Some arithmetic properties of order-sequences of algebraic curves

Arnaldo Garcia

Instituto de Matemática Pura e Aplicada, Estrada D. Castorina, 110 J. Botânico, 22460 Rio de Janeiro, Brazil

Communicated by C.A. Weibel
Received 13 July 1991
Revised 28 June 1992

Abstract


We give a short proof of a theorem of M. Homma on order-sequences of linear systems on curves. We characterize the order-sequences on curves having the 'maximal' number of Weierstrass points. We also give an inequality on order-sequences at Weierstrass points on canonical curves.

1. Introduction

Let \( X \) be a smooth projective curve embedded in the projective space of dimension \( N \) and let \( \mathcal{L} \) be the linear system of hyperplane sections on \( X \). To every point \( P \in X \) one can associate a sequence of natural numbers \( \epsilon_0(P) < \epsilon_1(P) < \cdots < \epsilon_N(P) \) that describes the possible intersection multiplicities at \( P \) of the curve with hyperplanes of \( \mathbb{P}^N \). For all but finitely many points \( P \) on the curve \( X \) this sequence is the same. We denote this generic sequence by \( \epsilon_0 < \epsilon_1 < \cdots < \epsilon_N \) and we call it the order-sequence of the linear system \( \mathcal{L} \). The finitely many points \( P \) having a sequence \( \epsilon_0(P) < \epsilon_1(P) < \cdots < \epsilon_N(P) \) different from the generic one are called the Weierstrass points of \( \mathcal{L} \).

If the characteristic of the base field, which we assume to be algebraically closed, is zero, then \( \epsilon_i = i \) for \( i = 0, 1, \ldots, N \). In prime characteristics, however, the order-sequence of a linear system is an important invariant having connections...
with the number of rational points on curves over finite fields, the inseparability
degrees of generalized Gauss maps, duality theory for curves, the theory of
Strange curves, etc.

The theory of Weierstrass points in prime characteristic was initiated by
Schmidt in [9] (see also [7], [8] and [11]). A basic result is that there is a positive
divisor having as support exactly the Weierstrass points on the curve; the degree
of this divisor being

\[(g - 2) + (N + 1)d.\]

Here \(g\) means the genus, \(d\) is the degree of a linear system and \(\varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N\)
its order-sequence. The importance of the order-sequence on the extrinsic
geometry of the curve has been investigated by several authors (e.g., see [2], [3],
[4] and [6]).

In order to have a curve and a linear system on the curve with no Weierstrass
points (i.e., the degree of the divisor above equal to zero), one must have \(g = 0\)
and \(2 \sum \varepsilon_j = (N + 1)d\). Since we have the inequalities

\[\varepsilon_j + \varepsilon_{N-j} \leq \varepsilon_N, \text{ for all } j.\quad (1)\]

it follows that one must have \(g = 0\), \(d = \varepsilon_N\) and the equalities

\[\varepsilon_j + \varepsilon_{N-j} = \varepsilon_N, \text{ for all } j.\quad (2)\]

Both the inequalities (1) and their application as above appeared first in a
recent paper of Homma [5]. In Section 3, we give a simpler and much shorter
proof of the inequalities (1). (See also [1] for a geometrical proof and an
interesting generalization.)

It is also clear from above that

\[\left(\sum_{i=0}^{N} \varepsilon_i\right)(2g - 2) + (N + 1)d \leq (N + 1)[\varepsilon_N(g - 1) + d]\]

and that equality occurs if and only if we have the equalities in (2). In Section 4,
we discuss the equalities above when the sequence \(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_N\) is such that the
non-gaps constitute a semigroup. For such sequences, we show that the equalities
above hold if and only if there exist a power \(q\) of the characteristic and an integer
\(r \geq 2\) such that

\[\{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_N\} = \{e \in \mathbb{N} \mid e \leq rq \text{ and } e \neq 1 \mod q\}.\]

Section 5 deals with semigroup-sequences; i.e., sequences having a semigroup
of non-gaps. We do not assume in this section that the sequence \(\varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N\)
is the order-sequence of a linear system and hence the results here hold also at Weierstrass points on canonical curves, even in characteristic zero. We show that if \( \varepsilon_k > \varepsilon_{k-1} + 1 \), then we have \( \varepsilon_{k} \leq \varepsilon_{k} + \varepsilon_{k-d(k)} \), where \( d(k) = (\varepsilon_k - k) \).

