#A25 INTEGERS 12 (2012)

THE CHARACTERISTIC SEQUENCE AND *P*-ORDERINGS OF THE SET OF *D*-TH POWERS OF INTEGERS

Y. Fares
Laboratoire de mathematiques fundamentales et appliquees d'Amiens, Amiens, France

K. Johnson
Department of Mathematics, Dalhousie University, Halifax, Nova Scotia, Canada

Received: 9/21/10, Accepted: 3/6/12, Published: 3/23/12

Abstract

If E is a subset of $\mathbb{Z}$ then the n-th characteristic ideal of the algebra of rational polynomials taking integer values on E, $Int(E,\mathbb{Z})$, is the fractional ideal consisting of 0 and the leading coefficients of elements of $Int(E,\mathbb{Z})$ of degree no more than n. For p a prime the characteristic sequence of $Int(E,\mathbb{Z})$ is the sequence of negatives of the p-adic values of these ideals. We give recursive formulas for these sequences for the sets $\{n^d : n = 0, 1, 2, \dots\}$ by describing how to recursively p-order them in the sense of Bhargava. We describe the asymptotic behavior of these sequences and identify primes, p, and exponents, d, for which there is a formula in closed form for the terms.

1. Introduction

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

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

Associated to this ring is its sequence of characteristic ideals, $\{I_n : n = 0, 1, 2, \dots\}$, with I_n the fractional ideal formed by 0 and the leading coefficients of the elements of $Int(E,\mathbb{Z})$ of degree no more than n. For p a prime the sequence of negatives of the p-adic valuations of the ideals I_n, $\{\alpha(n) : n = 0, 1, 2, \dots\}$, is called the characteristic sequence of E with respect to p. In this paper we will give a recursive method for computing these sequences, and so the characteristic ideals, of the power sets $E = \{n^d : n = 0, 1, 2, \dots\}$ for any prime p and any positive integer exponent d and identify cases in which a nonrecursive formula exists.

Our results are based on the idea of a p-ordering of a subset E of $\mathbb{Z}$ as introduced in [1], [2] and we will, in the course of establishing our results, also give recursive methods for constructing p-orderings of these sets. A p-ordering of E is a sequence $\{a_n : n = 0, 1, 2, \dots\} \subseteq E$ with the property that for each n the element a_n minimizes the p-adic valuation $\nu_p(\prod_{i=0}^{n-1}(x - a_i))$ over $x \in E$. It is shown in [1], [2] that the sequence $\{\nu_p(\prod_{i=0}^{n-1}(a_n - a_i)) : n = 0, 1, 2, \dots\}$ coincides with the characteristic sequence of E for the prime p. To state our main result we use the following notation:

Definition 1. *If E is a subset of $\mathbb{Z}$, p a prime, and $0 \leq s < p$, let $E_s = \{x \in E : x \equiv s \pmod p\}$. Also, if $\{\alpha(n) : n = 0, 1, 2, \dots\}$ is the characteristic sequence of E with respect to p, let $\{\alpha_s(n) : n = 0, 1, 2, \dots\}$ denote the characteristic sequence of E_s.*

Theorem 2. *If d is a positive integer and $E = \{n^d : n = 0, 1, 2, \dots\}$, then the characteristic sequence $\{\alpha_s(n)\}$ has the properties:*

(a) $\alpha_0(n) = dn + \alpha(n)$.

(b) *if $s \neq 0$, and $p \nmid d$, then $\alpha_s(n) = n + \nu_p(n!)$.*

(c) *if $p \mid d$ and $d = p^c d_1$ with $p \nmid d_1$, then $\alpha_s(n) = (c+1)n + \nu_p(n!)$ for $p \geq 3$ and $\alpha_s(n) = (c+2)n + \nu_2(n!)$ if $p = 2$.*

(d) *if $s \neq 0$ and a is such that $a^d \equiv s \pmod p$, then the increasing order on $\{(np + a)^d : n = 0, 1, 2, \dots\}$ is a p-ordering for E_s.*

(e) *the map $\phi(n^d) = (pn)^d$ from E to E_0 gives a one-to-one correspondences between the p-orderings of these two sets.*

