Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 22, 2016, No. 2, 23–35

On transitive polynomials modulo integers

Mohammad Javaheri[1] and Gili Rusak[2]

[1] School of Science, Siena College
515 Loudon Road, Loudonville, NY 12110, USA
e-mail: mjavaheri@siena.edu

[2] School of Engineering, Stanford University
353 Serra Mall, Stanford, CA 94305, USA
e-mail: gili@stanford.edu

Received: 27 August 2015 **Accepted:** 14 October 2015

Abstract: A polynomial $P(x)$ with integer coefficients is said to be transitive modulo m, if for every $x, y \in \mathbb{Z}$ there exists $k \geq 0$ such that $P^k(x) = y \pmod{m}$. In this paper, we construct new examples of transitive polynomials modulo prime powers and partially describe cubic and quartic transitive polynomials. We also study the orbit structure of affine maps modulo prime powers.
Keywords: Transitive polynomials, Permutation polynomials.
AMS Classification: 11T06.

1 Introduction

A permutation polynomial on a ring R is a polynomial

$$P(x) = a_n x^n + \cdots + a_1 x + a_0,$$

with coefficients in R that induces a bijection on R. Usually $R = F_q$, the finite field with q elements, or $R = \mathbb{Z}_n$, the ring of congruence classes modulo an integer n. Permutation polynomials have been studied by many mathematicians starting with Dickson, who discovered essential building blocks of permutation polynomials now known as Dickson polynomials [3]:

$$D_n(x, \alpha) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-\alpha)^i x^{n-2i}. \tag{1.1}$$

The Dickson polynomial $D_n(x, \alpha)$, $\alpha \neq 0$, is a permutation polynomial on a finite field F_q if and only if $\gcd(q^2 - 1, n) = 1$, while $D_n(x, 0) = x^n$ is a permutation polynomial on F_q if and only if $\gcd(n, q - 1) = 1$; [4].

For a short survey of known results and open problems on permutation polynomials, see the 1988 article [11] and the followup 1993 article [12] in the American Mathematical Monthly by Lidl and Mullen. Permutation polynomials have applications in cryptography and coding theory [6, 8, 13, 16].

In this paper, we are interested in transitive polynomials modulo integers. A map $f : X \to X$ on a set X is called transitive, if for every $x, y \in X$, there exists $k \geq 0$ such that $f^k(x) = y$, where f^k is the composition of f with itself k times. Equivalently, a self-map of X is transitive on X if it induces a *cyclic* permutation on X. Hence, in any ring, a transitive polynomial is in particular a permutation polynomial.

Dickson [2] published a table of permutation polynomials of degree ≤ 5 on finite fields. In the study of transitive polynomials, only affine and quadratic transitive polynomials are completely understood [9]. Starting with degree 3, it is unlikely that a complete list of transitive polynomials modulo primes can be given. For example, a computer search through the first one million primes did not return a prime $p > 3$ modulo which $x^3 + 1$ is transitive. One can ask if such a prime even exists. Beside polynomials of the form $ax^3 + 1$ (modulo an affine conjugation), our study of cubic and quartic polynomials in Section 3 is complete.

A polynomial permutes $\mathbb{Z}_n$ if and only if it permutes $\mathbb{Z}_{p^m}$ for every prime power p^m that divides n. Similarly, a polynomial is transitive modulo n if it is transitive modulo every prime power p^m that divides n. Let p be a prime number and $m \geq 2$. Then a polynomial $P(x)$ with integer coefficients is a permutation polynomial modulo p^m if and only if:

i) $P(x)$ is a permutation polynomial modulo p, and

ii) $P'(x) \neq 0 \pmod p$ for all $x = 0, 1, \ldots, p - 1$.