Finally, in Section 6, we show that if \( S_1 = \{ \varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N \} \) and \( S_2 = \{ \mu_0 < \mu_1 < \cdots < \mu_M \} \) are sequences satisfying the \( p \)-adic criterion (see definition below), then their sum

\[
S_1 + S_2 = \{ \varepsilon_i + \mu_j \mid \varepsilon_i \in S_1 \text{ and } \mu_j \in S_2 \}
\]

also satisfies the \( p \)-adic criterion.

2. Semigroup-sequences and order-sequences

Given a sequence of natural numbers \( 0 = \varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N \), we call gaps the elements of the following set:

\[
G = \{ (\varepsilon_0 + 1), (\varepsilon_1 + 1), (\varepsilon_2 + 1), \ldots, (\varepsilon_N + 1) \}.
\]

The non-gaps are then the elements of the complementary set \( \mathbb{N} \setminus G \). The given sequence will be called a \textit{semigroup-sequence} if the set of non-gaps is a semigroup (i.e. closed under addition).

For a divisor \( D \) on a non-singular projective curve \( X \) over an algebraically closed field \( K \), let \( \varepsilon(D, P) \) denote the order of \( D \) at the point \( P \) on \( X \). For a linear system \( \mathcal{L} \) of \( X \) of projective dimension \( N \) and for a point \( P \in X \), let \( \varepsilon_0(P) < \varepsilon_1(P) < \cdots < \varepsilon_N(P) \) be the \( (N+1) \) different orders at \( P \) as \( D \) runs through all divisors in \( \mathcal{L} \); i.e.,

\[
\{ \varepsilon_0(P) < \varepsilon_1(P) < \cdots < \varepsilon_N(P) \} = \{ \varepsilon(D, P) \mid D \in \mathcal{L} \}.
\]

The sequence \( \varepsilon_0(P) < \varepsilon_1(P) < \cdots < \varepsilon_N(P) \) is called the \textit{order-sequence at the point} \( P \) for the linear system. It is well-known that the order-sequences of \( \mathcal{L} \) at distinct points on \( X \) all coincide, except for finitely many points (called the \( \mathcal{L} \)-Weierstrass points on \( X \)). The generic order-sequence is then called the \textit{order-sequence of} \( \mathcal{L} \) and denoted by \( \varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N \).

If \( \text{char}(K) = 0 \), then \( \varepsilon_j = j \) for all \( j \). We have that the order-sequence \( \varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N \) of a linear system satisfies the following \( p \)-adic criterion (see [9] and [11]), \( p \) being the characteristic.

\textit{p-adic criterion}. If \( \mu \) is a natural number and \( (\mu) \not\equiv 0 \pmod{p} \), for some \( 0 \leq l \leq N \), then \( \mu = \varepsilon_j \) for some \( j \).

\textbf{Remark 1}. The \( p \)-adic criterion is actually sufficient to ensure that a given sequence of numbers \( \varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N \) is an order-sequence of a linear system.
This can be seen easily by considering the rational space curve given by 
\((1 : t^1 : t^2 : \cdots : t^n)\) (see Remark after Proposition 1.6 in [11] and also [10, Satz 7]).

**Remark 2.** If every order \(\varepsilon_j, 0 \leq j \leq N\), is a multiple of the characteristic \(p\) then, by factoring out the highest possible power \(q\) of \(p\) from the order-sequence, we obtain a new order-sequence with some order not a multiple of \(p\). By the \(p\)-adic criterion, we have that \(\varepsilon_i = 1\) in this new order-sequence. Hence \(\varepsilon_i = q\) in the original one and, moreover, every order is a multiple of \(q\). This power \(q\) is the inseparable degree of the morphism corresponding to the associated base-point-free linear system.

**Remark 3.** For two natural numbers \(a\) and \(b\), we write (for some \(m\))
\[
a = a_0 + a_1 p + a_2 p^2 + \cdots + a_m p^m, \\
b = b_0 + b_1 p + b_2 p^2 + \cdots + b_m p^m,
\]
with \(0 \leq a_j, b_j < p\).

It is not hard to see that
\[
\binom{a}{b} \not\equiv 0 \pmod{p} \quad \text{if and only if} \quad a_i \geq b_i, \quad \forall i.
\]
One can find a proof, e.g., in [10, Hilfssatz 3].

