Facultad de Ciencias Naturales y Exactas
Universidad del Valle

p-cycles, S_2-sets and Curves with Many Points

Álvaro Garzón R.
Universidad del Valle

Received: December 16, 2016 Accepted: June 13, 2017

Pag. 55-78

Abstract

We construct S_2-sets contained in the integer interval $I_{q-1} := [1, q-1]$ with $q = p^n$, p a prime number and $n \in Z^+$, by using the p-adic expansion of integers. Such sets come from considering p-cycles of length n. We give some criteria in particular cases which allow us to glue them to obtain good S_2-sets. After that we construct algebraic curves over the finite field $\mathbb{F}_q$ with many rational points via minimal ($\mathbb{F}_p$, $\mathbb{F}_p$)-polynomials whose exponent set is an S_2-set.

Key words: p-adic expansion, S_2-sets, finite field, Kummer cover, rational points.

Doi: http://dx.doi.org/10.25100/rc.v21i1.6340

1 Introduction

Let p be a prime number and $\mathbb{F}_q$ be a finite field with $q = p^n$ elements and let $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. Given a polynomial $f\ (x, y) \in \mathbb{F}_q\ [x, y]$ which is irreducible over $\overline{\mathbb{F}}_q$, the set

$$\mathfrak{C}f = \{(\alpha, \beta) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}q \text{ such that } f\ (\alpha, \beta) = 0\},$$

is an affine plane algebraic curve (over the finite field $\overline{\mathbb{F}}_q$) and the points $P = (\alpha, \beta) \in \mathfrak{C}f$ such that $(\alpha, \beta) \in \mathbb{F}_q\ x\ \mathbb{F}_q$ are called rational points over $\mathbb{F}_q$.

In 1940 A. Weil proved the Riemann hypothesis for curves over finite fields. As an immediate corollary he obtained an upper bound for the number of rational points on a geometrically irreducible nonsingular curve $\mathfrak{C}$ of genus $g(\mathfrak{C})$ over a finite field of cardinality q, namely

$$\#\mathfrak{C}(\mathbb{F}_q) \leq q + 1 + 2g(\mathfrak{C})\sqrt{q}, \quad (*)$$

where $\mathfrak{C}(\mathbb{F}_q)$ denotes the set of rational points of the curve $\mathfrak{C}$. If the cardinality of the finite field is not a square, the upper bound above was improved by Serre [1] substituting $2g\sqrt{q}$ by its integer part $[2g\sqrt{q}]$. If the cardinality is a square, (say $q = r^2$), then the $\mathfrak{C}$ curve is called *maximal over* $\mathbb{F}_{r^2}$ if $\#\mathfrak{C}(\mathbb{F}_q)$ attains the Weil's upper bound; i.e., $\#\mathfrak{C}(\mathbb{F}_q) = r^2 + 1 + 2rg(\mathfrak{C})$.

The interest in curves over finite fields with many rational points with respect to their genera (i.e., with $\#\mathfrak{C}.(\mathbb{F}_q)$) close to known upper bounds; e.g., see tables in [2] and [3] was greatly renewed after algebraic geometry codes (AG codes) were introduced by Goppa in [4]. Many constructions of curves over finite fields are often performed by using special polynomials $p(x) \in \mathbb{F}_q[x]$. The essential properties of $p(x)$ are sometimes of the following form:

Property I. One has that $p(\mathbb{F}_q) \subseteq \mathbb{F}_p$, and for most elements $\alpha \in \mathbb{F}_q, \alpha$ is a simple root of $p(x) - p(\alpha)$.

Property II. The set $\Sigma = \{\gamma \in \overline{\mathbb{F}}_q;\ p(x) - \gamma$ has multiple roots in $\overline{\mathbb{F}}_q\}$ has low cardinality, and one has a nice description of the multiplicities of the roots.

Polynomials satisfying property $p(\mathbb{F}_q) \subseteq \mathbb{F}_p$ are known as $(\mathbb{F}_p, \mathbb{F}_p)$-polynomials. A particular case of $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials, which are studied in detail in [5], are the so-called *minimal* $(\mathbb{F}_q, \mathbb{F}_p)$-polynomials; i.e., ($\mathbb{F}_q$,$\mathbb{F}_p$)-polynomials whose degree is $\leq q-1$ and whose exponent set is characterized as being the p-cycles (also introduced in [5]) of the integer interval $[1, q-1]$. We point out that in many cases the exponent set $\mathfrak{S}$ of a minimal $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial has a nice property that has been extensively studied in number theory, namely the S_2 property. More precisely: A subset $\mathfrak{S}$ of integers is an S_2-set (or has the S_2 property) if all the sums $a + a'$ with $a \neq a'$; $a, a' \in \mathfrak{S}$ are distinct.

It is known that if $\mathfrak{S} \subseteq [1, M]$ is an S_2-set, then its cardinality must be asymptotically equal to$\sqrt{M}$, see [6]. As we remarked above in many cases the p-cycles of the integer interval $[1, q-1]$ are S_2-sets, unfortunately its cardinality which is a divisor of n is almost always small respect to $\sqrt{q-1}$. The goal in this work is: firstly, provide some criteria to glue a set of S_2 p-cyles; i.e., p-cyles such that the underlying set has the S_2 property, to obtain S_2-sets whose cardinality is close to $\sqrt{q-1}$; secondly, use some of these S_2 sets obtained to construct algebraic curves $\mathfrak{C}$ over the finite field $\mathbb{F}_q$ whose set of rational points $\mathfrak{C}(\mathbb{F}_q)$ has cardinality close to know upper bounds. Again, we refer to [2] and [3].

The paper is organized as follows: In section 2 we give a brief exposition of some properties of p-cycles. We show how these can be constructed from a generator element. Section 3 contains some results which allow us to decide when a number $i \in I_{q-1} := [1, q-1]$ generates an S_2 p-cycle. We give some criteria to glue some of them and then, obtain sets with a good cardinality. Many examples are included. Section 4 is devoted to study a few particular cases to obtain good S_2 sets. Finally, in section 5 we construct Kummer covers of the projective line over finite fields with many rational points. The idea comes from [7] and that is the construction of

rational functions $\mu(x) \in \mathbb{F}_q\ (x)$ having the value 1 for many elements $\alpha \in \mathbb{F}_q$, such rational functions in our case are induced by $(\mathbb{F}_p,\mathbb{F}_p)$-polynomials whose exponent sets are S_2 sets constructed in section 4.

2 p-Cycles

Let p be a prime number and let $q = p^n$ be a non-negative power of p. The *p-adic expansion* of a positive integer a in the integer inter*val* $I_{q-1} := [1, q-1]$ is given by:

$$a = k_0 + k_1 p + k_2 p^2 + \cdots + k_{n-1} p^{n-1},$$

where the numerals k_j *satisfies* $0 \leq k_j < p$ for $j = 0, \cdots, n-1$.

If each $a = k_0 + k_1 p + k_2 p^2 + \cdots + k_{n-1} p^{n-1} \in I_{q-1}$ is represented by the n-tuple $(k_0, k_1, \ldots, k_{n-1}) \in \mathbb{F}_p^n$, then we denote by $a^{\sqcap}$, the integer number obtained after applying *the cyclic numeral-permutation:*

$$a^{\sqcap} = k_{n-1} + p\, k_0 + p^2\, k_1 + \cdots + p^{n-1}\, k_{n-2}.$$

By $\sqcap^k$ we will understand the iteration k times the cyclic numeral-permutation. The p-adic *period* of a is the small natural integer $l(a)$ such that $a^{\sqcap^{l(a)}} = a$ and it is clear that the period of an integer number a depends of p and n.

A *p-cycle* $\mathfrak{J}$ is an ordered set $\mathfrak{J} = (a, a^{\sqcap}, a^{\sqcap^2} \ldots, a^{\sqcap^{l(a)-1}})$, we will denote by $l(\mathfrak{J})$, the length of $\mathfrak{J}$ and is defined by $l(\mathfrak{J}) = l(a)$, (see [5] for more details).

Example 2.1 Let $p = 2$ and $n = 4$. The number $3 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 0 \cdot 2^2$ corresponds to the 4-tuple (1,1,0,0). Therefore $3^{\sqcap} = 0 \cdot 2^0 + 1 \cdot 2^1 + 1 \cdot 2^2 + 0 \cdot 2^2 = 6$, $6^{\sqcap} = 12$, $12^{\sqcap} = 9$. Consequently (3,6,12,9) is a 2-cycle of length 4. The element $3 \in [1.15]$ has period 4. On the other hand, if $n = 7$, then the ordered set (3,6,12,24,48,96,65) is a 2-cycle of length 7 and the element $3 \in [1.127]$ has period 7.

Since the process of determining p-cycles in I_{q-1} play an important role in this work, we will study some properties in detail.

