Journal of Number Theory 171 (2017) 155–168

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The valuative capacity of the set of sums of d-th powers

Marie-Andrée B. Langlois

ARTICLE INFO

Article history:
Received 18 December 2015
Received in revised form 23 July 2016
Accepted 24 July 2016
Available online 5 September 2016
Communicated by D. Goss

Keywords:
Integer valued polynomials
Valuative capacity
p-Orderings
Sums of powers

ABSTRACT

If E is a subset of the integers then the n-th characteristic ideal of E is the fractional ideal of $\mathbb{Z}$ consisting of 0 and the leading coefficients of the polynomials in $\mathbb{Q}[x]$ of degree no more than n which are integer valued on E. For p a prime the characteristic sequence of $Int(E, \mathbb{Z})$ is the sequence $\alpha_E(n)$ of negatives of the p-adic valuations of these ideals. The asymptotic limit $\lim_{n\to\infty} \frac{\alpha_{E,p}(n)}{n}$ of this sequence, called the valuative capacity of E, gives information about the geometry of E. We compute these valuative capacities for the sets E of sums of $\ell \geq 2$ integers to the power of d, by observing the p-adic closure of these sets.

1. Introduction

Given E a subset of $\mathbb{Z}$, the valuative capacity of E is a notion that was first introduced by Chabert in [Cha01], in analogy to the idea of capacity of a subset originally introduced by Fekete in 1923 in [Fek23]. Recent results [FP16] show that these notions actually coincide in many cases. The later has played a central role in several important results such as the Polya–Szegö theorem [PS72], integer polynomials approximation [Fer06] and algebraic geometry [Rum13]. Chabert's definition is by way of the theory of integer valued polynomials:

E-mail address: mblanglois@dal.ca.

http://dx.doi.org/10.1016/j.jnt.2016.07.006
0022-314X/

Definition 1. For any subset E of $\mathbb{Z}$ the ring of integer valued polynomials on E is defined to be

$$Int(E,\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid f(E) \subseteq \mathbb{Z}\}.$$

Definition 2. The sequence of characteristic ideals of E is $\{I_n \mid n = 0, 1, 2, \ldots\}$ where I_n is the fractional ideal formed by 0 and the leading coefficients of the elements of $Int(E,\mathbb{Z})$ of degree no more than n and the characteristic sequence of E with respect to the prime p, is the sequence of negatives of the p-adic valuations of these ideals, denoted $\alpha_{E,p}(n)$.

The valuative capacity arises from wanting to find the asymptotic behaviour of $\alpha_{E,p}(n)$. In [Cha01] Chabert shows that the limit of $\frac{\alpha_{E,p}(n)}{n}$ with respect to n exists, and defines:

Definition 3. The valuative capacity of E with respect to p is the following limit:

$$L_{E,p} = \lim_{n\to\infty} \frac{\alpha_{E,p}(n)}{n}.$$

In 1997, Bhargava introduced the following definition which is very important when studying integer valued polynomials:

Definition 4. A p-ordering of E is a sequence $(a_n)_{n\geq 0}$, such that, for each n, $a_n \in E$ is chosen to minimize

$$\nu_p((a_n - a_{n-1}) \cdots (a_n - a_0)),$$

where ν_p denotes the p-adic valuation.

Proposition 5. [Bha97] *Let $(a_n)_{n\geq 0}$ be a sequence of distinct elements of E. Then, $(a_n)_{n\geq 0}$ is a p-ordering of E if and only if for a given $0 \leq n$, the polynomials*

$$f_n(X) = \prod_{k=0}^{n-1} \frac{X - a_k}{a_n - a_k}$$

form a basis for the $\mathbb{Z}_{(p)}$-module $Int(E,\mathbb{Z}_{(p)}) = \{f(x) \in \mathbb{Q}[x] \mid f(E) \subseteq \mathbb{Z}_{(p)}\}$. Consequently, $\nu_p\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \alpha_{E,p}(n)$ for $0 \leq n \leq m$.

In this paper we are interested in finding the valuative capacity of the set of sums of $\ell \geq 2$ integers which are each d-th powers, for $d \geq 3$, since the details for the case $d = 2$ are in [FJ16] and those for $\ell = 1$ are in [FJ12].

Definition 6. For a fixed $d \in \mathbb{Z}$ with $d \geq 0$, we define D to be the set of d-th powers of integers, thus $D = \{x^d \mid x \in \mathbb{Z}\}$ and we let $\ell D = D + \cdots + D$, for ℓ terms in the sum.

The main result of this paper is:

Theorem 7. *Let p be a prime number, d a positive integer and ℓ an integer greater than or equal to 2. Then, $L_{\ell D,p}$ is an algebraic number of degree at most 2. Moreover, if 0 can be written non-trivially modulo p^e as a sum of ℓ elements to the power of d, where $e = 1 + 2\nu_p(d)$, then $L_{\ell D,p}$ is a rational number.*

We will divide the paper into the following sections: first we will go over background and notation, where we prove some general results about valuative capacity that will be needed, then we will prove the main theorem, and then discuss the cases where we know that we can write 0 as a non-trivial sum of ℓ elements to the power of d, and give formulas for the valuative capacity in those cases.