### 3. The inequalities \(\varepsilon_j + \varepsilon_{N-j} \leq \varepsilon_N\)

**Theorem 4.** Let \(\mathcal{I}\) be a linear system of projective dimension \(N\) on a smooth projective curve and let \(\varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N\) be its order-sequence. Then
\[
\varepsilon_j + \varepsilon_{N-j} \leq \varepsilon_N, \quad j = 0, 1, 2, \ldots, N.
\]

**Proof.** Suppose that there exists an order-sequence \(\varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N\) satisfying
\[
\varepsilon_j + \varepsilon_{N-j} > \varepsilon_N, \quad \text{for some} \ 0 \leq j \leq N.
\]
Let \(S\) be such a sequence with the smallest possible projective dimension \(N\). We can assume that \(\varepsilon_i = 1\) in this order-sequence \(S\). Since \(S \setminus \{\varepsilon_N\} = \{\varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_{N-1}\}\) is also an order-sequence (i.e. satisfies the \(p\)-adic criterion) and \(N\) is minimal, we have
\[
\varepsilon_j + \varepsilon_{N-1-j} \leq \varepsilon_{N-1} \quad \text{and} \quad \varepsilon_{j-1} + \varepsilon_{N-j} \leq \varepsilon_{N-1}.
\]
It follows that \( e_j + (1 + e_{N-j}) \leq e_N \) and \( 1 + e_j + e_{N-j} \leq e_N \). Since \( e_j + e_{N-j} > e_N \), we see that \( e_{N-j} > 1 + e_{N-1-j} \) and \( e_j > 1 + e_{j-1} \). By the \( p \)-adic criterion, we have that \( e_{N-j} \) and \( e_j \) are multiples of the characteristic. Let us denote by \( m \), \( 0 < m \leq p - 1 \), the biggest residue \( \pmod{p} \) in the sequence \( S \) and by \( S(m) \) the set of orders in \( S \) with residue \( m \pmod{p} \), i.e. \( S(m) = \{ e_j | e_j \equiv m \pmod{p} \} \). Since \( S \setminus S(m) = \{ e_j | e_j \not\equiv m \pmod{p} \} \) is also an order-sequence (see Remark 3), we must have

\[
\#(S(m) \cap [e_0, e_j]) < \#(S(m) \cap [e_{N-j}, e_N])
\]

Otherwise, \( S \setminus S(m) \) would be a smaller order-sequence satisfying (3). Consider now the following subset \( S_0 \) of \( S \): \( S_0 = \{ (e_i - m) | e_i \in S \} \). That \( S_0 \) is a subset of \( S \) follows from the fact that \( S \) is an order-sequence. Now \( S_0 \) is itself an order-sequence since we have: if \( e_i \in S \) and \( (e_i - m) \equiv 0 \pmod{p} \), then \( (e_i + m) \not\equiv 0 \pmod{p} \).

One can now easily check that

\[
\#(S_0 \cap [e_0, e_j]) = \#(S(m) \cap [e_0, e_j]), \quad \text{if } (e_j + m) \not\in S,
\]

\[
\#(S_0 \cap [e_0, e_j]) = \#(S(m) \cap [e_0, e_j]) + 1, \quad \text{if } (e_j + m) \in S.
\]

Let us write \( S_0 = \{ \mu_0 < \mu_1 < \cdots < \mu_n \} \). We denote by \( t \) the number of orders in \( S_0 \cap [e_0, e_j] \); i.e. \( S_0 \cap [e_0, e_j] = \{ \mu_0, \mu_1, \ldots, \mu_{n-1} \} \).

Case 1: \( (e_j + m) \not\in S \), i.e. \( e_j \not\in S_0 \). In this case, \( \#(S_0 \cap [e_{N-j}, e_N]) > t \) and hence \( \mu_{n-j} \geq e_{N-j} \). Since \( \mu_j = e_j \), we get a contradiction with the minimality of \( N \).

Case 2: \( (e_j + m) \in S \), i.e. \( e_j \in S_0 \). In this case, \( \#(S_0 \cap [e_{N-j}, e_N]) \equiv t \) and hence \( \mu_{n-j+1} \geq e_{N-j} \). Since \( \mu_{j-1} = e_j \), we get again a contradiction with the choice of \( N \).

