数理解析研究所講究録
第2003巻 2016年 44-54

Polynomial expressions of carries in p-ary arithmetics

産業技術総合研究所　縫田 光司
（科学技術振興機構（JST）さきがけ研究員）
k.nuida@aist.go.jp

Koji Nuida
National Institute of Advanced Industrial Science and Technology (AIST)
(JST PRESTO Researcher)

概 要

一般論として、素数位数 p の有限体 F について、F 上の任意の n 変数関数は各変数について p 次未満の何らかの n 変数多項式によって一意に表される、ということは広く知られている。ただし、具体的に与えられた関数が綺麗な多項式表示を持つかどうかはまた別の問題である。本稿では、整数を p 進法で表した際の掛け算における繰り上がりを表す具体的な多項式表示について、主に代数的な観点から紹介する。（本稿の内容は鍛冶静雄氏（山口大学）、前野俊昭氏（名城大学）、沼田泰英氏（信州大学）との共同研究に基づくものである。）

1　本研究について

本研究の出発点は、以下のよく知られた一般的事実である。

命題 1. p を素数とする。関数 $f\colon (\mathbb{F}_p)^n \to \mathbb{F}_p$ の各々について、各変数に関して $p-1$ 次以下である何らかの多項式 φ をとると、$f(a_1,\dots,a_n) = \varphi(a_1,\dots,a_n)$ がすべての $a_1,\dots,a_n \in \mathbb{F}_p$ で成り立つ。さらに、そのような多項式 φ はただ一つに定まる。

以下ではこのような φ を関数 f の多項式表示と呼ぶ。多項式表示の存在を示すよくある方法として、$a = (a_1,\dots,a_n) \in (\mathbb{F}_p)^n$ について多項式 $\varphi_a(x) = \prod_{i=1}^n (1-(x_i-a_i)^{p-1})$ を定義すると、Fermat の小定理により各変数について $1-(x_i-a_i)^{p-1}$ は $x_i = a_i$ のとき 1、$x_i \neq a_i$ のとき 0 を値にとるから、$\varphi_a(x)$ は Kronecker のデルタ $\delta_{x,a}$ の多項式表示を与えている。すると、一般の関数 f の多項式表示は $\varphi(x) = \sum_{a\in(\mathbb{F}_p)^n} f(a)\varphi_a(x)$ で得られる。（なお、多項式表示の一意性については、1 変数多項式の剰余定理を各変数に再帰的に適用することで、零関数 $f \equiv 0$ の（次数の条件を満たす）多項式表示が零多項式に限られることが示され、このことから一般の関数についての性質も直ちに得られる。）

上記の標準的議論で得られる多項式表示はデルタ関数 $\delta_{x,a}$ の多項式表示 φ_a の一次結合として構成されているが、φ_a の展開式自体が多くの項を持つことから、その一次結合をとる際に多くの係数の打ち消し合いが発生していると考えられる。この観点では、上記の一般的な多項式表示は冗長性を持っており、係数の打ち消し合い後の多項式が具体的にどのような形をしているかはまた別の問題である。本研究では、非負整数を p 進法で表した際の掛け算における繰り上がり関数を対象に、その具体的な多項式表示について調べた。なお、整数の p 進法表示の各桁の数字も掛け算の繰り上がりの値も、本来は 0 以上 $p-1$ 以下の整数なのであるが、以下ではそれらを $\mathbb{F}_p$ の元と自然に同一視することで、繰り上がり関数を $\mathbb{F}_p$ 上の関数とみている（後述）。

こうした関数の多項式表示の問題は、純粋に数学的な興味だけでなく、以下のように暗号理論の分野との関連性も存在する。近年の暗号分野で盛んに研究されている「完全準同型暗号」という特殊な暗号化技術においては、有限体 $\mathbb{F}_p$ を暗号化前のデータ（「平文」と呼ばれる）の集合とし、暗号文どうしにある特別な操作を施すことで、対応する平文どうしの和や積を計算することが可能である。標語的に述べるならば、平文 $m \in \mathbb{F}_p$ の暗号文を $\mathsf{Enc}(m)$ で表すとき（Enc は暗号化 encryption の略）、暗号文に対するある演算 $\boxplus, \boxtimes$ について、$\mathsf{Enc}(m_1) \boxplus \mathsf{Enc}(m_2) = \mathsf{Enc}(m_1 + m_2)$ および $\mathsf{Enc}(m_1) \boxtimes \mathsf{Enc}(m_2) = \mathsf{Enc}(m_1 m_2)$ が成り立つ。2009 年に提示された最初の方式 [2] では $p = 2$、つまり平文はビット 0 または 1 のみであったが、現在はより一般の素数 p を法とする平文を扱える方式も知られており、著者らによる方式 [6] はその一例である。さて、上記のように平文の和と積に対応する暗号文の演算が得られていると、その組合せにより平文の多項式関数を暗号化のまま計算することが可能となる。命題 1 を踏まえると、これは平文に対する任意の関数を暗号化のまま（少なくとも原理的には）計算できることを意味する。このように、完全準同型暗号を用いて平文の関数を暗号化状態で計算しようとする場合、まずはその関数の多項式表示を特定する必要があるため、本稿で扱う関数の多項式表示の研究が応用上も意味を帯びてくる。

なお、本研究で特に掛け算の繰り上がり関数の多項式表示を調べた理由として、まず、掛け算ではなく（二つに限らずより多くの数の）足し算の繰り上がり関数の多項式表示については、$p = 2$ の場合には基本対称多項式により与えられることが知られていた（初出は未確認であるが、少なくとも 2000 年の Boyar らの論文 [1] にて述べられている）。我々の研究ではまず、この足し算の繰り上がり関数についての結果を一般の素数 p の場合へと拡張した（本稿では割愛する。詳細はプレプリント [4] を参照されたい）。そして、足し算ができたのだから次は掛け算だろう、というごく健全な（？）動機で掛け算の繰り上がり関数について調べた、という経緯である。

