Problem 7: Friendly Polynomials

Team: France 2

June 21, 2010

Abstract

This problem consists in finding all friendly polynomials P in $\mathbb{F}_p[x]$ and in $\mathbb{C}[x]$. A polynomial is friendly when it is not coprime with any of its derivatives.
We have succeded in showing that all polynomials in the form of $P(X) = c(X-a)^n$ are friendly on $\mathbb{F}_p$ and on $\mathbb{C}$. In $\mathbb{F}_p$, We have also shown that all polynomials which have any root of multiplicity upper than p are friendly.
We have also proved that when all the roots of a polynomials have the same multiplicity in $\mathbb{C}$, this polynomial is not friendly. For all other cases, the polynomials seem not to be friendly. It is verified for $n \leq 5$.
In our proofs, we used the theorem of the algebraic closure and the d'Alembert-Gauss theorem to factorize all the polynomials. We also needed the Newton binomial coefficients in a field. To derivate the polynomials, we used the Leibniz Rule.

1 Problem exposition

Let K be some field, and K[x] the set of polynomials with coefficients from K. Given such a polynomial $P(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$, the following polynomial

$$P^{(1)}(x) = (P(x))' = n a_n x^{n-1} + \cdots + 2a_2 x + a_1$$

is called the *(first) derivative* of P. Denote by $P^{(k)}$ the k^{th} successive derivative of P, it is defined recursively by

$$P^{(k)}(x) = (P^{(k-1)}(x))' \text{ for } k \geq 2.$$

We say that $Q \in K[x]$ *divides* P if there is a polynomial $R \in K[x]$ such that $P = QR$. Two polynomials $P_1, P_2 \in K[x]$ are said to be *coprime* if there is no polynomial $Q \in K[x]$ of degree at least 1 that divides both P_1 and P_2.

We will call a polynomial $P \in K[x]$ of degree n friendly if it is not coprime with any of its derivatives, that is, for all $1 \leq k < n$, the polynomials P and $P^{(k)}$ share a common divisor of degree at least 1.

1. Consider the field $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ of residue classes modulo a prime p. Try to find all friendly polynomials $P \in F_p[x]$ of degree $n \in \mathbb{N}$.

2. Let $\mathbb{C}$ be the field of complex numbers. Is it true that if a polynomial $P \in \mathbb{C}[x]$ of degree n is friendly then $P(x) = c(x-a)^n$ for some $a, c \in \mathbb{C}$? Study this question for particular values of n (*e.g.*, $2, 3, 4, 5$), and also when n is a prime number, a power of a prime number, etc.

2 Preliminary:

Let's remind some usual theorems:

Theorem 1. *[1] every field* $\mathbb{K}$ *as an algebraic closure* $\bar{\mathbb{K}}$ *where any polynomial can be factorized into linear factors* $P(X) = c(X-\alpha_1)^{l_1}\cdots(X-\alpha_m)^{l_m}$

Definition 1. *[2] Let* $\mathbb{K}$ *a field and* $P \in \mathbb{K}[X]$ *a polynomial: the sub-field of* $\bar{\mathbb{K}}$ *generated by* $\mathbb{K}$ *and the roots of* P *is called the* splitting field *of* P

Theorem 2. (d'Alembert-Gauß) *[3]*
$\mathbb{C}$ *is algebraically closed i.e.* $\mathbb{C} = \bar{\mathbb{C}}$.

Definition 2. *Let's define the* falling factorial *[4] in the field* $\mathbb{K}$ *denoted with the following symbol by:*

$$(n)_k = n(n-1)\ldots(n-k+1) = \left(\frac{n!}{(n-k)!}\right)_{\mathbb{N}} \cdot 1_{\mathbb{K}}$$

Lemma 1. *Let's call* $\mathrm{mod}(n,p)$ *the rest of the euclidean division of* n *by* p.
If $\mathrm{char}(K) = p$ *we have*

$$(n)_d = 0 \Leftrightarrow \exists a, k \in \mathbb{N} \text{ such as } n-d < k \leq n \text{ and } k = ap$$

so

$$(n)_d = 0 \text{ for } d > \mathrm{mod}(n,p)$$

(see example in table 1 p. 3)