Since, by Lemma 3.5 of [6], the characteristic sequence $\{\alpha(n) : n = 0, 1, 2, \dots\}$ of E is the shuffle of the sequences $\{\alpha_s(n) : n = 0, 1, 2, \dots\}$ for $s = 0, 1, \dots, p-1$ into nondecreasing order, it follows that for each n the value of $\alpha(n)$ is equal to $\alpha_s(m)$ for some s and some $m < n$ and so that parts (a), (b) and (c) of this theorem determine $\alpha(n)$ for all n. Also, a p-ordering of E is given by combining p-orderings of the E_s's using the same shuffle and so is determined as well by parts (d) and (e).

For example, for $d = 3$ and $p = 2$ the sequence $\{\alpha(n) : n = 0, 1, 2, \dots\}$ is the nondecreasing shuffle of the sequence

$$\begin{aligned}\{\alpha_1(n) : n = 0, 1, 2, \dots\} \quad &= \{n + \nu_2(n) : n = 0, 1, 2, \dots\} \\ &= \{0, 1, 3, 4, 7, 8, 10, 11, 15, \dots\}\end{aligned}$$

with the sequence $\{\alpha_0(n) : n = 0, 1, 2, \dots\}$ which satisfies the equation $\alpha_0(n) = 3n + \alpha(n)$. Thus

$$\{\alpha_0(n) : n = 0, 1, 2, \dots\} = \{0, 3, 7, 12, 15, 19, 25, 28, 32, \dots\}$$

and

$$\{\alpha(n) : n = 0, 1, 2, \dots\} = \{0, 0, 1, 3, 3, 4, 7, 7, 8, \dots\}.$$

The corresponding 2-ordering is $\{0, 1, 27, 8, 125, 343, 216, 729, 1331, \ldots\}$. Similar calculations for the primes 3, 5, and 7 show that the sequence of inverses of characteristic ideals of the set of cubes is

$$\{(1), (1), (2), (72), (72), (2160), (51840), (362880), (6531840), \ldots\}.$$

Combining the results of Theorem 2 with those of [7] allows us to determine the asymptotic behavior of the characteristic sequences, i.e., the values of the limits $\lim_{n\to\infty} \alpha(n)/n$.

Theorem 3. *If $E = \{n^d : n = 0, 1, 2, \ldots\}$, the sets E_s are nonempty for $e + 1$ distinct residue classes modulo p and $L = \lim_{n\to\infty} \alpha(n)/n$, then*

(a) if $p \nmid d$, then L satisfies the equation

$$e(p-1)L^2 + ed(p-1)L - pd = 0.$$

(b) if $p \mid d$ and $d = p^c d_1$ with $p \nmid d_1$, then for $p \geq 3$ the limit L satisfies the equation

$$e(p-1)L^2 + ed(p-1)L - d((p-1)(c+1)+1) = 0,$$

while for $p = 2$ it satisfies

$$L^2 + dL - d(c+3) = 0.$$

The question of whether or not these limits are rational can be settled by examining the discriminants of the quadratic equations above.

Theorem 4. *If $S = \{n^d : n = 0, 1, 2, \ldots\}$ and $\{\alpha(n) : n = 0, 1, 2, \ldots\}$ is the characteristic sequence of S for the prime p, then the limit $L = \lim_{n\to\infty} \alpha(n)/n$ is rational if and only if $d \mid p-1$ or $d = p = 2$.*

In those cases where this limit is rational there is a closed form formula for the characteristic sequence:

Theorem 5. *If $d \mid p-1$ and $\{\alpha(n) : n = 0, 1, 2, \ldots\}$ is the characteristic sequence of the set $S = \{n^d : n = 0, 1, 2, \ldots\}$ then $\alpha(n) = \nu_p((dn)!)$.*

2. Characteristic Sequences and p-Orderings

The assertions in Theorem 2, parts (a) and (e), concerning E_0 and $\alpha_0(n)$ are obvious. We will, therefore, assume from this point on that $s \neq 0$ and provide a proof of the other assertions in the theorem. For this we need some preliminary results about the sets E_s.

Lemma 6. *The congruence* $x^d \equiv 1 \pmod{p}$ *has* $\gcd(d, p-1)$ *distinct solutions modulo* p.

