Riv. Mat. Univ. Parma (7) **3*** (2004), 187-204

WENCHANG CHU and PIERLUIGI MAGLI (*)

Algebraic structure of $\mathbb{Z}_p^\times$ and related integer functions (**)

For a real number x, denote by $\lfloor x \rfloor$ and $\lceil x \rceil$, respectively, the greatest integer $\leqslant x$ and the smallest integer $\geqslant x$. In the analysis of algorithms (see [**5**], Chapter 3 for example), it happens often to evaluate the following combinatorial sums on integer functions:

$$\sum_{k=1}^{p-1}\left\lfloor \frac{k^\ell}{p} \right\rfloor, \quad \sum_{k=1}^{p-1}\left\lfloor \frac{k^\ell}{p} \pm \frac{1}{2} \right\rfloor, \quad \sum_{k=1}^{p-1}\left\lceil \frac{k^\ell}{p} \right\rceil, \quad \sum_{k=1}^{p-1}\left\lceil \frac{k^\ell}{p} \pm \frac{1}{2} \right\rceil.$$

The primary purpose of this paper is to investigate the closed forms of these integer function sums. These evaluations have surprising relations with the algebraic structure of the group $\mathbb{Z}_p^\times$, consisting of nonzero residue classes modulo p under modular multiplication.

The paper will be organized as follows. As preparation, the first section will deal with the algebraic structure of $\mathbb{Z}_p^\times$. Then the closed formulas for the integer function sums displayed above will be established in the second section. The paper will end up with the third section, where the evaluation of another integer function sums $\sum_{k=1}^{m} \lfloor \sqrt[n]{kp} \rfloor$ will be presented as byproduct.

1 - Algebraic structure of $\mathbb{Z}_p^\times$

Let $\mathbb{P}$ and $\mathbb{N}$ be the sets of primes and natural numbers respectively. For $p \in \mathbb{P}$, the residue classes modulo p under addition and multiplication constitute a

(*) Dipartimento di Matematica, Università degli Studi di Lecce, Lecce-Arnesano P. O. Box 193, 73100 Lecce, Italia, e-mail: chu.wenchang@unile.it; e-mail: pierluigi.magli@libero.it

(**) Received December 3rd 2003 and in revised form September 21st 2004. AMS classification 11 A 15, 11 A 25.

finite field $\mathbb{Z}_p$. Its nonzero elements $\mathbb{Z}_p^\times$ with multiplication is a cyclic group of order $p-1$. For $n\in\mathbb{N}$, the nth powers of the elements of $\mathbb{Z}_p^\times$ form a subgroup $\mathbb{Z}_p^{\times n}$, the group of the *residues of nth power modulo* p.

On the algebraic structure of $\mathbb{Z}_p^\times$, the following lemma reveals some basic properties.

Lemma 1. *For* $p\in\mathbb{P}$, *there hold the following properties*:
(a) *For* $m, n\in\mathbb{N}$, *if* $m\equiv n\,(\mathrm{mod}\,p-1)$, *then* $\mathbb{Z}_p^{\times m}=\mathbb{Z}_p^{\times n}$;
(b) *For* $n\in\mathbb{N}$, *if* $(n, p-1)=d$, *then* $|\mathbb{Z}_p^{\times n}|=(p-1)/d$;
(c) *For* $m, n\in\mathbb{N}$, *if* $(m, p-1)=(n, p-1)$, *then* $\mathbb{Z}_p^{\times m}=\mathbb{Z}_p^{\times n}$.

Proof. The congruence notation $x\equiv_p y$ will be used instead of $x\equiv y\,(\mathrm{mod}\,p)$ for simplicity.

For $m, n\in\mathbb{N}$ with $m\equiv_{p-1} n$, there exists an integer q such that $m=q(p-1)+n$. For each $x\in\mathbb{Z}_p^{\times n}$, there exists $1\leqslant k<p$ such that $x\equiv_p k^n$. Recalling Fermat's little theorem ([3], p. 109) we have the following congruences

$$k^m=k^{(p-1)q+n}\equiv_p k^n\equiv_p x$$

which implies $x\in\mathbb{Z}_p^{\times m}$. Therefore $\mathbb{Z}_p^{\times n}\subseteq\mathbb{Z}_p^{\times m}$. Vice versa, we can check similarly $\mathbb{Z}_p^{\times m}\subseteq\mathbb{Z}_p^{\times n}$. This proves property (a).

Since $\mathbb{Z}_p^\times$ is a cyclic group of order $p-1$, there is a generator $\gamma\in\mathbb{Z}_p^\times$ such that $\mathbb{Z}_p^\times=\langle\gamma\rangle$ with order $o(\gamma)=p-1$. Then for every $n\in\mathbb{N}$, it is not hard to check that

$$o(\gamma^n)=\frac{p-1}{(n, p-1)}=\frac{p-1}{d}.$$

Noting that $\mathbb{Z}_p^{\times n}=\langle\gamma^n\rangle$, we have

$$|\mathbb{Z}_p^{\times n}|=o(\gamma^n)=(p-1)/d$$

which proves property (b).