Definition 3. *let's define the* Newton binomial coefficients *in* $\mathbb{K}$ *as:*

$$\binom{n}{k} = \left(\frac{n!}{k!(n-k)!}\right)_{\mathbb{N}} \cdot 1_{\mathbb{K}}$$

the properties of these coefficients and of the Pascal's triangle in $\mathbb{F}_p$ *where studied by Vincent Lefèvre (Fermat junior prize 1991) [5].*

$(n)_k$ | k	1	2	3	4	5
n					
1	1	0...			
2	2	2	0...		
3	3	1	1	0...	
4	4	2	4	4	0...
5	0...				
6	1	0...			
7	2	2	0...		

Table 1: falling factorials in $\mathbb{F}_5$

1
1 1
1 2 1
1 3 3 1
1 4 1 4 1
1 **0 0 0 0** 1
1 1 **0 0 0** 1 1
1 2 1 **0 0** 1 2 1
1 3 3 1 **0** 1 3 3 1
1 4 1 4 1 1 4 1 4 1
1 **0 0 0 0** 2 **0 0 0 0** 1
1 1 **0 0 0** 2 2 **0 0 0** 1 1
1 2 1 **0 0** 2 4 2 **0 0** 1 2 1
1 3 3 1 **0** 2 1 1 2 **0** 1 3 3 1
1 4 1 4 1 2 3 2 3 2 1 4 1 4 1
1 **0 0 0 0** 3 **0 0 0 0** 3 **0 0 0 0** 1
1 1 **0 0 0** 3 3 **0 0 0** 3 3 **0 0 0** 1 1
1 2 1 **0 0** 3 1 3 **0 0** 3 1 3 **0 0** 1 2 1
1 3 3 1 **0** 3 4 4 3 **0** 3 4 4 3 **0** 1 3 3 1
1 4 1 4 1 3 2 3 2 3 3 2 3 2 3 1 4 1 4 1
1 **0 0 0 0** 4 **0 0 0 0** 1 **0 0 0 0** 4 **0 0 0 0** 1
1 1 **0 0 0** 4 4 **0 0 0** 1 1 **0 0 0** 4 4 **0 0 0** 1 1
1 2 1 **0 0** 4 3 4 **0 0** 1 2 1 **0 0** 4 3 4 **0 0** 1 2 1
1 3 3 1 **0** 4 2 2 4 **0** 1 3 3 1 **0** 4 2 2 4 **0** 1 3 3 1
1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1
1 **0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0** 1
1 1 **0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0** 1 1
1 2 1 **0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0** 1 2 1

Table 2: Pascal triangle in $\mathbb{F}_5$

Lemma 2. *In $\mathbb{F}_p$, if $q = p^k$, $\binom{q}{k} = 0$ for $k \neq 1$ and $k \neq n$. (see example in table 2 p. 4)*

Lemma 3. *Let P, Q polynomials with coefficients in $\mathbb{K}$, assuming these definitions, the* Leibniz rule *[6] holds:*

$$(P.Q)^{(d)} = \sum_{k=0}^{d} \binom{d}{k}_{\mathbb{K}} P^{(k)} Q^{(d-k)}$$

Lemma 4. *If $P = cQ$ with $P, Q \in \mathbb{K}[X]$ and $c \in \mathbb{K} \setminus \{0\}$, P is friendly iff Q is friendly. So we can from now on drop the constant and work with monic polynomials.*

3 First question $\mathbb{K} = \mathbb{F}_p$:

Proposition 3.1. *Polynomials of the form*

$$P(X) = c(X - \alpha)^n$$

are friendly

Proof. The d^{th} derivative of P is:

$$P^{(d)}(X) = c(n)_d(X - \alpha)^{n-d}$$

If $\text{char}(K) = p$ we have

$$(n)_d = 0 \Leftrightarrow \exists a, k \in \mathbb{N} \text{ such as } n-d < k \leq n \text{ and } k = ap$$

so

$$(n)_d = 0 \text{ for } d > \text{mod}(n, p) \text{ by lemma 1}$$

If $n < p$, then $\text{mod}(n, p) = n$ and P shares the $(X - \alpha)$ factor with all its derivatives up to the $n - 1$ rank. Following derivatives are constant or null.

