JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

FRANÇOIS LAUBIE

A recursive definition of p-ary addition without carry

Journal de Théorie des Nombres de Bordeaux, tome 11, nº 2 (1999), p. 307-315

<http://www.numdam.org/item?id=JTNB_1999__11_2_307_0>

Journal de Théorie des Nombres
de Bordeaux **11** (1999), 307–315

A recursive definition of p-ary addition without carry

par FRANÇOIS LAUBIE

RÉSUMÉ. Soit p un nombre premier. Nous montrons dans cet article que l'addition en base p sans retenue possède une définition récursive à l'instar des cas où $p = 2$ et $p = 3$ qui étaient déjà connus.

ABSTRACT. Let p be a prime number. In this paper we prove that the addition in p-ary without carry admits a recursive definition like in the already known cases $p = 2$ and $p = 3$.

1. INTRODUCTION

Let p be a prime number. For any two natural integers a and b, let us denote by $a +_p b$ the natural integer obtained writing a and b in p-ary and then adding them without carry.

In the case where $p = 2$, this operation called nim-addition, plays a crucial role in the theory of some games [1] and in the theory of lexicographic codes of Levenstein [6], Conway and Sloane [2]. The map $(a, b) \mapsto a +_2 b$ is the Grundy function of the directed graph whose vertices are the pairs (a, b) of natural integers and arcs the pairs of vertices $((a', b'), (a, b))$ such that either $a' < a$ and $b' = b$ or $a' = a$ and $b' < b$. Therefore the nim-addition can be defined recursively as follows:

$$a +_2 b = \min(\mathbb{N} \setminus \{a' +_2 b, a +_2 b' \ ; \ a' < a, b' < b\}).$$

Thus the nim-addition is the first regular law on $\mathbb{N}$ in the sense that, given all $a' +_2 b$ and $a +_2 b'$ with $a' < a$ and $b' < b$, $a +_2 b$ is the smallest natural integer which is not excluded by the rule:

$$a +_2 b = a' +_2 b \Longrightarrow a = a' \text{ or } a +_2 b = a +_2 b' \Longrightarrow b = b'.$$

Surprisingly, it is a group law on $\mathbb{N}$.

For any prime number $p \geq 3$, the addition $+_p$ takes place in the theory of some generalized nim-games [7], [8] and also in the theory of some greedy codes [4]. Moreover this addition plays a crucial role in the recent determination of the least possible size of the sumset of two subsets of $(\mathbb{Z}/p\mathbb{Z})^N$

Manuscrit reçu le 11 mars 1998.

with given cardinalities (S. Eliahou, M. Kervaire, [3]). In [5] H.W. Lenstra announced the following formula due to S. Norton:

$$a +_3 b = \min(\mathbb{N}\backslash(\{a' +_3 b, a +_3 b' \; ; \; a' < a, b' < b\} \cup \\ \{a'' +_3 b'', a'' < a, b'' < b, a'' +_3 b = a +_3 b''\}))$$

and he asked the question if such a recursive definition exists for $+_p$ whenever p is a prime number.

The aim of this paper is to answer positively. This answer provides us with a definition "à la Conway" of prime numbers.

2. THE $+_p$-ADDITION TABLE AS A GRAPH

Let $\mathbb{F}_p$ be the finite field with p elements; for $\lambda \in \mathbb{F}_p$, let $\tilde{\lambda}$ be the representative number of the class λ belonging to $\{0, 1, \cdots, p-1\}$ and, for $a \in \mathbb{N}$, define $\lambda \cdot_p a = \tilde{\lambda} \cdot_p a = a +_p a +_p \cdots +_p a$ with $\tilde{\lambda}$ terms a.

The operations $+_p$ and $\cdot_p$ provide $\mathbb{N}$ with a structure of $\mathbb{F}_p$-vector space isomorphic to the $\mathbb{F}_p$-vector space of polynomials $\mathbb{F}_p[X]$.

We define a directed graph $\mathcal{G}_p$ as follows:
- the set of its vertices is $\mathbb{N} \times \mathbb{N}$,
- the arcs of $\mathcal{G}_p$ are the pairs of vertices $((a', b'), (a, b))$ such that
  - $a' \leq a$, $b' \leq b$,
  - $a' = a +_p \lambda \cdot_p r$, $b' = b +_p (1 - \lambda) \cdot_p r$ for some $r \in \mathbb{N}^*$ and $\lambda \in \mathbb{F}_p$.

