Kaprekar’s routine in polynomial rings

[a]Alan Daniel Villanueva Paredes, [b] José Alejandro Lara Rodríguez

[a,b]Facultad de Matemáticas, Universidad Autónoma de Yucatán, México.

[a]alanvp97@hotmail.com

[b]alex.lara@correo.uady.mx

Abstract

The process of *order, reverse and subtract* is taken from integers right to polynomial rings with coefficients in a finite field. We do such essentially for prime fields but we also comment a little on non prime fields. Given that Kaprekar’s routine depends so much in the order of the set we work in, we first give an order to the polynomial rings in question and then, we focus on the number and length of the cycles associated to this routine, specifically for the two and three digits polynomials case.

Resumen

El proceso de ordenar, invertir y sustraer es tomado de los enteros a los anillos de polinomios con coeficientes en un campo finito. Esto lo hacemos esencialmente para campos primos, pero también comentamos un poco acerca de campos no primos. Dado que la rutina de Kaprekar depende del orden del conjunto en cuestión, primero damos un orden a los anillos de polinomios y luego nos enfocamos en el número y longitud de los ciclos asociados a dicha rutina, específicamente para el caso de polinomios de dos y tres dígitos.

Keywords and phrases : Finite field, polynomial rings, Kaprekar’s routine, Kaprekar phenomena

2010 *Mathematics Subject Classification* : 11T06 Polynomials over finite fields.

1. Introduction

D. R. Kaprekar was an indian mathematician whose contributions to number theory were of such importance that some concepts were named after him. The reader might have stumbled upon the words Kaprekar phenomena or Kaprekar constant. This work is strongly related to the ideas behind these concepts.

We take a four digit integer, say, $n = 3047$ and compute the difference between the numbers that arise from rearranging its digits in ascending and descending order, that is, $7430 - 0347 = 7083$ and we do the exact same with the number we just got, $8730 - 0378 = 8352$ and one more time to finally arrive to

Fecha de recepción: agosto 7, 2020. Fecha de aceptación: diciembre 28, 2020.

$8532 - 2358 = 6174$ which is a special number since no matter which four digit number n with all digits not the same we had chosen at the beginning, we would have always end up with 6174 and the same process to this number would do nothing. This process of *order, reverse and subtract* is what we call *Kaprekar's routine* and the fact that 6174 is the arrival point for any four digit number is called *Kaprekar phenomena*. The information related to 6174 can be found in [2] as written by Kaprekar himself.

While there are several brilliant and interesting results regarding Kaprekar's routine that arise as one change the base and the number of digits, many of them found in [4], the main subject of this article is to apply this same idea of the routine to rings of polynomials with coefficients in finite fields. The main problem that awaits is that we will need an order for polynomials, but once we have made some agreements, we will be able to give number and length of the cycles associated to the cases with two and three digit polynomials.

2. Original routine

Let (B, D) be a pair of a base B and a number of digits D for a numeral system, $S_{(B,D)}$ the set of all integers of D digits in base B and $\overline{S}_{(B,D)}$ the set of integers of D digits in base B with all digits not the same. Also, for a given $n \in \mathbb{N} \cup \{0\}$, let $\overrightarrow{n}$ be the number that arises when rearranging the digits of n in descending order and $\overleftarrow{n}$ when rearranging in ascending order. Thus, Kaprekar's routine can be defined as $\kappa : \overline{S}_{(B,D)} \to \overline{S}_{(B,D)}$ such that $\kappa(n) = \overrightarrow{n} - \overleftarrow{n}$ and this function is well defined. A proof of the latter can be found in [4]. Consecutive iterations of this routine always lead to a cycle of integers since the set $\overline{S}_{(B,D)}$ is always finite for a given base and number of digits. That said, what is usually studied is the number and length of the cycles associated to this (B, D) and how many iterations it takes to reach the cycle. We give a few examples.

Example 2.1. The number 6174 is the fixed point for Kaprekar's function in the case with base 10 and 4 digits. Furthermore, we know that the smallest $m \in \mathbb{N}$ such that $\kappa^{(m)}(n) = 6174$ for any $n \in \overline{S}_{(B,D)}$ is $m = 7$, that is, it takes up to 7 iterations of Kaprekar's routine for any integer in $\overline{S}_{(B,D)}$ to reach 6174. A proof can be found in [3].