Let $G = \langle \sigma \rangle$ be the cyclic group of order n. The group G acts on the set I_{q-1} as follows:

$$\rho: G \times I_{q-1} \longrightarrow I_{q-1}$$

$$(\sigma^k, i) \longmapsto (p^k \cdot i)_{q-1} \quad k = 0,1,\ldots,n-1$$

where $(a)_{q-1}$ is a representative for the residual class of a modulus $q-1$.

Theorem 2.1 *For each $i \in I_{q-1}$, the p-cycle $(i, i^{\sqcap}, i^{\sqcap^2} \ldots, i^{\sqcap^{l(i)-1}})$ is the orbit of i with respect to the action ρ above.*

Proof: Observe that if $i = i_0 + i_1 p + i_2 p^2 + \cdots + i_{n-1}\, p^{n-1}$ is the p-adic expansion of i, then

$$i^{\sqcap} = i_{n-1} + i_0 p + i_1\, p^2 + \cdots + i_{n-2}\, p^{n-1}.$$

Hence

$$pi - i^{\sqcap} = i_0 p + i_1\, p^2 + \cdots + i_{n-1} p^n - (i_{m-1} + i_0 p + i_1\, p^2 + \cdots + i_{0n-2} p^{n-1})$$
$$= i_{n-1}(q - 1),$$

consequently $i^{\sqcap} \equiv pi \pmod{(q-1)}$.

Corollary 2.1 *If $q = p^n$ and $\Im$ is a p-cycle, then $l(\Im)|n$.*

Proof: We known that if G acts on a set S, then $G_x = \{g \in G \mid g \cdot x = x\}$ is a subgroup of G and the cardinal number of the orbit $\overline{x} = \{g \cdot x \mid g \in G\}$ of x, is $(G: G_x)$ the index of G_x in G. [8], II,4.3.

Proposition 2.1 *Every p-cycle has the form*

$$\Im = (i, pi, \ldots, p^k i, (p^{k+1} i)_{q-1}, \ldots, (p^{\ell} i)_{q-1})$$

where $\ell + 1$ is the length of $\Im$ and $k > 0$ is the smallest integer satisfying $p^k i < q - 1 \leq p^{k+1} i$.

Proof: Since

$$p^{k+j} i = r(q-1) + (p^{k+j} i)_{q-1},$$

then

$$p^{k+j+1} i = p(p^{k+j} i) = (rp + m)(q-1) + (p(p^{k+j} i)_{q-1})_{q-1}$$

where

$$p(p^{k+j} i)_{q-1} = m(q-1) + (p(p^{k+j} i)_{q-1})_{q-1}.$$

Hence,

$$(p^{k+j+1} i)_{q-1} = (p(p^{k+j} i)_{q-1})_{q-1}.$$

Remark 2.1 In accordance with Proposition (2.1), one can see that a p-cycle $\Im = (i, pi, \ldots p^k i, (p^{k+1} i)_{q-1}, \ldots, (p^{\ell} i)_{q-1})$, is nothing but the cyclotomic coset of i mod$(q-1)$. Cyclotomic cosets mod(N) play an important role in the factorization in $\mathbb{F}_p[x]$ of the polynomial $x^N - 1$ and consequently in coding theory. We refer to [9] for details.

Example 2.2 In the following Tables 1, 2 and 3 we exhibit the different p-cycles for $p = 2.3$ and $q = p^n$ for some values of n.

Table 1. 2-*cycles of length 1, 2, 3 and 6.*

$q = 2^6 = 64$	(63)	(21,42)
	(9,18,36)	(27,54,45)
	(1,2,4,8,16,32)	(3,6,12,24,48,33)
	(5,10,20,40,17,34)	(7,14,28,56,49,35)
	(11,22,44,25,50,37)	(13,26,52,41,19,38)
	(15,30,60,57,51,39)	(23,46,29,58,43,53)
	(31,62,61,59,55,47)	

Table 2. 3-*cycles of length 1 and 3.*

$q = 3^3 = 27$	(13)	(26)		
	(1,3,9)	(2,6,18)	(4,12,10)	(5,15,19)
	(7,21,11)	(8,24,20)	(14,16,22)	(17,25,23)

Table 3. 3-*cycles of length 1, 2 and 4.*

$q = 3^4 = 81$	(40)	(80)	
	(10,30)	(20,60)	(50,70)
	(1,3,9,27)	(2,6,18,54)	(4,12,36,28)
	(5,15,45,55)	(7,21,63,29)	(8,24,72,56)
	(11,33,19,57)	(13,39,37,31)	(14,42,46,58)
	(16,48,64,32)	(17,51,73,59)	(22,66,38,34)
	(23,69,47,61)	(25,75,65,35)	(26,78,74,62)
	(41,43,49,67)	(44,52,76,68)	(53,79,77,71)

Observe for example, that for $q = 64$ not all 2-cycle has length 6. The following proposition says when these situations occur. Before that we introduce a convenient notation. Although it is true that we can obtain a p-cycle from any of its elements, we will say that an integer i generates the p-cycle $\mathfrak{I}$ if

$$\mathfrak{I} = (i, pi, \ldots, p^k i, (p^{k+1} i)_{q-1}), \ldots, (p^{\ell} i)_{q-1}),$$

and $i < (p^{k+j} i)_{q-1}$ for $j = 1, \ldots, \ell - k$. In this case we write $\mathfrak{I} = \langle i \rangle$.

Proposition 2.2 *Let $q = p^n$ with $n = m \cdot l$. If $\mathfrak{I} = \langle i \rangle$, then $l = l(\mathfrak{I}) < n$ if and only if i is a multiple of $\sum_{j=0}^{m-1} p^{\ell \cdot j}$.*

Proof: By definition, ℓ = length($\mathfrak{I}$) if and only if, $p^{\ell} i = (q-1)h_{\ell} + i$ if and only if,

$$i = \left(\sum_{j=0}^{m-1} p^{\ell \cdot j} \right) h_{\ell}$$

Proposition 2.3 *The greatest integer $i \in I_{q-1}$ such that i generates a p-cycle of length n, is $i = p^n - (p^{n-1} + 1)$. The corresponding p-cycle is,*

$$(p^n - (p^{n-1} + 1), p^n - (p^0 + 1), p^n - (p + 1), p^n - (p^2 + 1), \ldots, p^n - (p^{n-2} + 1)).$$

Proof: First observe that

$$pi \;=\; p\cdot(\,p^{n}-p^{n-1}p\;-1)\;=\;(q-1)(p-1)-1\;\equiv\;(q-2)\;(\mathrm{mod}\;\;q-1).$$

Hence $p^2 i \equiv q-p-1(\mathrm{mod}\; q-1)$, so in general, $p^k i \equiv q-(p^{k-1}+1)(\mathrm{mod}\; q-1)$ which leads to the desired expression. Secondly, each number $i<j<q-1$ can be rewritten as $j=(q-1)-(p^{n-1}-k-1)$ with $0\le k\le p^{n-1}-2$. Now, the equation $px-(q-1)t=j$ with $0\le t\le p-1$ has unique solution in I_{q-1} which implies that j is the remainder modulus $q-1$ of some $x\in I_{q-1}$.

Remark 2.2 Is know that, if $\alpha \;=\; \beta^{i}\in\;\mathbb{F}_q=\mathbb{F}_p\,(\beta)$ and $m_\alpha(x)$ is its minimal polynomial, then

$$m_\alpha(x)=\prod_{t\in\langle i\rangle}(x-\beta^{t}),$$

(Cf [10], Theorem 4.1). Hence one can determine the number of p-cycles of length $d|n$ in I_{q-1}, such number is:

$$N_q\,(d)=\frac{1}{d}\sum_{d'|d}\mu\,(d')q^{d/d'}$$

(here $\mu(\cdot)$ is the Moebius function), as many as irreducible polynomials of degree d in $\mathbb{F}_p[x]$.

3 S_2- Sets

A subset $\mathfrak{S}$ of integers is an S_2-set if all the sums $a+a'$ with $a\neq a'; a,a';\in\mathfrak{S}$ are distinct. From now on, a set $\mathfrak{S}$ has the S_2 property if $\mathfrak{S}$ is an S_2-set. Similarly, a p-cycle $\Im\;=(\iota_1,\ldots,\iota_l)$ is an S_2 p-cycle if the underlying set $(\iota_1,\ldots,\iota_l)$ has the S_2 property. In this section we give some criteria that allows us to decide when a p-cycle $\Im=\langle i\rangle$ has the S_2 property. Also, we give conditions on the generators of a set of S_2 p-cycles such that the union of these retain this property.

Theorem 3.1 *If GCD* $(i,q-1)\;=\;1$, *then* $\Im=\langle i\rangle$ is an S_2 p-cycle.

Proof: Assume the contrary, so there exist integers $0\le r,s,u,v\le n-1$ such that

$$(p^{r}\,i)_{q-1}+(p^{s}\,i)_{q-1}=(p^{u}\,i)_{q-1}+(p^{v}\,i)_{q-1}\qquad r\;<\;s,u\;<\;v. \tag{1}$$

If $r=\min\{r,u\}$, then (1) implies $(p^{v-r}\;+\;p^{u-r}\;-p^{s-r}\;-1)\;\equiv\;0\;(\mathrm{mod}\;\;q-1)$ which is absurd.