The graph $\mathcal{G}_p$ does not admit circuit; thus the Grundy function of $\mathcal{G}_p$ is the unique map g of $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that:

$$g((a, b)) = \min(\mathbb{N}\backslash\{g((a', b')) \; ; \; ((a', b'), (a, b)) \text{ is an arc of } \mathcal{G}_p\}).$$

Proposition 1. *The Grundy function of* $\mathcal{G}_p$ *is the addition map:* $(a, b) \mapsto a +_p b$.

First of all, we give some lemmas on the natural ordering of the representative set $\{0, 1, \cdots, p-1\}$ of $\mathbb{F}_p$. It is sometimes more convenient to express them in terms of the following ordering on $\mathbb{F}_p$:

$$u \prec v \Longleftrightarrow \tilde{u} < \tilde{v}$$

where $\tilde{u}$ (resp. $\tilde{v}$) is the representative number of $u \in \mathbb{F}_p$ (resp. $v \in \mathbb{F}_p$) belonging to $\{0, 1, \cdots, p-1\}$.

Lemma 1. *For all* $u, v \in \mathbb{F}_p$,

$$\widetilde{u+v} = \tilde{u} +_p \tilde{v} = \begin{cases} \tilde{u} + \tilde{v} & \text{if} \quad \tilde{u} + \tilde{v} \leq p - 1, \\ \tilde{u} + \tilde{v} - p & \text{if} \quad \tilde{u} + \tilde{v} \geq p. \end{cases}$$

Thus $u + v \prec u \Longleftrightarrow \tilde{u} + \tilde{v} \geq p \Longleftrightarrow u + v \prec v$.

Lemma 2. *Let* u, r, s *be elements of* $\mathbb{F}_p$ *such that* $r \prec s$ *and* $u + r \prec u$. *Then* $r \prec r - s$ *and* $u + r - s \prec u$.

Proof. $\tilde{r} < \tilde{s} \Longrightarrow \widetilde{r-s} = p + \tilde{r} - \tilde{s} > \tilde{r} \Longrightarrow r \prec r - s$;
$\tilde{u} + \widetilde{r-s} = \tilde{u} + \tilde{r} + p - \tilde{s} > \tilde{u} + \tilde{r} \geq p \Longrightarrow u + r - s \prec u$. □

Lemma 3. *Let u, v, r be elements of $\mathbb{F}_p$ such that $u \prec u + r$, $v \prec v + r$ and $u + v + r \prec u + v$. Then there exist $s, t \in \mathbb{F}_p$ such that $s + t = r$, $u + s \prec u$ and $v + t \prec v$.*

Proof. Conditions:

$$\text{(C)} \quad \begin{cases} u + v + r \prec u + v, \\ u \prec u + r, \\ v \prec v + r, \end{cases}$$

are equivalent to:

$$\begin{cases} \widetilde{u+v} + \tilde{r} \geq p, \\ \tilde{u} + \tilde{r} \leq p - 1, \\ \tilde{v} + \tilde{r} \leq p - 1. \end{cases}$$

Since $\widetilde{u+v} \geq p - \tilde{r}$ with $\tilde{r} \leq p - 1 - \tilde{u}$, we have $\widetilde{u+v} \geq \tilde{u} + 1$. Hence $\widetilde{u+v} \geq \max(\tilde{u}, \tilde{v}) + 1$. Moreover $\tilde{u} + \tilde{v} - p < \tilde{u} < \widetilde{u+v}$. Therefore, by Lemma 1, $\tilde{u} + \tilde{v} \leq p - 1$ and the conditions (C) are equivalent to:

$$\begin{cases} p - \tilde{u} - \tilde{v} & \leq & \tilde{r} & \leq & p - 1, \\ 1 & \leq & \tilde{r} & \leq & p - 1 - \tilde{u}, \\ 1 & \leq & \tilde{r} & \leq & p - 1 - \tilde{v}, \end{cases}$$

or, more simply, to: $\max(\tilde{u}, \tilde{v}) + 1 \leq p - \tilde{r} \leq \tilde{u} + \tilde{v}$.

