & 182 & \overset{\text{mod } 5^4}{\longleftarrow\!\shortmid} & \cdots
\end{array}$$

$\Rightarrow (2, 7, 57, 182, \dots) \in \mathbb{Z}_5$

$$2 \overset{+1\cdot 5^1}{\Longrightarrow} 7 \overset{+2\cdot 5^2}{\Longrightarrow} 57 \overset{+1\cdot 5^3}{\Longrightarrow} 182 \overset{+?\cdot 5^4}{\Longrightarrow} \cdots \overset{+?\cdot 5^5}{\Longrightarrow} \cdots \overset{+?\cdot 5^6}{\Longrightarrow} \cdots$$

$\Rightarrow (2, 7, 57, 182, \dots) = 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + \cdots$

p 進数とは

Example.

$\mathbb{Z}_5 \ni (2, 7, 57, 182, \dots) = 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + \cdots$

※ $|p| < 1$: **p 進距離**

---

c.f. $\mathbb{R} \ni \sqrt{2} = 1.41421\dots$

$= \lim (1, 1.4, 1.41, 1.414, 1.4142, 1.41421, \dots)$

$= 1 + 4 \cdot (\frac{1}{10})^1 + 1 \cdot (\frac{1}{10})^2 + 4 \cdot (\frac{1}{10})^3 + 2 \cdot (\frac{1}{10})^4 + 1 \cdot (\frac{1}{10})^5 + \cdots$

※ $|\frac{1}{10}| < 1$, $|\frac{1}{10}^n| \to 0$ $(n \to \infty)$

p 進数とは

Example

$$\mathbb{Z}_5 = \varprojlim_n \mathbb{Z}/5^n\mathbb{Z} \ni (2, 7, 57, 182, \ldots) = 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + \cdots$$

Proposition

- $\mathbb{Z}_p = \left\{ \sum_{n=0}^{\infty} a_n p^n \;\middle|\; a_n \in \{0, 1, \ldots, p-1\} \right\}$: **p 進整数環**
- コンパクト, とくに完備, $\mathbb{N} \overset{\text{稠密}}{\subset} \mathbb{Z}_p$
- $\mathbb{Q}_p = \mathbb{Z}_p[\frac{1}{p}] = \left\{ \sum_{n=n_0}^{\infty} a_n p^n \;\middle|\; a_n \in \{0, \ldots, p-1\}, n_0 \in \mathbb{Z} \right\}$: **p 進数体**

c.f. ベキ級数環: $\mathbb{C}[[z]] \subset \mathbb{C}((z)) = \mathbb{C}[[z]][\frac{1}{z}]$:ローラン級数体

お勧めポイント

- “遊べる” e.g., PARI/GP では a+O(p^n) $\in \mathbb{Z}_p$

  http://pari.math.u-bordeaux.fr/gp.html

  - $\mathbb{Z}_5 \ni -1 = 4 + 4 \cdot 3^1 + 4 \cdot 3^2 + 4 \cdot 3^3 + 4 \cdot 3^4 + \cdots$
  - $\mathbb{Z}_5 \ni \frac{-1}{2} = 2 + 2 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \cdots$
  - $\mathbb{Z}_5 \ni \frac{1}{2} = 3 + 2 \cdot 3^1 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + \cdots$
  - $\mathbb{Z}_5 \ni \sqrt{-1} = \lim_{n \to \infty} 2^{5^n} = 2 + 1 \cdot 5^1 + 2 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \cdots$

- Hasse の原理 (局所大域原理) “$\mathbb{Q}$ を調べる $\Leftrightarrow$ $\mathbb{R}, \mathbb{Q}_p({}^\forall p)$ を調べる”

  e.g., $ax^2 + bxy + cy^2 = d$ $(a, b, c, d \in \mathbb{Q})$ に対し

$$\text{解} \in \underset{\text{大域, 難}}{\mathbb{Q}} \text{ を持つ} \Leftrightarrow \text{解} \in \underset{\text{局所, 易}}{\mathbb{R}, \mathbb{Q}_p} \ ({}^\forall p) \text{ を持つ}$$

- “代数の心を持った解析”

$$\mathbb{Z}_p = \left\{ (a_n)_n \in \underset{\text{代数}}{\prod \mathbb{Z}/p^n\mathbb{Z}} \;\middle|\; \cdots \right\} = \left\{ \underset{\text{解析}}{\sum a_n p^n} \;\middle|\; \cdots \right\}$$

岩澤理論周辺

- $\zeta_n := e^{\frac{2\pi i}{n}}$, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, $[\zeta_n \mapsto \zeta_n^a] \longleftrightarrow a \bmod n$
- $\mathbb{Q} \subset \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_p^2) \subset \cdots \quad \cdots \subset \mathbb{Q}(\zeta_{p^\infty}) := \cup_{n\in\mathbb{N}} \mathbb{Q}(\zeta_{p^n})$

