Polynomial Functions of the Ring of Dual Numbers Modulo m

Amr Al-Maktry[1] Hasan Al-Ezeh[2] Sophie Frisch[1]

[1]TU Graz University

[2]Jordan University

Conference on Rings and Factorizations, 2018

Outline

Background

Let R be a finite commutative ring with unity.

Background

Let R be a finite commutative ring with unity.

- A function $F : R \longrightarrow R$ is said to be a polynomial function over R if there exists a polynomial $f(x) \in R[x]$ such that $f(a) = F(a)$ for every $a \in R$. In this case we say that F is the induced function of $f(x)$ over R and $f(x)$ represents (induces) F.

Background

Let R be a finite commutative ring with unity.

- A function $F : R \longrightarrow R$ is said to be a polynomial function over R if there exists a polynomial $f(x) \in R[x]$ such that $f(a) = F(a)$ for every $a \in R$. In this case we say that F is the induced function of $f(x)$ over R and $f(x)$ represents (induces) F.
- If F is a bijection then F is called a permutation polynomial.

Background

Let R be a finite commutative ring with unity.

- A function $F : R \longrightarrow R$ is said to be a polynomial function over R if there exists a polynomial $f(x) \in R[x]$ such that $f(a) = F(a)$ for every $a \in R$. In this case we say that F is the induced function of $f(x)$ over R and $f(x)$ represents (induces) F.
- If F is a bijection then F is called a permutation polynomial.
- Let $f(x) \in R[x]$ such that $f(a) = 0$ for every $a \in R$. $f(x)$ is called null polynomial over R.

Background

Let R be a finite commutative ring with unity.

- A function $F : R \longrightarrow R$ is said to be a polynomial function over R if there exists a polynomial $f(x) \in R[x]$ such that $f(a) = F(a)$ for every $a \in R$. In this case we say that F is the induced function of $f(x)$ over R and $f(x)$ represents (induces) F.
- If F is a bijection then F is called a permutation polynomial.
- Let $f(x) \in R[x]$ such that $f(a) = 0$ for every $a \in R$. $f(x)$ is called null polynomial over R.

Background

Let R be a finite commutative ring with unity.

- A function $F : R \longrightarrow R$ is said to be a polynomial function over R if there exists a polynomial $f(x) \in R[x]$ such that $f(a) = F(a)$ for every $a \in R$. In this case we say that F is the induced function of $f(x)$ over R and $f(x)$ represents (induces) F.
- If F is a bijection then F is called a permutation polynomial.
- Let $f(x) \in R[x]$ such that $f(a) = 0$ for every $a \in R$. $f(x)$ is called null polynomial over R. In particular if $R = \mathbb{Z}_m$, $f(x)$ called null polynomial $(mod\ m)$.

Background

Throughout:

Background

Throughout:

- $\mathcal{F}(R)$ denote the set of polynomial functions over R.

Background

Throughout:

- $\mathcal{F}(R)$ denote the set of polynomial functions over R.
- $\mathcal{P}(R)$ denote the set of permutation polynomials over R.

Background

Throughout:

- $\mathcal{F}(R)$ denote the set of polynomial functions over R.
- $\mathcal{P}(R)$ denote the set of permutation polynomials over R.
- $\mu(m)$ denote the Kempner's function, the smallest positive integer such that m divides $\mu(m)!$.

Background

Throughout:

- $\mathcal{F}(R)$ denote the set of polynomial functions over R.
- $\mathcal{P}(R)$ denote the set of permutation polynomials over R.
- $\mu(m)$ denote the Kempner's function, the smallest positive integer such that m divides $\mu(m)!$.
- $f'(x)$ denote the formal derivative of $f(x)$.

Dual Numbers

When R is a commutative ring, then $R[\alpha]$ designates the result of adjoint α to R with $\alpha^2 = 0$; that is, $R[\alpha]$ is ${R[x]}/{(x^2)}$, where α denote $x + (x^2)$.