In particular, if $P(x)$ is a permutation polynomial modulo p^2, then it is a permutation polynomial modulo p^m for all $m \geq 1$; [10]. A similar statement is true about transitive polynomials. If $p \neq 3$ then any transitive polynomial modulo p^2 is transitive modulo p^m for all $m \geq 1$; [1, 9]. For $p = 3$, transitivity modulo 27 implies transitivity moudlo all powers of 3. The problem of finding transitive polynomials modulo p^m, $m \geq 3$, reduces to finding transitive polynomials modulo p^2 (if $p \neq 3$) or modulo 27 (if $p = 3$). A trivial example of a transitive polynomial modulo p^m for all m, $p \neq 3$, is given by $P(x) = p^2Q(x) + ax + b$, where $Q(x)$ is an arbitrary polynomial with integer coefficients and $ax + b$ is transitive modulo p. In the following theorem, we present new nontrivial examples of transitive polynomials modulo prime powers.

Theorem 1.1. *Let p be an odd prime number and $P(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial with integer coefficients such that $a_i = 0 \pmod p$ for all $2 \leq i \leq n$, $a_1 = 1 \pmod p$, and $a_0 \neq 0 \pmod p$. Let*

$$\Lambda = \{2 \leq i \leq n : p - 1 | i\}, \tag{1.2}$$

and suppose that

$$a_0 \neq \sum_{i \in \Lambda} \frac{a_i}{p} \pmod p. \tag{1.3}$$

Then $P(x)$ is transitive modulo p^m for all $m \geq 1$.

Condition (1.3) of Theorem 1.1 holds for example when $n < p - 1$.

This is how this paper is organized. In Section 2, we give the proof of Theorem 1.1. In Section 3, we study cubic and quartic transitive polynomials. In Section 4, we study transitive polynomials on nonprime fields and, among other results, we prove that $ax^p + 1$ is not transitive on any nonprime field with odd characteristic. Finally, in Section 5, we revisit affine (or linear congruential) maps and study their orbit structures modulo prime powers in detail.

2 Proof of Theorem 1.1

In this section, we prove Theorem 1.1, which gives sufficient conditions for a polynomial to be transitive modulo all powers of a given prime. In the sequel, we make use of Bernoulli numbers B_k, $k \geq 0$, which are defined by

$$\sum_{j=1}^{n} j^i = \sum_{k=0}^{i} \frac{B_k}{i+1-k} \binom{i}{k} n^{i+1-k}. \tag{2.1}$$

For odd $k > 1$, one has $B_k = 0$. When k is even, by the von Staudt-Clausen Theorem [14, Theorem 4.6], one has

$$B_k + \sum_{p-1|k} \frac{1}{p} \in \mathbb{Z}. \tag{2.2}$$

For rational numbers r, s and integer N, we write $r = s \pmod N$ if and only if $r - s = Nu/v$, where u, v are integers and $\gcd(v, N) = 1$.

Lemma 2.1. *Let p be a prime number and $i, m \geq 1$. If $(p, i) = (2, 1)$, or $(p, m) = (2, 1)$, or i is even and $p - 1$ divides i, then*

$$\sum_{j=1}^{p^m} j^i = -p^{m-1} \pmod{p^m}. \tag{2.3}$$

In all other cases:

$$\sum_{j=1}^{p^m} j^i = 0 \pmod{p^m}. \tag{2.4}$$

Proof. If $(p, m) = (2, 1)$, then $\sum_{j=1}^{2} j^i = 1 + 2^i = -1 \pmod 2$ as claimed by (2.3). Therefore, suppose $(p, m) \neq (2, 1)$. We now show that for $0 \leq k \leq i - 1$:

$$\frac{B_k}{i+1-k} \binom{i}{k} (p^m)^{i+1-k} = 0 \pmod{p^m}. \tag{2.5}$$

Let $i + 1 - k = Sp^r \geq 2$, where $r \geq 0$ and $\gcd(S, p) = 1$. By (2.2), it is sufficient to show that if $0 \leq k \leq i - 1$, then

$$m(i + 1 - k) - r - 1 - m \geq 0.$$

One has

$$\begin{aligned} m(i+1-k)-r-1-m &= m(Sp^r-1)-r-1 \\ &\geq Sp^r-r-2 \geq p^r-r-2 \geq 2^r-r-2 \geq 0, \end{aligned}$$