In order to graphically display cycles of length more than one, and by this we mean other than fixed points, we use the notation

$$\begin{tikzcd}
a \arrow[r] & \kappa(a) \arrow[r] & \kappa^{(2)}(a) \arrow[r] & \cdots \arrow[r] & \kappa^{(m)}(a) \arrow[r] & \kappa^{(m+1)}(a) \arrow[r] & \cdots \arrow[r] & \kappa^{(n-1)}(a) \arrow[r] \arrow[lll, bend right] & \kappa^{(n)}(a)
\end{tikzcd}$$

meaning that $\kappa^{(m)}(a)$ is the first image that is repeated and $\kappa^{(n)}(a)$ is the first time this image is repeated, that is, after n applications of Kaprekar's function over a certain integer a, we go back to the image of the m-th application, thus getting a cycle of length $n - m$.

Example 2.2. Let us consider $(B, D) = (56, 4)$. This pair has a cycle of length 4

$$\begin{tikzcd}
{[42,39,15,14]} \arrow[r] & {[28,23,31,28]} \arrow[r] & {[7,55,55,48]} \arrow[r] & {[48,6,48,8]} \arrow[lll, bend right]
\end{tikzcd}$$

and one with length 3

$$\begin{tikzcd}
{[40,7,47,16]} \arrow[r] & {[40,23,31,16]} \arrow[r] & {[24,7,47,32]}. \arrow[ll, bend right]
\end{tikzcd}$$

Furthermore, these are the only cycles associated to this base and number of digits, that is, no matter which integer of $\overline{S}_{(56,4)}$ we start the routine with, consecutive applications of Kaprekar's function will always lead to one of those cycles.

Now that we have met the routine in the very set it was thought for, we extend the notion to polynomial rings.

3. Routine in polynomial rings

Motivated by the usual comparison between $\mathbb{Z}$ and $\mathbb{F}_p[X]$ (reading on this subject can be found in [1]), we now adapt the idea behind Kaprekar's routine to $\mathbb{F}_p[X]$. First, we have to write a polynomial as a linear combination of the powers of a base, just as we do for integers and we leave here the appropriate proposition.

Proposition 3.1. *Let us consider a finite field with p elements $\mathbb{F}_p$ and take $B \in \mathbb{F}_p[X]$ such that it is not zero nor a unit. For any non zero $f \in \mathbb{F}_p[X]$ there exist unique $a_i \in \mathbb{F}_p[X]$ with $\deg a_i < \deg B$ for $0 \leq i \leq n$ where $n \in \mathbb{N} \cup \{0\}$ such that*

$$f = a_n B^n + a_{n-1} B^{n-1} + \cdots + a_1 B + a_0$$

and $a_n \neq 0$.

Now, we are going to simplify things when writing a polynomial on a base B by adopting the notation

$$f = a_n B^n + a_{n-1} B^{n-1} + \cdots + a_1 B + a_0 = [a_n, a_{n-1}, \cdots, a_1, a_0],$$

every time making very clear the base we are working on so that we do not have to make the base appear explicitly in the notation.

Since this routine is all about ordering the elements of the field we are working on, it is essential for us to decide the order of $\mathbb{F}_p[X]$. We cannot stick to the usual degree based norm because there are several polynomials that share the same degree while being different. What we propose here is an order based on the coefficients of the polynomials.

We start by giving $\mathbb{F}_p$ some order. Let us remember that

$$\mathbb{F}_p \cong \mathbb{Z}_p = \{0, 1, \cdots, p-1\}$$

where of course every element of $\mathbb{Z}_p$ is an equivalence class. Thus, the order we choose for $\mathbb{F}_p$ is none other than $0 < 1 < 2 < \cdots < p-1$ and this will allow us to work with $\mathbb{F}_p[X]$. Now, let us note there is a natural one to one correspondence from polynomials in $\mathbb{F}_p[X]$ to tuples, and this is

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \longleftrightarrow (a_n, a_{n-1}, \cdots, a_1, a_0)$$

so now we use the lexicographical order to order the tuples and consequently the polynomials.