Property (c) is in fact an extension of (a). It follows immediately from property (b) because for the cyclic group $\mathbb{Z}_p^\times$, its subgroup of the fixed order $(p-1)/d$ with $d:=(m, p-1)=(n, p-1)$ is unique. Therefore all the subgroups of $\mathbb{Z}_p^\times$ are characterized exclusively by the divisors of $p-1$. ∎

Remark. Furthermore, considering the endomorphism

$$\psi: \ \mathbb{Z}_p^\times \mapsto \mathbb{Z}_p^\times$$
$$x \mapsto x^n$$

we get the image $\psi(\mathbb{Z}_p^\times) = \mathbb{Z}_p^{\times n}$ and the kernel $\ker(\psi) = \langle \gamma^{(p-1)/d} \rangle$ induced by $\psi(\gamma) = \gamma^n$. From the homomorphism theorem we get the isomorphism

$$\mathbb{Z}_p^\times / \ker(\psi) \cong \mathbb{Z}_p^{\times n}. \tag{1.1}$$

Since all the cosets of $\ker(\psi)$ in $\mathbb{Z}_p^\times$ have the same order $d = (n, p-1)$, there are exactly d elements in $\mathbb{Z}_p^\times$ whose n-th powers result in the same element in the multiplicative group $\mathbb{Z}_p^{\times n}$. This leads us to the following multiset relation:

$$\left\{x^n \,|\, x \in \mathbb{Z}_p^\times\right\} = \{\mathrm{mod}\,[k^n, p] \,|\, 1 \leqslant k < p\} = (n, p-1) \times \mathbb{Z}_p^{\times n}. \tag{1.2}$$

Lemma 2. *Let $n \in \mathbb{N}$ and $p \in \mathbb{P}$. If $\dfrac{p-1}{(n, p-1)}$ is even, then for each $x \in \mathbb{Z}_p^{\times n}$, there exists a $y \in \mathbb{Z}_p^{\times n}$ such that $x + y = p$. This is equivalent to say that the elements in $\mathbb{Z}_p^{\times n}$ can be paired off so that every pair has the same sum p.*

Proof. Recall that $\mathbb{Z}_p^\times$ is a cyclic group (cf. [3], Thm 5.3). Suppose γ is a primitive root modulo p. Then for $d = (n, p-1)$, we have

$$o(\gamma^d) = o(\gamma^n) = \frac{p-1}{d}.$$

Both γ^d and γ^n are generators of the same subgroup

$$\mathbb{Z}_p^{\times n} = \left\{\gamma^{dk} \,|\, k = 1, 2, \ldots, \frac{p-1}{d}\right\}$$

for the cyclic group $\mathbb{Z}_p^\times$ has the unique subgroup of the fixed order $(p-1)/d$.

The Lagrange theorem asserts that the congruence equation

$$x^{\frac{p-1}{d}} \equiv 1 \pmod{p} \tag{1.3}$$

has at most $(p-1)/d$ solutions in the field $\mathbb{Z}_p$, which are effectively furnished by all the elements of $\mathbb{Z}_p^{\times d}$.

For each $x \in \mathbb{Z}_p^{\times n} = \mathbb{Z}_p^{\times d}$, it is obvious that x satisfies (1.3). By means of the bi-

nomial theorem, we have

$$(p-x)^{\frac{p-1}{d}} = \sum_{k=0}^{(p-1)/d} \binom{p-1}{d\ k} (-x)^k p^{\frac{p-1}{d}-k}$$

$$\equiv_p (-x)^{\frac{p-1}{d}} \equiv_p x^{\frac{p-1}{d}} \equiv_p 1$$

for $(p-1)/d$ is even. Therefore $y := p - x$ is a solution of (1.3) either, which implies that $y = p - x \in \mathbb{Z}_p^{\times n} = \mathbb{Z}_p^{\times d}$. This completes the proof of the lemma. ■

Lemma 3. *Let $n \in \mathbb{N}$ and $p \in \mathbb{P}$ with $p \equiv_8 7$. If $(2n, p-1) = 2$, then $2 \in \mathbb{Z}_p^{\times 2n}$; that is to say that 2 is a residue of $2n$-th power modulo p.*

Proof. For $n \in \mathbb{N}$ with $2 = (2, p-1) = (2n, p-1)$, The property (c) of Lemma 1 affirms that $\mathbb{Z}_p^{\times 2} = \mathbb{Z}_p^{\times 2n}$. When $p \in \mathbb{P}$ with $p \equiv_8 7$, we know that 2 is a quadratic residue modulo p thanks to Gauss' law of quadratic reciprocity (cf. [**6**], p. 53]), which is equivalent to the following

$$2 \in \mathbb{Z}_p^{\times 2} = \mathbb{Z}_p^{\times 2n}.$$

Therefore 2 is a residue of $2n$-th power modulo p. This proves the lemma. ■

2 - Summation formulas on integer functions

Let $\mathbb{Z}$ and $\mathbb{R}$ be the sets of integers and real numbers respectively. For $x \in \mathbb{R}$, denote by $\lfloor x \rfloor$, $\lceil x \rceil$ and $\{x\}$ the maximum integer $\leqslant x$, the minimum integer $\geqslant x$ and the fractional part $\{x\} = x - \lfloor x \rfloor$. Then we have the following obvious relations:

$$\lfloor x \rfloor = \lceil x \rceil, \qquad x \in \mathbb{Z}$$

$$\lfloor x \rfloor = \lceil x \rceil - 1, \quad x \notin \mathbb{Z}$$

$$\lfloor x \rfloor = x - \{x\}, \quad x \in \mathbb{R}.$$

For an odd prime $p \in \mathbb{P}$ and $n, k \in \mathbb{N}$ with $1 \leqslant k < p$, it is easy to check the following concrete facts:

(2.1a) $$\left\{ \frac{k^n}{p} \right\} = \frac{\operatorname{mod}[k^n, p]}{p}$$

$$\left\lfloor \frac{k^n}{p} \right\rfloor = \left\lceil \frac{k^n}{p} \right\rceil - 1 \qquad \text{for } \frac{k^n}{p} \notin \mathbb{Z} \tag{2.1b}$$

$$\left\lfloor \frac{k^n}{p} \pm \frac{1}{2} \right\rfloor = \left\lceil \frac{k^n}{p} \pm \frac{1}{2} \right\rceil - 1 \quad \text{for } \frac{2k^n}{p} \notin \mathbb{Z}\,. \tag{2.1c}$$

Then the sums of integer functions are transformed by the relation

$$\left\lfloor \frac{k^n}{p} \right\rfloor = \frac{k^n}{p} - \left\{ \frac{k^n}{p} \right\} = \frac{k^n}{p} - \frac{\mathrm{mod}\,[k^n, p]}{p} \tag{2.2}$$

into the sums on $\mathbb{Z}_p^{\times n}$, whose structure depends on only $(n, p-1)$ as affirmed in Lemma 1. Therefore, when there exists a summation formula on integer functions of power $d|(p-1)$, then there would be other formulas on those of the powers n with $(n, p-1) = d$.

Based on these relations and the lemmas demonstrated in the last section, we can establish some closed formulas concerning integer functions of $\mathbb{Z}_p^{\times}$, which are closely related to the partial sums of powers of natural numbers defined by

$$W_n(m) := \sum_{k=1}^{m} k^n \qquad \text{for } m, n \in \mathbb{N}\,. \tag{2.3}$$

We display the first closed formulas which will be used in the sequel of the paper.

$$W_1(m) = \binom{1+m}{2} \tag{2.4a}$$

$$W_2(m) = \binom{2+2m}{3} \frac{1}{4} \tag{2.4b}$$

$$W_3(m) = \binom{1+m}{2}^2 \tag{2.4c}$$

$$W_4(m) = \binom{2+2m}{3} \frac{3m^2+3m-1}{4\times 5} \tag{2.4d}$$

$$W_5(m) = \binom{1+m}{2}^2 \frac{2m^2+2m-1}{3} \tag{2.4e}$$

$$W_6(m)=\binom{2+2m}{3}\frac{3m^4+6m^3-3m+1}{4\times 7} \tag{2.4f}$$

$$W_7(m)=\binom{1+m}{2}^2\frac{3m^4+6m^3-m^2-4m+2}{6} \tag{2.4g}$$

$$W_8(m)=\binom{2+2m}{3}\frac{5m^6+15m^5+5m^4-15m^3-m^2+9m-3}{4\times 15} \tag{2.4h}$$

$$W_9(m)=\binom{1+m}{2}^2\frac{m^2+m-1}{5}(2m^4+4m^3-m^2-3m+3). \tag{2.4i}$$

2.1 - *The case* $2\,\Big|\,\dfrac{p-1}{(n,p-1)}$

As a preliminary result, we first prove the following summation formulas on fraction parts.

Lemma 4. *For* $p\in\mathbb{P}$ *and* $n\in\mathbb{N}$ *with* $\dfrac{p-1}{(n,p-1)}$ *being even, the following sums have the save value:*

$$\sum_{k=1}^{p-1}\left\{\frac{k^n}{p}\right\}=\sum_{k=1}^{p-1}\left\{\frac{k^n}{p}\pm\frac{1}{2}\right\}=\frac{p-1}{2}. \tag{2.5}$$

Proof. Separating the fractional parts by means of

$$\left\{\frac{k^n}{p}\pm\frac{1}{2}\right\}=\begin{cases}\left\{\dfrac{k^n}{p}\right\}+\dfrac{1}{2} & \text{if } \left\{\dfrac{k^n}{p}\right\}<\dfrac{1}{2}\\[2ex] \left\{\dfrac{k^n}{p}\right\}-\dfrac{1}{2} & \text{if } \left\{\dfrac{k^n}{p}\right\}>\dfrac{1}{2}\end{cases} \tag{2.6}$$

we can evaluate the fractional sums as follows

$$\sum_{k=1}^{p-1}\left\{\frac{k^n}{p}\pm\frac{1}{2}\right\}=\sum_{<}\left\{\frac{k^n}{p}\pm\frac{1}{2}\right\}+\sum_{>}\left\{\frac{k^n}{p}\pm\frac{1}{2}\right\} \tag{2.7a}$$

$$=\sum_{k=1}^{p-1}\left\{\frac{k^n}{p}\right\}+\left\{\sum_{<}\frac{1}{2}-\sum_{>}\frac{1}{2}\right\} \tag{2.7b}$$

where the summation index k for $\sum_<$ and $\sum_>$ runs over $1 \leqslant k < p$ subject to $\left\{ \frac{k^n}{p} \right\} < \frac{1}{2}$ and $\left\{ \frac{k^n}{p} \right\} > \frac{1}{2}$ respectively.