2. Background and notation

In this work we are interested in the sets ℓD, for d a positive integer with $d > 2$. Similarly to Definition 6:

Definition 8. Let D_{p^e} denote the set of d-th powers modulo p^e, for $e \geq 1$ and ℓD_{p^e} the sets of sums of ℓ elements to the power of D modulo p^e. We will also make use of $\overline{D} = \varprojlim_{m \in \mathbb{N}} D_{p^m}$, the p-adic closure of D in $\hat{\mathbb{Z}}_p$, and similarly we will consider $\overline{\ell D}$.

We will now recall some propositions that will help us to compute valuative capacities.

Proposition 9. *For a prime p, the valuative capacity of the set of integers is $L_{\mathbb{Z},p} = \frac{1}{p-1}$.*

Proof. The positive integers in increasing order are a p-ordering of $\mathbb{Z}$, hence, by Definition 3, we have that $\alpha_{\mathbb{Z},p}(n) = \nu_p(n!)$. By Legendre's formula $\nu_p(n!) = \frac{n-\sum n_i}{p-1}$, where $0 \leq n_i < p$ are the coefficients of the base p expansion of n, i.e. $n = \sum n_i p^i$. We can thus compute

$$L_{\mathbb{Z},p} = \lim_{n\to\infty} \frac{\alpha_{\mathbb{Z},p}(n)}{n} = \frac{1}{p-1}. \qquad \square$$

Given A a subset of the integers, for the remainder of this paper, $\overline{A}$ will denote the p-adic closure of A in $\hat{\mathbb{Z}}_p$. Also note that ℓD is the set previously defined of sums of ℓ elements to the power of d, but for a given integer k, a prime p, and $E \subseteq \mathbb{Z}$, $p^k E$ is the usual set $\{p^k a \mid a \in E\}$.

Proposition 10. *Let p be a fixed prime and A be a subset of $\mathbb{Z}$.*

1. [BC00] *We have that $L_{\alpha_{\overline{A},p}} = L_{\alpha_{A,p}}$, since $\alpha_{\overline{A},p} = \alpha_{A,p}$.*
2. [Joh09b] *If A has characteristic sequence $\alpha_{A,p}(n)$ then for any $c \in \mathbb{Z}$ the characteristic sequence of $A + c$ is also $\alpha_{A,p}(n)$ and the characteristic sequence of $p^k A$ is $\alpha_{A,p}(n) + kn$.*
3. [Joh09b] *If B is another subset of $\mathbb{Z}$, with the property that for any $x \in A$ and $y \in B$ it is the case that $\nu_p(x - y) = 0$, then the characteristic sequence of $A \cup B$ is the disjoint union of the sequences $\alpha_{A,p}(n)$ and $\alpha_{B,p}(n)$ sorted into nondecreasing order.*

Definition 11. For a fixed prime p, and A, B two subsets of $\mathbb{Z}$, the characteristic sequence of $A \cup B$ mentioned in Proposition 10(3) is called the shuffle product of $\alpha_{A,p}(n)$ and $\alpha_{B,p}(n)$ and is denoted $(\alpha_{A,p} \wedge \alpha_{B,p})(n)$.

Proposition 12. [Joh09a] *If $\alpha_{A,p}(n)$ and $\alpha_{B,p}(n)$ are the characteristic sequences of A and B respectively, for a prime p, and A, B satisfying Proposition 10(3), with $L_{A,p} = \lim_{n\to\infty} \frac{\alpha_{A,p}(n)}{n}$ and $L_{B,p} = \lim_{n\to\infty} \frac{\alpha_{B,p}(n)}{n}$ then*

$$\frac{1}{L_{A\cup B,p}} = \frac{1}{L_{A,p}} + \frac{1}{L_{B,p}}.$$

The next proposition is a generalization of the above, which will prove itself to be very useful when computing valuative capacities.

Proposition 13. [Joh15] *Given a prime p, if A and B are disjoint subsets with the property that there is a nonnegative integer k such that $\nu_p(a - b) = k$ for any $a \in A$ and $b \in B$, then*

$$\frac{1}{L_{A\cup B,p} - k} = \frac{1}{L_{A,p} - k} + \frac{1}{L_{B,p} - k}.$$

Proposition 14. *If E is a union of cosets modulo p^m for some m, then the valuative capacity of E is rational and recursively computable.*

Proof. We prove the above by induction on m, the case $m = 1$ being Proposition 12. Suppose $L_{E,p} \in \mathbb{Q}$ for all $E = \bigcup_{i=1}^{\ell}(a_i + p^k\mathbb{Z})$, for $1 < k < m$.