This finishes the proof of the theorem. \( \square \)

4. The equalities \( e_j + e_{N-j} = e_N \)

Theorem 5. Let \( e_0 < e_1 < e_2 < \cdots < e_N \) be a semigroup-sequence with \( e_N > N \). The following are equivalent:

(a) \( e_j + e_{N-j} = e_N \), for \( j = 0, 1, \ldots, N \).

(b) There exist integers \( q \) and \( r \geq 2 \) such that \( N = r(q - 1) - 1 \), \( e_N = rq - 2 \) and

\[
\{ e_0, e_1, \ldots, e_N \} = \{ e \in \mathbb{N} | e \leq rq - 2 \text{ and } e \not\equiv -1 \pmod{q} \}.
\]

Proof. It is a direct verification that (b) implies (a) and that the sequence in (b) is a semigroup-sequence.

Reciprocally, let \( k \) be such that \( e_k > e_{k-1} + 1 \). From the equalities

\[
e_k + e_{N-k} = e_N \quad \text{and} \quad e_{k-1} + e_{N-k+1} = e_N,
\]

the equalities (b) follow. \( \square \)
we have \( \varepsilon_{N-k+1} - \varepsilon_{N-k} = \varepsilon_k - \varepsilon_{k-1} > 1 \). In particular, \((\varepsilon_N + 2)\) is a non-gap. Since \((\varepsilon_N + 1)\) is a gap and since the non-gaps constitute a semigroup by hypothesis, we have that \( (\varepsilon_k - 1) \) is a gap, i.e. we have that \( \varepsilon_{k-1} = \varepsilon_k - 2 \). This follows from the following equality:

\[
(\varepsilon_k - 1) + (\varepsilon_N - k + 2) - (\varepsilon_N + 1).
\]

So far we have shown that every time there is a jump in the sequence, the jump is obtained by deleting just one integer, i.e. if \( \varepsilon_k > \varepsilon_{k-1} + 1 \), then \( \varepsilon_k = \varepsilon_{k-1} + 2 \). Let \((q - 1)\) be the smallest deleted integer, i.e. \( q \) is the smallest positive non-gap. Because of the semigroup property on non-gaps, we have that \( nq, \ n \in \mathbb{N} \), is also a non-gap. We claim that the non-gaps smaller than \( \varepsilon_N \) have the above form, i.e. the deleted integers \( Z \) are given by

\[
Z < \varepsilon_N \quad \text{and} \quad Z = (q - 1) + nq, \ n \in \mathbb{N}.
\]

Otherwise we would have the existence of two deleted integers \( Z_1, Z_2 \) with \(|Z_2 - Z_1| < q\). Using the semigroup property again we have \( Z_1 + nq \) and \( Z_1 + nq \), \( n \in \mathbb{N} \), are also deleted integers whenever smaller than \( \varepsilon_N \). Hence any two consecutive deleted integers occurring after the pair \( \{Z_1, Z_2\} \) give rise to a segment having length less than \( q \). In particular, this is also true for the last segment and we get a contradiction with the conditions in (a). The theorem now follows easily. \( \square \)

**Theorem 6.** Let \( \varepsilon_0 = 0 < \varepsilon_1 < \varepsilon_2 < \cdots < \varepsilon_N \) be the order-sequence of a base-point-free linear system of degree \( d \) on a smooth projective curve of genus \( g \) defined over an algebraically closed field of characteristic \( p > 0 \). If the sequence is non-classical (i.e. \( \varepsilon_N > N \)) and it is a semigroup-sequence, the following are equivalent:

(a) \( \varepsilon_j + \varepsilon_{N-j} = \varepsilon_N, \) for \( j = 0, 1, \ldots, N. \)

(b) There exist integers \( q \) and \( r \), \( q \) being a power of the characteristic \( p \), such that

\[
\{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_N\} = \{\varepsilon \in \mathbb{N} \mid \varepsilon \leq rq - 2 \text{ and } \varepsilon \not\equiv -1 \text{ (mod } q)\}\]

(c) The number \( W \) of Weierstrass points for the linear system is maximal, i.e.

\[
W = (N + 1) \cdot (\varepsilon_N(g - 1) + d).
\]

**Proof.** We just have to show that (a) implies (b). Because of Theorem 5, one just needs to show that \( q \) is a power of the characteristic \( p \). Let then \( m \) be defined by

\[
p^{m-1} < q \leq p^m.
\]