for all $r > 1$. If $r = 0$, then $S = i + 1 - k \geq 2$, and so

$$m(i+1-k)-r-1-m \geq m(S-1)-1 \geq S-2 \geq 0.$$

If $r = 1$, then

$$m(i+1-k)-r-1-m \geq m(Sp-1)-2 \geq 0,$$

since $(p, m) \neq (2, 1)$, and the proof of (2.5) is completed. It follows from (2.1) and (2.5) that

$$\sum_{j=1}^{p^m} j^i = B_i p^m \pmod{p^m}. \tag{2.6}$$

If $i > 1$ is odd, then $B_i = 0$. If $i = 1$, then $\sum_{j=1}^{p^m} j = p^m(p^m - 1)/2$, which is congruent to 0 modulo p^m for $p > 2$, and it is congruent to -2^{m-1} modulo 2^m if $p = 2$. If $i \geq 1$ is even, then it follows from (2.2) and (2.6) that

$$\sum_{j=1}^{p^m} j^i = B_i p^m = \begin{cases} 0 \pmod{p^m} & \text{if } p-1|i \\ -p^{m-1} \pmod{p^m} & \text{if } p-1|i \end{cases},$$

which completes the proof of the lemma. □

We also need the following lemma, which states four equivalent formulations of transitivity.

Lemma 2.2. *Let $f : X \to X$ be a function on a finite set X with m elements. The following statements are equivalent.*

i) f is transitive on X.

ii) X has no proper f-invariant subsets.

iii) f induces a cyclic permutation on X.

iv) For every integer $k \geq 0$ and $x \in X$: $f^k(x) = x \iff m|k$.

Proof. We only prove that (iii) implies (iv); the rest of the proof is similarly straightforward. If f induces a cyclic permutation on X, then $f^m(x) = x$ and $f^k(x) \neq x$ for all $0 < k < m$. Given an integer $k \geq 0$, let $k = rm + s$, where r, s are nonnegative integers and $0 \leq s < m$. One has $f^k(x) = f^s(x)$ which equals x if and only if $s = 0$, and (iv) follows. □

We are now ready to prove Theorem 1.1.

Proof is by induction on m. The case $m = 1$ follows from the affine case. Next, assume the claim is true for m i.e., $P(x)$ is transitive modulo p^m. Suppose

$$\Omega = \{x_1, x_2, \ldots, x_k\}$$

is a nonempty $P(x)$-invariant subset of $\mathbb{Z}_{p^{m+1}}$. Without loss of generality, we can assume that Ω is the orbit of x_1 such that $P(x_i) = x_{i+1} \pmod{p^{m+1}}$ for all $0 \leq i < k$ and $P(x_k) = x_1$. We need to show that $k = p^{m+1}$. Since Ω is $P(x)$-invariant, we have

$$0 = \sum_{j=1}^{k} P(x_j) - x_j = \sum_{i=2}^{n} a_i \sum_{j=1}^{n} x_j^i + (a_1 - 1) \sum_{j=1}^{k} x_j + a_0 k \pmod{p^{m+1}} \tag{2.7}$$

Since $P^k(x_1) = x_1 \pmod{p^m}$, Lemma 2.2 implies that $k = Kp^m$ for some integer $K \geq 1$, and so the set $\{P^{rp^m+i}(x_1) : 1 \leq i \leq p^m\}$ coincides with $\{1, \ldots, p^m\}$ modulo p^m for each $0 \leq r < K$. It follows that for all $1 \leq i \leq n$:

$$\sum_{j=1}^{k} x_j^i = K \sum_{j=1}^{p^m} j^i \pmod{p^m}. \tag{2.8}$$

By Lemma 2.1 and equations (2.7) and (2.8), one has

$$\begin{aligned} a_0 K p^m &= -(a_1 - 1) \sum_{j=1}^{k} x_j - \sum_{i=2}^{n} a_i \sum_{j=1}^{k} x_j^i \\ &= 0 - \sum_{i=2}^{n} a_i K \sum_{j=1}^{p^m} j^i \\ &= K \sum_{i \in \Lambda} a_i p^{m-1} \\ &= K \left(\sum_{i \in \Lambda} \frac{a_i}{p} \right) p^m \pmod{p^{m+1}}, \end{aligned} \tag{2.9}$$

which contradicts the assumption (1.3) after dividing both sides by Kp^m. This completes the induction step, hence the proof of Theorem 1.1 is completed.

