2019 HMMT T9

Tristan Shin

16 Feb 2019

Let $p > 2$ be a prime number. $\mathbb{F}_p[x]$ is defined as the set of all polynomials in x with coefficients in $\mathbb{F}_p$ (the integers modulo p with usual addition and subtraction), so that two polynomials are equal if and only if the coefficients of x^k are equal in $\mathbb{F}_p$ for each nonnegative integer k. For example, $(x+2)(2x+3) = 2x^2+2x+1$ in $\mathbb{F}_5[x]$ because the corresponding coefficients are equal modulo 5.

Let $f, g \in \mathbb{F}_p[x]$. The pair (f, g) is called *compositional* if

$$f(g(x)) \equiv x^{p^2} - x$$

in $\mathbb{F}_p[x]$. Find, with proof, the number of compositional pairs (in terms of p).

Clearly $(\deg f, \deg g) \in \{(1, p^2), (p^2, 1), (p, p)\}$.

Case 1: $\deg f = 1$.

Let $f(x) = ax + b$ with $a \neq 0$. Then

$$ag(x) + b = x^{p^2} - x.$$

It is clear that all choices of a and b give distinct g so there are $p(p-1)$ choices here.

Case 2: $\deg g = 1$.

Let $g(x) = ax + b$ with $a \neq 0$. Then

$$f(ax+b) = x^{p^2} - x.$$

Letting $y = ax + b$, we have

$$f(y) = \left(\frac{y-b}{a}\right)^{p^2} - \frac{y-b}{a} = \frac{1}{a}\left((y-b)^{p^2} - (y-b)\right).$$

It is clear that all choices of a and b give distinct g so there are $p(p-1)$ choices here.

Case 3: $\deg f = \deg g = p$.

We *take the derivative* of $f \circ g$ with respect to x to get

$$f'(g(x))\, g'(x) = -1.$$

Since $\mathbb{F}_p$ is a UFD, we must have that $g'(x) = a$ for a non-zero constant a. Then $f'(g(x)) = -\frac{1}{a}$. Now, we appeal to the fact that a polynomial in t has zero derivative in $\mathbb{F}_p$ if and only if its exponents are divisible by p. Then the exponents of $g(x) - ax$ are divisible by p. Since $\deg g = p$, we must have

$$g(x) = bx^p + ax + c$$

for some constants $b \neq 0$ and c. Similarly, the exponents of $f(g(x)) + \frac{1}{a}x$ (as a polynomial in $g(x)$) are divisible by p. Since $\deg f = p$, we have

$$f(g(x)) = dg(x)^p - \frac{1}{a}g(x) + e = dg(x^p) - \frac{1}{a}g(x) + e$$

for some constants $d \neq 0$ and e (where we used the fact that the Frobenius Endomorphism commutes with polynomials). Thus we have

$$\begin{aligned} x^{p^2} - x &= f(g(x)) \\ &= dg(x^p) - \frac{1}{a}g(x) + e \\ &= d\left(bx^{p^2} + ax^p + c\right) - \frac{1}{a}(bx^p + ax + c) + e \\ &= bdx^{p^2} + \left(ad - \frac{b}{a}\right)x^p - x + \left(cd - \frac{c}{a} + e\right) \end{aligned}$$

so

$$\begin{aligned} bd &= 1 \\ ad &= \frac{b}{a} \\ e &= \frac{c}{a} - cd \end{aligned}$$

which tells us that if we choose $b \neq 0$ and c arbitrarily, then $a = \pm b$, $d = \frac{1}{b}$, and $e = \frac{c}{a} - cd$. So there are $2p(p-1)$ choices here.

Combining these cases, we deduce that there are $\boxed{4p(p-1)}$ choices of (f, g). ■