Suppose $E = \bigcup_{i=1}^{\ell}(a_i + p^m\mathbb{Z})$ and, for $j = 0, 1, \ldots, p-1$, let $E_j = \bigcup\limits_{a_i \equiv j \pmod p} (a_i + p^m\mathbb{Z})$. We have that $E = \bigcup E_j$ and

$$L_{E,p} = \left(\sum_{j=0}^{p-1} \left(L_{E_j,p}\right)^{-1}\right)^{-1}$$

since the E_j satisfy the hypotheses of Proposition 12. Thus $L_{E,p}$ is a rational combination of the $L_{E_j,p}$'s, which are rational by induction and Proposition 13. Each E_j is the translate by j of p times a union of cosets (mod p^{m-1}), so our induction hypothesis applies and $L_{E,p} \in \mathbb{Q}$. □

Propositions 12 and 13 give a method of computing L_A for $A = A_1 \cup A_2$ in terms of L_{A_1} and L_{A_2} when A_1, A_2 are such that $\nu_p(x_1 - x_2)$ is constant for $x_i \in A_i$. To handle some cases in which this condition fails we proceed in several steps, expressing A as a nested union of sets B_i with $B_k = A_k \cup B_{k+1}$ and $\nu_p(x_1 - x_2)$ constant if $x_1 \in A_k$ and $x_2 \in B_{k+1}$.

The next propositions will involve continued fractions, and we will use the concise notation for these where $[a; a_0, a_1, \ldots, a_k]$ denotes

$$a + \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{}{\ddots + \cfrac{1}{a_k}}}}$$

for k a positive integer. More details about this notation can be found in [Dav82, IV p. 81]. (Note that in [Dav82, IV p. 81], the a_i's are integers, while in what follows they will be in $\mathbb{Q}$.)

Thus Proposition 13 becomes: given a prime p, if A and B are disjoint subsets with the property that there is a nonnegative integer k such that $\nu_p(a - b) = k$ for any $a \in A$ and $b \in B$, then $L_{A\cup B,p}$ has the continued fraction expansion:

$$L_{A\cup B,p} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + L_{B,p}}} = [a_0; a_1, a_2, a_3],$$

with $a_0 = k$, $a_1 = \frac{1}{L_{A,p} - k}$, $a_2 = -k$ and $a_3 = \frac{1}{L_{B,p}}$.

Proposition 15. *Fix a prime p. Let $A_0, A_1, \ldots, A_m$ be disjoint subsets of $\mathbb{Z}$ such that, whenever $0 \le k < h \le m$, $a \in A_k$, and $b \in A_h$, one has $\nu_p(a - b) = k$. Then, the p-valuative capacity of $A = A_0 \cup \cdots \cup A_m$, has the following continued fraction expansion:*

$$L_{A,p} = [0; a_0, a_1, \ldots, a_{2(m-1)}, a_{2m-1}]$$

where $a_{2k} = \frac{1}{L_{A_k} - k}$ for $0 \le k \le m - 1$, $a_{2k+1} = 1$ for $0 \le k < m - 1$, and $a_{2m-1} = L_{A_m} - (m - 1)$.

Proof. We prove the statement by induction on m. For $m = 0$, we are in the case $A = A_0$ and the continued fraction equals L_{A_0}. For $m = 1$ we have $A = A_0 \cup A_1$ and by assumption $\nu_p(a - b) = 1$ if $a \in A_0$ and $b \in A_1 = B$, then by Proposition 13:

$$L_{A_0 \cup A_1} = 1 + \cfrac{1}{\cfrac{1}{L_{A_0} - 1} + \cfrac{1}{L_{A_1} - 1}}.$$

Now suppose that these results hold for $1 < m \in \mathbb{Z}$, and we will prove the case $m + 1$. We have that $\nu_p(a - p) = m$ if $a \in A_m$ and $b \in A_{m+1}$ in this case, by Proposition 13:

$$L_{A_m \cup A_{M+1}} = m + \cfrac{1}{\cfrac{1}{L_{A_m} - m} + \cfrac{1}{L_{A_{M+1}} - m}},$$

by induction hypothesis

$$L_A = [0; a_0, a_1, a_2, \dots, a_{2m}, L_{(A_m \cup A_{M+1})} - (m - 1)].$$

Substituting appropriately yields:

$$\begin{aligned} L_A &= \left[0; a_0, a_1, a_2, \dots, a_{2m}, \left(m + \frac{1}{\frac{1}{L_{A_m} - m} + \frac{1}{L_{A_{M+1}} - m}}\right) - m + 1\right] \\ &= \left[0; a_0, a_1, a_2, \dots, a_{2m}, 1, \frac{1}{L_{A_m} - m} + \frac{1}{L_{A_{m+1} - m}}\right] \\ &= \left[0; a_0, a_1, a_2, \dots, a_{2m}, a_{2m+1}, a_{2m+2}, L_{A_{m+1}} - m\right] \end{aligned}$$

with $a_{2m+1} = 1$ and $a_{2m+2} = \dfrac{1}{L_{A_m} - m}$. $\square$

If E is a subset of $\mathbb{Z}$, which we can rearrange as a union of subsets $E = \left(\bigcup_{k=0}^{m-1} E_k\right) \cup p^m E$, where the E_k's are unions of cosets $E_k = \bigcup(c + p^m\mathbb{Z})$, $c \neq 0$, where $\nu_p(c) = k$, for all c from E_k, then the previous proposition applies.

Corollary 16. *If $E = E' \cup p^m E$, where E' is a union of nonzero cosets* $(\mathrm{mod}\ p^m)$, *then $L_{E,p}$ is the root of a quadratic polynomial in $\mathbb{Q}[x]$, whose coefficients are recursively computable.*

Proof. By Proposition 14 $L_{E',p} \in \mathbb{Q}$, and we can set up this situation as in Proposition 15, where in this case $A = E$, the sets A_k are separated according to the p-adic valuation of their elements and the differences of these with elements of other subsets.