From the proof of Theorem 5, one has that \( \varepsilon_{q-2} = q - 2 \) and \( \varepsilon_{q-1} = q \). It follows
that \( q = 0 \pmod{p} \). Hence we have the following \( p \)-adic expansion:

\[
(q - 1) = \sum_{i=0}^{m-1} a_i p^i, \quad a_0 = p - 1 \quad \text{and} \quad a_{m-1} \neq 0.
\]

If \( q \neq p^m \), then there exists a coefficient \( a_j \) in the expansion above such that \( 0 \leq a_j < (p - 1) \). Consider now the integer \( Z = (q - 1) + p^j \). Since \( Z < \varepsilon_N \) and \( (q - 1) \neq 0 \pmod{p} \), using again the \( p \)-adic criterion, we get that \( Z \) is also a deleted integer. This is an absurd, as follows from Theorem 5, since we have \( Z - (q - 1) = p^j < q \). Hence \( q = p^m \) and the theorem is proved.

**Remark 7.** It is easy to see that the sequences given in Theorem 6(b) are semigroup-sequences and satisfy the \( p \)-adic criterion. However, we do not know of any non-classical canonical curves having order-sequences of this type.

**Remark 8.** Let \( \varepsilon_0 = 0 < \varepsilon_1 < \cdots < \varepsilon_N \) be a non-classical (i.e. \( \varepsilon_N > N \)) semigroup-sequence. Suppose that \( \varepsilon_j > \varepsilon_{j-1} + 1 \) and that there exist \( \varepsilon_k \) and \( \varepsilon_h \) satisfying

\[
\varepsilon_{j-1} + \varepsilon_k = \varepsilon_h.
\]

Then, as in the proof of Theorem 5, we conclude that \( \varepsilon_k - 2 \) is also an element of the sequence by using the equality \( (\varepsilon_{j-1} + 2) + (\varepsilon_k - 1) = (\varepsilon_h + 1) \).

**Remark 9.** For a non-classical semigroup-sequence, let \( (j + 1) \) be the first non-gap, i.e. \( \varepsilon_{j-1} = j + 1 \) and \( \varepsilon_j > j \). Then we have

\[
\varepsilon_k - \varepsilon_{k-1} - 1 \leq j, \quad \text{for all} \quad k \geq j.
\]

This follows from the equality \((j + 1) + (\varepsilon_k - j) = (\varepsilon_k + 1)\).

### 5. The inequalities \( \varepsilon_h \leq \varepsilon_k + \varepsilon_{d(k)} \), \( d(k) = \varepsilon_k - k \)

We explore further the idea in the above two remarks to obtain inequalities on semigroup-sequences. We do not assume that the sequence satisfies the \( p \)-adic criterion and hence the result can be applied to Weierstrass points on canonical curves, even in characteristic zero.

**Theorem 10.** Let \( 0 = \varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N \) be a semigroup-sequence with \( \varepsilon_N > N \). Let \( k \) be such that \( \varepsilon_k > \varepsilon_{k-1} + 1 \) and denote \( d(k) = (\varepsilon_k - k) \). Then we have

\[
\varepsilon_h \leq \varepsilon_k + \varepsilon_{d(k)}, \quad \text{for} \quad h \geq k.
\]
Moreover, \((\varepsilon_h - \varepsilon_k)\) belongs to the sequence for \(h \geq k\), and

\[
\left[\frac{\varepsilon_N}{\varepsilon_k}\right] \cdot (\varepsilon_k - k) \leq (\varepsilon_N - N),
\]

where \(\left[\frac{\varepsilon_N}{\varepsilon_k}\right]\) denotes the integer part.

**Proof.** For each integer \(b < \varepsilon_k\) and not belonging to the sequence, we have that \((b + 1)\) is a non-gap. From the equalities

\[
(b + 1) + (\varepsilon_h - b) = (\varepsilon_h + 1), \quad b \text{ as above },
\]

and using the semigroup property, we conclude that \((\varepsilon_h - b - 1)\) is an element of the sequence. Clearly there are exactly \(d(k) = (\varepsilon_k - k)\) such elements \(b\) and we ordered them as follows \(b_1 < b_2 < \cdots < b_{d(k)} < \varepsilon_k\). Hence we have

\[
\varepsilon_h - b_j - 1 \leq \varepsilon_{h-j}, \quad \text{for } 1 \leq j \leq d(k).
\]