We are looking for s and $t \in \mathbb{F}_p$ such that:

$$\begin{cases} s + t & = & r \\ u + s & \prec & u \\ v + t & \prec & v \end{cases}$$

or equivalently such that:

$$\begin{cases} \sigma + \tau = \rho, \\ 1 \leq \sigma \leq \tilde{u} \leq p - 1, \\ 1 \leq \tau \leq \tilde{v} \leq p - 1 \end{cases}$$

with $\rho = p - \tilde{r}$, $\sigma = p - \tilde{s}$ and $\tau = p - \tilde{t}$. >From the condition $1 + \max(\tilde{u}, \tilde{v}) \leq \rho \leq \tilde{u} + \tilde{v}$, it is clear that such integers σ and τ do exist. Thus the lemma is proved. □

Now, for any natural integer x, let $\tilde{x}$ be its class modulo p, let $x = \sum_{i \geq 0} x_i p^i$ with $x_i \in \{0, 1, \cdots, p - 1\}$ its p-ary expansion, and let i_x be the largest index $i \geq 0$ such that $x_i \neq 0$. In order to summarize all these notations we set:

Lemma 4. *For all $x, y \in \mathbb{N}$ the following assertions are equivalent*

(i) $x +_p y < x$,

(ii) $x_{i_y} +_p y_{i_y} < x_{i_y}$,

(iii) $\overline{x_{i_y}} + \overline{y_{i_y}} \prec \overline{x_{i_y}}$,

(iv) $x_{i_y} + y_{i_y} \geq p$.

Proof of Proposition 1. Let a, b be natural integers. For any natural integer $c < a +_p b$, there exists $r \in \mathbb{N}^*$ so that $c = a +_p b +_p r$. We will prove that for any $r \in \mathbb{N}^*$ such that $a +_p b +_p r < a +_p b$, there exists $\lambda \in \mathbb{F}_p$ such that $a +_p \lambda \cdot_p r \leq a$ and $b +_p (1 - \lambda) \cdot_p r \leq b$. With the notations of Lemma 4, we have:

$$\begin{aligned} a +_p b +_p r < a +_p b \quad &\Longleftrightarrow \quad \overline{a_{i_r} + b_{i_r} + r_{i_r}} \prec \overline{a_{i_r} + b_{i_r}}, \\ a < a +_p r \quad &\Longleftrightarrow \quad \overline{a_{i_r}} \prec \overline{a_{i_r} + r_{i_r}}, \\ b < b +_p r \quad &\Longleftrightarrow \quad \overline{b_{i_r}} \prec \overline{b_{i_r} + r_{i_r}}. \end{aligned}$$

There exist $s, t \in \mathbb{F}_p$ such that $\overline{r_{i_r}} = s + t$, $\overline{a_{i_r}} + s \prec \overline{a_{i_r}}$ and $\overline{b_{i_r}} + t \prec \overline{b_{i_r}}$. Let $\lambda = s\, \overline{r_{i_r}}^{-1} \in \mathbb{F}_p$; then: $s = \lambda \overline{r_{i_r}}$, $t = (1 - \lambda)\overline{r_{i_r}}$, $\overline{a_{i_r}} + \lambda \overline{r_{i_r}} \prec \overline{a_{i_r}}$ and $\overline{b_{i_r}} + (1 - \lambda)\overline{r_{i_r}} \prec \overline{b_{i_r}}$; in other words : $a +_p \lambda \cdot_p r < a$ and $b +_p (1 - \lambda) \cdot_p r < v$ (Lemma 4).

Therefore $a +_p b = \min(\mathbb{N} \backslash E_p)$ where E_p is the set of all the natural integers $a' +_p b'$ with $a' < a$, $b' < b$ and such that there exist $\lambda \in \mathbb{F}_p$ and $r \in \mathbb{N}^*$ satisfying $a' = a +_p \lambda \cdot_p r$, $b' = b +_p (1 - \lambda) \cdot_p r$. This means that $(a, b) \mapsto a +_p b$ is the Grundy function of $\mathcal{G}_p$. □

Corollary. *(S. Eliahou, M. Kervaire* [3]*) - Let us denote by* $[0, a]$ *the interval* $\{a' \in \mathbb{N}\ ;\ a' \leq a\}$ *for* $a \in \mathbb{N}$. *Then for all* $a, b \in \mathbb{N}$ *there exists* $c \leq a + b$ *such that* $[0, a] +_p [0, b] = [0, c]$.