3 Cubic and quartic transitive polynomials

Proposition 3.1. Let $P(x) = ax^3 + bx^2 + cx + d$ be a polynomial, where $a, b, c, d \in \mathbb{Z}$, $n \geq 1$, and let p be an odd prime number. Then $P(x)$ is transitive modulo $p^n > 3$ if and only if one of the following occurs:

i) $p > 3$ and $a = b = c - 1 = 0 \pmod{p}$ and $\gcd(d, p) = 1$.

ii) $n = 1$, $p = 2 \pmod{3}$, and $P(x)$ can be conjugated to $Q(x) = Ax^3 + 1$ for some integer A such that $Q(x)$ is transitive modulo p.

iii) $p = 3^n > 3$ and $a = b = c - 1 = 0 \pmod{3}$, $\gcd(d, 3) = 1$, and $b/3 \neq d \pmod{3}$.

Proof. First, suppose that $a = 0 \pmod{p}$. It follows from the quadratic case [9] that $P(x) = ax^3 + bx^2 + cx + d$ is transitive modulo p if and only if $b = c - 1 = 0 \pmod{p}$ and $\gcd(d, p) = 1$. It then follows from Theorem 1.1 that $P(x)$ is transitive modulo p^n for all $n \geq 1$.

p	A	p	A	p	A	p	A
2	1	167	72, 115	461	211	797	720
3	1	173	123	467	324, 453	827	11, 401
5	3	197	58, 94	479	442	839	112
11	5	233	61	491	277	887	363
29	14	251	135, 218	503	445	929	97
47	7	257	48	569	27	971	751
59	15	269	158	587	345	977	93
71	40, 54	281	205	599	5, 466	983	343, 520, 917
83	9, 37	293	163	617	263		
101	61, 66	311	84	641	217		
131	35, 59	317	249	647	115, 169, 506		
137	113	347	183	677	310		
149	51, 98	443	38, 217	719	24		

Table 1: Transitive polynomials of the form $Ax^3 + 1$ modulo p for $p < 1000$.

Next, suppose that $P(x)$ is transitive modulo p^n, $a \neq 0 \pmod{p}$, and $p > 3$. Then $P(x)$ can be conjugated modulo p^n to $Q(x) = ax^3 + ex + f$ for some $e, f \in \mathbb{Z}_{p^i}$ (by $x \mapsto (x - b/(3a))$). From Dickson's study of cubic permutation polynomials [3], we conclude that $e = 0$ and $p = 2 \pmod 3$. Moreover, $Q(x)$ is not transitive modulo p^2, since $Q'(0) = 0$. Another conjugation ($x \mapsto fx$) gives $Q(x) = Ax^3 + 1$.

If $p = 3$ and $a = 0 \pmod 3$, it follows from the quadratic case again that $b = c - 1 = 0 \pmod 3$ and $\gcd(3, d) = 1$. We need to show that if $P(x)$ is transitive, then $b/3 \neq d \pmod 3$. On the contrary, suppose $P(x)$ is transitive and without loss of generality, suppose $d = 1 \pmod 3$ and $b = 3 \pmod 9$. Let $a = 3l$ and $c = 3m + 1$ for $l, m \in \mathbb{Z}$. Then a simple calculation shows that $P^3(0) = 0 \pmod 9$. This is a contraction and the claim follows.