The first assertion now follows taking \(j = d(k)\) and noticing that \(b_{d(k)} + 1 = \varepsilon_k\) since \(\varepsilon_k > \varepsilon_{k+1} + 1\). It also follows from above that \((\varepsilon_h - \varepsilon_k)\) belongs to the sequence for \(h \geq k\). Write now, using the euclidian algorithm,

\[
\varepsilon_h = n \cdot \varepsilon_k + \varepsilon, \quad n \in \mathbb{N} \text{ and } 0 \leq \varepsilon < \varepsilon_k.
\]

We must then have that \(\varepsilon\) is also an element of the sequence. Hence if \(b\) does not belong to the sequence and \(b < \varepsilon_k\), then \((n \varepsilon_k + b)\) does not belong to the sequence for each \(n \in \mathbb{N}\) satisfying \((n \varepsilon_k + b) < \varepsilon_N\). In particular, this is true for \(n = \left[\frac{\varepsilon_N}{\varepsilon_k}\right]\). Then we see that each element \(b\) as above, and there are \((\varepsilon_k - k)\) such elements, gives rise to at least \(\left[\frac{\varepsilon_N}{\varepsilon_k}\right]\) elements that do not belong to the sequence. We then conclude that

\[
\left[\frac{\varepsilon_N}{\varepsilon_k}\right] \cdot (\varepsilon_k - k) \leq (\varepsilon_N - N). \quad \square
\]

**Remark 11.** Let \(\varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N\) be a non-classical order-sequence which is a semigroup-sequence. If \(k\) is such that \(\varepsilon_k > \varepsilon_{k-1} + 1\), then

\[
\varepsilon_{N-k+d(k)} \leq \varepsilon_k + \varepsilon_{N-k} \leq \varepsilon_N.
\]

This follows from Theorems 4 and 10.

**Example.** It is easy to verify that the sequence 0,1,2,5,6,10 is a semigroup-sequence. Taking \(k = 3\), we have \(d(k) = d(3) = \varepsilon_k - k = 5 - 3 = 2\). From Theorem 10 we must have \((\text{taking } h = 5)\varepsilon_5 \leq \varepsilon_5 + \varepsilon_{5-2} = 2 \cdot \varepsilon_5 = 10\). This is then an example where we have the equality attained.
6. The sum of two order-sequences

**Theorem 12.** Let $p$ be a prime number and let

\[ S_1 = \{ \epsilon_0 = 0 < \epsilon_1 < \epsilon_2 < \cdots < \epsilon_N \}, \]
\[ S_2 = \{ \mu_0 = 0 < \mu_1 < \mu_2 < \cdots < \mu_M \} \]

be order-sequences, i.e. sequences satisfying the $p$-adic criterion. Then their sum

\[ S_1 + S_2 = \{ \epsilon_i + \mu_j \mid 0 \leq i \leq N \text{ and } 0 \leq j \leq M \} \]

is also an order-sequence.

**Corollary.** If $S_i$, $i = 1, 2, \ldots, n$, are order-sequences, then

\[ \sum_{i=1}^{n} S_i = (\sum_{i=1}^{n} s_i \mid s_i \in S_i) \]

is also an order-sequence.

**Proof of Theorem 12.** We have to prove that if $\alpha \in \mathbb{N}$ is such that

\[ \left( \frac{\epsilon_i + \mu_j}{\alpha} \right) \not\equiv 0 \mod p, \text{ for some } i \text{ and } j, \]

then $\alpha$ can be written as $\alpha = \epsilon_l + \mu_k$, for some $l$ and $k$. Write

\[ \epsilon_i = \sum_{n=0}^{\infty} a_n p^n, \quad 0 \leq a_n \leq p - 1, \quad \mu_j = \sum_{n=0}^{\infty} b_n p^n, \quad 0 \leq b_n \leq p - 1. \]

Hence $(\epsilon_i + \mu_j) = \sum_{n=0}^{\infty} (a_n + b_n) p^n$. If all $(a_n + b_n)$, for $n \geq 0$, are smaller than $p$, then the expression above for $(\epsilon_i + \mu_j)$ is its $p$-adic expansion. Writing the $p$-adic expansion of $\alpha$ as $\alpha = \sum_{n=0}^{\infty} \alpha_n p^n$, we have in this case that $\alpha_n \leq a_n + b_n$. Clearly, one can find $a'_n$ and $b'_n$ such that

\[ a'_n \leq a_n, \quad b'_n \leq b_n \quad \text{and} \quad \alpha_n = a'_n + b'_n. \]