Proof. Let $c = \max([0, a] +_p [0, b])$ and let $a_1 \leq a$, $b_1 \leq b$ such that $c = a_1 +_p b_1$. For all $d < c$ there exist $\lambda \in \mathbb{F}_p$ and $r \in \mathbb{N}^*$ such that $d = \lambda \cdot_p a_1 +_p (1 - \lambda) \cdot_p b_1$, $\lambda \cdot_p a_1 < a_1$ and $(1 - \lambda) \cdot_p b_1 < b_1$; therefore $d \in [0, a] +_p [0, b]$. □

Remark. With the notations of the proof of Proposition 1, we have:

1. $E_2 = \{a +_2 b', a' +_2 b\ ;\ a' < a, b' < b\}$,
2. $E_3 = \{a +_3 b', a' +_3 b\ ;\ a' < a, b' < b\} \cup \{a'' +_3 b'', a'' < a, b'' < b, a +_3 b'' = a'' +_3 b\}$ because in this case, $\lambda = 0$ or $\lambda = 1$ or $\lambda = 1 - \lambda$.
3. In the case where $p \geq 5$, the situation is a little more complicated because the formula $a +_p b = \min(\mathbb{N} \backslash E_p)$ will be effectively recursive only when we can describe the set E_p using only pairs $(\alpha, \beta) \in \mathbb{N} \times \mathbb{N}$ with $\alpha \leq a$, $\beta \leq b$ and $(\alpha, \beta) \neq (a, b)$.

3. A RECURSIVE EXCLUSION ALGORITHM FOR $a +_p b$

Given a prime number p and a pair (a, b) of natural integers, we will describe a rule that excludes for the calculation of $a +_p b$ all the natural integers of the kind $a' +_p b' \neq a +_p b$ with $a' \leq a$ and $b' \leq b$ without using any pair of integers (a'', b'') such that $a'' > a$ or $b'' > b$.

For all $S \subset \mathbb{N}$, S^* means $S \backslash \{0\}$.

Let $\mathcal{M}$ and $\mathcal{N}$ be two finite sets of natural integers such that $\mathcal{M} \cap \mathcal{N} = \{0, 1\}$ and let $(a_m)_{m \in \mathcal{M}}$ and $(b_n)_{n \in \mathcal{N}}$ be two sequences of natural integers (respectively indexed by $\mathcal{M}$ and $\mathcal{N}$) satisfying the conditions:

- $a_0 = a$, $b_0 = b$,
- $a_1 +_p b = a +_p b_1$,
- $\forall (m, n) \in \mathcal{M}^* \times \mathcal{N}^*$, $a_m < a$, $b_n < b$,
- $\forall m \in \mathcal{M}^* \backslash \{1\}$, $\exists k \in \mathcal{M}^*$ such that $k < m$, $m - k \in \mathcal{N}$ and $a_m +_p b = a_k +_p b_{m-k}$,
- $\forall n \in \mathcal{N}^* \backslash \{1\}$, $\exists \ell \in \mathcal{N}^*$ such that $\ell < n$, $n - \ell \in \mathcal{M}$ and $a +_p b_n = a_{n-\ell} +_p b_\ell$.

Such a pair of sequences $((a_m)_{m \in \mathcal{M}}, (b_n)_{n \in \mathcal{N}})$ is called a p-chain of (a, b) of length card $\mathcal{M}^*$+ card $\mathcal{N}^*$.

Remark. 1 - The p-chains of (a, b) of length 2 are the pairs $(\{a, a_1\}, \{b, b_1\})$ with $a_1 < a$, $b_1 < b$ and $a +_p b_1 = a_1 +_p b$ (see the formula of S. Norton in the introduction).

2 - For a p-chain of (a, b) of length ≥ 3, we have $a_2 +_p b = a_1 +_p b_1$ or $a +_p b_2 = a_1 +_p b_1$, $a_3 +_p b = a_2 +_p b_1$ provided that (a_2, b_1) lies in the p-chain, or $a_3 +_p b = a_1 +_p b_2$ provided that (a_1, b_2) lies in the p-chain.

For convenience we extend our definition to length 1 p-chain of (a, b): it is the pairs $(a, \{b, b_1\})$ or $(\{a, a_1\}, b)$ with $a_1 < a$, $b_1 < b$.

A p-chain $((a_m)_{m \in \mathcal{M}}, (b_n)_{n \in \mathcal{N}})$ of (a, b) is called a p-exclusion chain for $a +_p b$ (or of (a, b)) if $\forall\, n \in \mathcal{M}^* \cup \mathcal{N}^*$, $p \nmid n$.

Finally the set of all integers $a' +_p b'$ where (a', b') belongs to any p-exclusion chain for $a +_p b$ of length $\leq p - 1$ is called the p-exclusion set for $a +_p b$ (or of (a, b)); it's denoted by $E_p(a, b)$.