When $\frac{p-1}{(n, p-1)}$ is even, Lemma 2 tells us that the elements in $\mathbb{Z}_p^{\times n}$ are paired off so that for each $x \in \mathbb{Z}_p^{\times n}$, there exists $y \in \mathbb{Z}_p^{\times n}$ subject to

$$x + y = p \quad \Rightarrow \quad \frac{x}{p} + \frac{y}{p} = 1.$$

Hence there holds the following implication

$$\frac{x}{p} < \frac{1}{2} \;\Rightarrow\; \frac{y}{p} = 1 - \frac{x}{p} > \frac{1}{2}$$

and vice versa, which makes two sums displayed in the parenthesis of (2.7b) canceled each other on account of Lemma 2. This proves the first equality of the lemma.

In view of Lemma 1 and its Remark, we can compute the sum

$$\sum_{k=1}^{p-1} \left\{ \frac{k^n}{p} \right\} = \frac{(n, p-1)}{p} \sum_{x \in \mathbb{Z}_p^{\times n}} x = \frac{(n, p-1)}{p} \times \frac{p}{2} \times |\mathbb{Z}_p^{\times n}|$$

$$= \frac{(n, p-1)}{p} \times \frac{p}{2} \times \frac{p-1}{(n, p-1)} = \frac{p-1}{2}$$

where Lemma 3 has been applied to the simplification of the sum. This completes the proof of the lemma. ■

Now we are ready to show several closed formulas concerning the integer part of n-th power. The results are grouped in pairs of *floor* and *ceiling*, whose proofs are primarily based on (2.1) and Lemma 4.

Theorem 5 (Two summation formulas). *For $p \in \mathbb{P}$ and $n \in \mathbb{N}$ with $\frac{p-1}{(n, p-1)}$ being even, there hold the following summation formulas*:

(2.8a) $$\sum_{k=1}^{p-1} \left\lfloor \frac{k^n}{p} \right\rfloor = \frac{1}{p} W_n(p-1) - \frac{p-1}{2}$$

$$\sum_{k=1}^{p-1}\left\lceil \frac{k^n}{p} \right\rceil = \frac{1}{p}W_n(p-1) + \frac{p-1}{2}. \tag{2.8b}$$

Proof. By means of Lemma 4, we have

$$\sum_{k=1}^{p-1}\left\lfloor \frac{k^n}{p} \right\rfloor = \sum_{k=1}^{p-1}\frac{k^n}{p} - \sum_{k=1}^{p-1}\left\{ \frac{k^n}{p} \right\}$$

$$= \frac{1}{p}W_n(p-1) - \frac{p-1}{2}$$

which yields also the second formula in view of (2.1b). ■

Proposition 6 (Two summation formulas). *For $p\in\mathbb{P}$ and $n\in\mathbb{N}$ with $\dfrac{p-1}{(2n,\,p-1)}$ being even, there hold the following summation formulas*:

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{k^{2n}}{p} \right\rfloor = \frac{1}{p}W_{2n}\left(\frac{p-1}{2}\right) - \frac{p-1}{4} \tag{2.9a}$$

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lceil \frac{k^{2n}}{p} \right\rceil = \frac{1}{p}W_{2n}\left(\frac{p-1}{2}\right) + \frac{p-1}{4}. \tag{2.9b}$$

Proof. For k from 1 to $\dfrac{p-1}{2}$, its residues of $2n$-th power modulo p cover all the elements of $\mathbb{Z}_p^{\times 2n}$ since $k^{2n}\equiv_p (p-k)^{2n}$ with $1\leqslant k<p$.

Combining (2.1a) and Lemma 2 we get

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{k^{2n}}{p} \right\rfloor = \sum_{k=1}^{\frac{p-1}{2}}\frac{k^{2n}}{p} - \sum_{k=1}^{\frac{p-1}{2}}\left\{ \frac{k^{2n}}{p} \right\}$$

$$= \frac{1}{p}W_{2n}\left(\frac{p-1}{2}\right) - \frac{p-1}{4}$$

which gives us also the second formula thanks again to (2.1b). ■

In what follows, we will display four pairs of explicit summation formulas. Their proofs can analogously be fulfilled by means of Lemma 2 and Lemma 4, and therefore will not be reproduced for brevity.

Theorem 7 (Two summation formulas). *For $p \in \mathbb{P}$ and $n \in \mathbb{N}$ with $\frac{p-1}{(n, p-1)}$ being even, there hold the following summation formulas*:

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^n}{p} + \frac{1}{2} \right\rfloor = \frac{1}{p} W_n(p-1) \tag{2.10a}$$

$$\sum_{k=1}^{p-1} \left\lceil \frac{k^n}{p} - \frac{1}{2} \right\rceil = \frac{1}{p} W_n(p-1). \tag{2.10b}$$

Proposition 8 (Two summation formulas). *For $p \in \mathbb{P}$ and $n \in \mathbb{N}$ with $\frac{p-1}{(2n, p-1)}$ being even, there hold the following summation formulas*:

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{k^{2n}}{p} + \frac{1}{2} \right\rfloor = \frac{1}{p} W_{2n}\left(\frac{p-1}{2}\right) \tag{2.11a}$$

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lceil \frac{k^{2n}}{p} - \frac{1}{2} \right\rceil = \frac{1}{p} W_{2n}\left(\frac{p-1}{2}\right). \tag{2.11b}$$