If $n \geq p$, then $\text{mod}(n + 1, p)$ derivative and followings are null.

Both cases are friendly. □

Proposition 3.2. *Let $P \in \mathbb{K}[X]$ and $\mathbb{K}_P$ the splitting field of P, if any root of P in $\mathbb{K}_P$ as a multiplicity $\geq p$, then P is friendly.*

Proof. Let $P(X) = L(X)^l Q(X)$ with $L(X) = X - \alpha$ and $l \geq p$, by euclidean division, $\exists k, r \in \mathbb{N}$ such that $l = ap + r$ and $r < p$.

Let's express Leibniz formula for $d = r$

$$\begin{aligned} P^{(r)} = (L^l.Q)^{(r)} &= \sum_{k=0}^{r} \binom{r}{k} (l)_k L^{l-k} Q^{(r-k)} \\ &= \sum_{k=0}^{r} (l)_k \binom{r}{k} L^{ap+r-k} Q^{(r-k)} \\ &= L^{ap} \sum_{k=0}^{r} (l)_k \binom{r}{k} L^{r-k} Q^{(r-k)} \\ &= L^{ap} \left[\sum_{k=0}^{r-1} (l)_k \binom{r}{k} L^{r-k} Q^{(r-k)} + (l)_r Q \right] \end{aligned}$$

Let $R = \sum_{k=0}^{r-1} (l)_k \binom{r}{k} L^{r-k} Q^{(r-k)} + (l)_r Q$, R as degree $n - l$
We have

$$\begin{aligned} P^{(r+1)} &= apL^{ap-1}R + L^{ap}R' \\ &= L^{ap}R' \\ \forall i \geq 1 \; P^{(r+i)} &= L^{ap}R^{(i)} \end{aligned}$$

$R^{(i)}$ as degree $n-l-i$ so when $i = n-l$ we have $P^{(r+i)} = cL^{ap}$ and $P^{(r+i+1)} = 0$ and P is friendly

□

Remark : No result has been proved when all roots in $\bar{\mathbb{F}}_p$ have a multiplicity $< p$ and at least 2 roots have different multiplicities, but it seems that these polynomials are not friendly.

4 Second question $\mathbb{K} = \mathbb{C}$:

From theorem 2, $\mathbb{C}$ is algebraically closed and any polynomial can be expressed as a product of linear polynomials.

$$P(X) = c\prod_{i=1}^{m} L_i(X)^{l_i} \text{ with } L_i(X) = X - \alpha_i$$

Proposition 4.1. *Polynomials of the form*

$$P(X) = c(X-\alpha)^n$$

are friendly

Proof. The d^{th} derivative of P is:

$$P^{(d)}(X) = (n)_d(X-\alpha)^{n-d}$$

$(n)_d \neq 0$ for $d < n$, so P and $P^{(d)}$ share $(X-\alpha)$ as common factor
(Remark: for $d = n$ we have $P^{(n)}(X) = n!$ (constant), and
for $d > n$ we have $P^{(d)}(X) = 0$)
so P is friendly. □

Proposition 4.2. *Powers of separable polynomials i.e. polynomials of the form:*

$$P(X) = c\left[(X-\alpha_1)...(X-\alpha_m)\right]^l \text{ with } l, m \in \mathbb{N}^\star, m \geq 2 \text{ and } \alpha_i \neq \alpha_j \forall i \neq j$$

are not friendly.

Proof. Let's follow any one of the roots and call L the linear polynomial $X-\alpha$: we have $P = L^l Q$ with $\gcd(L, Q) = 1$

Let's express Leibniz formula for $d = l$:

$$\begin{aligned} P^{(l)} = (L^l.Q)^{(l)} &= \sum_{k=0}^{l} (l)_k \binom{l}{k} L^{l-k} Q^{(l-k)} \\ &= L\sum_{k=0}^{l-1} (l)_k \binom{l}{k} L^{l-1-k} Q^{(l-k)} + l!Q \end{aligned}$$

$P^{(l)}$ is the sum of a polynomial with factor L and of a polynomial without factor L, so $P^{(l)}$ is coprime with L.

