FRANÇOIS LAUBIE

A recursive definition of $p$-ary addition without carry


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

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

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 $(\mathbb{Z}/p\mathbb{Z})^N$.
with given cardinalities (S. Eliahou, M. Kervaire, [3]). In [5] H.W. Lenstra announced the following formula due to S. Norton:

\[ a +_p b = \min(\mathbb{N}\backslash\{a +_p b, a +_p b' ; a' < a, b' < b\} \cup \{a'' +_p b'' ; a'' < a, b'' < b, a'' +_p b = a +_p b''\})) \]

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 \(\bar{\lambda}\) be the representative number of the class \(\lambda\) belonging to \(\{0, 1, \ldots, p - 1\}\) and, for \(a \in \mathbb{N}\), define \(\lambda \cdot_p a = \bar{\lambda} \cdot_p a = a +_p a +_p \cdots +_p a\) with \(\bar{\lambda}\) 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 \(G_p\) as follows:
- the set of its vertices is \(\mathbb{N} \times \mathbb{N}\),
- the arcs of \(G_p\) 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 \(G_p\) does not admit circuit; thus the Grundy function of \(G_p\) is the unique map \(g\) of \(\mathbb{N} \times \mathbb{N} \to \mathbb{N}\) such that:

\[ g((a, b)) = \min(\mathbb{N}\backslash\{g((a', b')) ; ((a', b'), (a, b)) \text{ is an arc of } G_p\}) \]

**Proposition 1.** The Grundy function of \(G_p\) 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 \(\{0, 1, \ldots, p - 1\}\) of \(\mathbb{F}_p\). It is sometimes more convenient to express them in terms of the following ordering on \(\mathbb{F}_p\):

\[ u < v \iff \bar{u} < \bar{v} \]

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

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

\[ u + v = \bar{u} + \bar{v} = \begin{cases} \bar{u} + \bar{v} & \text{if } \bar{u} + \bar{v} \leq p - 1, \\ \bar{u} + \bar{v} - p & \text{if } \bar{u} + \bar{v} \geq p. \end{cases} \]

Thus \(u + v < u \iff \bar{u} + \bar{v} \geq p \iff u + v < v\).

**Lemma 2.** Let \(u, r, s\) be elements of \(\mathbb{F}_p\) such that \(r < s\) and \(u + r < u\). Then \(r < r - s\) and \(u + r - s < u\).
Lemma 3. Let $u, v, r$ be elements of $\mathbb{F}_p$ such that $u < u + r$, $v < v + r$ and $u + v + r < u + v$. Then there exist $s, t \in \mathbb{F}_p$ such that $s + t = r$, $u + s < u$ and $v + t < v$.

Proof. Conditions:

\[
\begin{align*}
\text{(C)} & \\
& \begin{cases}
    u + v + r < u + v, \\
    u < u + r, \\
    v < v + r,
\end{cases}
\end{align*}
\]

are equivalent to:

\[
\begin{align*}
& \begin{cases}
    \bar{u} + \bar{v} + \bar{r} \geq p, \\
    \bar{u} + \bar{r} \leq p - 1, \\
    \bar{v} + \bar{r} \leq p - 1.
\end{cases}
\end{align*}
\]

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

\[
\begin{align*}
& \begin{cases}
    p - \bar{u} - \bar{v} \leq \bar{r} \leq p - 1, \\
    1 \leq \bar{r} \leq p - 1 - \bar{u}, \\
    1 \leq \bar{r} \leq p - 1 - \bar{v},
\end{cases}
\end{align*}
\]

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

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

\[
\begin{align*}
\begin{cases}
s + t &= r \\
u + s &< u \\
v + t &< v
\end{cases}
\end{align*}
\]

or equivalently such that:

\[
\begin{align*}
\begin{cases}
\sigma + \tau = \rho, \\
1 \leq \sigma \leq \bar{u} \leq p - 1, \\
1 \leq \tau \leq \bar{v} \leq p - 1
\end{cases}
\end{align*}
\]

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

Now, for any natural integer $x$, let $\bar{x}$ be its class modulo $p$, let $x = \sum_{i>0} x_ip^i$ 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) \( x_{i_y} + y_{i_y} < x_{i_y} \),

(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 \( a + p \lambda \cdot r < a \) and \( b + p (1 - \lambda) \cdot r < b \). With the notations of Lemma 4, we have:

\[
\begin{align*}
a + p b + p r < a + p b & \iff a_{i_r} + b_{i_r} + r_{i_r} < a_{i_r} + b_{i_r}, \\
\lambda < a + p r & \iff \lambda a_{i_r} < a_{i_r} + r_{i_r}, \\
b < b + p r & \iff b_{i_r} < b_{i_r} + r_{i_r}. 
\end{align*}
\]