We will prove:

Theorem. *$((a', b'), (a, b))$ is an arc of $\mathcal{G}_p$ if and only if there exists a p-exclusion chain for $a +_p b$ of length $\leq p - 1$ containing (a', b'). In other words : $a +_p b = \min(\mathbb{N} \backslash E_p(a, b))$.*

Lemma 5. *Let $((a_m)_{m \in \mathcal{M}}, (b_n)_{n \in \mathcal{N}})$ be a p-chain of (a, b) of length ≥ 2. There exists $r \in \mathbb{N}^*$ such that $a_m = a +_p m \cdot_p r$ and $b_n = b +_p n \cdot_p r$ for all $(m, n) \in \mathcal{M} \times \mathcal{N}$. Thus if $p | m + n$ then $a_m +_p b_n = a +_p b$.*

Proof. Let $r \in \mathbb{N}^*$ such that $a_1 = a +_p r$; then $a +_p b_1 = a_1 +_p b = a +_p r +_p b$, therefore $b_1 = b +_p r$. Suppose that for any $k \in \mathcal{M}$ and $\ell \in \mathcal{N}$ with $1 \leq k \leq m - 1$ and $1 \leq \ell \leq n - 1$ we have $a_k = a +_p k \cdot_p r$ and $b_\ell = b +_p \ell \cdot_p r$, then there exists $k_0 \in \mathcal{M}$ such that $1 \leq k_0 \leq m - 1$, $m - k_0 \in \mathcal{N}$ and

$$a_m +_p b = a_{k_0} +_p b_{m-k_0} = a +_p k_0 \cdot_p r +_p b +_p (m - k_0) \cdot_p r = a +_p b +_p m \cdot_p r.$$

Therefore $a_m = a +_p m \cdot_p r$ and the lemma is proved by recurrence. □

Proposition 2. *Let $((a_m)_{m \in \mathcal{M}}, (b_n)_{n \in \mathcal{N}})$ be a p-chain of (a,b). Let $(m,n) \in \mathcal{M} \times \mathcal{N}$ such that $p \nmid m+n$, then $((a_m, b_n), (a,b))$ is an arc of $\mathcal{G}_p$.*

Proof. - If the length of this chain is 1, this is clear; if not, let $r \in \mathbb{N}^*$ such that $a_m = a +_p m \cdot_p r$ and $b_n = b +_p n \cdot_p r$ (Lemma 5). Let $\mu \in \mathbb{F}_p^*$ be the class modulo p of $m+n$. If $p|m$ then $a_m = a$ (Lemma 5) and $((a_m, b_n), (a,b))$ is an arc of $\mathcal{G}_p$ since $b_n < b$. If $p \nmid m$ and $p \nmid m+n$, let $\lambda \in \mathbb{F}_p$ $(\lambda \neq 0, 1)$ be the class modulo p of $\frac{m}{m+n}$ then $m \cdot_p r = \lambda \cdot_p s$ and $n \cdot_p r = (1-\lambda) \cdot_p s$ where $s = \mu \cdot_p r$. Thus $((a_m, b_n), (a,b))$ is an arc of $\mathcal{G}_p$. □

We just proved that if $((a_m)_{m \in \mathcal{M}}, (b_n)_{n \in \mathcal{N}})$ is a p-exclusion chain for $a +_p b$ then, for every $(m,n) \in \mathcal{M}^* \times \mathcal{N}^*$, $((a_m, b_n), (a,b))$ is an arc of $\mathcal{G}_p$. Now, in order to prove the converse, we will describe an algorithm looking like the Euclid algorithm for the gcd.

Let u_0, $v_0 \in \mathbb{F}_p^*$ such that $u_0 \neq v_0$. Define u_1, $v_1 \in \mathbb{F}_p^*$ as follows:

- if $u_0 \prec v_0$ then $u_1 = u_0 - v_0$ and $v_1 = v_0$,
- if $v_0 \prec u_0$ then $u_1 = u_0$ and $v_1 = v_0 - u_0$.

Then as long as $u_n \neq v_n$ we define u_{n+1}, $v_{n+1} \in \mathbb{F}_p^*$ as follows:

- if $u_n \prec v_n$ then $u_{n+1} = u_n - v_n$ and $v_{n+1} = v_n$,
- if $v_n \prec u_n$ then $u_{n+1} = u_n$ and $v_{n+1} = v_n - u_n$.