Dual Numbers

When R is a commutative ring, then $R[\alpha]$ designates the result of adjoint α to R with $\alpha^2 = 0$; that is, $R[\alpha]$ is ${}^{R[x]}/_{(x^2)}$, where α denote $x + (x^2)$. Simply $R[\alpha] = \{a + b\alpha : a, b \in R\}$

Fact

Let R be a commutative ring, then

1. *For $a, a', b, b' \in R$. We have*

Fact

Let R be a commutative ring, then

1. *For $a, a', b, b' \in R$. We have*
   - $(a + b\alpha)(a' + b'\alpha) = aa' + (ab' + a'b)\alpha$

Fact

Let R be a commutative ring, then

1. *For $a, a', b, b' \in R$. We have*
   - $(a + b\alpha)(a' + b'\alpha) = aa' + (ab' + a'b)\alpha$
   - $(a + b\alpha)$ *is a unit in* $R[\alpha]$ *iff* a *is a unit in* R.

Fact

Let R be a commutative ring, then

1. *For $a, a', b, b' \in R$. We have*
   - $(a + b\alpha)(a' + b'\alpha) = aa' + (ab' + a'b)\alpha$
   - $(a + b\alpha)$ *is a unit in* $R[\alpha]$ *iff* a *is a unit in* R.
   - $f(a + b\alpha) = f(a) + bf'(a)\alpha$ *for every* $f(x) \in R[x]$

Fact

Let R be a commutative ring, then

1. *For $a, a', b, b' \in R$. We have*
   - $(a + b\alpha)(a' + b'\alpha) = aa' + (ab' + a'b)\alpha$
   - $(a + b\alpha)$ *is a unit in* $R[\alpha]$ *iff* a *is a unit in* R.
   - $f(a + b\alpha) = f(a) + bf'(a)\alpha$ *for every* $f(x) \in R[x]$
2. $R[\alpha]$ *is a local ring iff* R *is a local ring.*

Fact

Let R be a commutative ring, then

1. *For $a, a', b, b' \in R$. We have*
   - $(a + b\alpha)(a' + b'\alpha) = aa' + (ab' + a'b)\alpha$
   - $(a + b\alpha)$ *is a unit in* $R[\alpha]$ *iff* a *is a unit in* R.
   - $f(a + b\alpha) = f(a) + bf'(a)\alpha$ *for every* $f(x) \in R[x]$
2. $R[\alpha]$ *is a local ring iff* R *is a local ring.*
3. *If R is a local ring with a maximal ideal $\mathfrak{m}$ has nilpotency n. then $R[\alpha]$ is a local ring whose maximal ideal $\mathfrak{m} + \alpha R$ has nilpotency $n + 1$*

Dual Numbers

Definition (Frisch (1999))

Let R be a finite commutative local ring with a maximal ideal $\mathfrak{m}$ whose nilpotency $K \in \mathbb{N}$. We call R *suitable*, if for all $a,\ b \in R$ and all $l \in \mathbb{N}$, $ab \in \mathfrak{m}^l \Rightarrow a \in \mathfrak{m}^i$ and $b \in \mathfrak{m}^j$ with $i + j \geq \min(K, l)$.

Dual Numbers

Definition (Frisch (1999))

Let R be a finite commutative local ring with a maximal ideal $\mathfrak{m}$ whose nilpotency $K \in \mathbb{N}$. We call R *suitable*, if for all a, $b \in R$ and all $l \in \mathbb{N}$, $ab \in \mathfrak{m}^l \Rightarrow a \in \mathfrak{m}^i$ and $b \in \mathfrak{m}^j$ with $i + j \geq \min(K, l)$.

Proposition

Let R be a finite commutative local ring. Then $R[\alpha]$ is suitable iff R is a field.

Dual Numbers

Definition (Frisch (1999))

Let R be a finite commutative local ring with a maximal ideal $\mathfrak{m}$ whose nilpotency $K \in \mathbb{N}$. We call R *suitable*, if for all a, $b \in R$ and all $l \in \mathbb{N}$, $ab \in \mathfrak{m}^l \Rightarrow a \in \mathfrak{m}^i$ and $b \in \mathfrak{m}^j$ with $i + j \geq \min(K, l)$.