Then we have that $A_m = p^m E$, hence the valuative capacity is

$$L_{E,p} = [0; a_0, a_1, \dots a_{2(m-1)}, a_{2m-1}]$$

where $a_{2k} = \frac{1}{L_{A_k,p}}$, $a_{2k+1} = 1$ for $0 \le k < m-1$ and $a_{2m-1} = L_{A_m} - (m-1) = L_A - 1$ by Proposition 10(2). The E_k also have rational valuative capacity by Proposition 13 and $L_{E',p} \in \mathbb{Q}$. Since this is a continued fraction of period $2(m-1)$, the argument in [Dav82, Chapter IV, section 9] gives that it is the root of a quadratic polynomial over $\mathbb{Q}[x]$, although the a_i's are not necessarily integers, the values may be rational, the result still applies. □

Now we look into how to rearrange a subset $E = E' \cup p^m E$ in practice. First we split E' into smaller subsets E_i such that $\nu(x_1 - x_2) = m - 1$, for all $x_1, x_2 \in E_i$ and $x_1 \neq x_2$. We then need to split up these subsets again depending on the valuation of the differences of their elements. There is no straightforward way of doing this, we illustrate the process in the following example. We then compute $L_{E_i,p}$ which is a rational number, and for the case we are interested in for our main theorem the E_i are finite, since we only get a finite number of residue classes that are a sum of ℓ elements to the power of d in $\mathbb{Z}/(p^m)$. Thus $L_{E_i,p}$ depends on p and the number of elements in E_i only. We then compute $\nu_p(E_i - E_i')$, for all of subsets. Now we calculate the valuative capacity for the union of subsets having the highest valuation using Proposition 13, and keep repeating the process until we can use Proposition 12.

Example 17.

(a) We illustrate the above with $p = 3$, and $A = \{0, 1, 2, 3, 10, 11, 12, 19, 20, 21\} + 3^3\mathbb{Z}$ (this set is actually $3D_{3^3}$ when $d = 6$). We write A such that it satisfies the decomposition from Proposition 15:

$$A_0 = \{1, 2, 10, 11, 19, 20\} + 3^3\mathbb{Z}$$
$$A_1 = \{3, 12, 21\} + 3^3\mathbb{Z}$$
$$A_2 = \{0\} + 3^3\mathbb{Z}$$

we have that $p \nmid a$ for all $a \in A_0$ and p divides exactly a for all $a \in A_1$. If $a \in A_0$, $b \in A_1 \cup A_2$, then $\nu_3(a - b) = 0$, since $p \nmid a$ and $p \mid b$. We can rewrite A_0:

$$A_0 = (1 + \{0, 9, 18\} + 3^3\mathbb{Z}) \cup (2 + \{0, 9, 18\} + 3^3\mathbb{Z}).$$

The valuative capacity of both sets in the union of A_0 is

$$L_{1+\{0,9,18\}+3^3\mathbb{Z}} = L_{2+\{0,9,18\}+3^3\mathbb{Z}} = L_{\{0,9,18\}+3^3\mathbb{Z}} = L_{9(\{0,1,2\}+3\mathbb{Z})}$$
$$= 2 + L_{\mathbb{Z}} = 2 + \frac{1}{2} = \frac{5}{2}$$

Now we can find the valuative capacity of A_0, A_1 and A_2 using Proposition 12, for which we obtain $L_{A_0} = \frac{5}{4}$, $L_{A_1} = \frac{5}{2}$ and $L_{A_2} = \frac{7}{2}$. We are ready to compute the valuative capacity of A:

$$L_A = \cfrac{1}{\cfrac{1}{L_{A_0}} + \cfrac{1}{1 + \cfrac{1}{\cfrac{1}{L_{A_1} - 1} + \cfrac{1}{L_{A_2} - 1}}}} = \cfrac{1}{\cfrac{1}{\frac{5}{4}} + \cfrac{1}{1 + \cfrac{1}{\cfrac{1}{\frac{5}{2} - 1} + \cfrac{1}{\frac{7}{2} - 1}}}} = \frac{155}{204}.$$

(b) Now we look into the valuative capacity of the set $E = E' \cup 3^6 E$, where E' is $A_0 \cup A_1$ from part (a). We use Proposition 15 with $A_2 = 3^6 E$.
Then we have that $L_E = [0; a_0, a_1, a_2, L_{A_2} - 1]$, where $a_0 = \frac{1}{L_{A_0}} = \frac{4}{5}$, $a_1 = 1$, $a_2 = \frac{1}{L_{A_1} - 1} = \frac{2}{3}$, and $L_{A_2} = L_{3^{12}E} = 6 + L_E$. Hence $L_E = [0; \frac{4}{5}, 1, \frac{2}{3}, L_{A_2} - 1]$. Solving the continued fractions gives that L_E is a solution to the following quadratic equation:

$$30L_E^2 + 152L_E - 140 = 0.$$

This equation has for positive root $L_E = \frac{\sqrt{2494}}{15} - \frac{38}{15}$.

3. Main theorem

Now we are ready to prove the main result. (Note that in saying that zero can be written non-trivially as the sum of ℓ elements to the power of d, we mean that p does not divide at least one element in the sum.)