Proof. Let $t = \gcd(d, p-1)$. The multiplicative group $(\mathbb{Z}/(p))^*$ is cyclic of order $p-1$ and so has a unique subgroup of order t consisting of those elements of $\mathbb{Z}/(p)$ whose multiplicative order divides t. Since t is a divisor of d, all elements of this subgroup are solutions of the given congruence. On the other hand, if $x \in \mathbb{Z}/(p)$ is a solution of this congruence then its order must be a divisor of d and also of the order of $(\mathbb{Z}/(p))^*$, i.e., of t. □

Let r be a generator of the cyclic subgroup of $(\mathbb{Z}/(p))^*$ consisting of the solutions of $x^d \equiv 1 \pmod{p}$ and, for $0 \leq i \leq \gcd(d, p-1) - 1$, let r_i be the representative of $r^i \pmod{p}$ which is between 1 and $p-1$ (so that in particular $r_0 = 1$ and $r_1 = r$).

Corollary 7. *If* $a^d \equiv s \pmod{p}$, *then the set* E_s *is the disjoint union of the sets* $E_{s,i} = \{(np + r_i a)^d : n = 0, 1, 2, \ldots\}$ *for* $0 \leq i < \gcd(d, p-1)$ *together with a finite (possibly empty) set. In particular, the disjoint union of the sets* $E_{s,i}$ *is* p*-adicly dense in* E_s.

Lemma 8. *If* $a^d \equiv s \pmod{p}$ *and* E_s *and the sets* $E_{s,i}$ *are as above, then* $E_{s,0}$ *is* p*-adicly dense in* E_s.

Proof. In order to prove that $E_{s,0}$ is p-adicly dense in E_s, we need only prove that for every $k \in \mathbb{N}$, every i such that $0 \leq i \leq \gcd(d, p-1) - 1$ and every $(yp + r_i a)^d \in E_{s,i}$, there exists $(xp + a)^d \in E_{s,0}$ such that $\nu_p((yp + r_i a)^d - (xp + a)^d) \geq k$.

Let $x \in \mathbb{Z}$ be a solution of the congruence $r_i^{p^k} x \equiv y \pmod{p^{k-1}}$. Such a solution exists because r_i is not divisible by p and so $r_i^{p^k}$ is a unit modulo p^{k-1}. For such an x we have

$$p(y - r_i^{p^k} x) \equiv 0 \equiv a(r_i^{p^k} - r_i) \pmod{p^k}$$

which is equivalent to

$$(py + r_i a) \equiv r_i^{p^k}(px + a) \pmod{p^k}$$

and so we have, taking d-th powers,

$$(py + r_i a)^d \equiv r_i^{dp^k}(px + a)^d \equiv (px + a)^d \pmod{p^k}$$

as required. □

Since $E_{s,0}$ is p-adicly dense in E_s, a p-ordering of $E_{s,0}$ will be one of E_s also and these sets will have the same characteristic sequences. To calculate this characteristic sequence some preliminary results concerning p-adic values of d-th powers are needed.

Let $\alpha \in \mathbb{Z}_{(p)} \setminus \{1\}$ be such that $\nu_p(\alpha - 1) \geq 1$ and let $d \geq 1$. We then have $\alpha^d - 1 = (\alpha - 1)(\sum_0^{d-1}(\alpha^k - 1) + d)$ and so, in particular, if p does not divide d, then $\nu_p(\alpha^d - 1) = \nu_p(\alpha - 1)$. If p does divide d, then we have the following:

Lemma 9. [([4], Prop 8)] *If $\alpha \in \mathbb{Z}_{(p)} \setminus \{1\}$ is such that $\nu_p(\alpha - 1) \geq 1$, then for every $d \in \mathbb{N}$ such that p divides d we have*

$$\nu_p(\alpha^d - 1) = \begin{cases} \nu_p(\alpha - 1) + \nu_p(d) & \text{if } p \geq 3 \text{ or } p = 2 \text{ and } \nu_p(\alpha - 1) \geq 2 \\ \nu_p(\alpha + 1) + \nu_p(d) & \text{if } p = 2 \text{ and } \nu_p(\alpha - 1) = 1 \end{cases}$$