Proposition

Let R be a finite commutative local ring. Then $R[\alpha]$ is suitable iff R is a field. In particular $\mathbb{Z}_{p^n}[\alpha]$ is suitable iff $n = 1$.

Null polynomials over $\mathbb{Z}_m[\alpha]$

Proposition

Suppose that $f(x) = f_1(x) + f_2(x)\alpha$, where $f_1(x), f_2(x) \in \mathbb{Z}[x]$. Then $f(x)$ is a null polynomial over $\mathbb{Z}_m[\alpha]$ iff $f_1(x)$, $f_1'(x)$ and $f_2(x)$ are null polynomials modulo m.

Null polynomials over $\mathbb{Z}_m[\alpha]$

Proposition

Suppose that $f(x) = f_1(x) + f_2(x)\alpha$, *where* $f_1(x), f_2(x) \in \mathbb{Z}[x]$. *Then* $f(x)$ *is a null polynomial over* $\mathbb{Z}_m[\alpha]$ *iff* $f_1(x)$, $f_1'(x)$ *and* $f_2(x)$ *are null polynomials modulo* m.

Corollary

$f(x) = (x)_{2\mu(m)} = \prod_{j=0}^{2\mu(m)-1}(x-j)$ *is a null polynomials over* $\mathbb{Z}_m[\alpha]$.

Null polynomials over $\mathbb{Z}_m[\alpha]$

Theorem

Let $n \leq p$. *For* $f(x) = \sum_{k=0}^{m}(f_k(x)(x^p - x)^k) \in \mathbb{Z}[x]$, $f_k(x) = \sum_{j=0}^{p-1} a_{jk}x^j$. *Then* $f(x), f'(x)$ *are null polynomials modulo* p^n *iff*

$$\begin{aligned} a_{j0} &\equiv 0 \pmod{p^n}, \\ a_{jk} &\equiv 0 \pmod{p^{n-k+1}} \text{ if } 1 \leq k < n, \\ a_{jn} &\equiv \begin{cases} 0 \pmod{p} & \text{if } n < p, \\ 0 \pmod{p^0} & \text{if } n = p, \end{cases} \\ a_{jk} &\equiv 0 \pmod{p^0} \text{ if } k > n. \text{ For } 0 \leq j \leq p-1. \end{aligned}$$

Null polynomials over $\mathbb{Z}_m[\alpha]$

Corollary

Let $n \leq p$ and $f(x) \in \mathbb{Z}[x]$ such that $f(x), f'(x)$ are null polynomials $\pmod{p^n}$ with deg $f \leq (n+1)p - 1$ with coefficient reduced $\pmod{p^n}$. Let N denote the number of all polynomials $f(x)$.

Then $N = \begin{cases} p^{\frac{n(n-1)p}{2}} & \text{if } n < p, \\ p^{\frac{(p^2-p+2)p}{2}} & \text{if } n = p. \end{cases}$

Polynomial Functions over $\mathbb{Z}_m[\alpha]$

Theorem

Let $F : \mathbb{Z}_m[\alpha] \longrightarrow \mathbb{Z}_m[\alpha]$ *defined by* $F(i + j\alpha) = c_i + d_{(i,j)}\alpha$, *where* $c_i, d_{(i,j)} \in \mathbb{Z}_m$ *for* $i, j = 0, 1, ..., m-1$. *T F A E:*

- F *is a polynomial function over* $\mathbb{Z}_m[\alpha]$.
- F *induced by* $f(x) = \sum_{k=0}^{2\mu-1} a_k x^k + \sum_{l=0}^{\mu-1} b_l x^l \alpha$.
- *The system of linear congruences,*
$$\begin{cases} \sum_{k=0}^{2\mu-1} i^k x_k \equiv c_i \\ \sum_{k=0}^{2\mu-1} k i^{k-1} j x_k + \sum_{l=0}^{\mu-1} i^l y_l \equiv d_{(i,j)} \pmod{m} \end{cases}$$
$i, j = 0, 1, ..., m-1$, *has a solution* $x_k = a_k, \ y_l = b_l$ *for* $k = 0, 1, ..., 2\mu-1, \ l = 0, 1, ..., \mu-1$.

