

# メモ: $B_{p,\chi}$ の $p$ 進付値について

石井 竣

2025 年 3 月 5 日作成

## 1 導入

$K$  を類数 1 の虚二次体とする.  $K$  の判別式の絶対値を  $d$ , 付随する Dirichlet 指標を  $\chi$  と書く. 指標  $\chi$  に付随する一般化 Bernoulli 数  $B_{n,\chi}$  は

$$\sum_{a=1}^d \frac{\chi(a)te^{at}}{e^{dt} - 1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!} t^n$$

で定義される [5, Chapter 4, p.31]. 例えば  $K = \mathbb{Q}(\sqrt{-1})$  の時には左辺は

$$\sum_{a=1,3} \frac{\chi(a)te^{at}}{e^{4t} - 1} = \frac{t(e^t - e^{3t})}{e^{4t} - 1} = \frac{-te^t}{e^{2t} + 1} = \frac{-t}{2} \sum_{n=0}^{\infty} \frac{E_n}{n!} t^n$$

となる. ここに  $E_n$  は Euler 数と呼ばれ, (hyperbolic) secant 関数の Taylor 展開の係数によって定義される, と <https://mathworld.wolfram.com/EulerNumber.html> に書いてあった. このことから  $K = \mathbb{Q}(\sqrt{-1})$  の時には等号

$$B_{n,\chi} = -\frac{E_{n-1}}{2}$$

が成立している. なお Euler 数は整数ゆえ  $2B_{n,\chi}$  は整数となる. Sagemath を用いて小さい  $n$  に対して組  $(2n-1, 2B_{2n-1,\chi} = -E_{2n})$  を計算してみると, 以下ようになった:

```
[5]: G = DirichletGroup(4)
x = G.0
for n in range(1,20):
    print(2*n-1, (2*x.bernoulli(2*n-1)).factor())

1 -1
3 3
5 (-1) * 5^2
7 7 * 61
9 (-1) * 3^2 * 5 * 277
11 11 * 19 * 2659
13 (-1) * 5 * 13^2 * 43 * 967
15 3 * 5 * 47 * 4241723
17 (-1) * 5 * 17^2 * 228135437
19 19 * 79 * 349 * 87224971
21 (-1) * 3 * 5^2 * 7 * 41737 * 354957173
23 23 * 31 * 1567103 * 1427513357
25 (-1) * 5^3 * 13 * 2137 * 111691689741601
27 3^3 * 67 * 61001082228255580483
29 (-1) * 5 * 19 * 29^2 * 71 * 30211 * 2717447 * 77980901
31 31 * 15669721 * 28178159218598921101
33 (-1) * 3 * 5 * 11 * 17 * 930157 * 42737921 * 52536026741617
35 5 * 7 * 4153 * 8429689 * 2305820097576334676593
37 (-1) * 5 * 13 * 37^2 * 9257 * 73026287 * 25355088490684770871
```

この表を眺めていると,  $p = 1 \pmod{4}$  の時には  $B_{p,\chi}$  が  $p^2$  で割れると推測できる. そしてこの推測は正しいことが Carlitz により証明されている:

**Theorem 1.1** ([1, Theorem 1]). 素数  $p$  が虚二次体  $K$  で *split* するならば,  $B_{p,\chi} = 0 \pmod{p^2}$ .

一步踏み込んで  $B_{p,\chi} = 0 \pmod{p^3}$  となるような ( $K$  で *split* する) 素数を探索してみる. Sage-math を用いて計算したところ,  $K = \mathbb{Q}(\sqrt{-1})$  の時には  $p = 29789$  が, また  $K = \mathbb{Q}(\sqrt{-3})$  の時には  $p = 13, 181, 2521$  が見つかった. なお  $2B_{29789,\chi}$  は大雑把には 11 万桁の整数であり, 計算機での取り扱いには注意を要するかもしれない.

個人的に  $p = 29789$  には見覚えがある. この素数は次のような性質を持っており, その性質 (と等値な Galois 群の構造に関するある帰結, 最終節にて紹介) が自分の研究と関係していた: 素数  $p = 29789$  は *split* するので, ある  $\mathbb{Z}[\sqrt{-1}]$  の素元  $\pi$  とその複素共役を用いて  $p = \pi\bar{\pi}$  と分解する. ここでは  $\pi := 110 + 133\sqrt{-1}$  としよう. この時,  $\mathbb{Z}[\sqrt{-1}]/(\pi) \cong \mathbb{F}_p$  と Fermat の小定理を用いることで, いわゆる Fermat 商に類似して