Lemma 6. *There is an integer $N \leq p-2$ such that $u_N = v_N$.*

Proof. If $u_n \neq v_n$ then $u_{n+1} + v_{n+1} = \min(u_n, v_n)$; moreover if $u_n \prec v_n$ then $u_n \prec u_n - v_n = u_{n+1}$ (Lemma 2) and $u_n \prec v_{n+1} (= v_n)$; therefore $\min(u_n, v_n) \prec \min(u_{n+1}, v_{n+1})$ and the sequence $(\min(u_n, v_n))$ is strictly increasing as long as $u_{n-1} \neq v_{n-1}$. Thus:

$$\min(u_0, v_0) \prec \min(u_1, v_1) \prec \cdots \prec \min(u_{N-1}, v_{N-1}) \prec u_N = v_N$$

where $N = 1 + \max\{k \in \mathbb{N} \ ; \ u_k \neq v_k\}$. Finally $N \leq p-2$ because $\min(u_0, v_0) \neq 0$. □

Let $w = u_N = v_N \in \mathbb{F}_p^*$ and define two increasing sequences of natural integers $(\mu_n)_{1 \leq n \leq N+1}$ and $(\nu_n)_{1 \leq n \leq N+1}$ as follows:

$\mu_1 = \nu_1 = 1$ and for $1 \leq n \leq N$,

- if $u_{N-n} \prec v_{N-n}$ then $\mu_{n+1} = \mu_n + \nu_n$ and $\nu_{n+1} = \nu_n$,
- if $v_{N-n} \prec u_{N-n}$ then $\mu_{n+1} = \mu_n$ and $\nu_{n+1} = \mu_n + \nu_n$.

Setting $\mathcal{M} = \{0\} \cup \{\mu_n \ ; \ 1 \leq n \leq N+1\}$ and $\mathcal{N} = \{0\} \cup \{\nu_n \ ; \ 1 \leq n \leq N+1\}$ we get by iteration:

Lemma 7. $\forall \mu \in \mathcal{M}^* \backslash \{1\}$, $\exists \mu' \in \mathcal{M}^*$, $\mu' < \mu$, $\mu - \mu' \in \mathcal{N}$.
$\forall \nu \in \mathcal{N}^* \backslash \{1\}$, $\exists \nu' \in \mathcal{N}^*$, $\nu' < \nu$, $\nu - \nu' \in \mathcal{M}$.

Lemma 8. *For $1 \leq n \leq N+1$, $\mu_n w = u_{N-n+1}$ and $\nu_n w = v_{N-n+1}$.*

Proof. $\mu_1 w = u_N$, $\nu_1 w = v_N$ and for $1 \le n \le N$, we have either $u_{N-n} = u_{N-n+1} + v_{N-n+1}$ and $v_{N-n} = v_{N-n+1}$, or $u_{N-n} = u_{N-n+1}$ and $v_{N-n} = u_{N-n+1} + v_{N-n+1}$. The lemma follows by recurrence. □

Lemma 9. *For* $1 \le n \le N+1$, $p \nmid \mu_n$ *and* $p \nmid \nu_n$.

Proof. Obvious by the preceding lemma. □

Lemma 10. $\mathrm{Card}\mathcal{M}^* + \mathrm{Card}\mathcal{N}^* = N + 1 \le p - 1$.

Proof. For $1 \le n \le N$, $u_n + v_n = \min(u_{n-1}, v_{n-1})$, therefore the sequence $((\mu_n + \nu_n)w)_{1 \le n \le N}$ is strictly decreasing in $\mathbb{F}_p^*$ for the ordering $\prec$. Moreover

$$\mathrm{Card}\mathcal{M}^* + \mathrm{Card}\mathcal{N}^* = \mathrm{Card}(\{w\} \cup \{(\mu_n + \nu_n)w \ ; \ 1 \le n \le N\}). \qquad \square$$

Now we can complete the *Proof of the theorem.* Let $((a',b'), (a,b))$ be an arc of $\mathcal{G}_p$ with $a' = a +_p \lambda \cdot_p r < a$, $b' = b +_p (1-\lambda) \cdot_p r < b$, $\lambda \in \mathbb{F}_p$, $r \in \mathbb{N}^*$. We will construct a p-exclusion chain for $a +_p b$, containing (a',b'), of length $\le p-1$.

If $\lambda = 0$ or 1 there exists such an obvious chain of length 1.

If $\lambda = \frac{1}{2}$, $(p \ge 3)$, $(\{a,a'\},\{b,b'\})$ is such a p-exclusion chain of length 2 for $a +_p b$.