Remark 3.1 The reciprocal of Theorem 5.1 is false, in fact if $p=3$ and $n=5$, then is easily proved that the 3-cycle generated by the divisor 11 of 242, $(11,33,99,55,165)$ has the S_2 property.

Corrollary 3.1 *If* $q-1$ *is a prime number, then any p-cycle is an* S_2*-set.*

Example 3.1 The following Table shows all the 2-cycles of length 5 which, by 3.1 are S_2-sets contained in the integer interval [1.31].

Table 4. *S_2 2-cycles of length 5.*

$(1,2,4,8,16)$	$(3,6,12,24,17)$	$(5,10,20,9,18)$
$(7,14,28,25,19)$	$(11,22,13,26,21)$	$(15,30,29,27,23)$

The next corollary give us information about the components of a p-cycle $\langle i \rangle$ when $i|q-1$. More precisely.

Corollary 3.2 Let $i|q-1$ and $\Xi = \langle i \rangle$, *then all its components are multiples of* i.

Proof: By Proposition (2.1), each component of Ξ has the form $(p^j i)_{q-1} = p^j i - (q-1)h_j$.

Remark 3.2 Let us consider the S_2 3-cycle of length $5, \Xi = (11,33,99,55,165)$ generated by 11, divisor of $242 = 3^5 - 1$ contained in the interval [1, 242]. It is clear that its cardinality 5 is very small respect to $\sqrt{242} \approx 15$ even so in accordance with the previous corollary, if we cancel the common factor 11 of each member of the 3-cycle Ξ, we obtain the set $\mathfrak{S}$ ={1, 3, 9, 5, 15} which is again an S_2-set although it is not the underlying set of a 3-cycle. The important fact here is that the cardinality of $\mathfrak{S}$ is 5 and now we have a nice S_2-set in the interval $[1,15]$ whose cardinality is now very good respect to $\sqrt{15} \approx 4$. We can obtain each member of this set as follows.

Corollary 3.3 *Let* $i \in [1, q-1]$, $d = GCD(i, q-1)$ *and* $\Xi = \langle i \rangle$,*The set obtained by canceling the common factor* d *to each component of* Ξ *has the for:*

$$\mathfrak{S} = \left\{ \frac{i}{d}, \dots, \frac{p^k i}{d}, \left(\frac{p^{k+1} i}{d}\right)_{\frac{q-1}{d}}, \dots, \left(\frac{p^{n-1} i}{d}\right)_{\frac{q-1}{d}} \right\}$$

Proof: It is clear from the uniqueness of the residue.

Example 3.2 If $p = 2$, $n = 8$ and $i = 27 \in [1,255]$, then the 2-cycle Ξ, generated by 27, $(27,54,108,216,177,99,198,141)$ is an S_2 2-cycle. Now since$(27,255) = 3$, then the set $\mathfrak{S}$={9, 18, 36, 72, 59, 33, 66, 47} obtained canceling the common factor 3 of each component of Ξ, is an S_2-set. Observe that $\mathfrak{S}$ as a subset of the interval $[1,72]$ has cardinality closed to $\sqrt{72} < 9$.

On the other hand, since $255/3 = 85$ and the first four terms 9,18,36,72 do not exceed 85, but $2 \times 72 = 144 = 85 \times 1 + 59$; $2 \times 59 = 108 = 85 \times 1 + 33$ and $2 \times 66 = 112 = 85 \times 1 + 47$, then we can generate the new set from 9 taking the remainder mod 85.

We emphasize that the set $\mathfrak{S}$ = {9, 18, 36, 72, 59, 33, 66, 47} is not the underlying set of the 2-cycle generated by 9, which is $\{9, 18, 36, 72, 144, 33, 66, 132\}$. This, as S_2-set is very poor respect to $\sqrt{255} \approx 15$, but by Corollary (3.2), induces a new S_2-set contained in the interval [1.48] namely, $\{3, 6, 12, 24, 48, 11, 22, 44\}$. Again this is not the underlying set of the 2-cycle generated by 3, which is $\{3, 6, 12, 24, 48, 96, 192, 129\}$. That is again an S_2-set of small cardinality respect to 255 but again induces a new S_2-set {1,2,4,8,16,32,64,43} ⊂ [1,64]. Clearly this is not the underlying set of the 2-canonical cycle $(1, 2, 4, 8, 16, 32, 64, 128)$.

As we can see, there are examples of p-cycles which have the S_2 property and whose generator i is neither prime with $q-1$ nor divisor of $q-1$. The following result provides a concrete example.

Proposition 3.1 *Let t be an integer number and $n = 4t$, then the underlying set of the p-cycle of length $n = 4t$ generated by*

$$\iota := \left(\sum_{\mu=0}^{2t} p^{\mu}\right) - p^t = 1 + p + p^2 + \ldots + p^{t-1} + \hat{p^t} + p^{t+1} + \ldots + p^{2t}$$

is an S_2*-set*. (*Here the hat means that the power p^t was excluded*.)

Proof: First observe that

$$\langle \iota \rangle = (\iota, p\iota, p^2\iota, \ldots, p^{2t-1}\iota, (p^{2t}\iota)_{q-1}, (p^{2t+1}\iota)_{q-1}, \ldots, (p^{4t-1}\iota)_{q-1})$$

where $(p^j\iota)_{q-1}$ denotes the remainder of $p^j\iota$ modulus $q-1$.

As always, we will suppose that such a set is not an S_2-set, therefore several cases may occur, namely:

1. Case 1. $p^r\iota + p^s\iota = p^u\iota + p^v\iota$ with $r, s, u, v \leq 2t-1$.
2. Case 2. $p^r\iota + p^s\iota = p^u\iota + (p^{2t+m_v}\iota)_{q-1}$ with $r, s, u, v \leq 2t-1$.
3. Case 3. $p^r\iota + p^s\iota = (p^{2t+m_u}\iota) + (p^{2t+m_v}\iota)_{q-1}$ with $r, s, u \leq 2t-1$.
4. Case 4. $p^r\iota + (p^{2t+m_s}\iota)_{q-1} = (p^{2t+m_u}\iota)_{q-1} + (p^{2t+m_v}\iota)_{q-1}$ with $r, s \leq 2t-1$.
5. Case 5. $(p^{2t+m_r}\iota)_{q-1} + (p^{2t+m_s}\iota)_{q-1} = (p^{2t+m_u}\iota)_{q-1} + (p^{2t+m_v}\iota)_{q-1}$.
6. Case 6. $p^r\iota + (p^{2t+m_s}\iota)_{q-1} = p^u\iota + (p^{2t+m_v}\iota)_{q-1}$ with $r, u \leq 2t-1$.

Our next goal is to determine the number $(p^{2t+m}\iota)_{q-1}$. For this end, let us denote by $\iota_{k,l}$ and θ_m the following natural numbers:

$$\iota_{k,l} := 1 + p + \ldots + \hat{p^l} + \ldots + p^{2t-k} \text{ and } \theta_m := 1 + p + \ldots + p^m.$$

With above notation, the number $(p^{2t+m}\iota)_{q-1}$ can be written as follows:

$$(p^{2t+m}\iota)_{q-1} = \begin{cases} \theta_m + p^{2t+m}\iota_{m+1,t} & \text{if } 0 \le m \le t-1, \\ \iota_{2t-m,m-t} + p^{2t-m}\theta_{2t-m-1} & \text{if } t \le m \le 2t-1. \end{cases} \quad (2)$$

As an illustration we consider the case 6. Let us suppose that

$$p^r\iota + (p^{2t+m_s}\iota)_{q-1} = p^u\iota + (p^{2t+m_v}\iota)_{q-1}.$$

For instance, if $0 \le r < u \le 2t-1 < 2t+m_s < 2t+m_v$ with $0 \le m_s \le t-1 < m_v$, then with the above notation we have:

$$(p^r\iota + \theta_{m_s} + p^{2t+m_s}\iota_{m_s} + 1, t = p^u\iota + \iota_{2t-m_v,m_v-t} + p^{2t+m_v}\theta_{2t-m_v-1}.$$

Now, if $r = 0$ after cancel common terms, we get the following equality

$$(p^{m_v-t}+\ldots+p^{2t}) + (1+p+\ldots+p^{m_s}) + p^{2t+m_s}\iota_{m_s+1,t} = p^u\iota + p^{2t+m_v}\theta_{2t-m_v-1},$$

which implies that $p|1$.