Theorem 18. *Let p be a prime number, d a positive integer and ℓ an integer greater than or equal to 2. Then, $L_{\ell D,p}$ is an algebraic number of degree at most 2. Moreover, if 0 can be written non-trivially modulo p^e as a sum of ℓ elements to the power of d, where $e = 1 + 2\nu_p(d)$, then $L_{\ell D,p}$ is a rational number.*

Proof. Note that the conditions on d imply that $d \geq e$. We start by looking at

$$E = \left\{ [c] \in \ell D_{p^e} \mid [c] = \sum_{i=1}^{\ell} [x_i]^d, \text{ where at least one of the } x_i \text{ is not divisible by } p \right\}.$$

Without loss of generality we may assume that for $[c] \in E$, $p \nmid x_1$. Suppose that $c \in \hat{\mathbb{Z}}_p$ is such that $[c] \in E$, and that $\{x_i\}_{i=1}^{\ell} \subseteq \hat{\mathbb{Z}}_p$ are such that $c \equiv \sum_{i=1}^{\ell} x_i^d \pmod{p^e}$. We claim that $c \in \overline{\ell D}$ in this case. Consider the polynomial $f(x) = x^d + \sum_{i=2}^{\ell} x_i^d - c$. f has at least one root (mod p^e), the integer x_1, with $p \nmid x_1$ and $f'(x) = dx^{d-1}$, is such that

$\nu_p(f'(x_1)) = \nu_p(d)$. Since $e = 2\nu_p(d)+1$ the general version of Hensel's Lemma [Gou97, 3.4.1] applies, and so there exists $\tilde{x}_1 \in \hat{\mathbb{Z}}_p$ such that $\tilde{x}_1 \equiv x_1 \pmod p$ and $f(\tilde{x}_1) = 0$, so $c \in \overline{\ell D}$. Thus, if $[0] \in E$, then $E = \ell D_{p^e}$ and $\overline{\ell D}$ is a union of cosets of the form $(c + p^e\hat{\mathbb{Z}}_p)$, Proposition 14 applies, and $L_{\ell D} = L_{\overline{\ell D}} \in \mathbb{Q}$.

If $E \neq \ell D_{p^e}$ then we claim that $\ell D_{p^e} \backslash E = \{[0]\}$. If $[c] \in \ell D_{p^e} \backslash E$ then there exists $\{x_i\}_{i=1}^{\ell}$ such that $c = \sum_{i=1}^{\ell} x_i^d \pmod{p^e}$ and $p \mid x_i$ for all i. This implies that $p^d \Big| \sum_{i=1}^{\ell} x_i^d$ and so $p^d \mid c$, hence $[c] = [0]$. Assume that $d \neq 2, 4$ and $p \neq 2$, then $d \geq e$. Let $x_i = p \cdot \tilde{x}_i$ and let $\tilde{c} = \sum_{i=1}^{\ell} \tilde{x}_i^d$. We then have $c = p^d\tilde{c}$ with $\tilde{c} \in \overline{\ell D}$. Conversely if $\tilde{c} \in \overline{\ell D}$, then $c = p^d\tilde{c} \in \overline{\ell D}$ and $c \equiv 0 \pmod{p^e}$. Thus $\overline{\ell D} = \left(\bigcup (c + p^e\hat{\mathbb{Z}}_p)\right) \cup p^d\overline{\ell D}$, where the union is over cosets for which $[c] \in E$. Corollary 16 applies here to show that $L_{\ell D,p} = L_{\overline{\ell D}}$ is the root of a quadratic polynomial over $\mathbb{Q}[x]$. Assume now that $p = 2$. Then, $L_{\ell D,2}$ is also a root of a quadratic polynomial by [FJ16, Theorem 3] when $d = 2$ and by Proposition 29 below when $d = 4$. □

Corollary 19. *For a fixed ℓ, if d is odd and p is a prime, then $L_{\ell D,p} \in \mathbb{Q}$.*

Proof. Write $0 = x^d + (-x)^d$, where $p \nmid x$, hence $L_{\ell D,p} \in \mathbb{Q}$ by Theorem 18. □

Proposition 15 and Corollary 16 give us algorithms that can be used to obtain $L_{\ell D,p}$ in either of the cases above.

The rest of this work will describe cases in which we can determine whether or not 0 can be non-trivially written as the sum of ℓ elements to the power of d and so determine the valuative capacity.

4. Specific valuative capacities

To begin this section we need to recall a definition and result from [Sma77a].

Definition 20. Given an integer d, a prime p and an integer $e > 1$, the Waring number $g(d, p^e) \pmod{p^e}$, is the smallest integer such that every element of $\mathbb{Z}/(p^e)$ can be written as a sum of $g(d, p^e)$ elements to the power of d.