2 記号など

本稿では p は素数を表す。整数を p で割った余りをとる写像 $\mathbb{Z} \to \mathbb{F}_p$、$a \mapsto a \bmod p$、は $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}$ に制限すると全単射になる。その逆写像による $x \in \mathbb{F}_p$ の像を $x_{\mathbb{Z}}$ で表す。紛らわしくないときは単に x と書いてしまうときもある。また、整数 $N \geq 2$ と、分母が N と互いに素である $a = \alpha/\beta \in \mathbb{Q}$（$\alpha, \beta \in \mathbb{Z}$）について、$a$ を自然に $\mathbb{Z}/N\mathbb{Z}$ の元とみなしたものを

$$a^{\langle N \rangle} := (\alpha \bmod N) \cdot (\beta \bmod N)^{-1} \in \mathbb{Z}/N\mathbb{Z}$$

で表す（$(\beta \bmod N)^{-1}$ は $\mathbb{Z}/N\mathbb{Z}$ における逆元である）。紛らわしくないときは単に a と書いてしまうこともある。a の表示が既約分数でなくても同じ元を定めることに念のため注意されたい。その他、本稿では整数 N を法とする合同関係を $x \equiv y \pmod N$ などの代わりに $x \equiv_N y$ と表す。

3 主結果

p 進法で 1 桁の数二つを掛け算したときに繰り上がりがどうなるかを考える。p 進法で 1 桁の数は $0, 1, \ldots, p-1$ のいずれかであり、それらは前述の記号を用いると $a_{\mathbb{Z}}$（$a \in \mathbb{F}_p$）のように表せる。同様に、掛け算の繰り上がりの値も 0 から $p-1$ まで（実際には $p-2$ まで）なので、やはり $\mathbb{F}_p$ の元によって表せる。このようにしてできる 2 変数関数 $(\mathbb{F}_p)^2 \to \mathbb{F}_p$ を ψ_1 と書く。前述の記号を用いると、$x, y \in \mathbb{F}_p$ について

$$x_{\mathbb{Z}} \cdot y_{\mathbb{Z}} = \psi_1(x, y)_{\mathbb{Z}} \cdot p + (xy)_{\mathbb{Z}}$$

である。なお、2進法のときは $1\cdot 1=1$ であるから、1桁の数を掛け算している分には繰り上がりは生じない。そこで、以下では $p>2$ と仮定する。

また、上記の一般化として、より多くの数を掛け算したときに下から i 桁目（最下位桁を0桁目と数える）への繰り上がり値を与える関数を ψ_i で表す。つまり、$x_1,\dots,x_n\in\mathbb{F}_p$ について

$$(x_1)_{\mathbb{Z}}(x_2)_{\mathbb{Z}}\cdots(x_n)_{\mathbb{Z}}=\psi_0(x_1,\dots,x_n)_{\mathbb{Z}}+\psi_1(x_1,\dots,x_n)_{\mathbb{Z}}\cdot p+\psi_2(x_1,\dots,x_n)_{\mathbb{Z}}\cdot p^2+\cdots$$

である。定義より直ちに $\psi_0(x_1,\dots,x_n)=x_1\cdots x_n$（$\mathbb{F}_p$ の元としての積）であることに注意されたい。なお、折角上位桁にまで一般化したものの、本稿で扱うのは ψ_1 のみである。$i\geq 2$ についての ψ_i がどのように多項式表示されるかは今後の研究課題である。

関数 ψ_1 の多項式表示について、筆者らのプレプリント [4] では下記の結果を与えている。

定理 2. $p>2$ を素数とする。このとき、下記の多項式

$$\Psi(t)=\sum_{j=1}^{p-2}\left(\frac{B_{p-1-j}}{p-1-j}\right)^{\langle p\rangle}t^j\in\mathbb{F}_p[t]$$

を用いると、整数 $n\geq 1$ と $x_1,\dots,x_n\in\mathbb{F}_p$ について

$$\psi_1(x_1,\dots,x_n)=x_1\cdots x_n\left(\Psi(x_1\cdots x_n)-\sum_{j=1}^{n}\Psi(x_j)+(n-1)\Psi(1)\right)\tag{1}$$

が成り立つ。ここで B_k は Bernoulli 数である。（どうやら Bernoulli 数の定義には二通りの流儀があるらしいのであるが、ここでは符号が $B_1=-1/2$ となる方を採用している。母関数による定義としては $t/(e^t-1)=\sum_{k\geq 0}B_kt^k/k!$ である。）

掛け算の繰り上がりといった素朴な対象の表示に Bernoulli 数が現れるのは興味深い現象ではないだろうか。[4] では定理の証明として、（Bernoulli 数についての事実をいくつか使う以外は）掛け算の結合法則に基づく初等的な方針と、群のコホモロジーを用いる代数的な方針[1]の二つを述べている。本稿では後者の道筋で上記定理の証明を紹介する。（なお、プレプリント [4] の公表時点では知らなかったことなのだが、実は上記の結果は論文 [8]（特に Theorem 9.1(a) と Theorem 11.2）において既に述べられていたのであった[2]。このことは本研究集会での発表後の休み時間に宗政昭弘先生より教えていただいた。ちなみに論文 [8] における証明の方針は上記二つの方針とも異なり、繰り上がり関数と Witt ベクトルとの関連性を手掛かりとするものである。）

証明の紹介の前に定理2についていくつか補足する。そのために以下の事実を用いる（例えば [3] の Chapter 15 を参照されたい）。

定理 3 (von Staudt–Clausen)**.** $k>0$ が偶数のとき、$B_k+\sum_{q;\text{ prime},\ q-1|k}1/q\in\mathbb{Z}$ が成り立つ。

