#A37 INTEGERS 10 (2010), 437-451

SUBSETS OF $\mathbb{Z}$ WITH SIMULTANEOUS ORDERINGS

David Adam
GAATI, Université de la Polynésie Française, Tahiti, Polynésie Française
david.adam@upf.pf

Jean-Luc Chabert
LAMFA CNRS-UMR 6140, Université de Picardie, France
jean-luc.chabert@u-picardie.fr

Youssef Fares
LAMFA CNRS-UMR 6140, Université de Picardie, France
youssef.fares@u-picardie.fr

Received: 1/28/10, Revised: 4/21/10, Accepted: 4/28/10, Published: 9/15/10

Abstract

We are interested in subsets S of $\mathbb{Z}$ which admit simultaneous orderings, that is, sequences $\{a_n\}_{n\geq 0}$ such that $\prod_{k=0}^{n-1}(a_n - a_k)$ divides $\prod_{k=0}^{n-1}(x - a_k)$ for every $x \in S$ (analogously to $n!$ which divides $(m+n)!/m!$ for every m). In particular, we characterize the polynomials f of degree 2 such that $f(\mathbb{N})$ admits a simultaneous ordering.

1. Introduction

Let D be an integral domain with quotient field K and let S be an infinite subset of D. Recall that we may define a sequence of generalized factorials associated to S in the following way:

Definition 1. (cf. [4, §§ I.1, II.1], [5] and [7])

1. The ring of *integer-valued polynomials* on S with respect to D is $\mathrm{Int}(S,D) = \{f \in K[X] \mid f(S) \subseteq D\}$.
2. The n-th *characteristic ideal* of S with respect to D is the fractional ideal $I_n(S,D)$ formed by the leading coefficients of the polynomials of $\mathrm{Int}(S,D)$ with degree $\leq n$.
3. The n-th *factorial ideal* of S with respect to D is the ideal $n!_S^D$ 'inverse' of $I_n(S,D)$, that is, $n!_S^D = \{x \in D \mid xI_n(S,D) \subseteq D\}$.

For instance, when $D = S = \mathbb{Z}$, the n-th factorial ideal $n!_{\mathbb{Z}}^{\mathbb{Z}}$ is exactly $n!\mathbb{Z}$.

When D is a Dedekind domain, these factorial ideals are defined locally by Bhargava [2] by means of what he called $\mathfrak{p}$-orderings. In [3] he showed that they satisfy several nice properties which generalize those of the classical factorials. Actually, we want to restrict our study to subsets of Dedekind domains which have simultaneous orderings in the following sense:

Definition 2. [3] A sequence $\{a_n\}_{n\geq 0}$ of elements of S is said to be a *simultaneous ordering* of S (with respect to the domain D) if the following equivalent asssertions are satisfied :

1. For all $n > 0$ and for all $x \in S$,
$$\prod_{k=0}^{n-1}(a_n - a_k) \text{ divides } \prod_{k=0}^{n-1}(x - a_k) \text{ in } D.$$
2. For all $n > 0$ and for all $x_0, x_1, \ldots, x_n \in S$,
$$\prod_{0\leq i<j\leq n}(a_j - a_i) \text{ divides } \prod_{0\leq i<j\leq n}(x_j - x_i) \text{ in } D.$$
3. The following polynomials form a basis of the D-module $\mathrm{Int}(S, D)$:
$$f_0(X) = 1 \quad \text{and} \quad f_n(X) = \prod_{k=0}^{n-1}\frac{X - a_k}{a_n - a_k} \quad \text{for } n \geq 0.$$

For a proof of the equivalences, see [7, §6] or [11, §2].

For instance, when $D = \mathbb{Z}$, the sequence $\{n\}_{n\geq 0}$ is a simultaneous ordering of $\mathbb{N}$ (resp. $\mathbb{Z}$). Moreover, $\{n\}_{n\geq k}$ for $k \in \mathbb{N}$ (resp. $\{n\}_{n\geq k}$ and $\{-n\}_{n\geq k}$ for $k \in \mathbb{Z}$) are simultaneous orderings of $\mathbb{N}$ (resp. $\mathbb{Z}$). Note that $\mathbb{N}$ denotes here the set of non-negative integers. More generally, the following lemma is obvious:

Lemma 3. *If the sequence $\{a_n\}_{n\geq 0}$ is a simultaneous ordering for S, then*

1. *For all $n > 0$,*
$$n!_S^D = \prod_{k=0}^{n-1}(a_n - a_k)D,$$
2. *for every $\alpha \in D \setminus \{0\}$, $\beta \in D$, the sequence $\{\alpha a_n + \beta\}_{n\geq 0}$ is a simultaneous ordering of the subset $\alpha S + \beta = \{\alpha s + \beta \mid s \in S\}$,*
3. *for all $n > 0$, for all $\alpha \in D \setminus \{0\}$, and for all $\beta \in D$,*
$$n!_{\alpha S+\beta}^D = \alpha^n n!_S^D.$$

Remark 4.

1. If D is a Dedekind domain, S is a subset of D, and $\mathfrak{p}$ is a maximal ideal of D, then we could define a $\mathfrak{p}$-ordering of S as a 'simultaneous ordering' of S with respect to the local domain $A = D_{\mathfrak{p}}$.