On the other hand, $r > 0$ implies

$$p^r\iota + p^{2t+m_s}\iota_{m_s+1,t} = p^u\iota + (p^{m_s+1}+\ldots+\widehat{p^{m_v-t}}+\ldots+p^{m_v}) + p^{2t+m_v}\theta_{2t-m_v-1},$$

if $m_s < m_v - t$ and

$$p^r\iota + p^{m_v-t} + p^{2t+m_s}\iota_{m_s+1,t} = p^u\iota + (p^{m_s+1}+\ldots+p^{m_v}) + p^{2t+m_v}\theta_{2t-mv-1}$$

if $m_s \ge m_v - t$.

If $m_s < m_v - t$, then $r > m_s + 1$ implies $p|1$; $r = m_s + 1$, implies $r = m_v > t$ which is absurd and finally $r < m_s + 1$ implies $p^{m_s+1}|2(1+p+\ldots+p^{m_s})$. Similar arguments led us to contradictions when we consider the case $m_s \ge m_v - t$; we omit details.

Example 3.3 If $p = 2$ and $t = 1$, then $n = 8$, $\iota = 27$, Proposition (2.2) says that the 2-cycle $(27, 54, 108, 216, 177, 99, 198, 141)$ is an S_2-set contained in $[1, 256]$.

Proposition 3.2 *If $i < p$, then the p-cycle $\langle i \rangle$ is an S_2 p-cycle.*

Proof: If there are different elements r, s, u, v such that

$$p^r i + p^s i = p^u i + p^u i,$$

then we would have $p|i$.

Corollary 3.4 *Let $i, j \in I_{q-1}$. Then if $i < p$ and $(j, q-1) = 1$, the p-cycle Ξ generated by ij is an S_2 p-cycle.*

Proof: If not, we should have $p^r ij + p^s ij \equiv p^u ij + p^u ij \pmod{q-1}$ for some integers r, s, u, v, but this congruence contradicts Proposition (3.2).

Proposition 3.3 *If n is odd, then the p-cycle generated by $p+1$ is an S_2 p-cycle.*

Proof: Observe that such p-cycle is

$$(p+1, p^2+p, \ldots, p^{n-2}+p^{n-3}, p^{n-1}+p^{n-2}, p^{n-1}+1).$$

First, let us suppose that there exist different integers $1 \leq r, s, u, v \leq n-1$ such that

$$p^{n-r} + p^{n-r-1} + p^{n-s} + p^{n-s-1} = p^{n-u} + p^{n-u-1} + p^{n-v} + p^{n-v-1},$$

then if $s = \max\{r, s, u, v\}$ we have $p|1$. On the other hand, if there exist different integers $1 \leq r, s, u \leq n-1$ such that

$$p^{n-r} + p^{n-r-1} + p^{n-s} + p^{n-s-1} = p^{n-u} + p^{n-u-1} + p^{n-1} + 1, \qquad (3)$$

then since

$$p^n + p^{n-1} - (q-1) = p^{n-1} + 1,$$

(3) can be written as

$$p^{n-r} + p^{n-r-1} + p^{n-s} + p^{n-s-1} = p^{n-u} + p^{n-u-1} + p^n + p^{n-1} - (q-1),$$

this implies that $p+1$ divides $q-1$ which is absurd.

Now we are interested in finding conditions to decide when the union of S_2 p-cycles is an S_2-set. A first approach is given in the following proposition:

Proposition 3.4 *If $1 < j < p$, then the set*

$$\mathfrak{S} := \{\langle 1 \rangle \cup \langle j \rangle\}$$

is an S_2-set.

Proof: Assume that $\mathfrak{S}$ is not an S_2-set. Then, there exist $a, b, c, d \in \{1, j\}$ and integer numbers $0 \leq r, s, u, v \leq n-1$ such that,

$$ap^r + bp^s = cp^u + dp^v, \tag{4}$$

with $r \neq s$ if $a = b$ and $u \neq v$ if $c = d$. The proof is somewhat technical and therefore divided into several cases. To begin suppose that $\delta = \min\{r, s, u, v\}$.

Case 1: If $a = b$ and $c = d$, then after canceling p^δ in (4) we obtain $p|a$ or $p|c$ which is a contradiction.

Case 2: $a = b$ and $c \neq d$. In this case, if $\delta = r$ or s, then after canceling p^δ in (4) we obtain $p|a$; if $\delta = u$ or v, then $p|c$ or $p|d$. The case $\delta = u = v$ leads to $ap^{r-\delta} + ap^{s-\delta} = c + d$, which is again a contradiction. On the other hand, if $\delta = r = u = v$ we obtain $a + ap^{s-\delta} = c + d$, now after to consider the different possibilities for a, c, d, we conclude that $p|1$ or $p|j$.

Case 3: $a \neq b$ and $c \neq d$. If r, s, u, v are distinct and $\delta = r, s, u \text{ or } v$, then $p|a$, b, c or d which is a contradiction. If two exponents are equal, for example, $r = u$ and $\delta = r = u$, then we have $a - c = dp^{v-\delta} - bp^{s-\delta}$ which is absurd. Finally, if three exponents are equal, for example $u = v = s$ and $\delta = u = v = s$, then equation (4) is nothing else but $ap^{r-\delta} + b = c + d$. Now again after considering all the possibilities for a, b, c, d, we obtain the same equations and conclusions as in the Case 2.

Example 3.4 If we take $p = 3$, then in this case $j = 2$. We show in the following Table some S_2-sets $S \subset [1, M = 3^n - 1]$ for different values of n.

Table 5. *S_2-sets as union of two* 3*-cycles.*

n	M	$\sqrt{M}$	S_2-sets
2	8	2.82	1, 2, 3, 6
3	26	5.09	1, 2, 3, 6, 9, 18
4	80	8.9	1, 2, 3, 6, 9, 18, 27, 54
5	242	15.55	1, 2, 3, 6, 9, 18, 27, 54, 81, 162

As we can see, the first two sets have a reasonable cardinality in respect to $\sqrt{M}$, while the latter two do not. However, it should be noted that since any subset of S_2-set retains the S_2 property, the set obtained for $M = 80$ is a nice S_2-set, if it is considered as subset of the integer interval $[1, 54]$, likewise the sets $\{1, 2, 3, 6, 9, 18, 27, 54, 81, \} \subseteq [1, 81]$ and $\{1, 2, 3, 6, 9, 18, 27\} \subseteq [1, 27]$ have also a nice cardinality with respect to 9 and 5 respectively.

Proposition 3.5 *If $1 < j < k < p$ and $k + j \neq p + 1$, then the set*

$$\mathfrak{S} := \{\langle 1\rangle \cup \langle j\rangle \cup \langle k\rangle\}$$

is an S_2-set.

Proof: Using the notation as in the proof of Proposition (3.4), let us assume that there exist $a, b, c, d \in \{1, j, k\}$ and integer numbers $0 \leq r, s, u, v \leq n-1$ such that,

$$ap^r + bp^s = cp^u + dp^v, \tag{5}$$

with $r \neq s$ if $a = b$ and $u \neq v$ if $c = d$. We distinguish three cases:

Case 1. If $a = b$ and $c = d$, then after canceling p^δ in (5) we obtain $p|a$ or $p|c$ which is a contradiction.

Case 2. $a = b$ and $c \neq d$. In this case, if $\delta = r$ or s, then after canceling p^δ in (5) we obtain $p|a$; if $\delta = u$ or v, then $p|c$ or $p|d$. The case $\delta = u = v$ leads to $ap^{r-\delta} + ap^{s-\delta} = c + d$, which is again a contradiction. On the other hand, if $\delta = r = u = v$ we obtain $a + ap^{s-\delta} = c + d$. Now after to consider the different possibilities for a, c, d, we obtain the following equalities:

$$p^{s-\delta} + 1 = j + k, \qquad j + jp^{s-\delta} = k + 1, \qquad k + kp^{s-\delta} = j + 1. \tag{6}$$

But $s - \delta \geq 1$ implies that none of the above equations are satisfied.

Case 3. $a \neq b$ and $c \neq d$. If r, s, u, v are distinct and $\delta = r$, s, u or v, then $p|a$, b, c or d which is a contradiction. If two exponents are equal, for example $r = u$ and $\delta = r = u$, then we have $a - c = dp^{v-\delta} - bp^{s-\delta}$ which is absurd. Finally, if three exponents are equal, for example $u = v = s$ and $\delta = u = v = s$, then equation (5) is nothing else but $ap^{r-\delta} + b = c + d$. Now again after consider all the possibilities for a, b, c, d, we obtain the same equations and conclusions as in (6).

Example 3.5 In the following Table we show some S_2-sets obtained for different values of $M = p^n - 1$

Table 6. *Examples based in Proposition 3.5.*

p	n	M	$\sqrt{M}$	S_2-sets
5	2	24	4.89	1, 2, 3, 5, 10, 15
7	2	48	6.9	1, 2, 3, 7, 14, 21
				1, 2, 4, 7, 14, 28
				1, 2, 5, 7, 14, 35
				1, 3, 4, 7, 21, 28
				1, 3, 6, 7, 21, 42
				1, 4, 5, 7, 28, 35
				1, 4, 6, 7, 28, 42
				1, 5, 6, 7, 35, 42

With a few modifications at the proof of Proposition (3.5), we have:

Corollary 3.5 *If $j < k < l < p$ and $k + l \neq pj + j$, then the set*

$$S := \{\langle j\rangle \cup \langle k\rangle \cup \langle l\rangle\}$$

is an S_2-set.