Lemma 10. *If $a^d \equiv s \pmod p$ and $(xp + a)^d$ and $(yp + a)^d$ are elements of $E_{s,0}$, then:*

i. if $p \geq 3$ then,

$$\nu_p\left((xp + a)^d - (yp + a)^d\right) = 1 + \nu_p(x - y) + \nu_p(d).$$

ii. if $p = 2$ and $\nu_p(x - y) \geq 1$, then

$$\nu_p\left((xp + a)^d - (yp + a)^d\right) = 1 + \nu_p(x - y) + \nu_p(d).$$

iii. if $p = 2$ and $\nu_p(x - y) = 0$, then

$$\nu_p\left((xp + a)^d - (yp + a)^d\right) = 1 + \nu_p(x + y + a) + \nu_p(d).$$

Proof. We have:

$$\nu_p\left((px + a)^d - (py + a)^d\right) = \nu_p\left(\left(\frac{px + a}{py + a}\right)^d - 1\right).$$

Since $\nu_p\left(\left(\frac{px + a}{py + a}\right) - 1\right) = \nu_p\left(\frac{p(x - y)}{py + a}\right) \geq 1$, using Lemma 9 we have:

i. if $p \geq 3$ or $\nu_p(x - y) \geq 1$, then

$$\begin{aligned} \nu_p\left((px + a)^d - (py + a)^d\right) &= \nu_p\left(\frac{p(x - y)}{py + a}\right) + \nu_p(d) \\ &= \nu_p\left(\left(\frac{px + a}{py + a}\right) - 1\right) + \nu_p(d) \\ &= 1 + \nu_p(x - y) + \nu_p(d). \end{aligned}$$

ii. if $p = 2$ and $\nu_p(x - y) \geq 1$, then

$$\nu_p\left((px + a)^d - (py + a)^d\right) = 1 + \nu_p(x - y) + \nu_p(d).$$

iii. if $p = 2$ and $\nu_p(x - y) = 0$, then

$$\begin{aligned}\nu_p\left((px+a)^d - (py+a)^d\right) &= \nu_p\left(\left(\frac{px+a}{py+a}\right)+1\right) + \nu_p(d)\\ &= 1 + \nu_p(x+y+a) + \nu_p(d).\end{aligned}$$ □

In fact, if $p = 2$ and $d = 2m$, then

$$\begin{aligned}\nu_p\left((px+a)^d - (py+a)^d\right) &= \nu_p\left(\left(\frac{px+a}{py+a}\right)^{2m} - 1\right)\\ &= \nu_p\left(\left(\frac{px+a}{py+a}+1\right)\left(\frac{px+a}{py+a}-1\right)\right) + \nu_p(m)\\ &= \nu_p\left(p^2(x+y+a)(x-y)\right) + \nu_p(m)\\ &= 1 + \nu_p\left((x^2+ax) - (y^2+ay)\right) + \nu_p(d).\end{aligned}$$

We are now ready to prove Theorem 2.

Proof. Since, as previously noted, $E_{s,0}$ is dense in E_s these two sets have the same characteristic sequence. For parts (b) and (d) we show by induction on n that the sequence $\{((np+a)^d) : n = 0, 1, 2, \dots\}$ is a p-ordering for $E_{s,0}$. Since $p \nmid d$ it follows from Lemma 10 that

$$\sum_{i=0}^{n-1} \nu_p\left((xp+a)^d - (ip+a)^d\right) = n + \sum_{i=0}^{n-1} \nu_p(x-i).$$

The term n in this sum is independent of x and the remaining sum is the same as that occurring in showing that the usual increasing order is a p-ordering of the integers. It is, therefore, minimized by taking $x = n$ in which case the value of the sum, which equals $\alpha_s(n)$, is $n + \nu_p(n!)$.

For part (c), if $p \geq 3$ and $p \mid d$ with $d = p^c d_1$ and $p \nmid d_1$, then the same argument shows that

$$\sum_{i=0}^{n-1} \nu_p\left((xp+a)^d - (ip+a)^d\right) = n + n\nu_p(d) + \sum_{i=0}^{n-1} \nu_p(x-i)$$

is minimized by taking $x = n$ which results in $\alpha_s(n) = (c+1)n + \nu_p(n!)$.