2. A priori, a simultaneous ordering of S is an infinite sequence of elements of S. But, we could also consider finite simultaneous orderings, specially when S is finite : a *simultaneous ordering of S of length m* is a sequence $\{a_0, a_1, \ldots, a_m\}$ of elements of S which satisfies the equivalent assertions of Definition 2 with the restriction: $1 \leq n \leq m$.

In fact, we want also to restrict our study to subsets of $\mathbb{Z}$. Note that in this case, factorial ideals are principal and so may be considered as represented by integers. The aim of this paper is to look for natural examples of sets of integers which admit simultaneous orderings. We have already seen the sequence $\{n\}_{n\in\mathbb{N}}$. The following examples are well-known.

Example 5.

1. For every integer $q \geq 2$, the sequence $\{q^n\}_{n\geq 0}$ is a simultaneous ordering of the subset $S = \{q^n \mid n \geq 0\}$ (cf. [3]). Indeed, for every $m \geq n$, the number:

$$\frac{(q^m-1)(q^m-q)\ldots(q^m-q^{m-1})}{(q^n-1)(q^n-q)\ldots(q^n-q^{n-1})}$$

$$= q^{\frac{(m-n)(m+n-1)}{2}}(q^m-1)(q^{m-1}-1)\ldots(q^{n+1}-1)$$

is an integer. (In fact, this is the number of n-dimensional subspaces of a m-dimensional $\mathbb{F}_q$-vector space, when q is a prime power.) Consequently, by Lemma 3,

$$n!_S^{\mathbb{Z}} = q^{\frac{n(n-1)}{2}}(q^n-1)(q^{n-1}-1)\ldots(q-1).$$

2. The sequence $\{n^2\}_{n\geq 0}$ is a simultaneous ordering of $S = \{n^2 \mid n \geq 0\}$ (cf. [3]). Indeed, for every $n > 0$, the polynomial

$$\prod_{k=0}^{n-1} \frac{X-k^2}{n^2-k^2}$$

of degree $2n$ takes integral values on $2n+1$ consecutive integers x ($-n \leq x \leq n$). And then, it takes integral values on every integer. Consequently,

$$n!_S^{\mathbb{Z}} = \frac{1}{2}(2n)!.$$

3. Analogously $\left\{\frac{n(n+1)}{2}\right\}_{n\geq 0}$ is a simultaneous ordering of $S = \left\{\frac{n(n+1)}{2} \mid n \geq 0\right\}$ (cf. [8, Exercise II.11.6]). Indeed, for every $n > 0$, the polynomial

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

of degree $2n$ takes integral values for $-n \leq X \leq n$. As a consequence,

$$n!_S^{\mathbb{Z}} = \frac{(2n)!}{2^n}.$$

Remark 6. Using Lemma 3.1, it is easy to construct other subsets which admit simultaneous orderings. But, are there other 'natural' examples? Note that it is more likely to find a subset with a simultaneous ordering by considering the polynomial closures of the subsets S, that is, the largest subsets $\overline{S}$ such that $\mathrm{Int}(S,\mathbb{Z}) = \mathrm{Int}(\overline{S},\mathbb{Z})$, since if S admits a simultaneous ordering then $\overline{S}$ does also. The converse is not always true: the subset $S = \{n + n! \mid n \in \mathbb{N}\}$ does not have any simultaneous ordering, while $\overline{S} = \mathbb{Z}$ does.

Let us consider the set $\mathbb{P}$ of prime numbers and its polynomial closure $\overline{\mathbb{P}} = \mathbb{P} \cup \{\pm 1\}$ [6]. Then, one may check that the sequence $\{1, 2, 3, 5\}$ is a simultaneous ordering (of length 3), but there are no simultaneous orderings of length 4 [10]. Note that we could construct infinite subsets S of $\mathbb{P}$ such that S admits a simultaneous ordering (see [9, Corollary 5.6]), but they are obtained by an *ad hoc* construction choosing the elements one by one, and they do not form 'natural' sets.

In order to find other 'natural' subsets, we are going to consider two types of subsets which in some sense generalize the sequence $\{n^2\}_{n\in\mathbb{N}}$: first the sets formed by the k-th powers of the integers, then the sets formed the range of integer-valued polynomials of degree 2.

2. General Remarks

Since, we are going to focus our study on the subsets S of the form $f(\mathbb{N}) = \{f(n) \mid n \in \mathbb{N}\}$ or $f(\mathbb{Z}) = \{f(n) \mid n \in \mathbb{Z}\}$ where f denotes a non-constant polynomial, we begin with two general results. The first proposition is obvious:

Proposition 7. *Let $f(X)$ be a non-constant polynomial with coefficients in $\mathbb{Z}$ such that $f(\mathbb{N})$ (resp. $f(\mathbb{Z})$) admits a simultaneous ordering $\{f(a_n)\}_{n\in\mathbb{N}}$. Let*

$$g(X) = \alpha(f(\varepsilon(X - \lambda)) + \gamma \quad \textit{where } \alpha, \gamma \in \mathbb{Z}, \varepsilon = 1, \lambda \in \mathbb{N}$$
$$(\textit{resp. } \varepsilon \in \{\pm 1\}, \lambda \in \mathbb{Z}).$$

Then the sequence $\{\varepsilon(a_n+\lambda)\}_{n\in\mathbb{N}}$ *is a simultaneous ordering for* $g(\mathbb{N})$ (*respectively,* $g(\mathbb{Z})$).