Example 3.6 If we take $p = 7$ and $n = 2$, we obtain the following Table:

Table 7. *Joining 3 7-cycles of length 2.*

$M = p^n - 1$	$\sqrt{M}$	S_2-sets
48	6.9	2, 3, 4, 14, 21, 28 2, 3, 5, 14, 21, 35 2, 3, 6, 14, 21, 42 2, 4, 5, 14, 28, 35 2, 4, 6, 14, 28, 42 2, 5, 6, 14, 35, 42 3, 4, 5, 21, 28, 35 3, 4, 6, 21, 28, 42 4, 5, 6, 28, 35, 42

Proposition 3.6 *If $1 < a_1 < a_2 < a_3 < p$, $a_i + a_j \neq p + 1$ and the set $\{1, a_1, a_2, a_3\}$ is an S_2-set, then the set*

$$\mathfrak{S} := \{\langle 1\rangle \cup \langle a_1\rangle \cup \langle a_2\rangle \cup \langle a_3\rangle\}$$

is an S_2-set.

Proof: By Proposition (3.5) in order to prove our assertion, we only have to analyze the equation

$$p^r + a_1 p^s = a_2 p^u + a_3 p^v, \tag{7}$$

with $0 < r, s, u, v < n$. As in the proof of Proposition (3.5) let $\delta =$ min{r,s,u,v}.

1. If $\delta = r = s = u \neq v$, then equation (7) becomes $0 < 1 + a_1 - a_2 = a_3 p^{v-\delta}$ which is a contradiction.
2. If $v \neq \delta = r = s \neq u$, we obtain $1 + a_1 = a_2 p^{u-\delta} + a_3 p^{v-\delta}$ which is absurd.
3. The cases $\delta = r$ with $\delta \neq s, u, v$ and $\delta = r = s = u = v$ are trivial.

Example 3.7 If $p = 11$ and $n = 2$, there exist 36 possibilities for a_1, a_2, a_3 which satisfies the hypothesis of the Proposition (3.6), we exhibit in the Table 8 only some of such sets. Before this note that although this example did not give sets whose cardinality is near to $\sqrt{120} \approx 11$, we point out that each of these sets provides examples of S_2 sets for any values less than $M = 120$. In some cases, we find good examples.

Table 8. *Joining 4* 11*-cycles of length 2.*

1, 2, 3, 5, 11, 22, 33, 55	1, 2, 3, 6, 11, 22, 33, 66
1, 2, 3, 7, 11, 22, 33, 77	1, 2, 3, 8, 11, 22, 33, 88
1, 3, 5, 10, 11, 33, 55, 110	1, 3, 6, 7, 11, 33, 66, 77
1, 3, 6, 10, 11, 33, 66, 110	1, 3, 7, 8, 11, 33, 77, 88
1, 3, 7, 10, 11, 33, 77, 110	1, 4, 6,7,11,44,66,77
1, 4, 6, 10, 11, 44, 66, 110	1,4,7,9,11,44,77,99
1, 4, 9, 10, 11, 44, 99, 110	1,5,9,10,11,55,99,110
1, 6, 7, 8, 11, 66, 77, 88	1,6,9,10,11,66,99,110
1, 7, 8, 9, 11, 77, 88, 99	1,7,9,10,11,77,99,110

4 Particular Examples

So far, we have provided some criteria that allow us to glue S_2 p-cycles $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$ such that, the resulting set $\mathfrak{S}:=\{\langle i\rangle \cup \langle j\rangle \cup \langle k\rangle\}$ maintains the S_2 property, the condition on their generators i,j,k is $1<i<j<k<p$. In this section we will try to go a little further.

4.1 The Case $q=p^2$

Let us suppose that $1\leq j<k<p<i$ are the generators of the the p-cycles (j,pj), (k,pk) and $(i,(pi)_{q-1})$. As always, we want to establish conditions on their generators so that the resulting set $\mathfrak{S}:=\{\langle i\rangle \cup \langle j\rangle \cup \langle k\rangle\}$ has the S_2 property. Now, observe that for this purpose it is easier to establish conditions for which $\mathfrak{S}$ does not have the S_2 property. In fact, $\mathfrak{S}=\{j,pj,k,pk,i,(pi)_{q-1}\}$ is not an S_2 set if there exist distinct $a_1,a_2,a_3,a_4\in\mathfrak{S}$ such that $a_1+a_2=a_3+a_4$, then it is evident that this equality leads us to consider a large number of equations. Fortunately many of these equations are not possible, for example it is impossible that $k+j=pk+pj$ or $k+j=pk+(pi)_{q-1}$ or $k+j=i+pj$. After check all the possibilities, we must consider only the following equations:

1) $i-(p+1)j+k=0$
2) $i-(p+1)j+pk=0$
3) $i-(p-1)j-pk=0$
4) $i-pj-(p-1)k=0$
5) $i-j-(p-1)k=0$
6) $i-j=(p+1)m$
7) $i+j-(p+1)k=0$
8) $i+j=(p+1)m$
9) $i+pj-(p+1)k=0$
10) $i-k=(p-1)m$
11) $pi-(p-1)j-pk=(p^2-1)m$
12) $pi-pj-(p-1)k=(p^2-1)m$
13) $pi+j-(p+1)k=(p^2-1)m$
14) $(p+1)i-pj-pk=(p^2-1)m$

Equation 6 corresponds to case $j+(pi)_{q-1}=i+pj$, equation 11 corresponds to case $j+(pi)_{q-1}=pj+pk$ and so on. To illustrate, we consider $p=7$ and we will to analyze the equations 3, 5, 6, 9, 10 and 12.

The following Table contains the solutions:

Equation	Solutions
(3) $i-(p-1)j-pk=0$	$(1,2,20);(1,3,27);(1,4,34);(1,5,39);$ $(1,6,48)$ $(2,3,33);(2,4,40);(2,5,47).$ $(3,4,46)$
(5) $i-j-(p-1)k=0$	$(1,2,13);(1,3,19);(1,4,25);(1,5,31);$ $(1,6,37).$ $(2,3,20);2,4,26);(2,5,32);(2,6,38).$ $(3,4,27);(3,5,33);(3,6,39).$ $(4,5,34);(4,6,40).$ $(5,6,41).$
(6) $i-j=(p+1)m$	$(1,k,9,1);(1,k,17,2);(1,k,25,3);$ $(1,k,33,4);(1,k,41,5).$ $(2,k,10,1);(2,k,18,2);(2,k,26,3);$ $(2,k,34,4);(2,k,42,5).$ $(3,k,11,1);(3,k,19,2);(3,k,27,3);$ $(3,k,35,4);(3,k,43,5).$ $(4,k,12,1);(4,k,20,2);(4,k,28,3);$ $(4,k,36,4);(4,k,44,5).$ $(5,k,13,1);(5,k,21,2);(5,k,29,3);$ $(5,k,37,4),(5,k,45,5).$ $(6,k,14,1);(6,k,22,2);(6,k,30,3);$ $(6,k,38,4);(6,k,46,5).$
(9) $i+pj-(p+1)k=0$	$(1,3,11);(1,4,17);(1,5,23);(1,6,29).$ $(2,4,10);(2,5,16);(2,6,22).$ $(3,5,9);(3,6,15).$ $(4,6,8).$
(10) $i-k=(p-1)m$	$(j,3,9,1)$ $(j,4,10,1).$ $(j,5,11,1);(j,5,17,2).$ $(j,6,12,1);(j,6,18,2).$
(12) $pi-pj-(p-1)k=(p\text{^}2-1)m$	$(1,2,37,5);(1,3,31,4);(1,4,25,3);$ $(1,5,19,2);(1,6,13,1).$ $(2,3,32,4);(2,4,26,3);(2,5,20,2).$ $(3,4,27,3).$

Note that equations containing $(pi)_{q-1}$ such that (6), (10) and (12), have as solutions quadruples (j,k,i,m). The value m appears because $i>p=7$ and therefore, $pi=(p^2-1)m+(pi)_{q-1}=48m+(7i)$. The other equations have as solutions triples (j,k,i). The first solution of the equation (6) for example, says that the set $\mathfrak{S}=\{1,\ 7,\ k,\ 7k,\ 9,\ 15\}$ is not an S_2 set for $2\leq k\leq 6$. The following Table contains all the S_2 sets which were obtained joining three 7-cycles of length 2 whose generators satisfy the condition $1=j<k<p<i$.