For $p = 2$ and $s = 1$ we may take $a = 1$. The corresponding expression is

$$\sum_{i=0}^{n-1} \nu_p\left((2x+1)^d - (2i+1)^d\right) = n + n\nu_2(d) + \sum_{i=0}^{n-1} \nu_2\left((x^2+x) - (i^2+i)\right)$$

and, since the increasing ordering on $\{n^2 + n \mid n \in \mathbb{N}\}$ is known to be a 2-ordering, it follows that $x = n$ minimizes the sum in this case also. □

3. Limits

By Proposition 7 of [7] the limit $L = \lim_{n\to\infty} \alpha(n)/n$ satisfies the equation

$$\frac{1}{L} = \sum \frac{1}{L_s}$$

if $L_s = \lim_{n\to\infty} \alpha_s(n)/n$ and the sum is taken over the residue classes for which E_s is infinite. Recall that if the expression of n in base p is $n = \sum n_i p^i$, then $\nu_p(n!) = (n - \sum n_i)/(p-1)$. It thus follows from part (b) of Theorem 2 that for $s \neq 0$ and $p \nmid d$

$$L_s = \lim_{n\to\infty} (n + \nu_p(n!))/n = \lim_{n\to\infty} \frac{(n + \dfrac{n - \sum n_i}{p-1})}{n} = p/(p-1)$$

while for $s = 0$ part (a) implies

$$L_0 = L + d.$$

We thus have that

$$\frac{1}{L} = \frac{1}{d+L} + \sum \frac{p-1}{p}$$

in which the sum has $e = (p-1)/\gcd(d, p-1)$ terms. Simplifying this equation yields the quadratic

$$e(p-1)L^2 + ed(p-1)L - pd = 0.$$

If $d = p^c d_1$ with $c > 0$, then for $p \geq 3$ we have

$$L_s = \lim_{n\to\infty} ((c+1)n + \nu_p(n!))/n = ((c+1)(p-1)+1)/(p-1)$$

and, for $p = 2$,

$$L_s = \lim_{n\to\infty} ((c+2)n + \nu_2(n!)) = c+3.$$

This gives, for $p \geq 3$, the equation

$$\frac{1}{L} = \frac{1}{d+L} + \sum \frac{p-1}{(c+1)(p-1)+1}$$

and, for $p = 2$,

$$\frac{1}{L} = \frac{1}{d+L} + \sum \frac{1}{c+3}.$$

The corresponding quadratics are, for $p \geq 3$,

$$e(p-1)L^2 + ed(p-1)L - d((p-1)(c+1)+1) = 0$$

and, for $p = 2$,

$$L^2 + dL - d(c+3) = 0.$$

The fact that these limits are roots of quadratic equations raises the natural question of whether or not these limits are rational. The answer is as follows:

Proposition 11. *If $\{\alpha(n) : n = 0, 1, 2, \dots\}$ is the characteristic sequence for the set $\{n^d : n = 0, 1, 2, \dots\}$ with respect to the prime p and $L = \lim_{n\to\infty} \alpha(n)/n$, then $L \in \mathbb{Q}$ if and only if d divides $p-1$ or $d = p = 2$.*

Proof. We consider separately the four cases $p > 2$ and $p \nmid d$, $p > 2$ and $p \mid d$, $p = 2$ and d odd, and $p = 2$ and d even. In each case we determine whether or not the discriminant of the quadratic equation given above is a square.

If $p > 2$ does not divide d, then the discriminant in question is $(ed(p-1))^2 + 4ed(p-1)p = (ed(p-1) + 2p)^2 - 4p^2$. If this is a square, y^2 say, then $(2p, y, ed(p-1)+2p)$ is a Pythagorean triple. A general Pythagorean triple with common divisor k is of the form (kx, ky, kz) with $\gcd(x, y, z) = 1$ and exactly one of x or y even. By a theorem of Euler if y is even, then there exist m, n such that $x = m^2 - n^2$, $y = 2mn$ and $z = m^2 + n^2$. In our case $k = 2$, since p is an odd prime, and so we must have $p = m^2 - n^2 = (m-n)(m+n)$. Since p is prime the only solution is $m = (p+1)/2$ and $n = (p-1)/2$. Since $2(m^2 + n^2) = ed(p-1) + 2p$ we have

$$(p+1)^2/2 + (p-1)^2/2 = p^2 + 1 = ed(p-1) + 2p$$

and so $p - 1 = ed$. Since $ed = d(p-1)/\gcd(d, p-1) = \mathrm{lcm}(d, p-1)$ this can occur if and only if d is a divisor of $p-1$.