Proposition 8. *Let* $f(X)\in\mathbb{Z}[X]$ *be a non-constant polynomial such that the subset* $f(\mathbb{N})$ *admits a simultaneous ordering* $\{f(a_n)\}_{n\in\mathbb{N}}$ *where the* a_n*'s are in* $\mathbb{N}$. *Then there exists an integer* m *such that, for* $n\geq m$, $a_{n+1}=1+a_n$.

Proof. We may assume that the leading coefficient of f is positive. Then, there exists $n_1\geq a_0$ such that f is strictly increasing on the interval $[n_1,+\infty[$ and $f(n_1)$ is the maximum value of f on $[0,n_1]$.

Let $l>0$ be the least integer such that $a_l>n_1$: all the elements $a_0,\ldots,a_{l-1}$ are $\leq n_1$. As $\prod_{k=0}^{l-1}(f(a_l)-f(a_k))$ divides $\prod_{k=0}^{l-1}(f(x)-f(a_k))$ for every $x>n_1$, as all the factors in both products are strictly positive and as f is increasing on $[n_1,+\infty[$, necessarily a_l, which is the least possible, is equal to n_1+1.

Let us consider a_{l+1}. Either $a_{l+1}<n_1$, or $a_{l+1}>n_1$. Asume that $a_{l+1}>n_1$, and hence, that $a_{l+1}>a_l=n_1+1$. The previous argument shows that $a_{l+1}=a_l+1$. And so on ... If $a_{l+s}>n_1$, then $a_{l+s}=1+\max\{a_l,a_{l+1},\ldots,a_{l+s-1}\}$.

As there are at most finitely many elements a_k's between 0 and n_1, there is some integer $m\geq l$ such that $a_n>n_1$ for every $n\geq m$. Consequently, for every $n\geq m$, one has: $a_{n+1}=1+a_n$. □

Remark 9.

1. Obviously, if m satisfies the condition in Proposition 8, then

$$n\geq m \;\Rightarrow\; a_n=a_m+n-m,$$

$$k<m<n<n' \;\Rightarrow\; a_k<a_m<a_n<a_{n'}.$$

2. The previous proof still holds if we replace the polynomial function f by any function $f:\mathbb{N}\to\mathbb{Z}$ such that f is ultimately strictly increasing.

3. Simultaneous Orderings for $\{n^r \mid n\in\mathbb{N}\}$ and $\{n^r \mid n\in\mathbb{Z}\}$

In the introduction we recalled that, for $r=1$ or $r=2$, the set $\{n^r \mid n\in\mathbb{N}\}$ admits a simultaneous ordering. In this section, we prove that this is no more true for $r\geq 3$.

Proposition 10. *The set* $\{n^r \mid n\geq 0\}$ *admits an infinite simultaneous ordering if and only if* $r=1$ *or* $r=2$.

Proof. Let $r \geq 2$. Assume that $S_r = \{n^r \mid n \geq 0\}$ admits a simultaneous ordering $\{a_n\}_{n\geq 0}$. Since $a_1 - a_0$ divides all the differences $x_1 - x_0$ for $x_0, x_1 \in S_r$, we necessarily have

$$\{a_0, a_1\} = \{0, 1\}.$$

Moreover, since for every $n \geq 2$, $\prod_{k=0}^{n-1}(a_n - a_k)$ divides $\prod_{k=0}^{n-1}(m^r - a_k)$ for all $m \geq a_n$, the sequence a_k is strictly increasing and

$$a_k = k^r \quad \text{for } k \geq 2.$$

Consequently, $2^r(2^r - 1)$ divides $m^r(m^r - 1)$ for every $m \geq 0$.

Assume now that $r \geq 3$. We know that the unit group of $\mathbb{Z}/2^r\mathbb{Z}$ is :

$$(\mathbb{Z}/2^r\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{r-2}\mathbb{Z}).$$

Thus, there exists an odd integer m whose class in $(\mathbb{Z}/2^r\mathbb{Z})^\times$ is of order 2^{r-2}. Since 2^r divides $m^r - 1$, 2^{r-2} divides r. Then, necessarily, $r = 4$. Since, the first terms of the sequence are $0, 1, 2, 3$ or $1, 0, 2, 3$, $3^4(3^4 - 1)(3^4 - 2^4)$ has to divide $4^4(4^4 - 1)(4^4 - 2^4)$. But, it does not. □

Remark 11.

1. The previous proof shows that a simultaneous ordering of $\{n^r \mid n \in \mathbb{N}\}$ has at most 3 terms if $r = 3$ or $r \geq 5$, and 4 terms if $r = 4$.

2. A simultaneous ordering of $\{n^2 \mid n \in \mathbb{N}\}$ is necessarily the sequence $\{n\}_{n\geq 0}$, except for the first two terms, which may be 1 and 0 instead of 0 and 1. It is then a natural question to ask whether the subset $\{n^2 \mid n \in \mathbb{N}^*\}$ admits also a simultaneous ordering. Strangely, it does not: $a_1^2 - a_0^2$ would divide $x^2 - y^2$ for all $x, y \in \mathbb{N}^*$, and then must be 1, and no such pair (a_0, a_1) exists.