Example 3.1. Let us consider $(x^3 + 4x + 8)$ and $(x^3 + 5x + 2)$ in $\mathbb{F}_p[X]$. Thus, we have

$$x^3 + 4x + 8 \longleftrightarrow (1, 0, 4, 8) < (1, 0, 5, 2) \longleftrightarrow x^3 + 5x + 2$$

and so

$$x^3 + 4x + 8 < x^3 + 5x + 2.$$

As for the size of the tuples, we have to take the biggest degree among the degrees of the polynomials we compare and add one, filling with zeros the tuple associated to the polynomial with the smaller degree so that the comparison has any sense.

Example 3.2. Let us consider $(4x^6 + 2x^3 + 1)$ and $(x^3 + 2x + 1)$ in $\mathbb{F}_p[X]$. We have

$$4x^6 + 2x^3 + 1 \longleftrightarrow (4, 0, 0, 2, 0, 0, 1) > (0, 0, 0, 1, 0, 2, 1) \longleftrightarrow x^3 + 2x + 1$$

so that

$$4x^6 + 2x^3 + 1 > x^3 + 2x + 1.$$

In these cases where we compare polynomials of different degree we can just compare the degrees.

Let $\overrightarrow{f}$ and $\overleftarrow{f}$ be the polynomials we get by rearranging the digits of $f \in \mathbb{F}_p[X]$ in descending and ascending order, respectively. We define Kaprekar's routine as $\kappa : \mathbb{F}_p[X] \to \mathbb{F}_p[X]$ with $\kappa(f) = \overrightarrow{f} - \overleftarrow{f}$ so we have

$$\begin{aligned}\kappa(f) &= [a_n, \cdots, a_1, a_0] - [a_0, a_1, \cdots, a_n]\\ &= (a_n B^n + \cdots + a_1 B + a_0) - (a_0 B^n + \cdots + a_{n-1} B + a_n)\\ &= (a_n - a_0)B^n + (a_{n-1} - a_1)B^{n-1} + \cdots + (a_1 - a_{n-1})B + (a_0 - a_n)\\ &= [a_n - a_0, a_{n-1} - a_1, \cdots, a_1 - a_{n-1}, a_0 - a_n]\end{aligned}$$

but there is a more general description. Let $D = n + 1$. Let $\overrightarrow{f} = [a_n, a_{n-1}, \cdots, a_1, a_0] \in \mathbb{F}_p[X]$ and let us consider the differences $d_i = a_{n-(i-1)} - a_{i-1}$ for $1 \le i \le \lfloor D/2 \rfloor$. Thus

$$\kappa(f) = \overrightarrow{f} - \overleftarrow{f} = [d_1, \cdots, d_{\lfloor D/2 \rfloor - 1}, d_{\lfloor D/2 \rfloor}, 0, -d_{\lfloor D/2 \rfloor}, -d_{\lfloor D/2 \rfloor - 1}, \cdots, -d_2, -d_1] \tag{3.1}$$

(with missing central zero for D even) and so, the only thing we need for calculating the *path* a polynomial is taking by iterating Kaprekar's routine is the differences.

Next, we see that when working with polynomials, there is no need for borrowing digits. We define

$$\mathbb{F}_p^{(n)}[X] = \{f \in \mathbb{F}_p[X] |\ \deg f < n\}$$

and notice this is an additive subgroup of $\mathbb{F}_p[X]$. Given a base $B \in \mathbb{F}_p[X]$ such that $\deg B = n$, each digit of a polynomial written on base B is actually an element of $\mathbb{F}_p^{(n)}[X]$ and, in order to be a digit of a polynomial written on base B, the digit has to be in $\mathbb{F}_p^{(n)}[X]$ meaning that when calculating any sum of polynomials on base B, the digits of the sum are still in $\mathbb{F}_p^{(n)}[X]$ given that a group is closed. Therefore, in contrast with the integer case, in the polynomial case there is no carry overs of digits and this derives on easier computation as we can see in equation (3.1) where we have a very regular form.