  $\leftarrow (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow$

  $\longleftarrow \cdots (\mathbb{Z}/p^2\mathbb{Z})^\times \cdots \longrightarrow$

  $\longleftarrow \cdots\cdots\cdots\cdots\cdots\cdots\cdots \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \cdots\cdots\cdots\cdots\cdots\cdots\cdots \longrightarrow$

  $\Rightarrow \mathbb{Q}(\zeta_{p^\infty}) = \varinjlim \mathbb{Q}(\zeta_{p^n}) \curvearrowleft \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times$
- 代数体 $K \rightsquigarrow \underset{\circlearrowleft\mathbb{Z}}{\mathrm{Cl}_K}$: イデアル類群 $\supset \underset{\circlearrowleft\mathbb{Z}_p}{\mathrm{Cl}_K[p^\infty]}$: p 部分群

  $\Rightarrow \mathrm{Cl}_{\mathbb{Q}(\zeta_{p^\infty})}[p^\infty] \curvearrowleft \Lambda := \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$: **岩澤加群**
- **岩澤主予想**: $\mathrm{Cl}_{\mathbb{Q}(\zeta_{p^\infty})}[p^\infty]^\chi \sim \Lambda/(L_p(\omega\chi^{-1}))$

  $\Rightarrow \cdots \Rightarrow$ 肥田理論, Wiles のガロア表現 (Fermat の最終定理, 1995), Dasgupta-Kakde (Brumer-Stark 予想, Hilbert の第 12 問題, 2021)

岩澤理論周辺

- $\mathbb{Q}(\zeta_{p^\infty}) := \mathbb{Q}(\zeta_{p^n} \mid n \in \mathbb{N}) \curvearrowleft \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}_p^\times$
- $\mathrm{Cl}_{\mathbb{Q}_{p^\infty}}[p^\infty] \curvearrowleft \Lambda := \mathbb{Z}_p[[\mathbb{Z}_p^\times]]$: “岩澤加群”
- **岩澤主予想**: $\mathrm{Cl}_{\mathbb{Q}(\zeta_{p^\infty})}[p^\infty]^\chi \sim \Lambda/(L_p(\omega\chi^{-1}))$
  $\Rightarrow \cdots \Rightarrow$ 肥田理論, Wiles のガロア表現 (Fermat の最終定理, 1995), Dasgupta-Kakde (Brumer-Stark 予想, Hilbert の第 12 問題, 2021)

- 数論 II (岩澤理論と保型形式), 黒川信重, 栗原将人, 斎藤毅 著, 岩波
- 重点解説岩澤理論 (理論から計算まで), 福田隆 著, サイエンス社
- 岩澤理論とその展望 (上下巻), 落合理 著, 岩波
- p 進ゼータ関数 (久保田-レオポルドから岩澤理論へ), 青木美穂 著
- *Introduction to cyclotomic fields*, GTM83, Washington 著
- “類数の結び目類似の p 進極限値” $\Rightarrow$ 吉崎彪雅氏 (本専攻 D2)

特殊関数の p 進類似

- $\Gamma(s) := \int_0^\infty t^{s-1}e^{-t}\,dt$ (Euler, 1729) $\Rightarrow \Gamma(n) = (n-1)!$, $\Gamma(\frac{1}{2}) = \sqrt{\pi}$
- $\Gamma_p(s) := \lim_{k\to s}(-1)^k \prod_{1\le k\le n-1, p\nmid k} k \in \mathbb{Z}_p$ ($s \in \mathbb{Z}_p$) (森田, 1975)

  $\Rightarrow \Gamma_5(\frac{1}{4}) = \sqrt{-2-\sqrt{-1}}$, $\Gamma_p(\frac{1}{p-1}) \in \overline{\mathbb{Q}}$ (Gross-Koblitz 公式, 1979)
- 多重 Γ 関数 (Barnes, 1904)

$$\Gamma(x,(\omega_1,\ldots,\omega_r)) := \exp\left(\frac{d}{ds}\sum_{m_i\ge 0}(x+m_1\omega_1+\cdots+m_r\omega_r)^{-s}\Big|_{s=0}\right)$$

  e.g., $\Gamma(z,(1)) = \dfrac{\Gamma(x)}{\sqrt{2\pi}}$
- p 進対数多重 Γ 関数 (加塩, 2005)

$$L\Gamma_p(x,(\omega_1,\ldots,\omega_r)) := \frac{d}{ds}\sum_{m_i\ge 0}(x+m_1\omega_1+\cdots+m_r\omega_r)^{-s}\Big|_{\mathbf{p}\text{ 進補完}}\Bigg|_{s=0}$$

  ※ $\log_p(\zeta_n) = \log_p(p) = 0$
- 問題. p 進多重 Γ 関数や $\Gamma_p(s)$ ($s \in \mathbb{Q}_p$) の "良い" 定義