Table 9. *S_2 sets as union of three 7-cycles of length 2.*

1,2,7,11,14,29	1,4,7,11,28,29	1,5,7,26,35,38
1,2,7,12,14,36	1,4,7,13,28,43	1,5,7,27,35,45
1,2,7,14,27,45	1,4,7,18,28,30	1,5,7,34,35,46
1,3,7,10,21,22	1,4,7,19,28,37	1,6,7,10,22,42
1,3,7,12,21,36	1,4,7,26,28,38	1,6,7,11,29,42
1,3,7,13,21,43	1,4,7,27,28,45	1,6,7,20,42,44
1,3,7,18,21,30	1,5,7,10,22,35	1,6,7,26,38,42
1,3,7,20,21,44	1,5,7,12,35,36	1,6,7,27,42,45
1,3,7,21,26,38	1,5,7,18,30,35	1,6,7,34,42,46
1,3,7,21,34,46	1,5,7,20,35,44	

The next Table should be read as follows: The two generators j,k that appear in the left-hand column can be put together with exactly one generator i in the second column to obtain an S_2 set $\mathfrak{S} = \{j, pj, k, pk, i, (pi)_{48}\}$. for example, line 4 says that the sets $\mathfrak{S}_1 = \{2, 6, 9, 14, 15, 42\}$, $\mathfrak{S}_2 = \{2, 6, 11, 14, 29, 42\}$, $\mathfrak{S}_3 = \{2, 6, 14, 17, 23, 42\}$, $\mathfrak{S}_4 = \{2, 6, 14, 20, 42, 44\}$, $\mathfrak{S}_5 = \{2, 6, 14, 27, 42, 45\}$, $\mathfrak{S}_6 = \{2, 6, 9, 14, 33, 39, 42\}$, and $\mathfrak{S}_7 = \{2, 6, 14, 41, 42, 47\}$ are S_2 sets.

Table 10.

j,k	i
2,3	12,17,25,41
2,4	9,11,13,17,19,25,27,33,41
2,5	9,12,19,25,27,33
2,6	9,11,17,20,27,33,41
3,4	5,6,13,17,18,25,26,33,41
3,5	6,10,12,18,20,26,34,41
3,6	10,13,17,20,25,26,34,41
4,5	6,9,18,19,25,26,33,41
4,6	9,11,13,17,19,25,27,33,34,41,
5,6	9,10,19,20,25,26,27,33

4.2 The Case $q = p^{4t}$

With the notations as in Proposition 3.1, let t be an integer number, $n = 4t$ and

$$\iota := 1 + p + p^2 + \ldots + p^{t-1} + \hat{p^t} + p^{t+1} + \ldots + p^{2t}.$$

With this assumption, we have the following proposition:

Proposition 4.2.1 *The set $\mathfrak{S} = \{\langle 1\rangle, \langle \iota\rangle\}$ is an S_2 set.*

Proof: As always, we will assume that $\mathfrak{S} = \{\langle 1\rangle, \langle \iota\rangle\}$ has not the S_2 property. If this occurs, then at least one of following equalities is satisfied. For simplicity we

write in this prove $(p^k i)$ instead of $(p^k i)_{q-1}$.

1) $p^r + p^s = p^u + p^v\iota$
2) $p^r + p^s = p^u + (p^{2t+m_v}\iota)$
3) $p^r + p^s = p^u\iota + p^v\iota$
4) $p^r + p^s = p^u\iota + (p^{2t+m_v}\iota)$
5) $p^r + p^s = (p^{2t+m_u}\iota) + (p^{2t+m_v}\iota)$.
6) $p^r + p^s\iota = p^u\iota + p^v\iota$
7) $p^r + p^s\iota = p^u\iota + (p^{2t+m_v}\iota)$
8) $p^r + p^s\iota = (p^{2t+m_u}\iota) + (p^{2t+m_v}\iota)$
9) $p^r + (p^{2t+m_s}\iota) = (p^{2t+m_u}\iota) + (p^{2t+m_v}\iota)$

We must show that if one of these equations is satisfied, then we obtain a contradiction. We give the proof of equations 4,7 and 9 only for some particular cases.

For equation 4, let us suppose that $0 \le u < 2t + m_v = r < s$ with $0 \le m_v \le t-1$, then by (2) the equation defined by item 4, can be rewritten as

$$p^r + p^s = p^u\iota + \theta_{m_v} + p^{2t+m_v}\iota_{m_v+1,t}. \tag{8}$$

If $u = 0$, after we cancel common powers in (8) we obtain:

$$p^r.(\text{sum of powers of } p) = 2 + 2p + 2p^2 + \ldots + 2p^{m_v} + p^{m_v+1} + \ldots + p^{2t}.$$

These equalities imply that $p^{m_v+1} | 2\theta_{m_v}$ which is absurd. On the other hand, $0 < u$ carries us again to the absurd divisibility relation $p^u | \theta_{m_v}$.

Now, suppose that the equation defined by item 7 holds; i.e.,

$$p^r + p^s\iota = p^u\iota + (p^{2t+m_v}\iota). \tag{9}$$

Note that implicitly $0 \le s, u \le 2t-1$. Moreover, we have assumed that $0 < r \le 4t-1$ and $0 \le s < u \le 2t-1 < 2t+m_v$ with $0 \le m_v \le t-1$.

Under these hypotheses and using (2), we have $p | \theta_{m_v}$ which is absurd. On the other hand, if $t \le m_v \le 2t-1$, then again by (2) we have:

$$p^r = p^s\iota(p^{u-s} - 1) + p^{2t+m_v}\theta_{2t-m_v-1} + \iota_{2t-m_v+1,m_v-t}. \tag{10}$$

And therefore, if $t < m_v$ it is clear that we have a contradiction, but if $m_v = t$ (10) becomes,

$$p^r = p^s\iota(p^{u-s} - 1) + p^{2t+m_v}\theta_{t-1} + \iota_{t,0}. \tag{11}$$

Now $s = 0$ implies $p | \iota$, while $s > 0$ lead us to $p | \theta_{t-1}$, both facts being absurd.

Finally, to analyze the equation $p^r + (p^{2t+m_s}\iota) = (p^{2t+m_u}\iota) + (p^{2t+m_v}\iota)$ defined by item 9, we will assume that $0 < r < 4t-1$ and $0 \le m_s < m_u < t \le m_v \le 2t-1$. Now again by (2), we have:

$$p^r + \theta_{m_s} + p^{2t+m_s} = \theta_{m_u} + p^{2t+m_u} + \iota_{2t-m_v,m_v-t} + p^{2t+m_v}\theta_{2t-m_v-1}. \quad (12)$$

Now this equality is the same as

$$p^r + p^{2t+m_s} = p^{m_s+1}\theta_{m_u-m_s-1} + p^{2t+m_u} + \iota_{2t-m_v,m_v-t} + p^{2t+m_v}\theta_{2t-m_v-1}. \quad (13)$$

and consequently $p|\iota_{2t-m_v,m_v-t}$ which is impossible.

Example 4.2.1 Taking $p = 2$ and $t = 1$, we have that $\iota = 27$ and by Propositions (4.2.1.) and (3.1) the set

$$\mathfrak{S} = \{1, 2, 4, 8, 16, 27, 32, 54, 64, 99, 108, 128, 141, 177, 198, 216\}$$

is an S_2 set in the integer interval $[1, 255]$. Note that we have actually provided a good example of an S_2 set which has a nice property: For each element $a_j \in \mathfrak{S}$ the subset $S_{aj} = \mathfrak{S} \cap I_{aj} \subset \mathfrak{S}$ is a good S_2 set.

4.3 The Case $q = 3^4$

The following Proposition provides a criterion to construct S_2 sets in the integer interval [1.80] by joining two S_2 3-cycles of length 4. By Theorem (5.1) and Corollary (3.4) we have that the set of generators of S_2 3-cycles of length 4 is $\Lambda = \{1, 2, 7, 11, 13, 14, 17, 22, 23, 26, 41, 53\}$.

Proposition 4.3.1 *Let* $i, j \in \Lambda$ *such that* $j - i \equiv 1\ (mod\ 2)$, then $\mathfrak{S} = \{\langle i \rangle \cup \langle j \rangle\}$ *is an* S_2 *set.*

Proof: To begin with, observe that $\mathfrak{S}$ is not an S_2 set if and only if there exists (r, s, u, v), with $r < s; u < v$ and $r, s, u, v \in \{0, 1, 2, 3\}$ such that one of the following congruencies is satisfied:

$$3^r i + 3^s i \equiv 3^u j + 3^v j\ (mod\ (80)) \quad (14)$$

$$3^r i + 3^v i \equiv 3^u j + 3^s i\ (mod\ (80)) \quad (15)$$

$$3^r i + 3^s i \equiv 3^u j + 3^v i\ (mod\ (80)) \quad (16)$$

If $3^r i + 3^u j + 3^v j$ (mod (80)) and $I = 2_\iota$. By parity arguments, the congruence (14) is equivalent to:

$$20t = 3^r \iota \left(\frac{3^{s-r}+1}{2}\right) - 3^u (2k+1) \left(\frac{3^{v-u}+1}{4}\right).$$

Now since $(3^{v-u}+1)/4$ is 1 or 7, then $(3^{s-r}+1)/2$ must be equal to 5 and hence $5|2_k$ +1 which is a contradiction.