There exist \( s, t \in \mathbb{F}_p \) such that \( r_{i_r} = s + t, a_{i_r} + s < a_{i_r} \) and \( b_{i_r} + t < b_{i_r} \). Let \( \lambda = s \cdot r_{i_r}^{-1} \in \mathbb{F}_p \); then: \( s = \lambda r_{i_r}, t = (1 - \lambda) r_{i_r}, \lambda a_{i_r} + \lambda r_{i_r} < a_{i_r} \) and \( b_{i_r} + (1 - \lambda) r_{i_r} < b_{i_r} \); in other words: \( a + p \lambda \cdot r < a \) and \( b + p (1 - \lambda) \cdot r < b \). This means that \( (a, b) \mapsto a + p b \) is the Grundy function of \( G_p \).

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

Proof. Let \( c = \max([0, a] + [0, b]) \) and let \( a_1 \leq a, b_1 \leq b \) such that \( c = a_1 + b_1 \). 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 \( d \in [0, a] + [0, b] \). \(\square\)

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

1. \( E_2 = \{ a + 2 b', a' + 2 b \mid a' < a, b' < b \} \),
2. \( E_3 = \{ a + 3 b', a' + 3 b \mid a' < a, b' < b \} \cup \{ a'' + 3 b'', a'' < a, b'' < b, a + 3 b'' = a'' + 3 b \} \) 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 \( a + p b = \min(\mathbb{N} \setminus E_p) \) will be effectively recursive only when we can describe the set \( E_p \) using only pairs \( (a, b) \in \mathbb{N} \times \mathbb{N} \) with \( a \leq a, \beta \leq b \) and \( (a, \beta) \neq (a, b) \).

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 \( S \subseteq \mathbb{N} \), \( S^* \) means \( S \setminus \{0\} \).

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:

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

**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 \( \geq 3\), 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: \( a +_p b = \min(\mathbb{N} \setminus E_p(a, b)). \)

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

**Proof.** Let \( r \in \mathbb{N}^* \) such that \( a_1 = a +_p r; \) then \( a +_p b_1 = a_1 +_p b = a +_p r +_p b_1 \), 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 \( a_k = a +_p k \cdot p \cdot r \) and \( b_\ell = b +_p \ell \cdot p \cdot r, \) then there exists \( k_0 \in \mathcal{M} \) such that \( 1 \leq k_0 \leq m - 1, \ m - k_0 \in \mathcal{N} \) and \( a_m +_p b = a_{k_0} +_p b_{m-k_0} = a +_p k_0 \cdot p \cdot r +_p b +_p (m - k_0) \cdot p \cdot r = a +_p b +_p m \cdot p \cdot r. \)
Therefore \( a_m = a + p \cdot m \cdot p \cdot r \) and the lemma is proved by recurrence.

\[ \Box \]

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

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

We just proved that if \((a_m)_{m \in M}, (b_n)_{n \in N}\) is a p-exclusion chain for \(a + p \cdot b\) then, for every \((m, n) \in M^* \times N^*\), \((a_m, b_n), (a, b)\) is an arc of \(G_p\).

Now, in order to prove the converse, we will describe an algorithm looking like the Euclid algorithm for the gcd.

Let \(u_0, v_0 \in F_p^*\) such that \(u_0 \neq v_0\). Define \(u_1, v_1 \in F_p^*\) as follows:
- If \(u_0 < v_0\) then \(u_1 = u_0 - v_0\) and \(v_1 = v_0\),
- If \(v_0 < u_0\) then \(u_1 = u_0\) and \(v_1 = v_0 - u_0\).

Then as long as \(u_n \neq v_n\) we define \(u_{n+1}, v_{n+1} \in F_p^*\) as follows:
- If \(u_n < v_n\) then \(u_{n+1} = u_n - v_n\) and \(v_{n+1} = v_n\),
- If \(v_n < u_n\) 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 \(u_n < v_n\) then \(u_n < u_n - v_n = u_{n+1} = v_n\) (Lemma 2) and \(u_n < v_{n+1} = v_n\); therefore \(\min(u_n, v_n) < \min(u_{n+1}, v_{n+1})\) and the sequence \((\min(u_n, v_n))\) is strictly increasing as long as \(u_n \neq v_n\). Thus:

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

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

Let \(w = u_N = v_N \in F_p^*\) 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:
- \(\mu_1 = v_1 = 1\) and for \(1 \leq n \leq N\):
- If \(u_{N-n} < u_{N-n}\) then \(\mu_{n+1} = \mu_n + \nu_n\) and \(\nu_{n+1} = \nu_n\),
- If \(v_{N-n} < u_{N-n}\) then \(\mu_{n+1} = \mu_n\) and \(\nu_{n+1} = \mu_n + \nu_n\).