$$\frac{\bar{\pi}^{p-1} - 1}{\pi} \in \mathbb{Z}[\sqrt{-1}]$$

が分かる. 素数  $p = 29789$  は  $\frac{\bar{\pi}^{p-1} - 1}{\pi} = 0 \pmod{\pi}$  を満たし<sup>1</sup>, この性質を満たす  $p = 1 \pmod{4}$  なる素数は  $p < 10^7$  の範囲でこれのみである, というのを以前確かめていた. この一致を不思議に感じて  $K = \mathbb{Q}(\sqrt{-3})$  の場合にも計算すると, 素数  $p = 13, 181, 2521$  も同様の性質を持つことが確認された. このことから次の仮説を立てた:

$$p \geq 5 \text{ は } K \text{ で split しているとする. この時, } B_{p,\chi} = 0 \pmod{p^3} \Leftrightarrow \frac{\bar{\pi}^{p-1} - 1}{\pi} = 0 \pmod{\pi}.$$

以下これを証明する<sup>2</sup>.

## 2 証明

証明には Kubota-Leopoldt の  $p$  進  $L$  関数  $L_p(s, \chi\omega)$  のいくつかの性質を用いる. ここに  $\omega$  は Teichmüller 指標を表す.  $p$  進  $L$  関数  $L_p(s, \chi\omega)$  の基礎事項については Washington [5, Chapter 5] を参照している. さて素数  $p$  が  $K$  で *split* している (i.e.  $\chi(p) = 1$ ) こと, そして  $L_p(s, \chi\omega)$  の補完性質 [5, Theorem 5.11] によって等式

$$L_p(0, \chi\omega) = 0 \quad \text{及び} \quad L_p(1-p, \chi\omega) = -(1-p^{p-1}) \frac{B_{p,\chi}}{p}$$

が成立する.  $p$  進  $L$  関数  $L_p(s, \chi\omega)$  を  $s = 1$  の周りで展開した

$$L_p(s, \chi\omega) = a_0 + a_1(s-1) + a_2(s-1)^2 + \dots$$

は [5, Theorem 5.12] より任意の整数について収束し,  $a_i \in \mathbb{Z}_p$  及び  $p \mid a_i$  ( $i \geq 1$ ) が成立している.  $p \geq 5$  ならば, 引用した定理の証明をそのままなぞると次のちょっとした一般化が従う:

**Lemma 2.1.** 上記の係数  $a_i$  について,  $i \geq 2$  ならば  $p^2 \mid a_i$  が成立する.

従って  $s = 0$  が  $p$  進  $L$  関数の零点ゆえ

$$a_0 = a_1 \pmod{p^2}$$

<sup>1</sup>この条件は  $p$  進対数関数を用いることで  $\log_p(\bar{\pi}) = 0 \pmod{p^2}$  とも言い換えることができる.

<sup>2</sup>私はこの事実を明記した文献を知らないが, 事実自体は昔から知られていると思われる. 1978 年の Ferrero-Washington の論文の末尾で既述のような観察が行われている, 気がする.

が従う. 一方で, 合同式  $B_{p,\chi_K} = 0 \pmod{p^3}$  は

$$L_p(1-p, \chi\omega) = a_0 + a_1(-p) + a_2(-p)^2 = a_0 = 0 \pmod{p^2}$$

と同値である. 従って, あとは

$$a_1 = 0 \pmod{p^2} \Leftrightarrow \log_p(\bar{\pi}) = 0 \pmod{p^2}$$

が言えれば良い. これについては, Gross-Koblitz の公式と Ferrero-Greenberg の公式を合わせることで,  $p$  進  $L$  関数の  $s=0$  での微分値が

$$L'_p(0, \chi\omega) = a_1 - 2a_2 + 3a_3 - \cdots = \frac{4}{w} \log_p(\bar{\pi})$$

と表せることを用いる [2, Proposition 1 及び p.100 最下段]. ここに  $w$  は虚二次体  $K$  に含まれる 1 の冪根の数である (2, 4 または 6). 補題 2.1 より,  $p^2$  を法として考えることで合同式

$$a_1 = \frac{4}{w} \log_p(\bar{\pi}) \pmod{p^2}$$

が成立する. 全て併せて望みの主張が示された.