On the other hand if $i = 2\iota+1$ and keeping in mind that $3^{\mu} - 1 = 2.8$ or 26, then congruence (15) is equivalent to:

$$20t = 3^{u}\, k \left(\frac{3^{v-u} - 1}{2}\right) - 3^{r}\,(2\iota + 1)\,\cdot 2\,.$$

This equality implies that $(3^{v-u} - 1)/2$ must be even and hence equals to 4. Consequently

$$10t = 3^{u} \cdot 2\ \cdot \mathrm{k} - 3^{r}(2\iota + 1),$$

which is again an contradiction.

Finally, congruence (16) is nothing but

$$80t = 3^{r} i(1 + 3^{s-r} - 3^{v-r}) - 3^{u} j.$$

But this is impossible since the RHS is negative.

Example 4.3.1 By Proposition (4.3.1), we can put together the following 3-cycles generated by i and j (Table):

i	j
1	2,14,22,26
2	7,11,13,17,23,41,53
7	14,22,26
11	14,22,26
13	14,22,26
14	17,23,41,53
17	22,26
22	23,41,53
23	26
26	41,53

The following Table contains some of these sets:

Table 11. *Union of two* 3*-cycles of length 4.*

1, 2, 3, 6, 9, 18, 27, 54	2, 6, 11, 18, 19, 33, 54, 57
2, 6, 18, 53, 54, 71, 77, 79	7, 14, 21, 29, 42, 46, 58, 63
7, 21, 22, 29, 34, 38, 63, 66	11, 14, 19, 33, 42, 46, 57, 58
13, 22, 31, 34, 37, 38, 39, 66	14, 42, 46, 53, 58, 71, 77, 79
17, 22, 34, 38, 51, 59, 66, 73	22, 34, 38, 53, 66, 71, 77, 79
23, 26, 47, 61, 62, 69, 74, 78	26, 53, 62, 71, 74, 77, 78, 79

5 Curves with many rational points over finite fields

We consider the non-singular complete irreducible Kummer curve $\mathfrak{E}$ over $\mathbb{F}_q$ defined by the affine equation:

$$y^r = \mu(x),$$

where $r|q-1$ and the rational function $\mu(x) \in \mathbb{F}_q(x)$ satisfies the following conditions:

1. μ is not the d-th power of an element $v \in \mathbb{F}_q(x)$ for any divisor $d > 1$ of r;
2. $\mu = 1$ on a substantial subset $\mathfrak{Z}_\mu$ of $\mathbb{P}^1(\mathbb{F}_q)$;
3. $\mu(x)$ has many multiple zeros and poles.

For details about this conditions and proofs we refer [7] and [11]. With above notation we have:

Proposition 5.1 ([11], *Proposition 2.1*) *The curve $\mathfrak{E}$ over the finite field $\mathbb{F}_q$ given by the Kummer equation $y^r = \mu(x)$, where r divides $q-1$ and the rational function $\mu(x)$ is not the d-th power of an element $v(x) \in \mathbb{F}_q(x)$ for any divisor d of r with $d > 1$, has the following properties:*

1. If $(\mu) = \sum_{i=1}^{n} d_i \cdot P_i$ is the divisor of μ with distinct $P_i \in \mathbb{P}^1(\mathbb{F}_q)$ and there exists i such that $gcd(r, |d_i|) = 1$, then the genus g of $\mathfrak{E}$ is given by

$$2g(\mathfrak{E}) - 2 = r \cdot (n-2) - \sum_{i=1}^{n} gdc(r, |di|).$$

2. The set of $\mathbb{F}_q$ −rational points (essentially) satisfies $|\mathfrak{E}(\mathbb{F}_q)| \geq r \cdot |\mathfrak{Z}_\mu|$.

Proof: For details and proofs, we refer to the literature on algebraic function fields for instance, [12].

Now, let us explain briefly how construct such rational functions μ: Let $\ell(x) \in \mathbf{F}_p[x]$, and we denote by $\mathfrak{V}_\ell$ the set $\{\alpha \in \mathbb{F}_q;\ \ell(\alpha) = 0\}$.

1. We split $\ell(x)$ as $\ell(x) = f(x) + g(x)$ with $f(x), g(x) \in \mathbb{F}_p[x]$. We denote the zero sets (in $\mathbb{F}_q$) of f (resp g) by $\mathfrak{V}_f$ (resp ,$\mathfrak{V}_g$), then the rational function

$$\mu(x) := -\frac{f(x)}{g(x)}$$

satisfies $\mu(\alpha) = 1$ for $\alpha \in \mathfrak{V}_\ell \setminus (\mathfrak{V}_f \cup \mathfrak{V}_g)$.

2. Given $f(x) \in \mathbb{F}_p(x)$, we will denote by $\mathcal{R}_{\ell}\,(f(x))$ the remainder of the Euclidean division of $f(x)$ by $\ell\,(x)$. In this way, we have (essentially):

$$\ell\,(\alpha) = 0 \;\Rightarrow \frac{f(x)}{\mathcal{R}_{\ell}\,(f(x))} = 1.$$

In accordance with above observation, we need consider polynomials $\ell\,(x) \in \mathbb{F}_p[x]$ having many roots in $\mathbb{F}_q$.

Definition 5.1 *A polynomial* $f(x) \in \mathbb{F}_q[x]$ *is a restricted range polynomial if* $f(\alpha) \in \mathfrak{V} \subsetneq \mathbb{F}_p$ *for some proper subset of* $\mathbb{F}_p$ *and for all* $\alpha \in \mathbb{F}_q$. *In particular, when* $\mathfrak{V} = \mathbb{F}_p$,*we say that* $f(x)$ is a $(\mathbb{F}_q, \mathbb{F}_p)$-*polynomial.*

A classical example of restricted range polynomial is the norm polynomial $N_{\mathbb{F}_q/\,\mathbb{F}_p}\,(x) = x^{p^{n-1}\,\ldots p+1} \in \mathbb{F}_q[x]$.

Definition 5.2 *A nonzero* $(\mathbb{F}_q, \mathbb{F}_p)$ *−polynomial* $f(x) \in \mathbb{F}_q[x]$ *will be called minimal, if* $deg(f(x)) \leq q-1$ *and none its proper partial sums is a* $(\mathbb{F}_q, \mathbb{F}_p)$-*polynomial*.

We recall briefly some properties of $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial. For proofs, we refer to [5] and [13].

Proposition 5.2 [13] $(\mathbb{F}_q,\ \mathbb{F}_p)$-*polynomials are surjective*.

Theorem 5.1 [5] (*Characterization of* $(\mathbb{F}_q,\ \mathbb{F}_p)$-*polynomials*) *The exponent sets of the minimal* $(\mathbb{F}_q,\ \mathbb{F}_p)$-*polynomials are the* p-*cycles of set* $\{0, \ldots, q-1\}$. *For each* p-*cycle* $\mathfrak{I}$, *all the minimal* $(\mathbb{F}_q,\ \mathbb{F}_p)$-*polynomials with exponent set* $\mathfrak{I}$ *are:*

$$\mathrm{f}_{\mathfrak{I}}\,(x, \alpha) = \sum_{k=0}^{\mathrm{o}(\mathfrak{I})-1} \alpha^{p^k}\, x^{i^{\sqcap k}} \qquad \alpha \in \mathbb{F}^*_{p^{\circ(\mathfrak{I})}}$$

where i *is an arbitrary but fixed representative of* $\mathfrak{I}$. *In addition, we have all the different* $(\mathbb{F}_q,\ \mathbb{F}_p)$-*polynomials of less or equal degree to* $q-1$ *by sums of polynomials* $f_{\mathfrak{I}}\,(x, \alpha)$ *corresponding to different cycles*.

Example 5.1 : Using Theorem 5.1 and Example 2.2, we exhibit some $(\mathbb{F}_{27} : \mathbb{F}_3)$-polynomials.

$$x^{26} \qquad x^{13}$$
$$x + x^3 + x^9 \qquad x^2 + x^6 + x^{18} \qquad x^4 + x^{12} + x^{10} \qquad x^5 + x^{15} + x^{19}$$
$$x^7 + x^{21} + x^{11} \qquad x^8 + x^{24} + x^{20} \qquad x^{14} + x^{16} + x^{22} \qquad x^{17} + x^{25} + x^{23}$$

Remark 5.1 Proposition 5.2 says that each $(\mathbb{F}_q, \mathbb{F}_p)$-polynomial is surjective, hence, we can use this fact to construct appropriate rational functions which leads us to obtain curves over the finite field $\mathbb{F}_q$ with good parameters. The following examples explain how. The reader who is not familiar with the concepts of algebraic function fields (i.e., algebraic curves) as genus, rational points etc is referred to [12].