Theorem 9 (Two summation formulas). *For $p \in \mathbb{P}$ and $n \in \mathbb{N}$ with $\frac{p-1}{(n, p-1)}$ being even, there hold the following summation formulas*:

$$\sum_{k=1}^{p-1} \left\lfloor \frac{k^n}{p} - \frac{1}{2} \right\rfloor = \frac{1}{p} W_n(p-1) - (p-1) \tag{2.12a}$$

$$\sum_{k=1}^{p-1} \left\lceil \frac{k^n}{p} + \frac{1}{2} \right\rceil = \frac{1}{p} W_n(p-1) + (p-1). \tag{2.12b}$$

Proposition 10 (Two summation formulas). *For $p \in \mathbb{P}$ and $n \in \mathbb{N}$ with $\frac{p-1}{(2n, p-1)}$ being even, there hold the following summation formulas*:

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{k^{2n}}{p} - \frac{1}{2} \right\rfloor = \frac{1}{p} W_{2n}\left(\frac{p-1}{2}\right) - \frac{p-1}{2} \tag{2.13a}$$

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lceil \frac{k^{2n}}{p}+\frac{1}{2}\right\rceil=\frac{1}{p}W_{2n}\left(\frac{p-1}{2}\right)+\frac{p-1}{2}. \tag{2.13b}$$

2.2 - *The case* $p\equiv_8 7$

For $n\in\mathbb{N}$ and $p\in\mathbb{P}$ with $p\equiv_8 7$, the structure of $\mathbb{Z}_p^{\times n}$ is not symmetric with respect to $p/2$. However on the basis of Lemma 3, we are able to establish some summation formulas.

Theorem 11 (Two summation formulas). *Let* $n\in\mathbb{N}$ *and* $p\in\mathbb{P}$ *with* $p\equiv_8 7$. *If* $(2n, p-1)=2$, *then there hold the summation formulas*

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{k^{2n}}{p}+\frac{1}{2}\right\rfloor=\frac{1}{p}W_{2n}\left(\frac{p-1}{2}\right) \tag{2.14a}$$

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lceil \frac{k^{2n}}{p}-\frac{1}{2}\right\rceil=\frac{1}{p}W_{2n}\left(\frac{p-1}{2}\right). \tag{2.14b}$$

The first identity stated in the theorem can be considered as a generalization of the formula appeared in [7]:

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{k^{2}}{p}+\frac{1}{2}\right\rfloor=\frac{p^2-1}{24}.$$

Proof. For each real number x, it holds that

$$\left\lfloor x+\frac{1}{2}\right\rfloor=\lfloor 2x\rfloor-\lfloor x\rfloor$$

which leads us to the following reformulation:

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{k^{2n}}{p}+\frac{1}{2}\right\rfloor=\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{2k^{2n}}{p}\right\rfloor-\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{k^{2n}}{p}\right\rfloor=\sum_{k=1}^{\frac{p-1}{2}}\frac{k^{2n}}{p} \tag{2.15a}$$

$$-\sum_{k=1}^{\frac{p-1}{2}}\left\{\frac{\operatorname{mod}[2k^{2n},\,p]}{p}-\frac{\operatorname{mod}[k^{2n},\,p]}{p}\right\}. \tag{2.15b}$$

From Lemma 3, we know that $2\in\mathbb{Z}_p^{\times 2n}$ which is equivalent to $\mathbb{Z}_p^{\times 2n}=2\mathbb{Z}_p^{\times 2n}$. Therefore as k runs from 1 to $(p-1)/2$, both $\operatorname{mod}[2k^{2n},\,p]$ and $\operatorname{mod}[k^{2n},\,p]$ generate exactly the same set $\mathbb{Z}_p^{\times 2n}$ with $|\mathbb{Z}_p^{\times 2n}|=\dfrac{p-1}{(2n,\,p-1)}=\dfrac{p-1}{2}$, in view of the remark contained at the end of Lemma 1. This cancels the two modular sums displayed in (2.15b) and proves the first formula in the theorem.

For $x\notin\mathbb{Z}$, we have $\lceil x\rceil=\lfloor x\rfloor+1$. This gives us the following

$$\left\lceil\frac{k^{2n}}{p}-\frac{1}{2}\right\rceil=\left\lfloor\frac{k^{2n}}{p}-\frac{1}{2}\right\rfloor+1=\left\lfloor\frac{k^{2n}}{p}+\frac{1}{2}\right\rfloor$$

whose combination with the formula just proved leads us immediately to the second formula displayed in the theorem. ■

In accordance with the facts

$$\left\lfloor\frac{k^{2n}}{p}-\frac{1}{2}\right\rfloor=\left\lceil\frac{k^{2n}}{p}-\frac{1}{2}\right\rceil-1$$

$$\left\lceil\frac{k^{2n}}{p}+\frac{1}{2}\right\rceil=\left\lfloor\frac{k^{2n}}{p}+\frac{1}{2}\right\rfloor+1$$

the formulas just demonstrated read through directly as the following:

Theorem 12 (Two summation formulas). *Let $n\in\mathbb{N}$ and $p\in\mathbb{P}$ with $p\equiv_8 7$. If $(2n,\,p-1)=2$, then there hold the summation formulas*