Taking now $a' = \sum a'_n p^n$ and $b' = \sum b'_n p^n$, we have that $a' + b' = \alpha$ and also that $a' = \epsilon_l$ for some $l$ and $b' = \mu_k$ for some $k$, since $(\epsilon_l) \not\equiv 0 \mod p$ and $(\mu_k) \not\equiv 0 \mod p$. So we can assume that $(a_n + b_n) \geq p$, for some $n \geq 0$. Let $s$ be the first time we have $(a_n + b_n) \geq p$, i.e. $(a_n + b_n) < p$ for $n < s$ and $a_n + b_n \geq p$. The coefficient of $p^s$ in the $p$-adic expansion of $(\epsilon_i + \mu_j)$ is then $(a_i + b_i - p)$. The one of $p^{s+1}$ is either

\[ (a_{s+1} + b_{s+1} + 1), \text{ if } a_{s+1} + b_{s+1} + 1 < p, \]
or

\[(a_{s+1} + b_{s+1} + 1 - p), \text{ if } a_{s+1} + b_{s+1} + 1 \geq p.\]

In the latter case, i.e. \(a_{s+1} + b_{s+1} + 1 \geq p\), the coefficient of \(p^{s+2}\) is either \((a_{s+2} + b_{s+2} + 1)\) or \((a_{s+2} + b_{s+2} + 1 - p)\). From this we see that we can think of the \(p\)-adic expansion of \((e_i + \mu_j)\) as constituted by ‘blocks’, the first ‘block’ being (just writing down the coefficients)

\[(a_s + b_s - p), (a_{s+1} + b_{s+1} + 1 - p), \ldots,\]
\[(a_t + b_t + 1 - p), (a_{t+1} + b_{t+1} + 1),\]

where \(t \geq s\) and \(t = s\) means that we do not have a coefficient of the form \((a_t + b_t + 1 - p)\) in this ‘block’. Now since \(\left(\frac{\epsilon_i}{a_i}\right) \not\equiv 0 \mod p\), we have that (see Remark 3)

\[\alpha_s \leq a_s + b_s - p,\]
\[\alpha_s \leq a_t + b_t + 1 - p, \quad s < l \leq t\]
\[\alpha_{r+1} \leq a_{r+1} + b_{r+1} + 1.\]

Now we consider two possibilities:

Case 1: \(a_{r+1} > 0\). In this case we choose \(a'_i\) and \(b'_i\) such that

\[a'_i \leq a_i, \quad b'_i \leq b_i \quad \text{and} \quad a'_i + b'_i = p + \alpha_i.\]

For \(s < l \leq t\), we choose \(a'_i\) and \(b'_i\) such that

\[a'_i \leq a_i, \quad b'_i \leq b_i \quad \text{and} \quad a'_i + b'_i + 1 = p + \alpha_i.\]

Finally take \(a'_{r+1} \leq a_{r+1}\) and \(b'_{r+1} \leq b_{r+1}\) such that \(a'_{r+1} + b'_{r+1} + 1 = \alpha_{r+1}\).

Case 2: \(a_{r+1} = 0\). In this case let \(h\) be the biggest index occurring in this ‘block’ satisfying \(a_h \neq 0\). We then choose \(a'_i\) and \(b'_i\) exactly as in the preceding case for each \(l, s \leq l < h\). Now we take \(a'_h \leq a_h\) and \(b'_h \leq b_h\) such that \(a'_h + b'_h + 1 = \alpha_h\) and \(a'_r = b'_r = 0\) for each \(r, h < r \leq t + 1\).

Applying this procedure to each ‘block’, we get that \(a' = \sum_{n=0}^{\infty} a'_n p^n\) and \(b' = \sum_{n=0}^{\infty} b'_n p^n\) are such that

\[\left(\frac{\epsilon_i}{a'}\right) \not\equiv 0 \mod p, \quad \left(\frac{\mu_i}{b'}\right) \not\equiv 0 \mod p \quad \text{and moreover} \quad \alpha = a' + b'.\]

Note that outside the ‘blocks’ the coefficients satisfy \((a_n + b_n) < p\). There we proceed as in the beginning of this proof. Thus the theorem is proved. \(\Box\)
References