この定理と、3以上の奇数 k について $B_k=0$ という事実から、Ψ の定義の係数に現れる有理数の分母は p と互いに素であり、Ψ は確かに $\mathbb{F}_p$ 上の多項式となる。また、$\Psi(t)$ は $(p-1)/2$ 個の（係数が0でない）単項式からなり、したがって $\psi_1(x_1,\dots,x_n)$ は $(p-1)(n+1)/2$ 個あるいは $(p-1)(n+1)/2+1$ 個の単項式からなる（最後の1個の有無は $(n-1)\Psi(1)$ が0かどうかに依存する）。一般の n 変数関数の（各変数について次数が最小な）多項式表示が最大で p^n 個の単項式

[1] この方針は山下剛氏の示唆に基づいている。

[2] 論文 [8] では $n=2$ の場合しか述べられていないため、一見すると今回の結果の方が強いようにも見えるが、実際には一般の n についての結果は $n=2$ での結果より簡単に導かれる。詳しくは [4] を参照されたい。

を持つことを鑑みると、ψ_1 は大幅に疎な多項式表示を持っているといえよう。さらに、上述の残りの項 $(n-1)\Psi(1)$ については、

$$\Psi(1) = \left(\frac{(p-1)!+1}{p}\right)^{\langle p\rangle} = \left(B_{p-1} + \frac{1}{p} - 1\right)^{\langle p\rangle}$$

が成り立つ（[4] あるいは [8]）。ここで $(p-1)!+1 \equiv_p 0$ であり（Wilson の定理）、また前述の von Staudt–Clausen の定理により $B_{p-1}+1/p \in \mathbb{Q}$ の分母は p と互いに素であるから、上の式の各項は確かに意味を持つ。$w_p := ((p-1)!+1)/p \in \mathbb{Z}$ は Wilson 商と呼ばれており、[7] の項目 A002068 によると、$w_p \equiv_p 0$（したがって $\Psi(1)=0$）となる素数 p は現時点で 5 と 13 と 563 の三つしか知られていないようである。

4 群のコホモロジー

この節では群のコホモロジーについての予備知識をまとめる。G を群（演算を乗法で書く）、A を G が左から作用する可換群（演算を加法で書く）とするとき、A に係数を持つ G の整数係数コホモロジー群は

$$H^n(G;A) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

で定義される。ここで A は G の作用により自然に左 $\mathbb{Z}[G]$-加群の構造を持ち、また $\mathbb{Z}$ も G の自明な作用を通じて左 $\mathbb{Z}[G]$-加群とみなしている。

$H^n(G;A)$ の計算に用いる $\mathbb{Z}$ の具体的な射影分解の構成法の一つとして以下のものが知られている。各 $k \geq 0$ について、$P_k := \mathbb{Z}[G^{k+1}]$ とし、対角的な埋め込み $G \hookrightarrow G^{k+1}$ を通して P_k への G の左作用を得る。つまり、$(g_0, g_1, \ldots, g_k) \in P_k$ と $h \in G$ について $h\cdot(g_0, g_1, \ldots, g_k) = (hg_0, hg_1, \ldots, hg_k)$ である。このとき、

$$\langle g_1|g_2|\cdots|g_k\rangle := (1, g_1, g_1g_2, \ldots, g_1g_2\cdots g_k)\ (g_1, \ldots, g_k \in G)$$

という形の元全体は P_k の左 $\mathbb{Z}[G]$-加群としての基底をなす。また、$\mathbb{Z}$-加群としての準同型写像 $d_{k-1}\colon P_k \to P_{k-1}$ を $d_{k-1}((g_0,\ldots,g_k)) = \sum_{i=0}^{k}(-1)^i(g_0,\ldots,g_{i-1},g_{i+1},\ldots,g_k)$ で定義する。ここで d_{-1} の定義においては $P_{-1} := \mathbb{Z}[G^0] = \mathbb{Z}[\{1\}] \simeq \mathbb{Z}$ としており、$d_{-1}(\sum_g c_g g) = \sum_g c_g$ が成り立つことを注意しておく。このように定義した d_k たちは G の作用と可換で $\mathbb{Z}[G]$-加群の準同型写像になり、また系列 $\cdots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{d_{-1}} \mathbb{Z} \to 0$ は完全であることが示される。こうして $\mathbb{Z}[G]$-加群としての $\mathbb{Z}$ の射影分解が得られたので、対応する複体

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A) \xrightarrow{\partial^0} \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A) \xrightarrow{\partial^1} \mathrm{Hom}_{\mathbb{Z}[G]}(P_2, A) \xrightarrow{\partial^2} \cdots$$

によって $H^n(G;A) = \ker(\partial^n)/\mathrm{Im}(\partial^{n-1})$ と計算できる。なお、$f \in \mathrm{Hom}_{\mathbb{Z}[G]}(P_n, A)$ と P_{n+1} の基底の元 $\langle g_1|\cdots|g_{n+1}\rangle$ について、

$$\begin{aligned}
&d_n(\langle g_1|\cdots|g_{n+1}\rangle) = d_n((1, g_1, g_1g_2, \ldots, g_1g_2\cdots g_{n+1}))\\
&= (g_1, g_1g_2, \ldots, g_1g_2\cdots g_{n+1}) + \sum_{j=1}^{n+1}(-1)^j(1, g_1, \ldots, \widehat{g_1\cdots g_j}, \ldots, g_1\cdots g_{n+1})\\
&= g_1\cdot(1, g_2, \ldots, g_2\cdots g_{n+1}) + \sum_{j=1}^{n}(-1)^j\langle g_1|\cdots|g_{j-1}|g_jg_{j+1}|g_{j+2}|\cdots|g_{n+1}\rangle + (-1)^{n+1}\langle g_1|\cdots|g_n\rangle\\
&= g_1\cdot\langle g_2|\cdots|g_{n+1}\rangle + \sum_{j=1}^{n}(-1)^j\langle g_1|\cdots|g_{j-1}|g_jg_{j+1}|g_{j+2}|\cdots|g_{n+1}\rangle + (-1)^{n+1}\langle g_1|\cdots|g_n\rangle
\end{aligned}$$