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

**Lemma 7.** \(\forall \mu \in M^* \setminus \{1\}, \exists \mu' \in M^*, \mu' < \mu, \mu - \mu' \in N\).
\(\forall \nu \in N^* \setminus \{1\}, \exists \nu' \in N^*, \nu' < \nu, \nu - \nu' \in M\).

**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 $1 \leq n \leq N$, 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 $1 \leq n \leq N+1$, $p \mid \mu_n$ and $p \mid \nu_n$.  

Proof. Obvious by the preceding lemma.

Lemma 10. $\text{Card}M^* + \text{Card}N^* = N + 1 \leq p - 1$.  

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

Now we can complete the proof of the theorem. Let $((a', b'), (a, b))$ be an arc of $G_p$ with $a' = a +_p \lambda \cdot p \cdot r < a$, $b' = b +_p (1 - \lambda) \cdot p \cdot r < b$, $\lambda \in F_p$, $r \in N^*$. We will construct a $p$-exclusion chain for $a +_p b$, containing $(a', b')$, of length $\leq p - 1$.

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

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

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

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

Proof. By Lemma 8, $\mu_{N+1}w = u_0 = \lambda \overline{a_r}$ and $\nu_{N+1}w = v_0 = (1 - \lambda) \overline{b_r}$ with $w \neq 0$ and $\overline{b_r} \neq 0$.

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

Lemma 12. $\overline{R_r} = w$.  

Proof. $\mu_{N+1}w = u_0 = \lambda \overline{a_r} = \mu_{N+1} \overline{R_r}$ with $p \mid \mu_{N+1}$.

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

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

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

$\Rightarrow a_r + u_0 < a_r$ and $b_r + v_0 < b_r$ (Lemma 4);  

$\Rightarrow a_r + u_1 < a_r$ and $b_r + v_1 < b_r$ (Lemma 2);  

$\Rightarrow a_r + \mu_N \overline{R_r} < a_r$ and $b_r + \nu_N \overline{R_r} < b_r$ (Lemmas 8 and 12);
\[ \Rightarrow a + p \mu_N \cdot _p R < a \text{ and } b + p \nu_N \cdot _p R < b \text{ (Lemma 4)}. \]

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 \(a, b \in \mathbb{N}; a', a'', a''', \ldots, a - 1\) (resp. \(b', b'', b''', \ldots, b - 1\)) be variables taking their values in \(\{0, 1, \ldots, a - 1\}\) (resp. \(\{0, 1, \ldots, b - 1\}\)); let us consider the sets:

\[
\begin{align*}
S_1(a, b) &= \{a' + b\} \\
S_2(a, b) &= \{a' + 5b'; a' + 5 b = a + 5 b'\} \\
S_3(a, b) &= \{a' + 5b'; \exists b', a + 5 b' = a' + 5 b, a + 5 b'' = a' + 5 b'\} \\
S_4(a, b) &= \{a' + 5 b''; \exists b'', a' + 5 b'' \in S_3(a, b), a + 5 b''' = a' + 5 b''\} \\
&\cup\{a' + 5 b''' ; \exists a''', b', (a', b') \in S_2(a, b), a'' + 5 b = a' + 5 b', a + 5 b''' = a'' + 5 b'\}
\end{align*}
\]

and let \(S_i = S_i(a, b) \cup S_i(b, a)\), for \(i = 1, 2, 3, 4\).

Then \(a + 5 b = \min(\mathbb{N}(S_1 \cup S_2 \cup S_3 \cup S_4))\).

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 \(\nu\) in the previous definition.

Thus a \(\nu\)-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 \(a *_\nu b = \min(\mathbb{N}\setminus E_\nu(a, b))\), \(_*\nu\) is a group law on \(\mathbb{N}\) if and only if \(\nu\) is a prime number.

**Proof.** In fact if \(\nu\) is a composite number then \(_*\nu\) is not an associative law. Let \(d\) be a proper divisor of \(\nu\); the following equalities hold:

\[
\begin{align*}
(d - 1) *_\nu 1 &= d, \\
(\nu - 1) *_\nu 1 &= 0, \\
(\nu - d) *_\nu d' &= \nu - (d - d') \text{ for all } d' < d \\
\text{and } (\nu - d) *_\nu d &= \nu \text{ because } ((\nu - d, \nu - 2d, \cdots, 0), (d, 0)) \text{ is a } \nu\text{-exclusion chain of length } \leq \nu - 1. \text{ Therefore: } ((\nu - d) *_\nu (d - 1)) *_\nu 1 &= 0 \\
\text{and: } (\nu - d) *_\nu ((d - 1) *_\nu 1) &= \nu. \quad \square
\end{align*}
\]

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


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