There is just one subtlety left. We can classify polynomials on equivalence classes by defining a relation $\sim$ where two polynomials are related if and only if their associated tuple of differences is the same.

Example 3.3. Let us consider the field $\mathbb{F}_{11}$ and the base $B = x^9 \in \mathbb{F}_{11}[X]$. We have

$$[x^8 + 6x^3 + 9, x^2, x^5 + x^3 + 7, 4x^6 + x^5, 9, x^7] \sim [x^8 + 6x^3, x^7 - x^2, 4x^6 - x^3 - 7, 0, 0, 0]$$

given that their tuple of differences is $(d_1, d_2, d_3) = (x^8 + 6x^3, x^7 - x^2, 4x^6 - x^3 - 7)$.

The reason to give such relation is that two related polynomials will lead to the same cycle given that their images are completely defined by their differences, this way, we can focus on a few class representatives instead of every polynomial while computing cycles.

The class representatives we choose are the polynomials with D digits and every element of the tuple zero except possibly the first $\lfloor D/2 \rfloor$ entries, meaning that we can restrict to work with polynomials of the form

$$[d_1, \cdots, d_{\lfloor D/2 \rfloor - 1}, d_{\lfloor D/2 \rfloor}, 0, 0, \cdots, 0, 0] \in \mathbb{F}_p[X]$$

with $d_i \in \mathbb{F}_p[X]$ for $1 \le i \le \lfloor D/2 \rfloor$ and p prime. With such polynomial we can get any possible image of Kaprekar's routine just by choosing the appropriates d_i's.

Two digits polynomials

Without loss of generality, we now work with polynomials of the form $f = [d_1, 0] \in \mathbb{F}_p$ with p prime. By induction, we get that $\kappa^r(f) = [2^{r-1}d_1, -2^{r-1}d_1]$ or $\kappa^r(f) = [-2^{r-1}d_1, 2^{r-1}d_1]$ where $r \in \mathbb{N}$ and $r \geq 1$ and this leads to the first proposition of the section.

Proposition 3.2. *Let us consider $p = 2$. For the case with the tuple $(B, 2)$ with $B \in \mathbb{F}_2[X]$ we have a unique cycle of length one (fixed point), namely, the constant 0 to which we arrive in up to 2 iterations of the routine.*

From now on, we work only with $p > 2$. Turns out in this case we cannot give a general form for the cycles since virtually every d_1 we give, leads to a different cycle. Given the latter, we focus our attention to get the exact number of different cycles.

At the beginning of the section we gave the form of the image of κ after any quantity of applications. We had two choices depending on the leading coefficient and now we explore the repercussions this may have. We will always refer to the leading coefficient of a polynomial as a_n. We have an example.

Example 3.4. We consider $f = [d_1, 0] = [3x^4 + 17x + 7, 0] \in \mathbb{F}_{31}[X]$ and identify $a_n = 3$. We have the cycle

$$\begin{tikzcd}
{[3x^4 + 17x + 7, 0]} \arrow[d] \\
{[3x^4 + 17x + 7, 28x^4 + 14x + 24]} \arrow[d] \\
{[25x^4 + 28x + 17, 6x^4 + 3x + 14]} \arrow[d] \\
{[19x^4 + 25x + 3, 12x^4 + 6x + 28]} \arrow[d] \\
{[7x^4 + 19x + 6, 24x^4 + 12x + 25]} \arrow[d] \\
{[17x^4 + 24x + 19, 14x^4 + 7x + 12]} \arrow[uuuu, bend right]
\end{tikzcd}$$

Notice that it is always a choice about the leading coefficient for it is the one that decides the order when doing the routine. For the second observation, we notice the apparition of the element $[d_1, -d_1]$ or $[-d_1, d_1]$ in the cycle and this is because as we saw in the beginning of the section, each iteration of the Kaprekar's routine is nothing more than a multiplication by a factor of 2 which eventually leads to multiply by 1 since 2 doesn't has an infinite order in $\mathbb{F}_p^\times$. Thus, our attention goes directly to the leading coefficient and the latter cycle would look like this if we were to limit ourselves to the leading coefficients

$$\begin{tikzcd}
{[3,0]} \arrow[r] & {[3,28]} \arrow[r] & {[25,6]} \arrow[r] & {[19,12]} \arrow[r] & {[7,24]} \arrow[r] & {[17,14]} \arrow[llll, bend right]
\end{tikzcd}$$