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{k^{2n}}{p}-\frac{1}{2}\right\rfloor=\frac{1}{p}W_{2n}\left(\frac{p-1}{2}\right)-\frac{p-1}{2} \tag{2.16a}$$

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lceil\frac{k^{2n}}{p}+\frac{1}{2}\right\rceil=\frac{1}{p}W_{2n}\left(\frac{p-1}{2}\right)+\frac{p-1}{2}\,. \tag{2.16b}$$

2.3 - *The case* $(p-1)\,|\,n$

For $p\in\mathbb{P}$ and $n\in\mathbb{N}$ with n being a multiple of $p-1$, Fermat's little theorem tells us that

$$\operatorname{mod}[k^n,\,p]=1 \;\Leftrightarrow\; \left\{\frac{k^n}{p}\right\}=\frac{1}{p} \qquad \text{for } 1\leqslant k<p\,.$$

When $p>2$ with p and n as before, it is obvious that n is even. Then we have the following particular results:

$$\sum_{k=1}^{\frac{p-1}{2}}\left\{\frac{k^n}{p}\right\}=\frac{p-1}{2p} \tag{2.17a}$$

$$\sum_{k=1}^{\frac{p-1}{2}}\left\{\frac{k^n}{p}\pm\frac{1}{2}\right\}=\frac{(p-1)(2+p)}{4p}\,. \tag{2.17b}$$

From them it is not hard to establish the following summation formulas.

Proposition 13. *For $p\in\mathbb{P}$ with $p\geqslant 3$ and $n\in\mathbb{N}$ subject to $(p-1)\,|\,n$, the following six summation formulas hold*:

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{k^n}{p}\right\rfloor=\frac{1}{p}W_n\!\left(\frac{p-1}{2}\right)-\frac{p-1}{2p} \tag{2.18a}$$

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lceil\frac{k^n}{p}\right\rceil=\frac{1}{p}W_n\!\left(\frac{p-1}{2}\right)+\frac{(p-1)^2}{2p} \tag{2.18b}$$

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{k^n}{p}+\frac{1}{2}\right\rfloor=\frac{1}{p}W_n\!\left(\frac{p-1}{2}\right)-\frac{p-1}{2p} \tag{2.18c}$$

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lceil\frac{k^n}{p}-\frac{1}{2}\right\rceil=\frac{1}{p}W_n\!\left(\frac{p-1}{2}\right)-\frac{p-1}{2p} \tag{2.18d}$$

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{k^n}{p}-\frac{1}{2}\right\rfloor=\frac{1}{p}W_n\!\left(\frac{p-1}{2}\right)-\frac{p^2-1}{2p} \tag{2.18e}$$

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lceil\frac{k^n}{p}+\frac{1}{2}\right\rceil=\frac{1}{p}W_n\!\left(\frac{p-1}{2}\right)+\frac{(p-1)^2}{2p}\,. \tag{2.18f}$$

2.4 - *The case* $n \equiv_2 1$

For an odd prime $p \in \mathbb{P}$ and an odd integer $n \in \mathbb{N}$, we see that $\dfrac{p-1}{(n, p-1)}$ is even. Then we have two summation formulas displayed in Theorem 5. Here we present an alternative and direct approach which permits us to generalize slightly these identities.

For non negative integers x, y, z and $p \in \mathbb{P}$ subject to $x + y = pz$, it is obvious that

$$p|x \quad \& \quad p|y \quad \Rightarrow \quad \begin{cases} \left\lfloor \dfrac{x}{p} \right\rfloor + \left\lfloor \dfrac{y}{p} \right\rfloor = z \\ \left\lceil \dfrac{x}{p} \right\rceil + \left\lceil \dfrac{y}{p} \right\rceil = z \end{cases}$$

and

$$p \nmid x \quad \& \quad p \nmid y \quad \Rightarrow \quad \begin{cases} \left\lfloor \dfrac{x}{p} \right\rfloor + \left\lfloor \dfrac{y}{p} \right\rfloor = z - 1 \\ \left\lceil \dfrac{x}{p} \right\rceil + \left\lceil \dfrac{y}{p} \right\rceil = z + 1 \,. \end{cases}$$

They can be used to prove the following formulas.

Theorem 14 (Two summation formulas). *For* $p \in \mathbb{P}$ *and* $m, n \in \mathbb{N}$ *with* n *being odd, there hold summation formulas*:

$$\sum_{k=1}^{pm-1} \left\lfloor \frac{k^n}{p} \right\rfloor = \frac{1}{p} W_n(pm-1) - \frac{(p-1)\,m}{2} \tag{2.19a}$$

$$\sum_{k=1}^{pm-1} \left\lceil \frac{k^n}{p} \right\rceil = \frac{1}{p} W_n(pm-1) + \frac{(p-1)\,m}{2} \,. \tag{2.19b}$$

Proof. Reversing the summation order, we can compute the first sum as follows:

$$\sum_{k=1}^{pm-1} \left\lfloor \frac{k^n}{p} \right\rfloor = \frac{1}{2} \sum_{k=1}^{pm-1} \left\{ \left\lfloor \frac{k^n}{p} \right\rfloor + \left\lfloor \frac{(pm-k)^n}{p} \right\rfloor \right\}$$

$$= \frac{1}{2}\sum_{k=1}^{pm-1}\frac{k^n+(pm-k)^n}{p} - \frac{1}{2}\sum_{\substack{k=1\\ p\nmid k}}^{pm-1} 1$$

$$= \sum_{k=1}^{pm-1}\frac{k^n}{p} - \frac{1}{2}\sum_{\substack{k=1\\ p\nmid k}}^{pm-1} 1 .$$

Then the first formula (2.19a) follows immediately from the observation

$$\big|\{1\leqslant k<pm \,|\, p\nmid k\}\big| = (pm-1) - \left\lfloor \frac{pm-1}{p}\right\rfloor = (p-1)\,m .$$

Similarly, we can demonstrate the second formula (2.19b). ■

Recalling summation formulas (2.4) of powers of natural numbers, we can exhibit, for $m=1$, the first five formulas of (2.19a) as follows.