Proposition 12. *The set $\{n^{2s+1} \mid n \in \mathbb{Z}\}$ with $s \geq 1$ does not admit any infinite simultaneous ordering.*

Proof. Let $s \geq 1$ and assume that $\{n^{2s+1} \mid n \in \mathbb{Z}\}$ admits a simultaneous ordering $\{a_n\}_{n\geq 0}$. Analogously to the previous proof, we necessarily have:

$$\{a_0, a_1, a_2\} = \{0, 1, -1\}.$$

Moreover, since $\prod_{k=0}^{2}(a_3 - a_k)$ divides $\prod_{k=0}^{2}(m^r - a_k)$ for all $m \in \mathbb{Z}$, we necessarily have $a_3 \in \{\pm 2\}$. Consequently, for every $m \in \mathbb{Z}$:

$$2^{2s+1}(2^{2s+1} - 1)(2^{2s+1} + 1) \mid m^{2s+1}(m^{2s+1} - 1)(m^{2s+1} + 1).$$

In particular, if m is odd:

$$2^{2s+1} \mid m^{2(2s+1)} - 1.$$

If we choose for m an odd integer whose class in $(\mathbb{Z}/2^{2s+1}\mathbb{Z})^\times$ is of order 2^{2s-1}, we then see that 2^{2s-1} divides $2(2s+1)$. This is impossible unless $s = 1$.

Let us look at the case $2s + 1 = 3$. We first check that $7 \times 8 \times 9$ divides $m^3(m^3 - 1)(m^3 + 1)$ for every $m \in \mathbb{Z}$, that is, $a_3 = \pm 2$ is the fourth term of a simultaneous ordering. Then, necessarily $a_4 = \mp 2$, but:

$$2^3(2^3 - 1)(2^3 + 1)(2^3 + 2^3) \nmid 3^3(3^3 - 1)(3^3 + 1)(3^3 + 2^3).$$

□

Remark 13. The previous proof shows that a simultaneous ordering of $\{n^{2s+1} \mid n \in \mathbb{Z}\}$ has at most 4 terms if $2s + 1 = 3$, and 3 terms if $2s + 1 \geq 5$.

4. The Range on $\mathbb{N}$ of Polynomials of Degree 2

Theorem 14. *Let $f \in \mathrm{Int}(\mathbb{Z}) = \{g \in \mathbb{Q}[X] \mid g(\mathbb{Z}) \subseteq \mathbb{Z}\}$ be a polynomial of degree 2. Then, the subset $f(\mathbb{N})$ admits a simultaneous ordering if and only if f is of one of the forms:*

$$\alpha X(X - 2\lambda) + \beta \quad \text{or} \quad \alpha \frac{X(X - 1 - 2\lambda)}{2} + \beta \quad \text{where } \alpha, \beta \in \mathbb{Z}, \lambda \in \mathbb{N}.$$

Proof. Assume that $f \in \mathrm{Int}(\mathbb{Z})$ has degree 2 and that $f(\mathbb{N})$ admits a simultaneous ordering. Then, $2f = aX^2 + bX + c$ belongs to $\mathbb{Z}[X]$ and has the same property. Of course, the polynomial $aX^2 + bX$ has the same property. Moreover, one may divide $aX^2 + bX$ by the g.c.d. of a and b, and hence, one may assume that a and b are relatively prime and also that $a > 0$. Thus, consider $g(X) = aX^2 + bX \in \mathbb{Z}[X]$ with $a > 0$ and a and b relatively prime, such that $g(\mathbb{N})$ admits a simultaneous ordering $\{g(a_n)\}_{n \geq 0}$.

Consider the subset $T = \{a_n \mid n \geq 0\}$. If $T \neq \mathbb{N}$, Lemma 15 below implies that $a = 1$ and $b < 0$, that is, $g(X)$ is of the form $X(X - 2\lambda)$ or $X(X - (2\lambda - 1))$ where $\lambda > 0$. Replacing X by $X + \lambda$, we are led to consider $(X + \lambda)(X - \lambda) = X^2 - \lambda^2$ or $(X + \lambda)(X - \lambda - 1) = X(X - 1) - \lambda(\lambda + 1)$. Now, with a translation on the values, we are led to consider X^2 or $X(X - 1)$. They are Examples 5. Consequently, when $T \neq \mathbb{N}$, f is of one of the given forms with $\lambda > 0$.