If $p > 2$ divides d with $d = p^c\ell$, then the discriminant is $(ed(p-1))^2 + 4de(p-1)((p-1)(c+1)+1) = (ed(p-1) + 2((p-1)(c+1)+1))^2 - 4((p-1)(c+1)+1)^2$. As in the previous case, if this forms a Pythagorean triple $(2((p-1)(c+1)+1), y, ed(p-1) + 2((p-1)(c+1)+1))$, then the greatest common divisor, k, is even and there exist integers $m > n$ such that $2((p-1)(c+1)+1) = k(m^2 - n^2)$ and $k(m^2+n^2) = ed(p-1) + 2((p-1)(c+1)+1)$. Let $D = 2((p-1)(c+1)+1)$. If $k(m^2 - n^2) = D$, then $k(m^2 + n^2) = 2kn^2 + D$. This is an increasing function of n and so is largest when n is largest subject to the constraint $m > n$, i.e., when $m = n+1$ in which case $n = ((D/k)-1)/2$ and $m = ((D/k)+1)/2$. For these values $k(m^2+n^2) = (D^2/2k) + (k/2)$ which is largest if $k = 2$ (since k is even). Combining this with our second equation we have the inequality $D^2/4 + 1 \geq D + ed(p-1)$ or

$$\begin{aligned}(p-1)^2(c+1)^2 - 1 &\geq (p-1)\mathrm{lcm}(d, p-1)\\ &= (p-1)p^c\mathrm{lcm}(\ell, p-1)\\ &\geq (p-1)^2p^c.\end{aligned}$$

This implies $(c+1)^2 \geq p^c$ which can occur only if $p = 3$ and $c = 1$ or $c = 2$. In both of these cases no pair m, n exists.

If $p = 2$ and d is odd, then the discriminant is $d^2 + 8d = (d+4)^2 - 4^2$. In this case in order for $(4, y, d+4)$ to be a Pythagorean triple there must exist integers k and $m > n$ such that $4 = 2kmn$ and $k(m^2+n^2) = 4 + d$. Since the first equation implies $m = 2$ and $k = n = 1$ the only possible value of d is $d = 1$.

If $p = 2$ and $d = 2^c\ell$, then the discriminant is $d^2+4d(c+3) = (d+2(c+3))^2-4(c+3)^2$ and so we must consider possible Pythagorean triples $(2(c+3), y, 2(c+3)+d)$. Since d is even the greatest common divisor, k, must be even also and either $\nu_2(2(c+3)+d) < \nu_2(2(c+3))$ or $\nu_2(2(c+3)+d) = \nu_2(2(c+3))$. In the first case there exist integers $m > n$ such that $c+3 = kmn$ with $k(m^2+n^2) = d+2(c+3) = 2^c\ell+2(c+3)$. The quantity $k(m^2+n^2)$ is subject to the constraints $c+3 = kmn$, $m > n$ and k even and so is largest if $n = 1$, $k = 2$ and $m = (c+3)/2$. We thus have $2(((c+3)/2)^2+1) \geq 2^c\ell + 2(c+3)$, which implies $(c+1)^2 \geq 2^{c+1}$ and so $c \leq 3$. The only value of c in this range for which there is a solution is $c = 1$ with $k = 2$, $\ell = 1$, $m = 2$ and $n = 1$. In the second case there must exist integers $m > n$ such that $2(c+3) = k(m^2-n^2)$ and $k(m^2+n^2) = d+2(c+3) = 2^c\ell+2(c+3)$. As in the case $p > 2$, above, the first of these equations implies that

$$k(m^2+n^2) \leq k((\frac{2(c+3)/k-1}{2})^2 + (\frac{2(c+3)/k+1}{2})^2).$$

The right-hand side is largest if $k = 2$ and simplifies to give

$$k(m^2+n^2) \leq (c+3)^2+1.$$

Combining this with the second equation gives the inequality

$$(c+3)^2+1 \geq 2(c+3)+d$$

or

$$(c+2)^2 \geq d = 2^c\ell$$

which occurs only if $c \leq 6$ and no value for c in this range has $\nu_2(2(c+3)+d) = \nu_2(2(c+3))$. □