Finally, a search through all cubic polynomials modulo 9 shows that the only transitive cubic polynomials modulo 9 (hence all higher powers of 3) come from case (iii). This completes the proof of the proposition. □

Theorem 3.1 shows that the only cubic polynomials that need further investigation in our search of transitive cubic polynomials modulo p^n are those of the form $Ax^3 + 1$ with $n = 1$ and $p = 2 \pmod 3$. In Table 1, we have listed all such polynomials for $p < 1000$.

Proposition 3.2. Let $P(x) = ax^4 + bx^3 + cx^2 + dx + e$, where $a, b, c, d, e \in \mathbb{Z}$, $n \geq 1$, and let p be an odd prime number. Then $P(x)$ is transitive modulo $p^n > 5$ if and only if one of the following occurs

i) $p = 3$, $a = b = c = d - 1 = 0 \pmod 3$, $\gcd(e, 3) = 1$, and $(a + c)/3 \neq e \pmod 3$.

ii) $p = 5$, $a = b = c = d - 1 = 0 \pmod 5$, $\gcd(e, 5) = 1$, and $a/5 \neq e \pmod 5$.

iii) $p > 5$, $a = b = c = d - 1 = 0 \pmod p$, and $\gcd(e, p) = 1$.

iv) $a = 0 \pmod p$, $n = 1$, and $P(x) - ax^4$ is transitive modulo p.

v) $p^n = 7$ and $P(x)$ can be conjugated to one of the following polynomials:

$$2x^4 + 6x + 1,\ 4x^4 + 5x + 1,\ 6x^4 + 3x + 1. \tag{3.1}$$

Proof. If (i)-(iii) hold, then Theorem 1.1 implies that $P(x)$ is transitive. The converses in parts (i) and (ii) are established by a computer program that searched through all quartic polynomials modulo 9 and 25. Part (iv) follows from Theorem 3.1. Part (v) is aided by a computer program that searched through quartic polynomials modulo 7 (since 7 is the only allowable odd prime according to [3]). Finally, an examination of the three polynomials in (3.1) shows that they are not transitive modulo 49. □

4 Nonprime fields

Let $G(v) = Av + b$ be an affine map on $\mathbb{Z}_p^n$, where A is an $n \times n$ matrix with entries in $\mathbb{Z}_p$ and $b \in \mathbb{Z}_p^n$. The following theorem and its proof are taken from [16].

Theorem 4.1. *Let A be an $n \times n$ matrix with entries in $\mathbb{Z}_p$ and b be a fixed vector in $\mathbb{Z}_p^n$, $n > 1$. Define $G : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ by $G(v) = Av + b$. The only pair (p, n) for which there exist b and A such that the p^n vectors $G^k(0), k = 1, 2, \ldots, p^n$, are distinct is $(p, n) = (2, 2)$.*

Proof. For $(p, n) = (2, 2)$, one takes

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},\ b = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Next, let $n \geq 2$ and G be such that $\{G^k(0) : 0 \leq k < p^n\} = \mathbb{Z}_p^n$. It follows that G is one-to-one on $\mathbb{Z}_p^n$ and it induces a cyclic permutation on $\mathbb{Z}_p^n$. Let I be the $n \times n$ identity matrix over $\mathbb{Z}_p$. The vector space $\mathbb{Z}_p^n$ is a direct sum of two subspaces V, W such that $A - I$ is nilpotent on V and invertible on W. Let $v = v_1 + v_2$, where $v_1 \in V$ and $v_2 \in W$. First suppose that $W \neq 0$. Since $A - I$ is invertible on W, it follows that there exists a unique $w \in W$ such that $(A - I)w = -v_2$. In particular, $G(w) - w = (A - I)w + v = v_1 \in V$. Therefore, by induction on $k \geq 0$, we have

$$G^{k+1}(w) - G^k(w) = A(G^k(w) - G^{k-1}(w)) \in V.$$

It follows that $G^k(w) - w \in V$ for all $k \geq 1$. Since $|V| < p^n$, there exists $0 \leq k_1 < k_2 < p^n$ such that $G^{k_1}(w) - w = G^{k_2}(w) - w$, and so $G^{k_1}(w) = G^{k_2}(w)$, which contradicts the assumption that G induces a cyclic permutation on $\mathbb{Z}_p^n$.