Then again, since this is all about multiplying by 2, we think of cosets of $\langle 2 \rangle$ in $\mathbb{F}_p^\times$ so each leading coefficient of the digits is in $3\langle 2 \rangle \cup 28\langle 2 \rangle = \{3, 6, 12, 24, 17\} \cup \{28, 25, 19, 7, 14\}$, meaning that, in general, the leading coefficients of a cycle in $\mathbb{F}_p[X]$ can be found in $a_n\langle 2 \rangle \cup -a_n\langle 2 \rangle$ where a_n is the leading coefficient of the polynomial we started the iterations with. Even more, we can conjecture that the length of the cycle is $|a_n\langle 2 \rangle \cup -a\langle 2 \rangle|/2$ and this also tells us that, given a p, the length of every cycle is the same. Not even the base appears in the calculation of the length of the cycle.

Example 3.5. Let us consider $[2x^7 + x^3 + 1, 0] \in \mathbb{F}_{17}[X]$. The leading coefficient is 2 so the cycle is

$$\begin{tikzcd}
{[2,0]} \arrow[r] & {[2,15]} \arrow[r] & {[13,4]} \arrow[r] & {[9,8]} \arrow[r] & {[1,16]} \arrow[r] & {[15,2]} \arrow[lll, bend right]
\end{tikzcd}$$

and we notice that all the leading coefficients are in the set $2\langle 2\rangle \cup 15\langle 2\rangle = \{2,4,8,16,15,13,9,1\}$ whose cardinality is consistent with the estimation of the length of the cycle we gave, $|2\langle 2\rangle \cup 15\langle 2\rangle|/2 = 4$.

If we change the leading coefficient for another in the same coset, we will have the same cycle. It is necessary to remark that we mean *same cycle* in the sense of the cycle with just the leading coefficients because it takes the change of only one coefficient (other than the leading one) to get a different cycle in the general sense.

Example 3.6. We now consider $[8x^9 + 7x^3 + 15, 0] \in \mathbb{F}_{17}[X]$. Now the leading coefficient is 8 so the cycle is

$$\begin{tikzcd}
{[8,0]} \arrow[r] & {[8,9]} \arrow[r] & {[1,16]} \arrow[r] & {[15,2]} \arrow[r] & {[13,4]} \arrow[r] & {[9,8]} \arrow[llll, bend right]
\end{tikzcd}$$

which is exactly the same cycle as before.

Now, since $\mathbb{F}_{17}^{\times}$ has actually two cosets of the subgroup $\langle 2\rangle$, namely, $2\langle 2\rangle$ and $3\langle 2\rangle$ we now give an example taking the leading coefficient from the latter.

Example 3.7. Let us consider $[12x^7 + 3x^4 + 2x + 13, 0] \in \mathbb{F}_{17}[X]$. The leading coefficient is $12 \in 3\langle 2\rangle$ and the cycle is

$$\begin{tikzcd}
{[12,0]} \arrow[r] & {[12,5]} \arrow[r] & {[7,10]} \arrow[r] & {[3,14]} \arrow[r] & {[11,6]} \arrow[r] & {[5,12]} \arrow[llll, bend right]
\end{tikzcd}$$

which has the same length as in the cases before but being a visibly different cycle.