Assume now that $T = \mathbb{N}$. Then, Lemma 16 below implies that $a = 1$ and $b \leq 1$. If $b < 0$, we are led to the previous forms. If $b = 0$ or 1, then f is of the forms given in the theorem with $\lambda = 0$. □

Lemma 15. *Let $f = aX^2 + bX \in \mathbb{Z}[X]$ with $a > 0$ and a and b relatively prime. Assume that the subset $f(\mathbb{N})$ admits a simultaneous ordering $\{f(a_n)\}_{n\geq 0}$ where $a_n \in \mathbb{N}$ and consider the subset $T = \{a_n \mid n \in \mathbb{N}\}$. If $T \neq \mathbb{N}$, then $a = 1$ and $b < 0$.*

Proof. It follows from Proposition 8 that there exists m such that:

$$n \geq m \;\Rightarrow\; a_n = n - m + a_m.$$

Consequently, there exists a greatest integer r such that $r - 1 \notin T$. The hypothesis $T \neq \mathbb{N}$ means that $r \geq 1$. For every $n > m$, let

$$T_n = \{a_k \mid 0 \leq k < n\} = \{t \in T \mid t \leq a_{n-1}\}.$$

By definition of a simultaneous ordering,

$$\forall n \in \mathbb{N}^* \; \forall x \in S \quad \prod_{k=0}^{n-1}(f(a_n) - f(a_k)) \quad \text{divides} \quad \prod_{k=0}^{n-1}(x - f(a_k)).$$

In particular, for $x = f(a_{n+1})$:

$$\prod_{k=0}^{n-1}(f(a_n) - f(a_k)) \quad \text{divides} \quad \prod_{k=0}^{n-1}(f(a_{n+1}) - f(a_k)). \tag{$*$}$$

Taking into account the form of f, we have:

$$\forall x, y \in \mathbb{Z} \quad f(x) - f(y) = (x - y)(a(x + y) + b).$$

Consequently, (*) is equivalent to

$$\prod_{k=0}^{n-1} \frac{a_{n+1} - a_k}{a_n - a_k} \times \prod_{k=0}^{n-1} \frac{a(a_{n+1} + a_k) + b}{a(a_n + a_k) + b} \in \mathbb{Z},$$

which may be written

$$\prod_{t\in T_n} \frac{a_{n+1} - t}{a_n - t} \times \prod_{t\in T_n} \frac{a(a_{n+1} + t) + b}{a(a_n + t) + b} \in \mathbb{Z}.$$

Note that, for $n > m$, one has

$$\prod_{t\in T_n} \frac{a_{n+1} - t}{a_n - t} = \prod_{t\in T_n, t\leq r-2} \frac{a_n + 1 - t}{a_n - t} \times \prod_{r\leq t\leq a_{n-1}} \frac{a_n - (t - 1)}{a_n - t}$$

and

$$\prod_{r\le t\le a_n-1}\frac{a_n-(t-1)}{a_n-t}=a_n-r+1.$$

Similarly,

$$\prod_{t\in T_n}\frac{a(a_{n+1}+t)+b}{a(a_n+t)+b}=\prod_{t\in T_n,t\le r-2}\frac{a(a_n+1+t)+b}{a(a_n+t)+b}\times\prod_{r\le t\le a_{n-1}}\frac{a(a_n+1+t)+b}{a(a_n+t)+b}$$

and

$$\prod_{r\le t\le a_{n-1}}\frac{a(a_n+t+1)+b}{a(a_n+t)+b}=\frac{2aa_n+b}{a(a_n+r)+b}.$$

Consequently, if (*) is satisfied, then $a(a_n+r)+b$ divides:

$$(a_n-r+1)\times(2aa_n+b)\times\prod_{t\in T_n,\,t\le r-2}(a_n+1-t)\times\prod_{t\in T_n,\,t\le r-2}(a(a_n+1+t)+b).$$

For $n>m$, $a(a_n+r)+b=an+c$ where $c=a(a_m+r-m)+b$ and a and c are relatively prime. Hence, by Dirichlet's theorem, one may choose n as large as we want such that $a(a_n+r)+b$ is a prime number.

From now on, we fix such an n with $a_n>2|b|+3r$. Then, $\pi=a(a_n+r)+b$ being prime must divide at least one of the factors of the above product, and clearly, it does not divide a_n-r+1. We consider three cases: the first one is impossible, the two others imply the announced conclusion.

1. For $t\le r-2$, $a(a_n+1+t)+b<a(a_n+r)+b=\pi$, and hence, π does not divide the product $\prod_{t\in T_n,\,t\le r-2}(a(a_n+1+t)+b)$.
2. If π divides $2aa_n+b$, then it divides the difference $2\pi-(2aa_n+b)=2ar+b$. Since a_n is choosen large enough such that $\pi>|2ar+b|$, if π divides $2aa_n+b$, one has $2ar+b=0$. And, $r=-b/2a$ implies $b<0$ and $a=1$ (since $r\ge1$ and $(a,b)=1$).
3. Finally, $\pi-(a_n+1-t)=(a-1)a_n+ar+b-1+t>(a-1)a_n+b$ (since $r\ge1$ and, if $t=0$, then $r\ge2$) and this last number is ≥0 if $a\ge2$ or if $b\ge0$. Thus, if π divides the product $\prod_{t\in T_n,\,t\le r}(a_n+1-t)$, necessarily $a=1$ and $b<0$. .

□

Lemma 16. *Let $f=aX^2+bX\in\mathbb{Z}[X]$ with $a>0$, and a and b relatively prime. Assume that the subset $f(\mathbb{N})$ admits a simultaneous ordering $\{f(a_n)\}_{n\ge0}$ and that $T=\{a_n\mid n\ge0\}=\mathbb{N}$. Then, $a=1$ and $b\le1$.*

Proof. We may assume that $b \neq 0$. It follows from Proposition 8 that there exists an integer m such that, for $n \geq m$, we have $a_n = n - m + a_m$. Then, for every $n \geq m$, we have $a_n = n$, since $T = \mathbb{N}$.