Now we suppose that $\lambda \ne 0, 1, \frac{1}{2}$ and therefore that $p \ge 5$. Writing $r = \sum_{i \ge 0} r_i p^i$ in p-ary, let us recall that i_r denotes the largest index i such that $r_{i_r} \ne 0$. Let $u_0 = \lambda \overline{r_{i_r}} \in \mathbb{F}_p^*$, $v_0 = (1-\lambda)\overline{r_{i_r}} \in \mathbb{F}_p^*$; then $u_0 + v_0 \ne 0$ and $u_0 - v_0 \ne 0$. So we can construct as above the sequences $(u_n)_{0 \le n \le N}$, $(v_n)_{0 \le n \le N}$ with $u_N = v_N = w$, the increasing sequences of integers $(\mu_n)_{1 \le n \le N+1}$, $(\nu_n)_{1 \le n \le N+1}$ with $\mu_1 = \nu_1 = 1$ and their associated sets $\mathcal{M} = \{0\} \cup \{\mu_n ; 1 \le n \le N+1\}$, $\mathcal{N} = \{0\} \cup \{\nu_n \ ; \ 1 \le n \le N+1\}$.

Lemma 11. *The equality* $\mu_{N+1}(1-\lambda) = \nu_{N+1}\lambda$ *holds in* $\mathbb{F}_p^*$.

Proof. By Lemma 8, $\mu_{N+1} w = u_0 = \lambda \overline{r_{i_r}}$ and $\nu_{N+1} w = v_0 = (1-\lambda)\overline{r_{i_r}}$ with $w \ne 0$ and $\overline{r_{i_r}} \ne 0$. □

Thus there exists a unique natural integer R such that $\mu_{N+1} \cdot_p R = \lambda \cdot_p r$ and $\nu_{N+1} \cdot_p R = (1-\lambda) \cdot_p r$.

Lemma 12. $\overline{R_{i_r}} = w$.

Proof. $\mu_{N+1} w = u_0 = \lambda \overline{r_{i_r}} = \mu_{N+1} \overline{R_{i_r}}$ with $p \nmid \mu_{N+1}$. □

For every $(\mu, \nu) \in \mathcal{M} \times \mathcal{N}$, let $a_\mu = a +_p \mu \cdot_p R$ and $b_\nu = b +_p \nu \cdot_p R$.

Lemma 13. *For every* $(\mu,\nu) \in \mathcal{M}^* \times \mathcal{N}^*$, $a_\mu < a$ *and* $b_\mu < b$.

Proof. $a' = a +_p \lambda \cdot_p r < a$ and $b' = b +_p (1-\lambda) \cdot_p r < b$;

$\Longrightarrow \overline{a_{i_r}} + u_0 \prec \overline{a_{i_r}}$ and $\overline{b_{i_r}} + v_0 \prec \overline{b_{i_r}}$ (Lemma 4);

$\Longrightarrow \overline{a_{i_r}} + u_1 \prec \overline{a_{i_r}}$ and $\overline{b_{i_r}} + v_1 \prec \overline{b_{i_r}}$ (Lemma 2);

$\Longrightarrow \overline{a_{i_r}} + \mu_N \overline{R_{i_r}} \prec \overline{a_{i_r}}$ and $\overline{b_{i_r}} + \nu_N \overline{R_{i_r}} \prec \overline{b_{i_r}}$ (Lemmas 8 and 12);

$\Longrightarrow a +_p \mu_N \cdot_p R < a$ and $b +_p \nu_N \cdot_p R < b$ (Lemma 4).
Then we complete the proof by recurrence. $\square$

Now $((a_\mu)_{\mu \in \mathcal{M}}, (b_\nu)_{\nu \in \mathcal{N}})$ is clearly a p-chain of (a, b) (Lemmas 7 and 13), containing (a', b') (Lemma 11), of length $\leq p - 1$ (Lemma 10), which is a p-exclusion chain for $a +_p b$ (Lemma 9).

Remark. 1. In the cases where $p = 2$ or 3, every p-chain of (a, b) of length $\leq p - 1$ is a p-exclusion chain for $a +_p b$.

