Problem 7 :
Friendly Polynomials

Team : France 3

Abstract

For this problem we found one sufficient condition in $\mathbb{F}_p[X]$. In $\mathbb{C}[X]$, we studied the cases $n = 4$ and $n = 5$, the solving of cases $n = 2$ and $n = 3$ being obvious enough not to be mentioned.

Question 1

Lemma : $\forall P \in \mathbb{F}_p[X],\ P^{(p)}(X) = 0$

Proof: Let P be a polynomial of degree $n > p$ (the case $n \leq p$ needn't be studied.)

P can be written thus :

$$P(X) = \sum_{i=0}^{n} a_i X^i \text{ with } a_i \in \mathbb{F}_p$$

We define M_i the monomial of degree i of P : hence $M_i(X) \ = \ a_i X^i$

- either $i < p$ then we have $M_i^{(p)}(X) \ = 0.$
- or $i \geq p$ then we have $M_i^{(p)}(X) \ = a_i(i-1)(i-2)...(i-p)X^{i-p}$
  however $(i-1)(i-2)...(i-p) = 0 \ mod(p)$ so $M_i^{(p)}(X) = 0$

hence, by addition : $\boxed{P^{(p)}(X) = 0}$

1.1 Sufficient condition in $\mathbb{F}_p[X]$.

Let $Q \in \mathbb{F}_p[X],\ deg(Q) \geq 1$, $R \in \mathbb{F}_p[X]$ and $n \geq p$, if $P = Q^n R$ then P is friendly.

Proof :

- **Corollary** : Let $F \in \mathbb{F}_p[X]$, let $n \in \mathbb{N}^*$, $\forall j < n \quad F|(F^n)^{(j)}$

  We show by induction that $F^{n-j}|(F^n)^{(j)} \quad \forall j \ \in [0;n]$

  Basis : $(F^n)' = nF'F^{n-1}$ so $F^{n-1}|(F^n)'$

  Inductive step : Suppose, for $j \in [0; n-1]$: $F^{n-j}|(F^n)^{(j)}$, which means that $\exists G \in \mathbb{F}_p[x]$ such as $(F^n)^{(j)} = GF^{n-j}$

  Derivate : $(F^n)^{(j+1)} \ = \ G'F^{n-j}(n-j)GF'F^{n-(j+1)} \ = \ F^{n-(j+1)}(G'F + (n-j)GF'F)$

  Hence $F^{n-(j+1)}|(F^n)^{(j+1)}$.

  So $F^{n-j}|(F^n)^{(j)} \quad \forall j \ \in [0;n]$ hence $\forall j < n \quad F|(F^n)^{(j)}$

- Back to P : proving that P is friendly comes down to proving that, $\forall i \in [0; p-1]$, P shares a divider of degree at least 1 with $P^{(i)}$.
  As, according to Leibniz:

$$P^{(i)} = \sum_{k=0}^{i} \binom{i}{k} \ R^{(k)}(Q^n)^{(i-k)} \quad \forall i \in [0; p-1]$$

We have, thanks to the corollary :

$$Q|P^{(i)} \qquad \forall i \in [0;p] \text{ so } \boxed{P \text{ is friendly}}$$

Question 2 In $\mathbb{C}[X]$ polynomials can be factored as a product of polynomials of degree 1.

$$P(x) = c(x-a_1)(x-a_2)\cdots(x-a_n)$$

for a polynomial of degree$n$. The a_i are necessarily distinct. P is friendly if he shares at least one root with each of his derivates.

P and his first derivate P' share a root iff this root is double for P

$$P(x) = (x-a)Q(x)$$
$$P'(x) = (x-a)Q'(x) + Q(x)$$

$P'(a) = 0$ iff $Q(a) = 0$ and $P(x) = (x-a)^2R(x)$
so if P is , he has at least a double root.

- Case $n = 2$

  P is *friendly* iff $P(x) = c(x-a)^2$

- Case $n = 3$

  $$P(x) = c(x-a_1)^2(x-a_2)$$
  $$P'(x) = c(x-a_1)((x-a_1) + 2(x-a_2))$$
  $$P"(x) = 3c(x-a_1) + c((x-a_1) + 2(x-a_2) = (4c)(x-a_1) + 2c(x-a_2)$$

  If $P"(a_i) = 0$, then $a_1 = a_2 = a$ and $P(x) = c(x-a)^3$

  From now on define :

  $$P(x) = (x-a_1)^2R(x)$$
  $$P'(x) = (x-a_1)^2R'(x) + 2(x-a_1)R(x)$$
  $$P"(x) = (x-a_1)^2R"(x) + 4(x-a_1)R'(x) + 2R(x)$$
  $$P^{(k)}(x) = (x-a_1)^2R^{(k)}(x) + 2k(x-a_1)R^{(k-1)}(x) + k(k-1)R^{(k-2)}(x)$$

- Case $n = 4$

  $$R(x) = (x-a_2)(x-a_3)$$
  $$R'(x) = (x-a_2) + (x-a_3)$$
  $$R"(x) = 2$$

  For $i \neq 1$, $R(a_i) = 0$, $R(a_i) = (a_i - a_j)$
  Define $b_i = a_i - a_1$, thus $a_i - a_j = b_i - b_j$