Moreover, since $T = \mathbb{N}$, the integer r that we introduced in the proof of Lemma 15 is equal to 0. Thus, the divisibility condition (*) reduces to:

$$an + b \text{ divides } (n+1) \times (2an + b).$$

One may choose $n > 2|b|$ such that $an + b$ is prime. Since $an + b$ does not divide $2an + b$, $an + b$ has to divide $n + 1$, and hence, to be $\leq n + 1$. Then, necessarily, $a = 1$ and $b \leq 1$. □

5. The Range on $\mathbb{Z}$ of Polynomials of Degree 2

Theorem 17. *Let $f \in \mathrm{Int}(\mathbb{Z}) = \{g \in \mathbb{Q}[X] \mid g(\mathbb{Z}) \subseteq \mathbb{Z}\}$ be a polynomial of degree 2. Then, the subset $f(\mathbb{Z})$ admits a simultaneous ordering if and only if f is of one of the forms:*

$$\alpha X(X - 2\lambda) + \beta,\ \alpha\frac{X(X-1-2\lambda)}{2} + \beta \text{ or } \alpha X(2X - 1 - 2\lambda) + \beta \text{ where } \alpha, \beta, \lambda \in \mathbb{Z}.$$

Proof. Let $f(X) = aX^2 + bX + c$ with $a \neq 0$. As previously seen, we may assume that $a, b, c \in \mathbb{Z}$. Write:

$$a = \alpha d,\ b = -\varepsilon\alpha e \text{ with } d > 0,\ e \geq 0,\ \varepsilon \in \{\pm 1\} \text{ and } (d, e) = 1.$$

Let

$$e = 2dq + r \text{ with } 0 \leq r < 2d.$$

If $Y = \varepsilon X - q$, then

$$aX^2 + bX + c = \alpha(dY^2 - rY) + \beta \text{ for some } \beta \in \mathbb{Z}.$$

It follows from Proposition 7 that it is enough to restrict our study to polynomials of the form

$$f(X) = aX^2 - bX \quad \text{with} \quad a \geq 1, 0 \leq b < 2a \text{ and } (a, b) = 1.$$

If $a = 1$, then $b = 0$ or 1, $f(X) = X^2$ or $X(X - 1)$, $f(\mathbb{Z}) = f(\mathbb{N})$ and we saw that the corresponding subsets have simultaneous orderings. This case corresponds to the first and the second types of polynomials given in the theorem.

Consequently, from now on, we assume that $a \geq 2$ and $b \geq 1$. Then, $b/a \notin \mathbb{Z}$, and hence, f is injective on $\mathbb{Z}$ since:

$$f(x) - f(y) = (x - y)(a(x + y) - b).$$

Assume that $f(\mathbb{Z})$ admits a simultaneous ordering $\{f(a_n)\}_{n\in\mathbb{N}}$. It follows from the fact that $0 < b < 2a$ and from the minimality of $|f(a_0) - f(a_1)|$ that $\{a_0, a_1\} = \{0, 1\}$. Consequently,

$$f(1) - f(0) = a - b \text{ divides } f(-1) - f(0) = a + b.$$

As a consequence, $a - b$ divides $2b$ and so, since $(a, b) = 1$, $a - b$ divides 2..

Assume first that $0 < b < a$. Then $a_2 = -1$ and, more generally, $a_{2n} = -n$, while $a_3 = 2$ and, more generally, $a_{2n+1} = n + 1$. Then,

$$(f(-1) - f(0))(f(-1) - f(1)) = 2(a + b)b = 2(ab + b^2)$$

divides

$$(f(2) - f(0))(f(2) - f(1)) = 2(2a - b)(3a - b) = 2(6a^2 - 5ab + b^2).$$

Equivalently,

$$b(a + b) \quad \text{divides} \quad 6a(a - b).$$

Consequently,

$$b(a + b) \quad \text{divides} \quad 12.$$

With $a - b|2$ and $0 < b < a$, that is, $b = a - 1$ or $b = a - 2$, necessarily, $a = 2$ or 3 and $b = 1$.

The case $a = 3$ and $b = 1$ does not work since

$$\prod_{k=0}^{2}(f(2) - f(a_k)) \nmid \prod_{k=0}^{2}(f(-2) - f(a_k)).$$

On the other hand, $a = 2$ and $b = 1$; that is, $f(X) = 2X^2 - X$ works, since $f(\mathbb{Z}) = g(\mathbb{Z}) = g(\mathbb{N})$ where $g(Y) = \frac{1}{2}Y(Y - 1)$.

Assume now that $a < b < 2a$. Then, $a_2 = 2$, $a_3 = -1$ and, more generally, $a_{2n} = n + 1$ and $a_{2n+1} = -n$. Then, conversely,

$$6a^2 - 5ab + b^2 \quad \text{divides} \quad b(a + b).$$

Consequently,

$$6a^2 - 5ab + b^2 \quad \text{divides} \quad 6a(b - a),$$

and analogously,

$$6a^2 - 5ab + b^2 \quad \text{divides} \quad 12.$$

With $(a-b)|2$ and $a < b < 2a$, that is $b = a+1$ or $b = a+2$, necessarily, either $a = 2$ and $b = 3$, or $a = 3$ and $b = 5$.