2. In the case where $p = 5$, a 5-chain of length 4 is not necessarily a 5-exclusion chain; we can however write a complete readable formula of the same kind as Norton's formula for $p = 3$: let $a, b \in \mathbb{N}$; a', a'', a''' (resp. b', b'', b''') are variables taking their values in $\{0, 1, \cdots, a - 1\}$ (resp. $\{0, 1, \cdots, b - 1\}$); let us consider the sets:
$$\begin{aligned}
S_1(a,b) &= \{a' +_5 b\} \\
S_2(a,b) &= \{a' +_5 b' \; ; \; a' +_5 b = a +_5 b'\} \\
S_3(a,b) &= \{a' +_5 b'' \; ; \; \exists b', a +_5 b' = a' +_5 b, \; a +_5 b'' = a' +_5 b'\} \\
S_4(a,b) &= \big\{a' +_5 b''' ; \exists b'', a' +_5 b'' \in S_3(a,b), a +_5 b''' = a' +_5 b''\big\} \\
&\quad \cup \big\{a' +_5 b''' \; ; \; \exists a'', b', (a', b') \in S_2(a,b), \\
&\qquad\qquad a'' +_5 b = a' +_5 b', a +_5 b''' = a'' +_5 b'\big\}
\end{aligned}$$
and let $S_i = S_i(a, b) \cup S_i(b, a)$, for $i = 1, 2, 3, 4$.
Then $a +_5 b = \min \mathbb{N} \backslash (S_1 \cup S_2 \cup S_3 \cup S_4)$.

3. Given a natural integer $\nu \geq 2$ not necessarily prime and two natural numbers a, b, let us generalize the definition of the p-exclusion set $E_p(a, b)$ of (a, b) replacing p by ν in the previous definition.

   Thus a ν-exclusion chain $((a_m)_{m \in \mathcal{M}}, (b_n)_{n \in \mathcal{N}})$ of (a, b) is of length $\leq \nu - 1$ and such that $\forall\, m \in \mathcal{M}^*$, $\forall\, n \in \mathcal{N}^*$, $\nu \nmid m$ and $\nu \nmid n$. Then setting $a *_\nu b = \min(\mathbb{N} \backslash E_\nu(a, b))$, $*_\nu$ is a group law on $\mathbb{N}$ if and only if ν is a prime number.

   Proof. In fact if ν is a composite number then $*_\nu$ is not an associative law. Let d be a proper divisor of ν; the following equalities hold:
   $(d - 1) *_\nu 1 = d$,
   $(\nu - 1) *_\nu 1 = 0$,
   $(\nu - d) *_\nu d' = \nu - (d - d')$ for all $d' < d$
   and $(\nu - d) *_\nu d = \nu$ because $((\nu - d, \nu - 2d, \cdots, 0), (d, 0))$ is a ν-exclusion chain of length $\leq \nu - 1$. Therefore: $((\nu - d) *_\nu (d - 1)) *_\nu 1 = 0$ and: $(\nu - d) *_\nu ((d - 1) *_\nu 1) = \nu$. $\square$

4. If we replace in the definition of $*_\nu$ the previous conditions $(m, n) \in \mathcal{M}^* \times \mathcal{N}^* \Longrightarrow \nu \nmid m$ and $\nu \nmid n$ by ν is relatively prime to m and n, then we get $*_\nu = +_p$ where p is the smallest prime divisor of ν.

Acknowledgments. I thank T. Moreno and P. Segalas, students at the University of Limoges, for testing several algorithms in Turbo Pascal on a PC.

REFERENCES

[1] C. L. Bouton, *Nim, a game with a complete mathematical theory.* Ann. Math. Princeton **3** (1902), 35–39.

[2] J. H. Conway, N.J.A. Sloane, *Lexicographic Codes, Error Correcting Codes from Game Theory.* IEEE Trans. Inform. Theory **32** (1986), 337–348.

[3] S. Eliahou, M. Kervaire, *Sumsets in vector spaces over finite fields.* J. Number Theory **71** (1998), 12–39.

[4] F. Laubie, *On linear greedy codes.* to appear.

[5] H. W. Lenstra, *Nim Multiplication.* Séminaire de Théorie des Nombres de Bordeaux 1977-78, exposé 11, (1978).

[6] V. Levenstein, *A class of Systematic Codes.* Soviet Math Dokl. **1** (1960), 368–371.

[7] S. Y. R. Li, *N-person Nim and N-person Moore's Games.* Int. J. Game Theory **7** (1978), 31–36.

[8] E. H. Moore, *A generalization of the Game called Nim.* Ann. Math. Princeton **11** (1910), 93–94.

François LAUBIE
UPRESA CNRS 6090 et INRIA de Rocquencourt
Département de Mathématiques
Faculté des Sciences de Limoges
123, avenue Albert Thomas
87060 LIMOGES Cedex
E-mail : `laubie@unilim.fr`