* Suppose $P^i(a_i) = 0$

$$P^{(2)}(a_2) = (a_2 - a_1)^2 R^{(2)}(a_2) + 4(a_2 - a_1)R'(a_2)$$
$$P^{(3)}(a_3) = (a_3 - a_1)^2 R^{(3)}(a_3) + 6(a_3 - a_1)R"(a_3) + 6R'(a_3)$$

Replace,

$$P^{(2)}(a_2) = 2b_2^2 + 4b_2(b_2 - b_3) = 2b_2(3b_2 - 2b_3) = 0$$
$$P^{(3)}(a_3) = 12b_3 + 6(b_3 - b_2) = 6(3b_3 - b_2) = 0$$

either $b_2 = 0$, and so $b_3 = 0$ either $b_2 = 0$ and so $b_3 = 0$, so $a_1 = a_2 = a_3$ and $P(x) = c(x - a)^4$

* $P"(a_1) = 0$ and $P^{(3)}(a_2) = 0$

$$P(x) = (x - a_1)^3 R(x)$$
$$P'(x) = (x - a_1)^3 R'(x) + 3(x - a_1)^2 R(x)$$
$$P"(x) = 6(x - a_1)^2 R'(x) + 3R(x)$$
$$P^{(k)}(x) = (x - a_1)^2 R^{(k)}(x) + 2k(x - a_1)R^{(k-1)}(x) + k(k-1)R^{(k-2)}(x)$$

$P"(a_2) = 6c(a_2 - a_1) = 0$ so $a_2 = a_1$ and $P(x) = c(x - a)^4$

* $P"(a_2) = 0$ and $P^{(3)}(a_2) = 0$

$$P^{(2)}(a_2) = 2b_2^2 + 4b_2(b_2 - b_3) = 2b_2(3b_2 - 2b_3) = 0$$
$$P^{(3)}(a_2) = 12b_2 + 6(b_2 - b_3) = 6(3b_2 - b_3) = 0$$

Same conclusion.

* $P"(a_2) = 0$ and $P^{(3)}(a_1) = 0$

$$P^{(2)}(a_2) = 2b_2^2 + 4b_2(b_2 - b_3) = 2b_2(3b_2 - 2b_3) = 0$$
$$P^{(3)}(a_1) = 6b_2 b_3 = 0$$

Same conclusion.

- Case $n = 5$

$$R(x) = (x - a_2)(x - a_3)(x - a_4)$$
$$R'(x) = (x - a_2)(x - a_3) + (x - a_3)(x - a_4) + (x - a_4)(x - a_2)$$
$$R"(x) = 2((x - a_2) + (x - a_3) + (x - a_4))$$
$$R"'(x) = 6$$

For $i \neq 1$, $R(a_i) = 0$, $R'(a_i) = (a_i - a_j)(a_i - a_k) = (b_i - b_j)(b_i - b_k)$, $R"(a_i) = 2((a_i - a_j) + (a_i - a_k)) = 2(2b_i - b_j - b_k)$

* Suppose $P^{(i)}(a_i) = 0$

$$P^{(2)}(a_2) = (a_2 - a_1)^2 R^{(2)}(a_2) + 4(a_2 - a_1)R'(a_2)$$
$$P^{(3)}(a_3) = (a_3 - a_1)^2 R^{(3)}(a_3) + 6(a_3 - a_1)R"(a_3) + 6R'(a_3)$$
$$P^{(4)}(a_4) = (a_4 - a_1)^2 R^{(4)}(a_4) + 8(a_4 - a_1)R^3(a_3) + 12R"(a_4)$$

Replace,

$$P^{(2)}(a_2) = 2b_2^2(2b_2 - b_3 - b_4) + 4b_2(b_2 - b_3)(b_2 - b_4) = 0$$
$$P^{(3)}(a_3) = 6b_3^2 + 12b_3(2b_3 - b_2 - b_4) + 6(b_3 - b_2)(b_3 - b_4) = 0$$
$$P^{(4)}(a_4) = 48b_4 + 24(2b_4 - b_3 - b_2) = 0$$

Factor

$$(1) \quad b_2(b_2 - b_3 + b_2 - b_4) + 2(b_2 - b_3)(b_2 - b_4) = 0$$
$$(2) \quad b_3^2 + 2b_3(2b_3 - b_2 - b_4) + (b_3 - b_2)(b_3 - b_4) = 0$$
$$(3) \quad 4b_4 - (b_3 + b_2) = 0$$

In equation (3), $b_4 = \frac{1}{4}(b_3 + b_2) = 0$
Equation 2 is solved thus : $b_2 - 2b_3 = 0$ ou $b_4 - 2b_3 = 0$.
With equation (2), $4b_3^2 + 2b_3(7b_3 - 5b_2) + (b_3 - b_2)(3b_3 - b_2) = 0$
Hence $21b_3^2 - 14b_3b_2 + b_2^2 = 0$ and $b_3 = \pm 2\sqrt{7}b_2$
Thus b_4 and b_3 are linear functions of b_2
At last, equation (1) gives a function of b_2 : we have $(1) \Leftrightarrow \lambda b_2^2 = 0$, $\lambda \neq 0$ so $b_3 = b_2 = b_4 = 0$ hence $a_1 = a_2 = a_3 = a_4$ and $P(x) = c(x - a)^5$

* As for $n = 4$, we can study every case and we always end up with $P(x) = c(x - a)^5$