Polynomial Functions over $\mathbb{Z}_m[\alpha]$

Theorem

Let $f(x) = f_1(x) + f_2(x)\alpha$, where $f_1(x), f_2(x) \in \mathbb{Z}[x]$. Then $f(x)$ is a permutation polynomial over $\mathbb{Z}_{p^n}[\alpha]$ iff $f_1(x)$ is a permutation polynomial (mod p) and $f_1'(a) \not\equiv 0$ for every $a \in \mathbb{Z}_p$.

Polynomial Functions over $\mathbb{Z}_m[\alpha]$

Let $Stab_\alpha(\mathbb{Z}_m) = \{F \in \mathcal{P}(\mathbb{Z}_m[\alpha]) : F(a) = a \text{ for every } a \in \mathbb{Z}_m\}$.

Polynomial Functions over $\mathbb{Z}_m[\alpha]$

Let $Stab_\alpha(\mathbb{Z}_m) = \{F \in \mathcal{P}(\mathbb{Z}_m[\alpha]) : F(a) = a \text{ for every } a \in \mathbb{Z}_m\}$.

Proposition

Let $m = p_1^{n_1} ... p_k^{n_k}$ where $p_1, .., p_k$ are distinct primes and suppose that $n_j > 1$ for $j = 1, .., k$. Then $Stab_\alpha(\mathbb{Z}_m) = \{F \in \mathcal{P}(\mathbb{Z}_m[\alpha]) :$ F is represented by $x + h(x), h(x) \in \mathbb{Z}[x]$ where $h(x)$ is a null polynomial modulo $m\}$.

Counting Formulas

Theorem

Let $n > 1$. The number of polynomial functions over $\mathbb{Z}_{p^n}[\alpha]$ is given by $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])| = |\mathcal{F}(\mathbb{Z}_{p^n})|^2 \times |Stab_\alpha(\mathbb{Z}_{p^n})|$.

Counting Formulas

Theorem

Let $n > 1$. The number of polynomial functions over $\mathbb{Z}_{p^n}[\alpha]$ is given by $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])| = |\mathcal{F}(\mathbb{Z}_{p^n})|^2 \times |Stab_\alpha(\mathbb{Z}_{p^n})|$.

Theorem

Let $n > 1$. The number of permutation polynomials over $\mathbb{Z}_{p^n}[\alpha]$ is given by $|\mathcal{P}(\mathbb{Z}_{p^n}[\alpha])| = |\mathcal{F}(\mathbb{Z}_{p^n})| \times |\mathcal{P}(\mathbb{Z}_{p^n})| \times |Stab_\alpha(\mathbb{Z}_{p^n})|$.

Counting Formulas

Proposition

Let $1 < n \leq p$

$$|Stab_\alpha(\mathbb{Z}_{p^n})| = \begin{cases} p^{np} & \text{if } n < p, \\ p^{(p-1)p} & \text{if } n = p. \end{cases}$$

Counting Formulas

Theorem

For $n \leq p$ the number of polynomial functions over $\mathbb{Z}_{p^n}[\alpha]$ is given by

$$|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])| = \begin{cases} p^{(n^2+2n)p} & \text{if } n < p, \\ p^{(p^2+2p-1)p} & \text{if } n = p. \end{cases}$$

Counting Formulas

Theorem

For $n \leq p$ the number of polynomial functions over $\mathbb{Z}_{p^n}[\alpha]$ is given by

$$|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha])| = \begin{cases} p^{(n^2+2n)p} & \text{if } n < p, \\ p^{(p^2+2p-1)p} & \text{if } n = p. \end{cases}$$

Corollary

For $n \leq p$ the number of permutation polynomials over $\mathbb{Z}_{p^n}[\alpha]$ is given by $|\mathcal{P}(\mathbb{Z}_{p^n}[\alpha])| = \begin{cases} p!(p-1)^p p^{(n^2+2n-2)p} & \text{if } n < p, \\ p!(p-1)^p p^{(p^2+2p-3)p} & \text{if } n = p. \end{cases}$.