Lemma 21. *Let $d = 2^\alpha\beta$, $\alpha \geq 0$, β odd, and let p be an odd prime. Then*

1. *-1 is a d-th power $\pmod p$ if and only if $p \equiv 1 \pmod{2^{\alpha+1}}$.*
2. *If $p \not\equiv 1 \pmod{2^{\alpha+1}}$, then $g(d, p^e) \geq 3$ for all $e > 1$.*

4.1. When p is odd

If $p \nmid d$, we have $e = 1$, and we obtain the following formula for the valuative capacity:

Proposition 22. *For a fixed ℓ, if $p \nmid d$ and $d = 2^\alpha\beta$, with β odd, if $p \equiv 1 \pmod{2^{\alpha+1}}$ then*

$$L_{\ell D,p} = \tfrac{1}{|\ell D_p|}\left(1 + \tfrac{1}{p-1}\right).$$

Proof. Theorem 18 gives that $L_{\ell D,p} \in \mathbb{Q}$, since by Lemma 21(1), there exists $x \in \mathbb{Z}$ such that $x^d \equiv -1 \pmod p$, hence $1^d + x^d \equiv 0 \pmod p$. Since $p \nmid d$, $e = 1$. For any $c \in \ell D_p$, the coset $c + p\mathbb{Z}$, has for valuative capacity $L_{(c+p\mathbb{Z}),p} = 1 + \frac{1}{p-1}$ by Proposition 10, and then $L_{\ell D,p} = \frac{1}{|\ell D_p|}\left(1 + \frac{1}{p-1}\right)$ by Proposition 12. $\square$

The above means, in particular, that when d is odd, we have a rational valuative capacity. When d is even, with $p \nmid d$ and $p \not\equiv 1 \pmod{2^{\alpha+1}}$, we can obtain explicitly the quadratic polynomial for which $L_{\ell D,p}$ is a root.

Proposition 23. *Let p be odd and d an even integer such that $d = 2^\alpha\beta$, with β odd. If $p \not\equiv 1 \pmod{2^{\alpha+1}}$ and $p \nmid d$, then $L_{\ell D,p}$ is the positive root of the quadratic equation with coefficients in $\mathbb{Q}$:*

$$L_{\ell D,p}^2 + dL_{\ell D,p} - \tfrac{(p-1)d}{|\ell D_p|} = 0.$$

Proof. When d is even, if $p \nmid d$, we have that $e = 1$ in the proof of Theorem 18 and $\overline{\ell D} = \left(\bigcup (c + p\hat{\mathbb{Z}}_p)\right) \cup p^d\overline{\ell D}$ for all c_i that can be written as ℓ d-th powers $\pmod p$. Thus

$$L_{\overline{\ell D},p} = L_{\ell D,p} = \cfrac{1}{\cfrac{|\ell D_p|}{p-1} + \cfrac{1}{d + L_{\ell D,p}}}$$

by Propositions 12. Solving for $L_{\ell D,p}$, gives the stated quadratic equation. Its discriminant is $d^2 + \frac{4(p-1)d}{|\ell D_p|}$ which is greater than d^2, hence the equation only has one positive root. $\square$

Next we look into the case $p > (d-1)^4$, where $p \nmid d$ and a result from [Sma77b] gives a very nice formula for the valuative capacity in the case where d is odd, and using the above, we can still get more details about the valuative capacity when $d = 2^\alpha\beta$ and $p \equiv 1 \pmod{2^{\alpha+1}}$.

Proposition 24. *If $p > (d-1)^4$ and $d > 2$ then:*

1. *For d odd, $L_{\ell D,p} = \frac{1}{p-1}$.*
2. *For d even, with $d = 2^\alpha\beta$ and β odd:*
   (a) *If $p \equiv 1 \pmod{2^{\alpha+1}}$, then $g(d, p^e) = 2$ and $L_{\ell D,p} = \frac{1}{p-1}$.*

(b) *If* $p \not\equiv 1 \pmod{2^{\alpha+1}}$, *then* $g(d, p^e) = 2$ *for* $e = 1$ *and* $g(d, p^e) = 3$ *otherwise, and, since* $p \nmid d$,

i. *if* $\ell = 2$, *then* $L_{2D,p}$ *is the root of the quadratic equation* $L_{2D,p}^2 + dL_{2D,p} - \frac{(p-1)d}{|2D_p|} = 0$,

ii. *if* $\ell \geq 3$, *then* $L_{\ell D,p} = \frac{1}{|\ell D_p|}\left(1 + \frac{1}{p-1}\right)$.

Proof. For both d odd and even we have that $g(d, p) \leq 2$, for $p > (d - 1)^4$ by [Sma77a], so this gives us that, $\ell D_p = \mathbb{Z}/(p)$. Now a lifting lemma in a paper by the same author [Sma77b, 2.1], gives us that if d is odd, and if $c \equiv x^d + y^d \pmod p$ has a solution, then $c \equiv x^d + y^d \pmod{p^e}$, for any $e > 1$, hence $g(d, p^e) = g(d, p)$ and, $D_{p^e} = \mathbb{Z}/(p^e)$. Using Proposition 9 we get that $L_{\ell D,p} = \frac{1}{p-1}$.

For d even and $p \equiv 1 \pmod{2^{\alpha+1}}$, then Lemma 21(1) gives that $g(d, p) = 2$. Thus 0 can be written as a sum of non-trivial d-th powers, and then we can lift any solution of $x^d + y^d \equiv c$ in $\mathbb{Z}/(p)$, to a solution in $\mathbb{Z}/(p^e)$ for $e > 1 \in \mathbb{Z}$. Now by [Sma77a], for $\ell > 2$, we have $\ell D = \mathbb{Z}/(p)$, hence $L_{\ell D_p,p} = \frac{1}{p-1}$ in this case as well.