By reitering the operation on all roots we can see that no root of P can be a root of $P^{(l)}$.

So $\gcd(P, P^{(l)}) = 1$.

□

Let's study the other cases for $n = 2, \ldots, 5$:
Case $n = 2$

There are only two possibilities:

- $P(X) = (X - \alpha_1)^2$ is friendly from prop. 4.1.
- $P(X) = (X - \alpha_1)(X - \alpha_2)$ is not friendly from prop. 4.2.

Case $n = 3$

- $P(X) = (X - \alpha_1)^2 (X - \alpha_2)$

  $P^{(1)}(X) = (X - \alpha_1)(3X - 2\alpha_2 - \alpha_1)$
  $\gcd(P(X), P^{(1)}(X)) = X - \alpha_1$

  $P^{(2)}(X) = 2(3X - \alpha_2 - 2\alpha_1)$
  $\boxed{\gcd(P(X), P^{(2)}(X)) = 1 \text{ if } \alpha_1 \neq \alpha_2}$

Case $n = 4$

- $P(X) = (X - \alpha_1)^3 (X - \alpha_2)$

  $P^{(1)}(X) = (X - \alpha_1)^2 (4X - 3\alpha_2 - \alpha_1)$
  $\gcd(P(X), P^{(1)}(X)) = (X - \alpha_1)^2$

  $P^{(2)}(X) = 6(X - \alpha_1)(2X - \alpha_2 - \alpha_1)$
  $\gcd(P(X), P^{(2)}(X)) = X - \alpha_1$

  $P^{(3)}(X) = 6(4X - \alpha_2 - 3\alpha_1)$
  $\boxed{\gcd(P(X), P^{(3)}(X)) = 1 \text{ if } \alpha_1 \neq \alpha_2}$

- $P(X) = (X - \alpha_1)^2 (X - \alpha_2)(X - \alpha_3)$

  $P^{(1)}(X) = (X - \alpha_1)(4X^2 - 3\alpha_3 X - 3\alpha_2 X - 2\alpha_1 X + 2\alpha_2\alpha_3 + \alpha_1\alpha_3 + \alpha_1\alpha_2)$
  $\gcd(P(X), P^{(1)}(X)) = X - \alpha_1$

  $P^{(2)}(X) = 2(6X^2 - 3\alpha_3 X - 3\alpha_2 X - 6\alpha_1 X + \alpha_2\alpha_3 + 2\alpha_1\alpha_3 + 2\alpha_1\alpha_2 + \alpha_1^2)$
  $P^{(2)}(X) = (x - \alpha_2)[2(x - \alpha_3) + 4(x - \alpha_1)] + 2(x - \alpha_1)(3x - 2\alpha_3 - \alpha_1)$
  if α_2 is the common root between P and $P^{(2)}$ we must have $\alpha_2 = \frac{2\alpha_3 + \alpha_1}{3}$.

  $P^{(3)}(X) = 6(4X - \alpha_3 - \alpha_2 - 2\alpha_1)$
  $\Rightarrow \frac{2\alpha_1 + \alpha_2 + \alpha_3}{4} = \frac{5\alpha_3 + 7\alpha_1}{12} = \{\alpha_1 \text{ or } \alpha_2 \text{ or } \alpha_3\}$ all cases lead to $\alpha_1 = \alpha_2 = \alpha_3$

Case $n = 5$

- $P(X) = (X - \alpha_1)^4 (X - \alpha_2)$

  $P^{(1)}(X) = (X - \alpha_1)^3 (5 X - 4 \alpha_2 - \alpha_1)$
  $\gcd(P(X), P^{(1)}(X)) = (X - \alpha_1)^3$

  $P^{(2)}(X) = 4 (X - \alpha_1)^2 (5 X - 3 \alpha_2 - 2 \alpha_1)$
  $\gcd(P(X), P^{(2)}(X)) = (X - \alpha_1)^2$