### 3 余談

この余談でも引き続き, 素数  $p$  は  $K$  で split すると仮定する. 記号  $\Omega$  で  $K$  の  $p$  外不分岐最大副  $p$  拡大体を表すと,  $\text{Gal}(\Omega/K)$  は階数 2 の副  $p$  自由群であることが知られている [4, (10.7.13) Theorem]. 一方, 素数  $p$  の上にある  $K$  の素点  $\mathfrak{p}$  を  $\Omega$  に延長したものの (の 1 つ) を固定すれば, それは  $p$  進数体  $\mathbb{Q}_p$  の絶対 Galois 群  $G_{\mathbb{Q}_p}$  の最大副  $p$  商  $G_{\mathbb{Q}_p}^{(p)}$  からの準同型写像

$$G_{\mathbb{Q}_p}^{(p)} \rightarrow \text{Gal}(\Omega/K)$$

を定める. そして実は副  $p$  群  $G_{\mathbb{Q}_p}^{(p)}$  も階数 2 の副  $p$  自由群であることが知られている [4, (7.5.11) Theorem (i)]. 問題はこの副有限群としては同型な 2 つの間に生じた準同型が同型か<sup>3</sup>というものであり, 実はこの写像が同型であることと, 前節でも論じた

$$\frac{\bar{\pi}^{p-1} - 1}{\pi} \neq 0 \pmod{\pi}$$

が同値になっている. そして前節で証明したことから, これは

$$B_{p,\chi} \neq 0 \pmod{p^3}$$

とも同値である. こうして Bernoulli 数  $B_{p,\chi_K}$  の  $p$ -非可除性は Galois 理論的な言い換えを持つ.

ところで Hao-Parry は通常の正則素数の判定法の類似として次の定理を証明している.

**Theorem 3.1** ([3, Theorem 1]).  $K(\zeta_p)$  の類数が  $p$  で割れないことと,  $p$  が正則であり, かつ  $B_{1,\chi}, B_{3,\chi}, \dots, B_{p-2,\chi}$  がいずれも  $p$  で割れないことは同値.

そもそも私が前節に証明したことを考え始めたきっかけは, この定理に  $B_{p,\chi}$  が含まれないよなとふと思ったからなのだが, それはさておき以前示した定理を合わせると以下が従う:

<sup>3</sup>全射なら同型であることも比較的簡単に分かる.

**Theorem 3.2.**  $K(\zeta_p)$  の  $p$  外不分岐最大副  $p$  拡大を  $\Omega_K^{\text{cyc}}$  と書くことにする.  $p$  の上の  $\Omega_K^{\text{cyc}}$  の素点に付随する準同型

$$G_{\mathbb{Q}_p(\zeta_p)}^{(p)} \rightarrow \text{Gal}(\Omega_K^{\text{cyc}}/K(\zeta_p))$$

が同型であることと,  $B_2, B_4, \dots, B_{p-3}, B_{1,\chi}, B_{3,\chi}, \dots, B_{p-2,\chi}$  がいずれも  $p$  で割れず,  $B_{p,\chi}$  が  $p^3$  で割れないことは同値である.

これで (一般化)Bernoulli 数の  $p$  進付値が最小という条件に Galois 理論的な言い換えを与えることができた.

*Remark 3.3.* 通常の素数の正則性についても類似した言い換えがある: 体  $\Omega^{\text{cyc}}$  を  $\mathbb{Q}(\zeta_p)$  の  $p$  外不分岐最大副  $p$  拡大体とすると,  $p > 2$  が正則であることと  $p$  上の分解群 (共役を除いて一つ) に付随して定まる準同型

$$G_{\mathbb{Q}_p(\zeta_p)}^{(p)} \rightarrow \text{Gal}(\Omega^{\text{cyc}}/\mathbb{Q}(\zeta_p))$$

が全射であることは同値. さて両辺の  $\mathbb{F}_p$  係数の  $H^1$  の次元を比べると右辺は左辺のちょうど半分 ( $= \frac{p+1}{2}$ ) になっていて, 残り半分は定理 3.2 が満たされる状況下において

$$\begin{array}{ccc} G_{\mathbb{Q}_p(\zeta_p)}^{(p)} & \xrightarrow{\sim} & \text{Gal}(\Omega_K^{\text{cyc}}/K(\zeta_p)) \\ & \searrow & \downarrow \\ & & \text{Gal}(\Omega^{\text{cyc}}/\mathbb{Q}(\zeta_p)) \end{array}$$

のように  $K(\zeta_p)$  の Galois 群に持ち上がっている.

## References

- [1] Leonard Carlitz. Arithmetic properties of generalized Bernoulli numbers. *J. Reine Angew. Math.*, 202:174–182, 1959.
- [2] Bruce Ferrero and Ralph Greenberg. On the behavior of  $p$ -adic  $L$ -functions at  $s = 0$ . *Invent. Math.*, 50(1):91–102, 1978/79.
- [3] Fred H. Hao and Charles J. Parry. Generalized Bernoulli numbers and  $m$ -regular primes. *Math. Comp.*, 43(167):273–288, 1984.
- [4] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.
- [5] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.