In the case d even and $p \not\equiv 1 \pmod{2^{\alpha+1}}$, Lemma 21(2) gives that $g(d, p^e) = 2$ for $e = 1$ and since $p > (d - 1)^4$ by [Sma77a] $g(d, p^e) = 3$ otherwise, thus (b)i. is Proposition 23 and (b)ii. is Proposition 22. □

There is one last case of d odd, when $2 < p < (d - 1)^4$, where we can obtain a nice formula for the valuative capacity:

Theorem 25. *For* p *a prime, with* $p \nmid d$, *and* $d > 2$, *if* $\gcd(d, p - 1) = 1$, *then* $D = \mathbb{Z}/(p^e)$ *for* $e \geq 1$, *and for* $\ell > 1$, $L_{\ell D,p} = \frac{1}{p-1}$.

Proof. For both d odd and even we have that the d-th power map $\mathbb{Z}/(p) \to \mathbb{Z}/(p)$, is onto if $\gcd(d, p - 1) = 1$. Thus, in this case $D = \mathbb{Z}/(p)$, and so $\ell D = \mathbb{Z}/(p)$ also. Note that in this case 0 can be non-trivially written as the sum of two elements to the power of d. This allows us to use a lifting Lemma [Sma77b, 2.1], giving us that if d is odd, and $c \equiv x^d + y^d \pmod p$ has a solution, then $c \equiv x^d + y^d \pmod{p^e}$, for $e > 1$, hence $g(d, p^e) = g(d, p)$ and $\ell D = \mathbb{Z}/(p^e)$. Thus $L_{\ell D,p} = \frac{1}{p-1}$ as in Proposition 24. □

Note that for the previous theorem the case $\ell = 1$ can be found in [FJ12].

4.2. When $p = 2$

We also look into the case $p = 2$, where we might not find explicit formulas for valuative capacities, but we look at how one would search for them and we get different proofs of known results. In order to compute the valuative capacity when $p = 2$ and d is even, we need to establish something similar to Hensel's Lemma to allow us to lift values to $\mathbb{Z}/(2^e)$, with $e > 1$.

Proposition 26. *Let a be an odd integer and $e > 1$, then*

1. $x^{2^e} \equiv a \pmod 2$ *has a solution for all a.*
2. *For $n \leq e+2$, $x^{2^e} \equiv a \pmod{2^n}$ has a solution if and only if $a \equiv 1 \pmod{2^n}$.*
3. *For $n > e+2$, $x^{2^e} \equiv a \pmod{2^n}$ has a solution if and only if $a \equiv 1 \pmod{2^{e+2}}$.*

Proposition 27. *For d an odd integer, $n \in \mathbb{N}$, the image of the d-th power map on odd values is $\{2m+1 \pmod{2^n} \mid m \in \mathbb{Z}\}$.*

Using the above we can now figure out which elements can be lifted, since the odd powers have the same characterization as the 2^αth powers.

Proposition 28. *If $d = 2^\alpha \beta$, where $\alpha \geq 1$ and β is an odd integer ≥ 1, then we can write $\overline{D}$ in the following way:*

$$\overline{D} = \{0\} \cup (1 + 2^{\alpha+2}\hat{\mathbb{Z}}_2) \cup 2^d(1 + 2^{\alpha+2}\hat{\mathbb{Z}}_2) \cup 2^{2d}(1 + 2^{\alpha+2}\hat{\mathbb{Z}}_2) \cup 2^{3d}(1 + 2^{\alpha+2}\hat{\mathbb{Z}}_2) \ldots.$$

Proof. Using Proposition 26, we get that the odd d-th powers have the same characterization as the 2^α-th, since they are the 2^α-th powers of odd values, which are all the odd values, then Proposition 26 can be used again to show that this maps onto odd values. The even d-th powers are of the form $2^{dn}c$, where $n \in \mathbb{N}$ and c is an odd d-th power. Hence the result. $\square$

Proposition 29. *For $\ell = 2$ and any $d = 2^\alpha \beta$, where $\alpha \geq 1$ and β is an odd integer ≥ 1, L_{D+D} is the positive root of the following polynomial depending on d:*

$$(2\alpha + 6)L^2 + (2\alpha d - 2\alpha + 6d - 7)L + (\alpha + 3 - \alpha d^2 - 6\alpha d - 9d) = 0.$$

Proof. Using Proposition 28, we obtain that

$$\begin{aligned}\overline{D} + \overline{D} &= \{0\} \cup (\{1,2\} + 2^{\alpha+2}\hat{\mathbb{Z}}_2) \cup 2^d(\{1,2\} + 2^{\alpha+2}\hat{\mathbb{Z}}_2) \cup 2^{2d}(\{1,2\} + 2^{\alpha+2}\hat{\mathbb{Z}}_2) \\ &\quad \cup 2^{3d}(\{1,2\} + 2^{\alpha+2}\hat{\mathbb{Z}}_2) \ldots \\ &= \overline{D} \cup 2\overline{D}.\end{aligned}$$