The case $a = 3$ and $b = 5$ does not work since

$$\prod_{k=0}^{2}(f(-1) - f(a_k)) \nmid \prod_{k=0}^{2}(f(3) - f(a_k)).$$

On the other hand, if $a = 2$ and $b = 3$, the polynomial $f(X) = 2X^2 - 3X$ works (consider the translation $X \to X - 1$). □

6. Orbits Under the Action of a Polynomial

We end this paper with a surprising example which could be considered as a generalization of Example 5.1.

Proposition 18. *Consider the discrete dynamical system $(\mathbb{Z}, f)$ formed by the set $\mathbb{Z}$ and a non-constant polynomial $f \in \mathbb{Z}[X]$. Then, for every $x \in \mathbb{Z}$, the orbit of x under the action of f, that is,*

$$\Omega_f(x) = \{f^n(x) \mid n \geq 0\},$$

where f^n denotes the n-th iterate of f, admits a simultaneous ordering, namely, the sequence $\{f^n(x)\}_{n\geq 0}$.

In other words, for every $x \in \mathbb{Z}$ and for all $m, n \in \mathbb{N}$ with $m \geq n \geq 1$:

$$\prod_{j=0}^{n-1}(f^n(x) - f^j(x)) \text{ divides } \prod_{j=0}^{n-1}(f^m(x) - f^j(x)).$$

Note that this is equivalent to the fact that the following rational function

$$\prod_{j=0}^{n-1}\frac{f^m(X) - f^j(X)}{f^n(X) - f^j(X)}$$

belongs to $\mathrm{Int}(\mathbb{Z})$ since a rational function $\varphi \in \mathbb{Q}(X)$ such that $\varphi(x) \in \mathbb{Z}$ for infinitely many $x \in \mathbb{Z}$ is necessarily an integer-valued polynomial [4, Prop. X.1.1].

We remark also that this assertion is already known when $\deg(f) = 1$ since the rational function $\prod_{j=0}^{n-1}\frac{f^m(X)-f^j(X)}{f^n(X)-f^j(X)}$ is an integer equal to $\binom{m}{n}$ if $f(X) = X + b$ with $b \neq 0$ and to $\prod_{j=0}^{n-1}\frac{a^m-a^j}{a^n-a^j}$ if $f(X) = ax + b$ with $a \neq 1$.

In fact, Proposition 18 is an obvious consequence of Proposition 19 below which says that the coefficients of the previous integer-valued polynomial are in $\mathbb{Z}$.

Proposition 19. *For every $f \in \mathbb{Z}[X]$ and for all $m, n \in \mathbb{N}$ such that $m \geq n \geq 1$:*

$$\prod_{j=0}^{n-1}(f^n(X) - f^j(X)) \text{ divides } \prod_{j=0}^{n-1}(f^m(X) - f^j(X)) \text{ in } \mathbb{Z}[X].$$

For the proof of Proposition 19 we may assume that $\deg(f) \geq 2$. The proposition is then a consequence, obtained by specialization, of the still more general following result:

Proposition 20. *Let $G(X) = t_d X^d + \cdots + t_0 \in \mathbb{Z}[t_d, \cdots, t_0][X]$ where $d \geq 2$. Then, for $m > n \geq 1$,*

$$\prod_{j=0}^{n-1}(G^n(X) - G^j(X)) \text{ divides } \prod_{j=0}^{n-1}(G^m(X) - G^j(X)) \text{ in } \mathbb{Z}[t_d, t_{d-1}, \cdots, t_0, X].$$

Although not explicitely stated, we may find in Bézivin's paper [1] all the elements for the proof of Proposition 20. We recall them below in order to give a self-contained proof and begin with a technical lemma:

Lemma 21. *Let $g \in \mathbb{Z}[X]$ and $n \in \mathbb{N}$ be such that, for every $j < n$, the polynomial $g^j(X) - X$ has only simple roots. Then,*

1. *For every $z \in \mathbb{C}$ and every $j < n$ such that $g^n(z) = g^j(z)$, the multiplicity of the root z in $g^n(X) - g^j(X)$ is equal to the multiplicity of z in $g^j(X) - g^j(z)$.*
2. *For every $m \geq n$:*

$$\prod_{j=0}^{n-1}(g^n(X) - g^j(X)) \text{ divides } \prod_{j=0}^{n-1}(g^m(X) - g^j(X)) \text{ in } \mathbb{Q}[X].$$

Proof. (See the proof of [1, Lemma 2.6]) Assume that $j < n$ is such that $g^n(z) = g^j(z)$ and let $h(X) = g^{n-j}(X) - X$. Then, $g^j(z)$ is a simple root of h. Thus,

$$g^n(X) - g^j(X) = h(g^j(X)) = (g^j(X) - g^j(z))l(g^j(X)) \text{ where } l(g^j(z)) \neq 0.$$

This is the first assertion.