であることから

$$\partial^n(f)(\langle g_1|\cdots|g_{n+1}\rangle) = f(d_n(\langle g_1|\cdots|g_{n+1}\rangle))$$
$$= g_1 \cdot f(\langle g_2|\cdots|g_{n+1}\rangle) + \sum_{j=1}^{n}(-1)^j f(\langle g_1|\cdots|g_{j-1}|g_jg_{j+1}|g_{j+2}|\cdots|g_{n+1}\rangle) + (-1)^{n+1} f(\langle g_1|\cdots|g_n\rangle)$$

となる。今、P_n の基底の元 $\langle g_1|\cdots|g_n\rangle$ を $(g_1,\ldots,g_n)\in G^n$ と同一視することで、$f\in \mathrm{Hom}_{\mathbb{Z}[G]}(P_n,A)$ も $f\colon G^n\to A$ と自然に同一視されるが、このとき写像 $\partial^n(f)\colon G^{n+1}\to A$ は

$$\partial^n(f)(g_1,\ldots,g_{n+1})$$
$$= g_1 \cdot f(g_2,\ldots,g_{n+1}) + \sum_{j=1}^{n}(-1)^j f(g_1,\ldots,g_{j-1},g_jg_{j+1},g_{j+2},\ldots,g_{n+1}) + (-1)^{n+1} f(g_1,\ldots,g_n)$$

で与えられる。

次に、G を群、A を可換群とし、$0\to A\xrightarrow{\iota} W\xrightarrow{\pi} G\to 1$ を群の完全列とする（W の演算は乗法で書く）と、$\iota(\pi(x)\cdot a) := x\iota(a)x^{-1}$（$x\in W$、$a\in A$）により G の A への作用が矛盾なく定義される。また、$G\ni g\mapsto \widetilde{g}\in W$ を（必ずしも分裂しない）セクションとすると、$x,y\in G$ のとき $\widetilde{x}\cdot\widetilde{y}\cdot\widetilde{xy}^{-1}\in\ker(\pi)=\mathrm{Im}(\iota)$ が成り立つので、写像 $f\colon G^2\to A$ が $\iota(f(x,y)) := \widetilde{x}\cdot\widetilde{y}\cdot\widetilde{xy}^{-1}$ により定義される。この写像は前述の複体における 2-cocycle になることが知られており、したがって $H^2(G;A)$ の元を定める。（主に著者自身の）確認のため証明も記しておく。

補題 4. 上記の写像 $f\colon G^2\to A$ は $\ker(\partial^2)$ に属する。

証明. A の可換性を用いて項を入れ替えると、$x,y,z\in G$ について

$$\partial^2(f)(x,y,z) = f(x,yz) - f(xy,z) - f(x,y) + x\cdot f(y,z)$$

が成り立つ。よって

$$\begin{aligned}\iota(\partial^2(f)(x,y,z)) &= \left(\widetilde{x}\widetilde{yz}\widetilde{xyz}^{-1}\right)\left(\widetilde{xy}\widetilde{z}\widetilde{xyz}^{-1}\right)^{-1}\left(\widetilde{xy}\widetilde{xy}^{-1}\right)^{-1}\left(\widetilde{xy}\widetilde{yz}\widetilde{yz}^{-1}\widetilde{x}^{-1}\right)\\ &= \left(\widetilde{x}\widetilde{yz}\widetilde{xyz}^{-1}\right)\left(\widetilde{xyz}\widetilde{z}^{-1}\widetilde{xy}^{-1}\right)\left(\widetilde{xy}\widetilde{y}^{-1}\widetilde{x}^{-1}\right)\left(\widetilde{xy}\widetilde{yz}\widetilde{yz}^{-1}\widetilde{x}^{-1}\right) = 1\end{aligned}$$

すなわち $\partial^2(f)(x,y,z)=0$ である。 □

以下、上記の完全列が分裂する場合を考え、$G\ni x\mapsto[x]\in W$ を対応するセクションとする。すなわち $W=\iota(A)\rtimes[G]$ である。ここで、$\widetilde{(\cdot)}$ も $[\cdot]$ もセクションなので、各 $x\in G$ について $\widetilde{x}[x]^{-1}\in\ker(\pi)=\iota(A)$ であり、$\widetilde{x}=\iota(\eta(x))[x]$ によって写像 $\eta\colon G\to A$ が定まる。このとき以下が成り立つ。

補題 5. 上記の状況において $f=\partial^1(\eta)$ が成り立つ。

証明. A の可換性により項を入れ替えると、$x,y\in G$ について $\partial^1(\eta)(x,y)=\eta(x)+x\cdot\eta(y)-\eta(xy)$ が成り立つ。よって

$$\iota(\partial^1(\eta)(x,y)) = \iota(\eta(x))\cdot\left([x]\iota(\eta(y))[x]^{-1}\right)\cdot\iota(\eta(xy))^{-1} = \widetilde{x}\cdot\widetilde{y}[y]^{-1}\cdot[x]^{-1}\cdot[xy]\widetilde{xy}^{-1}$$

となる。定義より $[xy]=[x][y]$ であるから、上式の右辺は $\widetilde{x}\widetilde{y}\widetilde{xy}^{-1}=\iota(f(x,y))$ に等しい。 □

5 主結果の証明（前半）

以下、定理2の証明を述べる。まず、ψ_1 の定義より

$$(x_1)_{\mathbb{Z}}\cdots(x_{n-1})_{\mathbb{Z}} \equiv_{p^2} (x_1\cdots x_{n-1})_{\mathbb{Z}} + \psi_1(x_1,\ldots,x_{n-1})_{\mathbb{Z}}\cdot p$$