Example 15 (Five summation formulas).

(2.20a) $$\sum_{k=1}^{p-1}\left\lfloor \frac{k}{p}\right\rfloor = 0$$

(2.20b) $$\sum_{k=1}^{p-1}\left\lfloor \frac{k^3}{p}\right\rfloor = \frac{(p^2-1)(p-2)}{4} \qquad \text{(cf. [4])}$$

(2.20c) $$\sum_{k=1}^{p-1}\left\lfloor \frac{k^5}{p}\right\rfloor = \frac{(p^2-1)(p-2)}{12}(3-2p+2p^2)$$

(2.20d) $$\sum_{k=1}^{p-1}\left\lfloor \frac{k^7}{p}\right\rfloor = \frac{(p^2-1)(p-2)}{24}(6-2p+5p^2-6p^3+3p^4)$$

(2.20e) $$\sum_{k=1}^{p-1}\left\lfloor \frac{k^9}{p}\right\rfloor = \frac{(p^2-1)(p-2)}{20}(5-4p+3p^2+5p^4-6p^5+2p^6).$$

3 - Summation formulas on the integer parts of radicals

In this section, we will investigate the sums of the integer functions of radicals by connecting them to the summation formulas established in the previous sections.

For $p\in\mathbb{P}$ and $n\in\mathbb{N}$, consider the integer sequence $\{\lfloor\sqrt[n]{kp}\rfloor\}_{k\geqslant 1}$. Given a natural number m, denote by $\pi_n(m)$ the turning point k on which the value of the

next term in the integer sequence just mentioned switches from m to $m+1$. That means

$$\pi_n(m) = \max\{k \in \mathbb{N} \mid \lfloor \sqrt[n]{kp} \rfloor \leqslant m\} \tag{3.1}$$

from which we get explicitly

$$m \leqslant \sqrt[n]{p\pi_n(m)} < m+1 \quad \Leftrightarrow \quad \pi_n(m) = \left\lfloor \frac{(m+1)^n - 1}{p} \right\rfloor. \tag{3.2}$$

Now we define the frequency function $f_n(m)$ as the multiplicity of m in the sequence $\{\lfloor \sqrt[n]{kp} \rfloor\}_{k \geqslant 1}$. It is not difficult to check that this function is determined by the difference

$$f_n(m) = \pi_n(m) - \pi_n(m-1) = \left\lfloor \frac{(m+1)^n - 1}{p} \right\rfloor - \left\lfloor \frac{m^n - 1}{p} \right\rfloor. \tag{3.3}$$

Then we can evaluate the integer sum $\sum \lfloor \sqrt[n]{kp} \rfloor$ by collecting the same terms together with their multiplicities in the sequence $\{\lfloor \sqrt[n]{kp} \rfloor\}_{k \geqslant 1}$. The main result may be stated as follows.

Theorem 16 (Summation formula on radicals). *For $p \in \mathbb{P}$ and $m, n \in \mathbb{N}$, there holds the summation formula*

$$\sum_{k=1}^{\pi_n(m)} \lfloor \sqrt[n]{kp} \rfloor = \left\lfloor \frac{m}{p} \right\rfloor + m\pi_n(m) - \sum_{k=1}^{m} \left\lfloor \frac{k^n}{p} \right\rfloor \tag{3.4}$$

where $\pi_n(m)$ is given by (3.2).

Proof. Denote by $\Omega_n(m)$ the sum stated in (3.4). It can be manipulated as follows:

$$\begin{aligned}
\Omega_n(m) &:= \sum_{k=1}^{\pi_n(m)} \lfloor \sqrt[n]{kp} \rfloor = \sum_{k=1}^{m} k f_n(k) \\
&= \sum_{k=1}^{m} k \left\{ \left\lfloor \frac{(k+1)^n - 1}{p} \right\rfloor - \left\lfloor \frac{k^n - 1}{p} \right\rfloor \right\} \\
&= \sum_{k=1}^{m+1} (k-1) \left\lfloor \frac{k^n - 1}{p} \right\rfloor - \sum_{k=1}^{m} k \left\lfloor \frac{k^n - 1}{p} \right\rfloor \\
&= m \left\lfloor \frac{(m+1)^n - 1}{p} \right\rfloor - \sum_{k=1}^{m} \left\lfloor \frac{k^n - 1}{p} \right\rfloor.
\end{aligned}$$