Proposition 12. *If d divides $p-1$, then the characteristic sequence $\{\alpha(n) : n = 0, 1, 2, \dots\}$ of the set $\{n^d : n = 0, 1, 2, \dots\}$ is given by $\alpha(n) = \nu_p((dn)!)$.*

Proof. Let $e = (p-1)/d$ and let $\beta(n) = \nu_p((dn)!)$. Also let ϕ and $\{\psi_s : s = 1, 2, \dots, e\}$ be the following maps from $\mathbb{Z}^{\geq}0$ to $\mathbb{Z}^{\geq 0}$:

$$\phi(n) = dn$$

$$\psi_s(n) = en + \lfloor n/d \rfloor + s.$$

It is straightforward to verify that these $e+1$ maps define a shuffle, i.e., that each is strictly increasing and that any element of $\mathbb{Z}^{\geq 0}$ is in the image of exactly one of them. By Theorem 2 $\{\alpha(n) : n = 0, 1, 2, \dots\}$ is the nondecreasing shuffle of the e sequences $\{\alpha_s(n) : n = 0, 1, 2, \dots\}$ with $\alpha_s(n) = n + \nu_p(n!)$ for $s = 1, 2, \dots, e$ and the sequence $\{\alpha_0(n) : n = 0, 1, 2, \dots\}$ with $\alpha_0(n) = dn + \alpha(n)$. Thus it will suffice, by induction on n, to show that $\{\beta(n) : n = 0, 1, 2, \dots\}$, which is nondecreasing, is the $(\phi, \psi_1, \dots, \psi_s)$-shuffle of $dn + \beta(n)$ and the sequences $\alpha_1, \dots, \alpha_s$.

For the first of these let $\sum n_i p^i$ be the base p expansion of dn and note that the base p expansion of pdn will then be $\sum n_i p^{i+1}$. We thus have

$$\begin{aligned} \beta(\phi(n)) &= \beta(pn) \\ &= \nu_p(pdn!) \\ &= \frac{pdn - \sum n_i}{p-1} \\ &= dn + \frac{dn - \sum n_i}{p-1} \\ &= dn + \beta(n). \end{aligned}$$

For the others, note that for $0 \le r < d$ we have $\psi_s(dn + r) = pn + er + s$ and so, that

$$\beta(\psi_s(dn + r)) = \beta(pn + er + s) = \nu_p((pdn + (p-1)r + ds)!)$$

while

$$\alpha_s(dn + r) = \nu_p((p(dn + r))!) = \nu_p((pdn + pr)!).$$

Since $(p-1)r + ds - pr = ds - r$ and $1 \le ds - r < p$ these two p-adic norms are equal, i.e., $\beta(\psi_s(dn + r)) = \alpha_s(dn + r)$. □

References

[1] Bhargava, M., *P*-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. Reine Angew. Math.* **490** (1997), 101–127.

[2] Bhargava, M., The factorial function and generalizations, *Am. Math. Monthly* **107** (2000), 783–799.

[3] Cahen,P.-J. and Chabert,J.-L., Integer Valued Polynomials, Amer. Math. Soc., Providence, R.I., 1997.

[4] Chabert, J-L, Fan, A-H, and Fares, Y, Minimal dynamical systems on a discrete valuation domain, *Discrete and Continuous Dynamical Systems* **425** (2009), 751–777.

[5] Fares, Y and Johnson, K., Characteristic sequences of quadratic sets, submitted.

[6] Johnson, K., *P*-orderings of Finite Subsets of Dedekind Domains, *J. Algebraic Combinatorics* **30** (2009), 233–253.

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