であるから、

$$\begin{aligned}&\big((x_1)_{\mathbb{Z}}\cdots(x_{n-1})_{\mathbb{Z}}\big)(x_n)_{\mathbb{Z}}\\ &\equiv_{p^2} ((x_1\cdots x_n)_{\mathbb{Z}} + \psi_1(x_1\cdots x_{n-1},x_n)_{\mathbb{Z}}\cdot p) + (\psi_1(x_1,\ldots,x_{n-1})x_n)_{\mathbb{Z}}\cdot p \qquad (2)\\ &= (x_1\cdots x_n)_{\mathbb{Z}} + (\psi_1(x_1\cdots x_{n-1},x_n)_{\mathbb{Z}} + (\psi_1(x_1,\ldots,x_{n-1})x_n)_{\mathbb{Z}})\cdot p\end{aligned}$$

よって

$$\psi_1(x_1,\ldots,x_n) = \psi_1(x_1\cdots x_{n-1},x_n) + \psi_1(x_1,\ldots,x_{n-1})x_n$$

が成り立つ。この漸化式を用いると、$n\geq 3$ についての定理の主張を $n=2$ の場合に帰着できる。そこで以下では $n=2$ のときを考える。

（変数の名前を置き換えて）上の議論より

$$\psi_1(x,y,z) = \psi_1(xy,z) + \psi_1(x,y)z$$

が成り立つ。一方、(2) 式で $(x_{\mathbb{Z}}y_{\mathbb{Z}})z_{\mathbb{Z}}$ の代わりに $x_{\mathbb{Z}}(y_{\mathbb{Z}}z_{\mathbb{Z}})$ を考えることで、

$$\psi_1(x,y,z) = \psi_1(x,yz) + x\psi_1(y,z)$$

が得られる。よって

$$\psi_1(xy,z) + \psi_1(x,y)z = \psi_1(x,yz) + x\psi_1(y,z) \qquad (3)$$

となる。この関係式の両辺における各単項式の係数を比較して ψ_1 の形を絞り込むのが [4] における元々の方針であるが、ここでは群のコホモロジーを経由する方針を紹介する。群の完全列

$$1\to 1+p\mathbb{Z}/p^2\mathbb{Z}\hookrightarrow(\mathbb{Z}/p^2\mathbb{Z})^\times \overset{\bmod p}{\to} {\mathbb{F}_p}^\times\to 1$$

と群の同型 $1+p\mathbb{Z}/p^2\mathbb{Z}\simeq\mathbb{F}_p$、$a\mapsto(a-1)/p$ を合わせると、完全列

$$0\to\mathbb{F}_p\overset{\iota}{\to}(\mathbb{Z}/p^2\mathbb{Z})^\times \overset{\bmod p}{\to} {\mathbb{F}_p}^\times\to 1$$

が得られる。すると4節の議論により ${\mathbb{F}_p}^\times$ の $\mathbb{F}_p$ への作用が定まるが、$(\mathbb{Z}/p^2\mathbb{Z})^\times$ が可換群であることからそれは自明な作用であることを注意する。また、セクション $\widetilde{(\cdot)}\colon {\mathbb{F}_p}^\times\to(\mathbb{Z}/p^2\mathbb{Z})^\times$、$x \bmod p\mapsto x \bmod p^2$ から得られる 2-cocycle を $f\colon({\mathbb{F}_p}^\times)^2\to\mathbb{F}_p$ で表すと、$f(x,y) = (\widetilde{x}\widetilde{y}\widetilde{xy}^{-1}-1)/p$ である。ここで $\widetilde{x}\widetilde{y} = (xy)_{\mathbb{Z}} + \psi_1(x,y)_{\mathbb{Z}}\cdot p \equiv_{p^2} \widetilde{xy} + \psi_1(x,y)_{\mathbb{Z}}\cdot p$ であるから、$x,y\in{\mathbb{F}_p}^\times$ について

$$f(x,y) = \frac{\psi_1(x,y)_{\mathbb{Z}}}{\widetilde{xy}} \equiv_p \frac{\psi_1(x,y)}{xy}$$

である。この f が 2-cocycle であるという条件を書き下すと、${\mathbb{F}_p}^\times$ の作用が自明なので

$$\frac{\psi_1(y,z)}{yz} - \frac{\psi_1(xy,z)}{xyz} + \frac{\psi_1(x,yz)}{xyz} - \frac{\psi_1(x,y)}{xy} = 0$$

となり、これは条件 (3) と等価である。

次に、Fermat の小定理により $\mathbb{F}_p{}^\times \ni x \mapsto [x] := (\widetilde{x})^p \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ は上記の完全列のセクションである。また $\widetilde{x}\widetilde{y} \equiv_{p^2} \widetilde{xy} + \psi_1(x,y)_{\mathbb{Z}} \cdot p$ と二項定理より $(\widetilde{x}\widetilde{y})^p \equiv_{p^2} (\widetilde{xy})^p$ であり、$[\cdot]$ は準同型となる。こうして上記の完全列は分裂する。すると補題 5 により、ある $\overline{\Psi}\colon \mathbb{F}_p{}^\times \to \mathbb{F}_p$ を用いて

$$\frac{\psi_1(x,y)}{xy} = f(x,y) = \partial^1(\overline{\Psi})(x,y) = \overline{\Psi}(y) - \overline{\Psi}(xy) + \overline{\Psi}(x)$$

すなわち $x, y \in \mathbb{F}_p{}^\times$ について

$$\psi_1(x,y) = xy(-\overline{\Psi}(xy) + \overline{\Psi}(x) + \overline{\Psi}(y)) \tag{4}$$