  $P^{(3)}(X) = 12 (X - \alpha_1) (5 X - 2 \alpha_2 - 3 \alpha_1)$
  $\gcd(P(X), P^{(3)}(X)) = X - \alpha_1$

  $P^{(4)}(X) = 24 (5 X - \alpha_2 - 4 \alpha_1)$
  $\boxed{\gcd(P(X), P^{(4)}(X)) = 1 \text{ if } \alpha_1 \neq \alpha_2}$

- $P(X) = (X - \alpha_1)^3 (X - \alpha_2)^2$

  $P^{(1)}(X) = (X - \alpha_1)^2 (X - \alpha_2) (5 X - 3 \alpha_2 - 2 \alpha_1)$
  $\gcd(P(X), P^{(1)}(X)) = (X - \alpha_1)^2 (X - \alpha_2)$

  $P^{(2)}(X) = 2 (X - \alpha_1) (10 X^2 - 12 \alpha_2 X - 8 \alpha_1 X + 3 \alpha_2^2 + 6 \alpha_1 \alpha_2 + \alpha_1^2)$
  $\gcd(P(X), P^{(2)}(X)) = X - \alpha_1$

  $P^{(3)}(X) = 6 (10 X^2 - 8 \alpha_2 X - 12 \alpha_1 X + \alpha_2^2 + 6 \alpha_1 \alpha_2 + 3 \alpha_1^2)$

  $P^{(4)}(X) = 24 (5 X - 2 \alpha_2 - 3 \alpha_1)$
  $\boxed{\gcd(P(X), P^{(4)}(X)) = 1 \text{ if } \alpha_1 \neq \alpha_2}$

- $P(X) = (X - \alpha_1)^3 (X - \alpha_2) (X - \alpha_3)$

  $P^{(1)}(X) = (X - \alpha_1)^2 (5 X^2 - 4 \alpha_3 X - 4 \alpha_2 X - 2 \alpha_1 X + 3 \alpha_2 \alpha_3 + \alpha_1 \alpha_3 + \alpha_1 \alpha_2)$
  $\gcd(P(X), P^{(1)}(X)) = (X - \alpha_1)^2$

$P^{(2)}(X) = 2\,(X-\alpha_1)\,(10\,X^2-6\,\alpha_3\,X-6\,\alpha_2\,X-8\,\alpha_1\,X+3\,\alpha_2\,\alpha_3+3\,\alpha_1\,\alpha_3+3\,\alpha_1\,\alpha_2+\alpha_1^2)$
$\gcd(P(X), P^{(2)}(X)) = X-\alpha_1$

$P^{(3)}(X) = 6\,(10\,X^2-4\,\alpha_3\,X-4\,\alpha_2\,X-12\,\alpha_1\,X+\alpha_2\,\alpha_3+3\,\alpha_1\,\alpha_3+3\,\alpha_1\,\alpha_2+3\,\alpha_1^2)$

$P^{(4)}(X) = 24\,(5\,X-\alpha_3-\alpha_2-3\,\alpha_1)$

- $P(X) = (X-\alpha_1)^2\,(X-\alpha_2)^2\,(X-\alpha_3)$

$P^{(1)}(X) = (X-\alpha_1)\,(X-\alpha_2)\,(5\,X^2-4\,\alpha_3\,X-3\,\alpha_2\,X-3\,\alpha_1\,X+2\,\alpha_2\,\alpha_3+2\,\alpha_1\,\alpha_3+\alpha_1\,\alpha_2)$
$\gcd(P(X), P^{(1)}(X)) = (X-\alpha_1)\,(X-\alpha_2)$

$P^{(2)}(X) = 2\,(10\,X^3-6\,\alpha_3\,X^2-12\,\alpha_2\,X^2-12\,\alpha_1\,X^2+6\,\alpha_2\,\alpha_3\,X+6\,\alpha_1\,\alpha_3\,X+3\,\alpha_2^2\,X+12\,\alpha_1\,\alpha_2\,X+3\,\alpha_1^2\,X-\alpha_2^2\,\alpha_3-4\,\alpha_1\,\alpha_2\,\alpha_3-\alpha_1^2\,\alpha_3-2\,\alpha_1\,\alpha_2^2-2\,\alpha_1^2\,\alpha_2)$