On account of the fact

$$p \nmid k \;\Rightarrow\; \left\lfloor \frac{k^n-1}{p} \right\rfloor = \left\lfloor \frac{k^n}{p} \right\rfloor$$

$$p \mid k \;\Rightarrow\; \left\lfloor \frac{k^n-1}{p} \right\rfloor = \left\lfloor \frac{k^n}{p} \right\rfloor - 1$$

we have

$$\sum_{k=1}^{m} \left\lfloor \frac{k^n-1}{p} \right\rfloor = \sum_{k=1}^{m} \left\lfloor \frac{k^n}{p} \right\rfloor - \left\lfloor \frac{m}{p} \right\rfloor$$

which leads us to the following

$$\Omega_n(m) = \left\lfloor \frac{m}{p} \right\rfloor + m \left\lfloor \frac{(m+1)^n-1}{p} \right\rfloor - \sum_{k=1}^{m} \left\lfloor \frac{k^n}{p} \right\rfloor.$$

This is exactly the same as (3.4) and the proof of the theorem is completed. ■

For $m \to mp-1$, it is easy to check $\pi_n(pm-1) = m^n p^{n-1} - 1$. Then the summation formula (3.4) reads as

$$\sum_{k=1}^{m^n p^{n-1}-1} \lfloor \sqrt[n]{kp} \rfloor = m\{(mp)^n - (mp)^{n-1} - p + 1\} - \sum_{k=1}^{mp-1} \left\lfloor \frac{k^n}{p} \right\rfloor. \tag{3.5}$$

Combining (2.19a) with (3.5), we obtain the following formula.

Proposition 17 (Summation formula on radicals). *For $p \in \mathbb{P}$ and $m, n \in \mathbb{N}$ with n being odd, there holds the summation formula*

$$\sum_{k=1}^{m^n p^{n-1}-1} \lfloor \sqrt[n]{kp} \rfloor = m\left\{(mp)^n - (mp)^{n-1} - \frac{p-1}{2}\right\} - \frac{1}{p} W_n(pm-1). \tag{3.6}$$

Furthermore, the combination of the case $m = 1$ of (3.5) with Theorem 5 results in another summation formula.

Proposition 18 (Summation formula on radicals). *For* $p \in \mathbb{P}$ *and* $n \in \mathbb{N}$ *with* $\dfrac{p-1}{(n, p-1)}$ *being even, there holds the summation formula*

$$\sum_{k=1}^{p^{n-1}-1} \lfloor \sqrt[n]{kp} \rfloor = (p-1)\left\{p^{n-1} - \frac{1}{2}\right\} - \frac{1}{p} W_n(p-1). \tag{3.7}$$

Applying (2.4) to Proposition 17, we obtain the following formulas.

Example 19 (Three summation formulas on radicals).

$$\Omega_3(p-1) = \frac{(p-1)(p+1)(3p-2)}{4} \tag{3.8a}$$

$$\Omega_5(p-1) = \frac{(p-1)(p+1)}{12}(10p^3 - 6p^2 + 5p - 6) \tag{3.8b}$$

$$\Omega_7(p-1) = \frac{(p-1)(p+1)}{24}(21p^5 - 12p^4 + 7p^3 - 12p^2 + 14p - 12). \tag{3.8c}$$

Similarly applying (2.4) to the case $m = p-2$ of Theorem 16, we can establish the following formulas.

Example 20 (Three summation formulas on radicals).

$$\Omega_3(p-2) = \frac{(p-1)(p-2)(3p-5)}{4} \quad \text{(cf. [4])} \tag{3.9a}$$

$$\Omega_5(p-2) = \frac{(p-1)(p-2)}{12}(10p^3 - 36p^2 + 47p - 27) \tag{3.9b}$$

$$\Omega_7(p-2) = \frac{(p-1)(p-2)}{24}(21p^5 - 117p^4 + 265p^3 - 315p^2 + 212p - 78) \tag{3.9c}$$

where we have applied explicitly

$$\pi_n(p-2) = \frac{1 - p + (p-1)^n}{p} \quad \text{with } n \equiv_2 1 .$$

When n is even, the evaluation of $\Omega_n(m)$ are closely related to the integer sums displayed in Section 2. The details are omitted for the limit of space.

References

[1] T. M. APOSTOL, *Introduction to Analytic Number Theory*, Springer, Berlin 1976.

[2] D. M. BLOOM, *Problem 10718*, Amer. Math. Monthly **106** (3) (1999), Problem; **108** (2) (2001), Solution.

[3] J. B. DENCE and T. P. DENCE, *Elements of the Theory of Numbers*, Academic Press, London 1999.

[4] D. DOSTER, *Problem 10346*, Amer. Math. Monthly **100** (10) (1993), Problem; **104** (1) (1997), Solution.

[5] R. L. GRAHAM, D. E. KNUTH and O. PATASHNIK, *Concrete Mathematics*, Addison-Wesley Publ. Company, Reading, Massachusetts 1989.

[6] K. IRELAND and M. ROSEN, *A Classical Introduction to Modern Number Theory*, GTM 84, Springer-Verlag, Berlin 1982.

[7] C. POPESCU, *Problem 10852*, Amer. Math. Month. **108** (2) (2001), Problem; **109** (2) (2002), Solution.

Abstract

For an odd prime p, the algebraic structure of the group $\mathbb{Z}_p^{\times}$ under modular multiplication is investigated. Arithmetical identities on the sums related to integer functions are established. Other closed formulas on integer sums of radicals are obtained as consequences.

* * *