特殊関数の p 進類似

- **問題**. p 進多重 Γ 関数や $\Gamma_p(s)$ $(s \in \mathbb{Q}_p)$ の "良い" 定義

- K., On a p-adic analogue of Shintani's formula, *J. Math. Kyoto Univ.* **45**(1), (2005)
  ※ "p 進対数多重 Γ 関数"
- Dasgupta, Shintani zeta-functions and Gross–Stark units for totally real fields, *Duke Math. J.* **143**(2), (2008)
  ※ "乗法的 p 進積分" $\Rightarrow$ Hilbert の第 12 問題 (Dasgupta-Kakde, 2021)
- K., p-adic measures associated with zeta values and p-adic log multiple gamma functions, *Int. J. Number Theory* **15**(5), (2019)
  $\Rightarrow$ "p 進対数多重 Γ 関数 $= \log_p$ (乗法的 p 進積分)"
- K., Fermat curves and a refinement of the reciprocity law on cyclotomic units, *J. Reine Angew. Math.* **741** (2018)
  ※ 暫定的な $\Gamma_p(s)$ $(s \in \mathbb{Q}_p)$
- Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, GTM58
- Robert, *A Course in p-adic Analysis*, GTM198

Hilbert の第 12 問題 (類体構成)

- "Kroneckler-Weber の定理" (…, Hilbert, 1896) $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\zeta_n \mid n \in \mathbb{N})$
- "Kronecker の青春の夢" (…, Hasse, 1931) K: 虚二次体,
  $E\colon y^2 = x^3 + ax + b$, $a, b \in H_K$, $\mathrm{End}(E) = \mathcal{O}_K$
  $\Rightarrow K^{\mathrm{ab}} = K(j_E, x^* \mid (x,y) \in E[n],\ n \in \mathbb{N})$, $* = \frac{|\mathcal{O}_K^\times|}{2} \in \{1,2,3\}$
- F: 総実体 (Dasgupta-Kakde, 2021)
  $\Rightarrow F^{\mathrm{ab}} = F($"Brumer-Stark 単数", $\sqrt{\alpha_i})$
  "Brumer-Stark 単数" $= \epsilon^a \pi^b \times\!\!\!\!\!\!\int x\, d\nu$ (乗法的 p 進積分)
- 問題. 射類体の明示 (c.f. $\mathbb{Q}(\zeta_n)$, $K(j_E, x^* \mid (x,y) \in E[n])$)

- Dasgupta-Kakde, Brumer-Stark units and Hilbert's 12th Problem, preprint.
- Dasgupta, Computations of elliptic units for real quadratic fields, *Canad. J. Math.* **59**(3), (2007), 553–574
- Fleischer-Liu, Computations of Brumer-Stark units (SageMath)

p 進 Hodge 理論の応用

- c.f. $H^{\mathrm{sing}}(M) \times H_{\mathrm{dR}}(M) \to \mathbb{C}$, $(\gamma, \omega) \mapsto \int_\gamma \omega$
  $\Leftrightarrow$ de Rham の同型: $H_{\mathrm{sing}}(M) \otimes \mathbb{C} \cong H_{\mathrm{dR}}(M) \otimes \mathbb{C}$
- p 進 Hodge 理論 $\rightsquigarrow H_{\mathrm{sing}}(M) \otimes \mathbb{Q}_p \cong H_{p,\text{ét}}(M) \otimes \mathbb{Q}_p$,
  $H_{p,\text{ét}}(M) \otimes B_{\mathrm{dR}} \cong H_{\mathrm{dR}}(M) \otimes B_{\mathrm{dR}}, \ldots \Rightarrow$ "付加構造"
  e.g, 楕円曲線 $E/\mathbb{Q}$, $H_{p,\text{ét}}(E) \cong \varprojlim E[p^n]^\vee \curvearrowleft \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \Rightarrow L(s, E)$
- Fermat 曲線: $x^n + y^n = 1$ & p 進 Hodge 理論, 絶対フロベニウス作用
  $\Rightarrow \sigma_a(\sin(\frac{b}{n}\pi)) \equiv \sin(\frac{ab}{n}\pi) \bmod \mu_\infty$ $(\sigma_a : \zeta_n \mapsto \zeta_n^a)$ (加塩, 2018)
- 問題. 厳密版, 単数性 $\Rightarrow \cdots \wr\wr \cdots \Rightarrow$ Stark 予想

- 辻雄, p 進 Hodge 理論, 数学 **57**(4), (2005), 337-349
- 中村健太郎, p 進表現論入門, 2009 年整数論サマースクール「l 進ガロア表現とガロア変形の整数論」報告集
- K., Fermat curves and a refinement of the reciprocity law on cyclotomic units, *J. Reine Angew. Math.* **741** (2018), 255–273