Once the importance of cosets has been pointed out, we give the next example

Example 3.8. Let us consider $p = 31$ and $B \in \mathbb{F}_p[X]$ such that $\deg B = 4$. For this case, we have the cycles of leading coefficients

$$\begin{tikzcd}
{[1,30]} \arrow[r] & {[29,2]} \arrow[r] & {[27,4]} \arrow[r] & {[23,15]} \arrow[r] & {[15,16]} \arrow[llll, bend right]
\end{tikzcd}$$

$$\begin{tikzcd}
{[3,28]} \arrow[r] & {[25,6]} \arrow[r] & {[19,12]} \arrow[r] & {[7,24]} \arrow[r] & {[17,14]} \arrow[llll, bend right]
\end{tikzcd}$$

$$\begin{tikzcd}
{[5,26]} \arrow[r] & {[21,10]} \arrow[r] & {[11,20]} \arrow[r] & {[9,22]} \arrow[r] & {[13,18]} \arrow[llll, bend right]
\end{tikzcd}$$

which are taken from the sets

$$\langle 2\rangle \cup 30\langle 2\rangle = \{1,2,4,8,16,30,29,27,23,15\}$$

$$3\langle 2\rangle \cup 28\langle 2\rangle = \{3,6,12,24,17,28,25,19,7,14\}$$

$$5\langle 2\rangle \cup 26\langle 2\rangle = \{5,10,20,9,18,26,21,11,22,13\}$$

respectively.

Thus, no matter the leading coefficient we start with, we always end up in one of those cycles and the rest of coefficients of the digits don't have a say.

By now, we have noticed that if we want to know the exact number of different cycles, we have to know the exact number of the subsets of the form $a\langle 2\rangle \cup -a\langle 2\rangle$ that $\mathbb{F}_p^\times$ has and we denote this number by $\eta(p)$.

In the next proposition we give a computable value for $\eta(p)$.

Proposition 3.3. *Given a prime number $p > 2$,*

$$\eta(p) = \begin{cases} [\mathbb{F}_p^\times : \langle 2\rangle] & \text{if } -1 \in \langle 2\rangle \\ \dfrac{[\mathbb{F}_p^\times : \langle 2\rangle]}{2} & \text{if } -1 \notin \langle 2\rangle. \end{cases}$$

Now, putting our attention to the rest of the digits that are not the leading one, given that $[d_1, -d_1]$ (or its negative) is always an element of its respective cycle and that what happens with the leading coefficient is all described, we now want to know how many polynomials up to degree $n-1$ (given a base B such that $\deg B = n$) there exist. This is a straightforward computation since we just fix the leading coefficient and by multiplicative principle, we get that we have p^i polynomials of degree i with the fixed leading coefficient. We conclude that there exist

$$1 + p + p^2 + \cdots p^{n-2} + p^{n-1} = \frac{p^n - 1}{p - 1}$$

polynomials of degree less than n whose leading coefficient is fixed.

Thus, we get the final statement of the section, however, it remains a conjecture.

Conjecture 3.4. *Let us consider a prime number $p > 2$ and $B \in \mathbb{F}_p[X]$ a base such that $\deg B = n$. The number of cycles associated to Kaprekar's routine for the two digits polynomials on base B case is*

$$\eta(p)\left(\frac{p^n - 1}{p - 1}\right)$$

each of these cycles having length $\frac{|\langle 2\rangle \cup -1\langle 2\rangle|}{2}$. All that without considering the trivial cycle.

Example 3.9. Taking up example 3.8, we are now able to compute exactly how many different cycles there are. We see that $\eta(31) = 3$, since we explicitly computed the sets. Therefore, there is a total of

$$\eta(31)\left(\frac{31^4 - 1}{31 - 1}\right) = 92352$$

different cycles not considering the trivial one.

Three digits polynomials

For this case, we give directly the number of cycles, first for the case $p = 2$ and then for $p > 2$.

Proposition 3.5. *Let $B \in \mathbb{F}_2[X]$ be a base such that $\deg B = n$. The number of fixed points associated to Kaprekar's routine for the three digits polynomials on base B case is*

$$p^n = 2^n.$$

Even more, we reach these fixed points in up to two iterations.