Example 5.2 The curve $\mathfrak{C}$ over $\mathbb{F}_9$ given by $y^2 = -(x^6 + x^5 + x^4 + 2x^2 + 2)$ has $g(\mathfrak{C}) = 2$ and 20 rational points. The best value possible, cf [2].

The affirmation is clear. Let us briefly explain how we obtained this equation. Observe that there are 3 3-cycles of length 2, namely $(1,3), (2,6)$ and $(5,7)$, then set $\{1,3,5,7\}$ which is not an S_2 set! induces the $(\mathbb{F}_9, \mathbb{F}_3)$-polynomial $\ell(x) = x^7 + x^5 + x^3 + x$ which has its roots in $\mathbb{F}_9$. We will take advantage of this fact to construct our curve. In general, given two co-primes polynomials $\ell(x), f(x) \in \mathbb{F}_p[x]$ and $r|q-1$, the Euclidean division

$$f(x)^r = \ell(x) \cdot h(x) + \mathcal{R}_\ell(f(x)^r),$$

implies that for each $\alpha \in \mathbb{F}_q$ root of $\ell(x), \mathcal{R}_\ell(f(x)^r)(\alpha) = f(\alpha)^r$; i. e., $\mathcal{R}_\ell(f(x)^r)(\alpha)$ is an r-th power in $\mathbb{F}_q$, therefore the polynomial $y^r = \mathcal{R}_\ell(f(x)^r)(\alpha)$ splits completely en $\mathbb{F}_q[y]$, this means many points. Now in our situation taking $f(x) = (x-1)(x+1)(x^4 + 2x^2 + 2)$ we have, $\mathcal{R}_\ell(f(x)^2) = -(x^6 + x^5 + x^4 + 2x^2 + 2)$, this carry us to our equation.

Example 5.3 The curve $\mathfrak{C}$ over $\mathbb{F}_{27}$ given by $y^2 = -(x^4 + 2x^3 + x^2 + 1)^3$ has $g(\mathfrak{C}) = 1$ and $\#\mathfrak{C}(\mathbb{F}_{27}) = 38$.

By Proposition 3.4, the union of the underlying sets of the 3-cycles $(1,3,9)$ and $(2,6,18)$ is an S_2 set. This set induces the $(\mathbb{F}_{27} : \mathbb{F}_3)$-polynomial $\ell(x) = x^{18} + x^9 + x^6 + x^3 + x^2 + x$ which induces the rational function $\mu(x) = -x^2(x+1)^2(x^4 + 2x^3 + x^2 + 1)^3$ and consequently the algebraic curve $\mathfrak{C}$ over $\mathbb{F}_{27}$\$ defined by the equation:

$$y^2 = -(x^4 + 2x^3 + x^2 + 1)^3.$$

(Here we split $\ell(x)$ as $\ell(x) = \ell_1(x) + \ell_2(x)$ where $\ell_1(x) = x + x^2$ and $\ell_2(x) = x^3 + x^6 + x^9 + x^{18} = x^3(x+1)^3(x^4 + 2x^3 + x^2 + 1)^3$. Observe that the places corresponding to $x = 0$ and $x = -1$ are unramified.)

It is easy to see that the curve $\mathfrak{C}$ has genus $g = 1$. For the number of rational points (or places of degree one in the language of algebraic function fields), observe that $GCD(\ell(x), x^{27} - x) = x + x^2 + x^4 + 2x^5 + x^6 + 2x^7 + x^9$, therefore the curve $\mathfrak{C}$ has at least $\$2 \cdot \#\ell^{-1}(0) = 2 \cdot 9 = 18$. We use computer program Mathematica to complete the determination of the rational points, we refer to [11], Remark 2.2 for details.

Example 5.4 The S_2 3-cycle of length 3, $(17, 25, 23)$ induces the minimal $(\mathbb{F}_{27} : \mathbb{F}_3)$-polynomial $\ell(x) = x^{17} + x^{25} + x^{23}$ which has 9 roots in $\mathbb{F}_{27}$, namely the zeros

Example 5.4 The S_2 3-cycle of length 3, $(17, 25, 23)$ induces the minimal $(\mathbb{F}_{27} : \mathbb{F}_3)$-polynomial $\ell(x) = x^{17} + x^{25} + x^{23}$ which has 9 roots in $\mathbb{F}_{27}$, namely the zeros

of the polynomial $f(x) = x + x^7 + x^9 = x(1 + x)(2 + x)(2 + x^2 + x^3)(1 + 2x^2 + x^3)$. If we split $\ell(x)$ as $\ell(x) = x^{17} + x^{23}(x^2 + 1)$ and consider the rational function $\mu(x) := -x^6(x^2 + 1)$, then for each α root of $f(x)$, $\mu(\alpha) = 1$.

Now, the curve $\mathfrak{C}$ over $\mathbb{F}_{27}$ defined by the Kummer equation

$$y^{26} = \mu(x) := -x^6(x^2 + 1),$$

has genus $g = 24$ and 208 rational points. This is the best value know for $(q, g) = (27,24)$ (see [2]).

Example 5.5 We will construct here two maximal curves $\mathfrak{C}_1$ and $\mathfrak{C}_2$ over $\mathbb{F}_{49}$ with $g(\mathfrak{C}_1) = 1$ and $g(\mathfrak{C}_2) = 3$.

In Table 9, we exhibit some S_2 sets $\mathfrak{S} \subset I_{48}$ which was obtained as union of 3 7-cycles of length 2. For this example we consider the set $\mathfrak{S} = \{1,2,7,11,14,29\} = \{\langle 1\rangle \cup \langle 2\rangle \cup \langle 11\rangle$, this set induces the $(\mathbb{F}_{49} : \mathbb{F}_7)$-polynomial $\ell(x) = x + x^2 + x^7 + x^{11} + x^{14} + x^{29}$. By Proposition 5.2 there exist a subset $\mathfrak{V} \subset \mathbb{F}_{49}$ such that $\ell(\mathfrak{V}) = 1$ and after some computations we obtain that $\mathfrak{V}$ is the zero set of the polynomial $l(x) = 1 + x + x^2 + 6x^3 + x^4$. We use this polynomial to construct our curves instead of $\ell(x)$, the reason is that $\ell(x)$ has high degree compared to $|\mathfrak{V}|$. Now we split $l(x)$ as $l(x) = (1 + x + 4x^2 + x^4) + (6x^3)$, the polynomial $1 + x + 4x^2 + x^4$ can be factored as $1 + x + 4x^2 + x^4 = (5 + x)^3(6 + x)$ and therefore we consider the Kummer cover defined by the equation

$$y^r = \frac{x^3}{(5 + x)^3\,(6 + x)} \qquad r|4.$$

This algebraic function field has genus $g = r - d$ with $d = GCD(r, 3)$. This gives, for $r = 2, g(\mathfrak{C}_1) = 1$ and for $r = 4, g(\mathfrak{C}_2) = 3$, the rational points satisfies $\#\mathfrak{C}_1 = 64\ and\ \#\,\mathfrak{C}_2 = 92$ (see tables in [3]).

References

1. Serre JP. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. CR Acad Sci Paris Sér I Math. 1983; 296: 397-402.

2. Van der Geer G, Van der Vlugt M. Tables for the function $N_q(g)$. The Netherlands: Universiteit van Amsterdam. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.45.710&rep=rep1&type=pdf.

3. Van der Geer G, Howe EW, Lauter KE, Ritzenthaler C. Tables of curves with many points. 2009. Available in http://www.manypoints.org.

4. Goppa VD. Codes on algebraic curves. Sov Math Dokl. 1981; 24: 170-172.

5. Redei L. Lacunary polynomials over finite fields. North-Holland, Amsterdam; 1973.

6. Erdos P, Turán P. On problem of Sidon in additive number theory and some related problems. J London Math Soc. 1941; 16 (2): 212-215.

7. Van der Geer G, Van der Vlugt M. Kummer covers with many rational points. Finie Fields Appl. 2000; 6(4): 327-341.

8. Hungerford T. Algebra. Springer-Verlag, Berlin; 1974.

9. Vermani LR. Elements of algebraic coding theory. Springer - Science+Business Media, B.V.;1996.

10. Pless V. Introduction to the theory of error correcting codes. Second Edition. John-Wiley and Sons; 1989.

11. Garzon A. Euclidean algorithm and Kummer covers with many points. Rev Colomb Matemáticas. 2003; 37: 37-50.

12. Stichtenoth H. Algebraic function fields and codes. Berlin: Springer-Verlag; 1993.

13. Andrade C, Garzon A. Polynomials with a restricted range and curves with many points. Rev Academia Colombiana Ciencias. 2010; 131(34): 229-240.

Dirección del autor

Álvaro Garzón R.
Departamento de Matemáticas, Universidad del Valle, Santiago de Cali – Colombia
alvaro.garzon@correounivalle.edu.co