Let us prove the second assertion. Let z be any element of $\mathbb{C}$ such that $g^j(z) = g^n(z)$ for some $j < n$. Then, z is a preperiodic point for g with a least period l.

Write $n = lr + n_0$ with $0 \leq n_0 < l$ and $m = ls + m_0$ with $0 \leq m_0 < l$. Clearly, the exponents $j < n$ such that $g^j(z) = g^n(z)$ (resp. $g^j(z) = g^m(z)$) are of the form $j = lh + n_0$ (resp. $j = lh + m_0$) with $0 \leq h < r$ (resp. $0 \leq h < r$ if $n_0 \leq m_0$ and $0 \leq h \leq r$ if $m_0 < n_0$). Consequently, to each $j = lh + n_0$ such that $g^j(z) = g^n(z)$ corresponds some $j' = lh + m_0$ if $n_0 \leq m_0$ and $j' = l(h+1) + m_0$ else which is such that $g^{j'}(z) = g^m(z)$ and $j \leq j'$. The second assertion follows then from the first one and the fact that the multiplicity of z in $f^j(X) - f^j(z)$ is clearly an increasing function of j. □

Proof. of Proposition 20. Note first that, for every $i > 0$, the discriminant $\Delta_j(t_d, \ldots, t_0)$ of the polynomial $G^j(X) - X$ is a polynomial function which is not identically zero [1, Lemma 2.7]. Clearly, it is enough to give, for each degree d, an example of a polynomial $g(X) \in \mathbb{Z}[X]$ such that, for each $j > 0$, $g^j(X) - X$ has only simple roots. For instance, for $d \geq 2$, we may choose $g(X) = (X+1)^d - 1$ (cf. [1]) since $g^j(X) - X = (X+1)^{d^j} - X$.

Let us prove now the proposition. Fix $m > n \geq 1$ and put

$$N = \prod_{j=0}^{n-1} (G^n(X) - G^j(X)) \text{ and } M = \prod_{j=0}^{n-1} (G^m(X) - G^j(X)).$$

Since the leading coefficient of N is a power of t_d, there is an integer γ such that:

$$t_d^\gamma M = HN + R \text{ with } \deg_X R < \deg_X N \text{ and } H, R \in \mathbb{Z}[t_d, \ldots, t_0][X].$$

It follows from Lemma 21(2) that $R(y_d, \ldots, y_0) = 0$ for all $(y_d, \ldots, y_0) \in \mathbb{C}^{d+1}$ such that $\prod_{j=0}^{n-1} \Delta_j(y_d, \ldots, y_0) \neq 0$. Since the interior of a hypersurface of $\mathbb{C}^{d+1}$ is empty, we have $R = 0$, and hence, $t_d^\gamma M = HN$.

Considered as polynomials in X with coefficients in the unique factorization domain $\mathbb{Z}[t_d, \ldots, t_0]$, M and N have a content equal to 1 since the leading coefficient of $G^j(X) - G^i(X)$, for $i \neq j$, is a power of t_d while the constant term is prime to t_d. Thus, by Gauss' lemma, t_d^γ divides the coefficients of H, and Proposition 20 is proved. □

Application. Proposition 18 applied to the orbit of the integer 3 under the iteration of the polynomial $f(X) = X^2 - 2X + 2$ shows that the set

$$\{F_n = 2^{2^n} + 1 \mid n \geq 0\}$$

formed by the Fermat numbers has a simultaneous ordering.

Acknowledgments The authors express their gratitude to the Princess of Cleves for her unfailing support and to Pr. Keith Johnson for his very relevant remarks.

References

[1] J.-P. Bézivin, Itération de polynômes et fonctions entières arithmétiques, *Acta Arith.*, **68.1** (1994), 11-25.

[2] M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. reine angew. Math.*, **490** (1997), 101-127.

[3] M. Bhargava, The factorial function and generalizations, *Amer. Math. Monthly*, **107** (2000), 783-799.

[4] P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials*, Amer. Math. Soc. Surveys and Monographs **48**, Providence, R.I., 1997.

[5] P.-J. Cahen and J.-L. Chabert, Old Problems and New Questions around Integer-Valued Polynomials and Factorial Sequences, in *MultiplicativeIdeal Theory in Commutative Algebra*, Springer 2006, 89-108.

[6] J.-L. Chabert, Une caractérisation des polynômes prenant des valeurs entières sur tous les nombres premiers, *Canad. Math. Bull.*, **39** (1996), 402-407.

[7] J.-L. Chabert, Generalized factorial ideals, *The Arabian Journal for Science and Engineering* **26** (2001), 51-68.

[8] J.-L. Chabert, Autour de l'algèbre des polynômes dans un corps de nombres ou un corps de fonctions, Cours de Master 2, Amiens, Spring 2006.

[9] J.-L. Chabert, A generalization of an Erdös inequality connected to $n!$, *Aequationes Math.* **77** (2009) 243-258.

[10] J.-L. Chabert, S. Chapman and W. Smith, A Basis for the Ring of Polynomials Integer-Valued on Prime Numbers, in *Factorization in integral domains*, 271-284, Lect. Notes Pure Appl. Math., **189**, Dekker, New York, 1997.

[11] Y. Fares, Factorial preservation, *Arch. Math.* **83** (2004), 497-506.