Using Proposition 12 we obtain $\dfrac{1}{L_{\overline{D}+\overline{D}}} = \dfrac{1}{L_{\overline{D}}} + \dfrac{1}{L_{2\overline{D} \cup 2^d(\overline{D}+\overline{D})}}$. Using Proposition 10 and 13, we get the above polynomial. $\square$

For the next we will visit the case $d = 2$, note that our results coincide with the ones from [FJ16]. Our results can also be used to generalize the following theorem of Legendre on sums of squares:

Proposition 30. *When $\ell = 3$ and $d = 2$,*

$$\overline{3D}_2 = \{0\} \cup \bigcup_{i=0}^{\infty} 2^{2i}(\{1,2,3,4,5,6\} + 8\hat{\mathbb{Z}}_2).$$

Proof. We have shown in Proposition 28 that $\overline{D}_2 = \{0\} \cup \bigcup_{i=0}^{\infty} 2^i(1+8\hat{\mathbb{Z}}_2)$. When adding the cosets triple-wise, we get

$$\overline{3D}_2 = \{0\} \cup \bigcup_{i=0}^{\infty} 2^{2i}(\{1,2,3,4,5,6\} + 8\hat{\mathbb{Z}}_2).$$

The only elements not in $\overline{3D}_2$ are those of the form $2^{2i}(7 + 8\hat{\mathbb{Z}}_2)$, which corresponds to Legendre's theorem. □

Proposition 31. *If $d = 2$, $\ell \geq 4$ and $n \geq 1$, we have that $\overline{\ell D}_{2^n} = \mathbb{Z}/(2^n)$ and $L_{\overline{\ell D}_2} = 1$.*

Proof. By Proposition 30, the only cosets missing are those of the form $2^i(7+8\hat{\mathbb{Z}}_2)$, which can now be obtained since 7 can be written as the sum of 4 squares, $7 = 4 + 1 + 1 + 1$. Thus $\overline{\ell D}_{2^n} = \mathbb{Z}/(2^n)$. By Proposition 10 $L_{\overline{3D_2}} = L_{3D} = \frac{1}{p-1} = 1$. □

To conclude this paper we have added a table of various other valuative capacities (L) for $3D$, for both odd and even p:

p	d	$e = 2\nu_p(d) + 1$	L
2	2	3	$\frac{21}{22}$
2	4	5	$\frac{3}{2}$
2	6	3	$\frac{5}{4}$
2	8	7	$\frac{14}{15}$
3	6	3	$\frac{155}{204}$
3	12	3	$\frac{155}{204}$
3	18	5	$\frac{511}{488}$
3	27	7	$\frac{143}{170}$

References

[Bha97] M. Bhargava, p-Orderings and polynomial functions on arbitrary subsets of Dedekind rings, J. Reine Angew. Math. 490 (1997) 101–127.
[BC00] J. Boulanger, J.-L. Chabert, Asymptotic behavior of characteristic sequences of integer-valued polynomials, J. Number Theory 80 (2000) 238–259.
[Cha01] J.-L. Chabert, Generalized factorial ideals, Arab. J. Sci. Eng. 26 (2001) 51–68.
[Dav82] H. Davenport, The Higher Arithmetic, Cambridge University Press, 1982.
[FJ12] Y. Fares, K. Johnson, The characteristic sequence and p-orderings of the set of d-th powers of integers, Integers 12 (5) (2012).
[FJ16] Y. Fares, K. Johnson, The valuative capacities of the sets of sums of two and of three squares, Integers 16 (2016).

[FP16] Y. Fares, S. Petite, The valuative capacity of subshifts of finite type, J. Number Theory 158 (2016) 165–184.

[Fek23] M. Fekete, Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, Math. Z. (1) (1923) 228–249.

[Fer06] L.B.O. Ferguson, What can be approximated by polynomials with integer coefficients, Amer. Math. Monthly 113 (5) (2006) 403–414.

[Gou97] F. Gouvêa, p-Adic Numbers: An Introduction, second ed., Universitext, Springer-Verlag, Berlin, 1997.

[Joh09a] K. Johnson, Limits of characteristic sequences of integer-valued polynomials on homogeneous sets, J. Number Theory 129 (2009) 2933–2942.

[Joh09b] K. Johnson, p-Orderings of finite subsets of Dedekind domains, J. Algebraic Combin. 30 (2) (2009) 233–253.

[Joh15] K. Johnson, p-Orderings of noncommutative rings, Proc. Amer. Math. Soc. 143 (8) (2015) 3265–3279.

[PS72] G. Polya, G. Szegö, Problems and Theorems in Analysis, vol. I: Series, Integral Calculus, Theory of Functions, Grundlehren Math. Wiss., Band 193, Springer-Verlag, 1972, translated from the German by D. Aeppli.

[Rum13] R. Rumely, Capacity theory with local rationality. The strong Fekete–Szegö theorem on curves, Math. Surveys Monogr., vol. 193, American Mathematical Society, Providence, RI, 2013.

[Sma77a] C. Small, Solution of Waring's problem (mod n), Amer. Math. Monthly 84 (5) (1977) 356–359.

[Sma77b] C. Small, Waring's problem (mod n), Amer. Math. Monthly 84 (1) (1977) 12–25.