と表せる。ここで $|\mathbb{F}_p{}^\times| = p-1$ より、$\overline{\Psi}$ は高々 $p-2$ 次の多項式で定まる関数 $\mathbb{F}_p \to \mathbb{F}_p$ へと一意に拡張される。このように定義域を拡張しても (4) 式は引き続き成り立つ（$\psi_1(0,y) = \psi_1(x,0) = 0$ なので）。(4) 式と $\psi_1(1,1) = 0$ より $\overline{\Psi}(1) = 0$ であることに注意されたい。$\Psi(x) := \overline{\Psi}(0) - \overline{\Psi}(x)$ と定義すれば Ψ も高々 $p-2$ 次の多項式で、$\Psi(0) = 0$、$\Psi(1) = \overline{\Psi}(0)$、$\overline{\Psi}(x) = \Psi(1) - \Psi(x)$ となり、これらを (4) 式に代入することで定理 2 の表示 (1) が得られる。

なお、4 節の議論により、上記の写像 $\overline{\Psi}$ は $\overline{\Psi}(x) \equiv_p (\widetilde{x}[x]^{-1} - 1)/p$（$x \in \mathbb{F}_p{}^\times$）により定まる。すると

$$x\overline{\Psi}(x) \equiv_p [x]\left(\frac{\widetilde{x}[x]^{-1} - 1}{p}\right)^{\langle p\rangle} = \left(\frac{\widetilde{x} - [x]}{p}\right)^{\langle p\rangle} = -x \cdot q_p(x_{\mathbb{Z}})^{\langle p\rangle}$$

したがって $\overline{\Psi}(x) = -q_p(x_{\mathbb{Z}})^{\langle p\rangle}$ が成り立つ。ここで $q_p(a) := (a^{p-1} - 1)/p$ であり、Fermat 商と呼ばれている。この Fermat 商と Wilson 商 w_p の間には以下の関係が知られている [5]：

$$\sum_{a=1}^{p-1} q_p(a) \equiv_p w_p \ .$$

この関係式と、$1 \le j \le p-2$ について $\sum_{x\in\mathbb{F}_p{}^\times} x^j = 0$ という事実から、

$$w_p \equiv_p -\sum_{x\in\mathbb{F}_p{}^\times} \overline{\Psi}(x) \equiv_p -(p-1)\overline{\Psi}(0) \equiv_p \overline{\Psi}(0) = \Psi(1)$$

が得られる。

6 主結果の証明（後半）

最後に、定理 2 にある Ψ の表示の証明を述べる。なお、前述の通り Ψ が Fermat 商や Wilson 商を用いて表されたのであるからそれらの数の性質を用いた証明も存在してしかるべきであるが、ここでは [4] と同じく関数 ψ_1 の定義に立ち戻った証明の方針を採る。

前節で示した通り、多項式 $\Psi(t)$ は高々 $p-2$ 次であり $\Psi(0) = 0$ であるので、それを $\Psi(t) = \sum_{j=1}^{p-2} \beta_j t^j$ と表しておく。また、$\mathbb{F}_p{}^\times$ の生成元 ξ を一つ選んでおく。すると、各 $1 \le i \le p-2$ について、$\psi_1(x,\xi) = \xi x(\Psi(\xi x) - \Psi(x) - \Psi(\xi) + \Psi(1))$ における x^{i+1} の係数は $\beta_i\xi(\xi^i - 1)$ と表せる。他方、各整数 $0 \le k \le \xi_{\mathbb{Z}} - 1$ について、ψ_1 の定義より $x \in \mathbb{F}_p$ が $\psi_1(x,\xi) = k$ を満たすのは $\lceil kp/\xi_{\mathbb{Z}}\rceil \le x_{\mathbb{Z}} \le \lceil (k+1)p/\xi_{\mathbb{Z}}\rceil - 1$ のときである。このことから、

$$\psi_1(x,\xi) = \sum_{k=1}^{\xi_{\mathbb{Z}}-1} \sum_{z=\lceil kp/\xi_{\mathbb{Z}}\rceil}^{\lceil (k+1)p/\xi_{\mathbb{Z}}\rceil - 1} k \cdot \delta_{x,z} = \sum_{k=1}^{\xi_{\mathbb{Z}}-1} \sum_{z=\lceil kp/\xi_{\mathbb{Z}}\rceil}^{\lceil (k+1)p/\xi_{\mathbb{Z}}\rceil - 1} k \cdot (1 - (x-z)^{p-1})$$

と表せる。右辺における x^{i+1} の係数を計算すると

$$-\sum_{k=1}^{\xi_{\mathbb{Z}}-1}\sum_{z=\lceil kp/\xi_{\mathbb{Z}}\rceil}^{\lceil (k+1)p/\xi_{\mathbb{Z}}\rceil-1} k\binom{p-1}{i+1}(-z)^{p-i-2} \equiv_p -\sum_{k=1}^{\xi_{\mathbb{Z}}-1}\sum_{z=\lceil kp/\xi_{\mathbb{Z}}\rceil}^{\lceil (k+1)p/\xi_{\mathbb{Z}}\rceil-1} kz^{p-i-2}$$

となる。ここで関係式 $\binom{p-1}{i+1} \equiv_p (-1)^{i+1}$ と $(-1)^{p-1}=1$ を用いた。さらに、右辺について

$$\begin{aligned}
-\sum_{k=1}^{\xi_{\mathbb{Z}}-1}\sum_{z=\lceil kp/\xi_{\mathbb{Z}}\rceil}^{\lceil (k+1)p/\xi_{\mathbb{Z}}\rceil-1} kz^{p-i-2} &= -\sum_{k=1}^{\xi_{\mathbb{Z}}-1} k\left(\sum_{z=1}^{\lceil (k+1)p/\xi_{\mathbb{Z}}\rceil-1} z^{p-i-2} - \sum_{z=1}^{\lceil kp/\xi_{\mathbb{Z}}\rceil-1} z^{p-i-2}\right)\\
&= -(\xi-1)\sum_{z=1}^{p-1} z^{p-i-2} + \sum_{k=1}^{\xi_{\mathbb{Z}}-1}\sum_{z=1}^{\lceil kp/\xi_{\mathbb{Z}}\rceil-1} z^{p-i-2}\\
&\equiv_p (\xi-1)\delta_{i,p-2} + \sum_{k=1}^{\xi_{\mathbb{Z}}-1}\sum_{z=1}^{\lceil kp/\xi_{\mathbb{Z}}\rceil-1} z^{p-i-2}
\end{aligned}$$