$P^{(3)}(X) = 6\,(10\,X^2-4\,\alpha_3\,X-8\,\alpha_2\,X-8\,\alpha_1\,X+2\,\alpha_2\,\alpha_3+2\,\alpha_1\,\alpha_3+\alpha_2^2+4\,\alpha_1\,\alpha_2+\alpha_1^2)$

$P^{(4)}(X) = 24\,(5\,X-\alpha_3-2\,\alpha_2-2\,\alpha_1)$

- $P(X) = (X-\alpha_1)^2\,(X-\alpha_2)\,(X-\alpha_3)\,(X-\alpha_4)$

$P^{(1)}(X) = (X-\alpha_1)\,(5\,X^3-4\,\alpha_4\,X^2-4\,\alpha_3\,X^2-4\,\alpha_2\,X^2-3\,\alpha_1\,X^2+3\,\alpha_3\,\alpha_4\,X+3\,\alpha_2\,\alpha_4\,X+2\,\alpha_1\,\alpha_4\,X+3\,\alpha_2\,\alpha_3\,X+2\,\alpha_1\,\alpha_3\,X+2\,\alpha_1\,\alpha_2\,X-2\,\alpha_2\,\alpha_3\,\alpha_4-\alpha_1\,\alpha_3\,\alpha_4-\alpha_1\,\alpha_2\,\alpha_4-\alpha_1\,\alpha_2\,\alpha_3)$
$\gcd(P(X), P^{(1)}(X)) = X-\alpha_1$

$P^{(2)}(X) = 2\,(10\,X^3-6\,\alpha_4\,X^2-6\,\alpha_3\,X^2-6\,\alpha_2\,X^2-12\,\alpha_1\,X^2+3\,\alpha_3\,\alpha_4\,X+3\,\alpha_2\,\alpha_4\,X+6\,\alpha_1\,\alpha_4\,X+3\,\alpha_2\,\alpha_3\,X+6\,\alpha_1\,\alpha_3\,X+6\,\alpha_1\,\alpha_2\,X+3\,\alpha_1^2\,X-\alpha_2\,\alpha_3\,\alpha_4-2\,\alpha_1\,\alpha_3\,\alpha_4-2\,\alpha_1\,\alpha_2\,\alpha_4-\alpha_1^2\,\alpha_4-2\,\alpha_1\,\alpha_2\,\alpha_3-\alpha_1^2\,\alpha_3-\alpha_1^2\,\alpha_2)$

$P^{(3)}(X) = 6\,(10\,X^2-4\,\alpha_4\,X-4\,\alpha_3\,X-4\,\alpha_2\,X-8\,\alpha_1\,X+\alpha_3\,\alpha_4+\alpha_2\,\alpha_4+2\,\alpha_1\,\alpha_4+\alpha_2\,\alpha_3+2\,\alpha_1\,\alpha_3+2\,\alpha_1\,\alpha_2+\alpha_1^2)$

$$P^{(4)}(X) = 24\,(5\,X - \alpha_4 - \alpha_3 - \alpha_2 - 2\,\alpha_1)$$

We can see that no other polynomial than those of the form $P(X) = c(X - \alpha)^n$ are friendly for $n = 2, \ldots, 5$.

Remark : No result has been proved in general when at least 2 roots in $\mathbb{C}$ have different multiplicities, but it seems that these polynomials are not friendly.

References

[1] `http://en.wikipedia.org/wiki/Algebraic_closure`

[2] `http://en.wikipedia.org/wiki/Splitting_field`

[3] `http://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra`

[4] Weisstein, Eric W. "Falling Factorial." From MathWorld–A Wolfram Web Resource. `http://mathworld.wolfram.com/FallingFactorial.html`

[5] Vincent Lefèvre, Triangle de Pascal dans Z/pZ avec p premier `http://www.vinc17.org/math/trg_pascal.pdf`

[6] `http://en.wikipedia.org/wiki/General_Leibniz_rule`