Example 3.10. Let us consider $p = 2$ and $B \in \mathbb{F}_2[X]$ a base such that $\deg B = 3$. The class representatives are $[0,0,0]$, $[1,0,0]$, $[x,0,0]$, $[x^2,0,0]$, $[x+1,0,0]$, $[x^2+1,0,0]$, $[x^2+x,0,0]$ y $[x^2+x+1,0,0]$ and, the fixed points associated to each class are $[0,0,0]$, $[1,0,1]$, $[x,0,x]$, $[x^2,0,x^2]$, $[x+1,0,x+1]$, $[x^2+1,0,x^2+1]$, $[x^2+x,0,x^2+x]$ y $[x^2+x+1,0,x^2+x+1]$, respectively. This way, we have a total of $2^{\deg B} = 2^3 = 8$ fixed points, just as we expected.

Proposition 3.6. *Let us consider a prime number $p > 2$ and $B \in \mathbb{F}_p[X]$ a base such that $\deg B = n$. The number of fixed points associated to Kaprekar's routine for the three digits polynomials on base B case is*

$$\frac{p^n - 1}{2}.$$

without considering the trivial fixed point. Even more, we reach these fixed points in up to two iterations.

Example 3.11. Let us consider $p = 3$ and $B \in \mathbb{F}_3[X]$ a base such that $\deg B = 2$. In this case, the class representatives are $[0,0,0]$, $[x,0,0]$, $[1,0,0]$, $[x+1,0,0]$, $[2x,0,0]$, $[2,0,0]$, $[2x+2,0,0]$, $[2x+1,0,0]$ and $[x+2,0,0]$ but we notice that a polynomial and its additive inverse both lead to the same fixed point, so aside from the zero polynomial, we can rule out half of the class representatives. Thus, we reach the fixed points $\kappa([0,0,0]) = [0,0,0]$, $\kappa([x,0,0]) = [x,0,2x]$, $\kappa([1,0,0]) = [1,0,2]$, $\kappa([x+1,0,0]) = [x+1,0,2x+2]$, $\kappa([x+2,0,0]) = [x+2,0,2x+1]$, that is to say that, without considering the trivial fixed point, we have exactly $\frac{3^2-1}{2} = 4$ non trivial fixed points just as the formula stated.

Some examples on non prime finite fields

Despite us only working with finite fields of prime characteristic, we will see that these same formulae and results work fine with non prime finite fields just making the proper changes.

Regarding the order of the elements of $\mathbb{F}_q$ with $q = p^n$, we remember that

$$\mathbb{F}_q = \frac{\mathbb{F}_p[X]}{(f)}$$

where f is an irreducible polynomial of $\mathbb{F}_p[X]$, and thus, the elements of $\mathbb{F}_q$ are polynomials of $\mathbb{F}_p[X]$ whose degree is less than $\deg f$ and so we stick to the polynomial order we gave before.

Proposition 3.2 can be generalized to non prime finite fields, that is to say, the result provided is still true for $\mathbb{F}_{2^n}[X]$ with $n \in \mathbb{N}$, since the characteristic does not change.

Example 3.12. Let us consider $\mathbb{F}_4$ and a base $B \in \mathbb{F}_4[X]$. Thus,

$$\mathbb{F}_4 = \frac{\mathbb{F}_2[X]}{(x^2+x+1)} = \{\alpha+1, \alpha, 1, 0\}$$

given that α is a root of $x^2+x+1 \in \mathbb{F}_2[X]$. Now, we start the routine with a polynomial $f = [(\alpha+1)x^2 + 1, 0] \in \mathbb{F}_4[X]$ and get

$$\kappa(f) = [(\alpha+1)x^2+1, 0] - [0, (\alpha+1)x^2+1] = [(\alpha+1)x^2+1, (\alpha+1)x^2+1]$$

$$\kappa^{(2)}(f) = [(\alpha+1)x^2+1, (\alpha+1)x^2+1] - [(\alpha+1)x^2+1, (\alpha+1)x^2+1] = [0,0]$$

just as expected.