Some Generalizations

Theorem

Let $\mathbb{Z}_{p^n}[\alpha_1, ..., \alpha_k] = \{a + b_1\alpha_1 + ... + b_k\alpha_k : \alpha_i\alpha_j = 0, a, b_i \in \mathbb{Z}_{p^n}$ *for* $i, j = 1, .., k\}$.

Some Generalizations

Theorem

Let $\mathbb{Z}_{p^n}[\alpha_1, ..., \alpha_k] = \{a + b_1\alpha_1 + ... + b_k\alpha_k : \alpha_i\alpha_j = 0, a, b_i \in \mathbb{Z}_{p^n}$ *for* $i, j = 1, .., k\}$*. Then:*

1. *For* $n > 1$, $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha_1, ..., \alpha_k])| = |\mathcal{F}(\mathbb{Z}_{p^n})|^{k+1} \times |Stab_{\alpha}(\mathbb{Z}_{p^n})|$.

Some Generalizations

Theorem

Let $\mathbb{Z}_{p^n}[\alpha_1, ..., \alpha_k] = \{a + b_1\alpha_1 + ... + b_k\alpha_k : \alpha_i\alpha_j = 0, a, b_i \in \mathbb{Z}_{p^n}$ *for* $i, j = 1, .., k\}$. *Then:*

1. *For* $n > 1$, $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha_1, ..., \alpha_k])| = |\mathcal{F}(\mathbb{Z}_{p^n})|^{k+1} \times |Stab_\alpha(\mathbb{Z}_{p^n})|$.
2. *For* $n \leq p$,
   - $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha_1, ..., \alpha_k])| = \begin{cases} p^{(n^2+2n)p} p^{\frac{n(n+1)(k-1)p}{2}} & \text{if } n < p, \\ p^{(p^2+2p-1)p} p^{\frac{n(n+1)(k-1)p}{2}} & \text{if } n = p. \end{cases}$

Some Generalizations

Theorem

Let $\mathbb{Z}_{p^n}[\alpha_1, ..., \alpha_k] = \{a + b_1\alpha_1 + ... + b_k\alpha_k : \alpha_i\alpha_j = 0, a, b_i \in \mathbb{Z}_{p^n}$ *for* $i, j = 1, .., k\}$. *Then:*

1. *For* $n > 1$, $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha_1, ..., \alpha_k])| = |\mathcal{F}(\mathbb{Z}_{p^n})|^{k+1} \times |Stab_\alpha(\mathbb{Z}_{p^n})|$.
2. *For* $n \leq p$,
   - $|\mathcal{F}(\mathbb{Z}_{p^n}[\alpha_1, ..., \alpha_k])| = \begin{cases} p^{(n^2+2n)p} p^{\frac{n(n+1)(k-1)p}{2}} & \text{if } n < p, \\ p^{(p^2+2p-1)p} p^{\frac{n(n+1)(k-1)p}{2}} & \text{if } n = p. \end{cases}$
   - $|\mathcal{P}(\mathbb{Z}_{p^n}[\alpha_1, ..., \alpha_k])| =$
     $\begin{cases} p!(p-1)^p p^{(n^2+2n-2)p} p^{\frac{n(n+1)(k-1)p}{2}} & \text{if } n < p, \\ p!(p-1)^p p^{(p^2+2p-3)p} p^{\frac{p(p+1)(k-1)p}{2}} & \text{if } n = p. \end{cases}$

References

Chen, Z. (1995). On polynomial functions from Z_n to Z_m. *Discrete Math.*, 137(1-3):137–145.

Frisch, S. (1999). Polynomial functions on finite commutative rings. In *Advances in commutative ring theory (Fez, 1997)*, volume 205 of *Lecture Notes in Pure and Appl. Math.*, pages 323–336. Dekker, New York.

Frisch, S. and Krenn, D. (2013). Sylow p-groups of polynomial permutations on the integers $\bmod p^n$. *J. Number Theory*, 133(12):4188–4199.

Kempner, A. J. (1918). Miscellanea. *Amer. Math. Monthly*, 25(5):201–210.

Kempner, A. J. (1921). Polynomials and their residue systems. *Trans. Amer. Math. Soc.*, 22(2):240–266, 267–288.