と変形できる。したがって

$$\beta_i\xi(\xi^i-1) \equiv_p (\xi-1)\delta_{i,p-2} + \sum_{k=1}^{\xi_{\mathbb{Z}}-1}\sum_{z=1}^{\lceil kp/\xi_{\mathbb{Z}}\rceil-1} z^{p-i-2} \tag{5}$$

が成り立つ。

ここからは、以下のように定義される Bernoulli 多項式

$$B_m(x) = \sum_{s=0}^{m}\binom{m}{s}B_{m-s}x^s \tag{6}$$

の性質を用いる。ここで $B_m(0)=B_m$ である。また、二項係数の定義と von Staudt–Clausen の定理により、$0 \le m \le p-2$ の範囲では $B_m(x)$ を $\mathbb{F}_p$ 上の多項式とみなせることに注意されたい。この Bernoulli 多項式に関する事実として、整数 $m, N \ge 0$ について

$$\sum_{k=1}^{N} k^m = \frac{1}{m+1}\big(B_{m+1}(N+1) - B_{m+1}(1)\big) \tag{7}$$

が成り立つ（例えば [3] の Chapter 15 を参照されたい）[3]。すると、(5) 式の右辺について

$$\begin{aligned}
&(\xi-1)\delta_{i,p-2} + \sum_{k=1}^{\xi_{\mathbb{Z}}-1}\sum_{z=1}^{\lceil kp/\xi_{\mathbb{Z}}\rceil-1} z^{p-i-2}\\
&= (\xi-1)\delta_{i,p-2} + \sum_{k=1}^{\xi_{\mathbb{Z}}-1}\frac{1}{p-i-1}\big(B_{p-i-1}(\lceil kp/\xi_{\mathbb{Z}}\rceil) - B_{p-i-1}(1)\big)\\
&= (\xi-1)\delta_{i,p-2} + \frac{1}{p-i-1}\left(\sum_{k=1}^{\xi_{\mathbb{Z}}-1} B_{p-i-1}(\lceil kp/\xi_{\mathbb{Z}}\rceil) - (\xi-1)B_{p-i-1}(1)\right)
\end{aligned}$$

となる。ここで各 $1 \le k \le \xi_{\mathbb{Z}}-1$ について $\delta_k := kp \bmod \xi_{\mathbb{Z}}$ と定めると、$\xi_{\mathbb{Z}}$ と p が互いに素であることから δ_1 は巡回群 $\mathbb{Z}/\xi_{\mathbb{Z}}\mathbb{Z}$ の生成元となる。このことから、$\delta_1, \ldots, \delta_{\xi_{\mathbb{Z}}-1}$ は 1 から $\xi_{\mathbb{Z}}-1$ までの値

[3] プレプリント [4] で用いた関係式を類似した別の式に変更したことで以下の議論の場合分けが不要になった。この改良は金子昌信先生の示唆に基づいている。

をちょうど一度ずつとることがわかる。さらに、δ_k の定義より $\lceil kp/\xi_{\mathbb{Z}} \rceil = kp/\xi_{\mathbb{Z}} + (\xi_{\mathbb{Z}} - \delta_k)/\xi_{\mathbb{Z}}$ と表せて、$\xi_{\mathbb{Z}} - \delta_k$ たちも 1 から $\xi_{\mathbb{Z}} - 1$ までの値をちょうど一度ずつとる。上の表示より $\lceil kp/\xi_{\mathbb{Z}} \rceil^{\langle p \rangle} = ((\xi_{\mathbb{Z}} - \delta_k)/\xi_{\mathbb{Z}})^{\langle p \rangle}$ が成り立つので、

$$\left(\sum_{k=1}^{\xi_{\mathbb{Z}}-1} B_{p-i-1}(\lceil kp/\xi_{\mathbb{Z}} \rceil) \right)^{\langle p \rangle} = \left(\sum_{k=1}^{\xi_{\mathbb{Z}}-1} B_{p-i-1} \left(\frac{\xi_{\mathbb{Z}} - \delta_k}{\xi_{\mathbb{Z}}} \right) \right)^{\langle p \rangle} = \left(\sum_{k=1}^{\xi_{\mathbb{Z}}-1} B_{p-i-1} \left(\frac{k}{\xi_{\mathbb{Z}}} \right) \right)^{\langle p \rangle}$$

となる。さらに以下の事実を用いる（例えば [3] の Chapter 15 を参照されたい）。

定理 6. 整数 $m \geq 1$ と $n \geq 0$ について、

$$B_n(mx) = m^{n-1} \sum_{k=0}^{m-1} B_n \left(x + \frac{k}{m} \right)$$

が成り立つ。

この関係式を用いると、（$\xi^{p-1} \equiv_p 1$ なので）

$$\left(\sum_{k=1}^{\xi_{\mathbb{Z}}-1} B_{p-i-1} \left(\frac{k}{\xi_{\mathbb{Z}}} \right) \right)^{\langle p \rangle} = \left(\frac{B_{p-1-i}(0)}{\xi_{\mathbb{Z}}^{p-i-2}} - B_{p-1-i}(0) \right)^{\langle p \rangle} = (\xi^{i+1} - 1)(B_{p-1-i})^{\langle p \rangle}$$

となる。以上より、(5) 式の右辺は $\mathbb{F}_p$ において

$$(\xi - 1)\delta_{i,p-2} + \frac{1}{p-1-i} \left((\xi^{i+1} - 1)B_{p-1-i} - (\xi - 1)B_{p-1-i}(1) \right)$$