As for the case with $p > 2$

Example 3.13. We take $\mathbb{F}_9$ and a base $B \in \mathbb{F}_9[X]$ such that $\deg B = 2$. Now,

$$\mathbb{F}_9 = \frac{\mathbb{F}_3[X]}{(x^2+1)} = \{2\alpha+2, 2\alpha+1, 2\alpha, \alpha+2, \alpha+1, \alpha, 2, 1, 0\}$$

given that α is a root of $x^2+1 \in \mathbb{F}_3$. Now, we calculate $\eta(9)$, where of course we extend the definition of η now considering powers of p, and get

$$1\langle 2\rangle \cup -1\langle 2\rangle = \{1, 2\}$$

$$\alpha\langle 2\rangle \cup -\alpha\langle 2\rangle = \{\alpha, 2\alpha\}$$
$$(\alpha+1)\langle 2\rangle \cup -(\alpha+1)\langle 2\rangle = \{\alpha+1, 2\alpha+2\}$$
$$(\alpha+1)\langle 2\rangle \cup -(\alpha+2)\langle 2\rangle = \{\alpha+2, 2\alpha+1\}$$

meaning that $\eta(9) = 4$. For a better understanding, we consider $f = [2x + (2\alpha+1), 0] \in \mathbb{F}_9[X]$ (notice that $a_n = 2 \in 1\langle 2\rangle \cup -1\langle 2\rangle$) and start the routine to get

$$\begin{tikzcd}
{[2x+(2\alpha+1),0]} \arrow[d] \\
{[2x+(2\alpha+1), x+(\alpha+2)]} \arrow[d] \\
{[x+(\alpha+2), 2x+(2\alpha+1)]} \arrow[loop right]
\end{tikzcd}$$

a cycle of length $|\langle 2\rangle \cup -1\langle 2\rangle|/2 = 1$. As stated in the prime case, the leading coefficients stay the same and we just have to use the multiplicative principle over the non leading coefficients and this has to be done for each set of the form $a\langle 2\rangle \cup -a\langle 2\rangle$. Thus, we can conclude we have

$$\eta(9)\left(\frac{9^2-1}{9-1}\right) = 40$$

different cycles without considering the trivial one.

Regarding the three digits polynomials, we see that the situation is pretty much the same than that of the two digits polynomials. We first consider $q = 2^n$, but since the characteristic is still 2 and $1 = -1$, the result will be the same as if we stuck with q prime.

Example 3.14. Let us consider $q = 4$ and a base $\mathbb{B} \in \mathbb{F}_4[X]$ such that $\deg B = 2$. Thus, the equivalence classes are $[(\alpha+1)x+(\alpha+1),0]$, $[(\alpha+1)x+\alpha,0]$, $[(\alpha+1)x+1,0]$, $[(\alpha+1)x,0]$, $[\alpha x+(\alpha+1),0]$, $[\alpha x+\alpha,0]$, $[\alpha x+1,0]$, $[\alpha x,0]$, $[x+(\alpha+1),0]$, $[x+\alpha,0]$, $[x+1,0]$, $[x,0]$, $[(\alpha+1),0]$, $[\alpha,0]$, $[1,0]$, $[0,0]$ and after one iteration of Kaprekar's routine we reach the fixed points and they are all different. We conclude that there are exactly $p^n = 4^2 = 16$ different cycles.

Now, regarding the $p > 2$ case, we do not make an explicit computation since the smaller case $q = 3^2$ with a base of degree 2 would give us 81 classes to deal with, but we do mention it is still true that a polynomial and its additive inverse they both reach the same fixed points so the computation is the same as in the case with q prime, namely, $\frac{q^n-1}{2}$ different cycles plus the trivial one.

Acknowledgments

The authors would like to thank Dinesh S. Thakur for his careful reading and valuable suggestions.

Referencias

[1] G. Effinger, K. Hicks and G. Mullen. Integers and polynomials: comparing the close cousins **Z** and $\mathbf{F}_q[x]$. *Math. Intelligencer*, **27**(2):26-34, 2005.

[2] D. Kaprekar. An interesting property of the number 6174. *Scripta Mathematica*, 1955.

[3] M. Moreira. Dihedral symmetry in Kaprekar's problem. *Math. Mag.*, **90**(1):39-47, 2017.

[4] D. Thakur. Kaprekar Phenomena. *Number theory: Arithmetic, Diophantine and Transcendence.* Proceeding of Ropar Conference, RMS-Lecture Notes Series No. 26, 61-70, 2020.