に等しい。ここで、整数 $n \geq 1$ について $B_n(1) = (-1)^{\delta_{n,1}} B_n$ であることが知られているため、上記の値はさらに

$$\begin{aligned} &(\xi - 1)\delta_{i,p-2} + \frac{1}{p-1-i} \left((\xi^{i+1} - 1)B_{p-1-i} - (-1)^{\delta_{i,p-2}}(\xi - 1)B_{p-1-i} \right) \\ &\quad = (\xi - 1)\delta_{i,p-2} + ((\xi^{i+1} - 1) - (-1)^{\delta_{i,p-2}}(\xi - 1)) \frac{B_{p-1-i}}{p-1-i} \end{aligned}$$

に等しい。なお、$i = p - 2$ のとき、（$B_1 = -1/2$ と $\xi^{p-1} \equiv_p 1$ より）右辺は

$$\xi - 1 + (\xi^{p-1} - 1 + \xi - 1)\frac{B_1}{1} = (\xi - 1)(1 + B_1) = (1 - \xi)B_1 = (\xi^{i+1} - \xi)\frac{B_{p-1-i}}{p-1-i}$$

と変形される。よって、(5) 式より $1 \leq i \leq p - 2$ について

$$\beta_i \xi(\xi^i - 1) = (\xi^{i+1} - \xi) \left(\frac{B_{p-1-i}}{p-1-i} \right)^{\langle p \rangle}$$

となる。ξ は ${\mathbb{F}_p}^{\times}$ の生成元であったから $\xi^i - 1 \neq 0$ であり、

$$\beta_i = \left(\frac{B_{p-1-i}}{p-1-i} \right)^{\langle p \rangle}$$

が得られる。以上で定理 2 が証明された。

例 7. $p=3$ のとき、$B_1{}^{\langle 3\rangle}=(-1/2)^{\langle 3\rangle}=1$ より $\Psi(t)=t$ であり、定理 2 より

$$\psi_1(x,y)=xy(xy-x-y+1)=xy(x-1)(y-1)$$

が得られる。この分解は、mod 3 で繰り上がりが生じるのは 2 掛ける 2 の場合のみであるという事実を反映している。

また、いくつかの p について $\Psi(t)$ を具体的に計算すると、

$$\begin{cases}
\left(2t^3+\frac{1}{12}t^2\right)^{\langle 5\rangle}=2t^3+3t^2 & (p=5)\\
\left(3t^5+\frac{1}{12}t^4-\frac{1}{120}t^2\right)^{\langle 7\rangle}=3t^5+3t^4-t^2 & (p=7)\\
\left(5t^9+\frac{1}{12}t^8-\frac{1}{120}t^6+\frac{1}{252}t^4-\frac{1}{240}t^2\right)^{\langle 11\rangle}=5t^9+t^8+t^6-t^4-5t^2 & (p=11)\\
\left(6t^{11}+\frac{1}{12}t^{10}-\frac{1}{120}t^8+\frac{1}{252}t^6-\frac{1}{240}t^4+\frac{1}{132}t^2\right)^{\langle 13\rangle}\\
\quad =6t^{11}-t^{10}+4t^8-5t^6+2t^4-6t^2 & (p=13)\\
\left(8t^{15}+\frac{1}{12}t^{14}-\frac{1}{120}t^{12}+\frac{1}{252}t^{10}-\frac{1}{240}t^8+\frac{1}{132}t^6-\frac{691}{32760}t^4+\frac{1}{12}t^2\right)^{\langle 17\rangle}\\
\quad =8t^{15}-7t^{14}-t^{12}-6t^{10}+8t^8+4t^6+6t^4-7t^2 & (p=17)\\
\left(9t^{17}+\frac{1}{12}t^{16}-\frac{1}{120}t^{14}+\frac{1}{252}t^{12}-\frac{1}{240}t^{10}+\frac{1}{132}t^8-\frac{691}{32760}t^6+\frac{1}{12}t^4-\frac{3617}{8160}t^2\right)^{\langle 19\rangle}\\
\quad =9t^{17}+8t^{16}+3t^{14}+4t^{12}-8t^{10}-t^8+3t^6+8t^4-5t^2 & (p=19)
\end{cases}$$

となる。さらに、これらの p について $\Psi(1)=0$ となるのは $p=5$ および $p=13$ の場合のみである（3 節の最後の注意を参照されたい）。

謝辞 本文でも触れた通り、本研究に関して宗政昭弘先生、金子昌信先生、山下剛氏より貴重なご意見をいただいたので深く感謝する。また、本研究集会での発表の機会を下さった島倉裕樹氏にも深く感謝する。

参考文献

[1] J. Boyar, R. Peralta, D. Pochuev, On the Multiplicative Complexity of Boolean Functions over the Basis (cap, +, 1), Theoretical Computer Science **235** (2000) 43–57

[2] C. Gentry, Fully Homomorphic Encryption Using Ideal Lattices, in: Proceedings of STOC 2009, 2009, pp.169–178

[3] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory (second edition), Springer GTM vol.84 (1998)

[4] S. Kaji, T. Maeno, K. Nuida, Y. Numata, Polynomial Expressions of Carries in p-ary Arithmetics, Preprint, arXiv:1506.02742 (2015)

[5] M. Lerch, Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p}=q(a)$, Math. Ann. **60**(4) (1905) 471–490

[6] K. Nuida, K. Kurosawa, (Batch) Fully Homomorphic Encryption over Integers for Non-Binary Message Spaces, in: Proceedings of EUROCRYPT 2015 (Part I), Springer LNCS vol.9056, 2015, pp.537–555

[7] The Online Encyclopedia of Integer Sequences, `http://oeis.org/`

[8] C. Sturtivant, G. S. Frandsen, The Computational Efficacy of Finite-Field Arithmetic, Theoretical Computer Science **112** (1993) 291–309