Next, suppose $W = 0$. It follows that $(A - I)^n = 0$. For any positive integer k, we have

$$G^k(0) = A^{k-1}v + \cdots + Av + v = \sum_{j=0}^{k-1} \sum_{i=0}^{n-1} \binom{j}{i} (A - I)^i v = \sum_{i=0}^{n-1} \binom{k}{i+1} (A - I)^i v.$$

If $n \geq 2$ and $(p, n) \neq (2, 2)$, then $p^{n-1} > n$, and so each binomial coefficient $\binom{k}{i+1}$ is divisible by p. It follows that $G^{p^{n-1}}(0) = 0 \pmod p$, which contradicts the assumption that G induces a cyclic permutation on $\mathbb{Z}_p^n$. □

Proposition 4.2. Let F be a nonprime field with $p^n > 4$ elements, where p is prime, and

$$P(x) = d + \sum_{i=1}^{n-1} a_i x^{p^i},$$

where $a_i \in \mathbb{Z}$ for all $1 \leq i \leq k$, and $d \in F$. Then $P(x)$ is not transitive on F.

Proof. Let

$$X = \left\{ \sum_{j=0}^{n-1} u_j d^{p^j} : \forall j \; u_j \in \mathbb{Z}_p \right\}.$$

Then $0 \in X$ and X is $P(x)$-invariant, since

$$\begin{aligned} P\left(\sum_{j=1}^{n-1} u_j d^{p^j}\right) &= d + \sum_{i=1}^{n-1} a_i \left(\sum_{j=0}^{n-1} u_j d^{p^j}\right)^{p^i} && (4.1) \\ &= d + \sum_{i=1}^{n-1}\sum_{j=0}^{n-1} a_i u_j d^{p^{i+j}} && (4.2) \\ &= d + \sum_{k=0}^{n-1}\sum_{j=0}^{n-1} (a_{k-j} + a_{n+k-j}) u_j d^{p^k}, && (4.3) \end{aligned}$$

where $a_l = 0$ for all $l < 1$ and $l \geq n$. and so $P(x)$ induces an affine map $G : \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^n}$ given by

$$v = \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{bmatrix} \mapsto Av + \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

on $\mathbb{Z}_{p^n}$, where A is an $n \times n$ matrix with entries $A_{kj} = a_{k-j} + a_{n+k-j}$, $0 \leq k, j \leq n-1$. If $(p, n) \neq (2, 2)$, by Thoerem 4.1, the map G is not transitive on $\mathbb{Z}_{p^n}$, and so there exists $m < p^n$ and $v \in \mathbb{Z}_{p^n}$ such that $G^m(v) = v$. It then follows that there exists $\mathbf{u} \in X$ such that $P^m(\mathbf{u}) = \mathbf{u}$, which implies that P is not transitive on F.

When $p^n = 4$ i.e. when $(p, n) = (2, 2)$, the polynomial $P(x) = x^2 + a$ is transitive on F_4, where $F_4 = \{0, 1, a, 1 + a\} = \mathbb{Z}_2[a]$ with $a^2 + a + 1 = 0$. □

Proposition 4.3. Let F be a nonprime field with p^n elements, where p is an odd prime. Then $P(x) = ax^p + 1$ is not transitive on F for any $a \in F$.

Proof. Let $t = p - 1$. Then for each $1 \leq j \leq p - 1$

$$p^{jnt} - 1 = (p^n - 1)(1 + p^n + \ldots + p^{(jt-1)n}) = 0 \pmod{t(p^n - 1)},$$

and so for all $0 \leq j \leq p - 1$, one has

$$\frac{p^{i+jnt} - 1}{p - 1} = \frac{p^i - 1}{p - 1} \pmod{p^n - 1}.$$

And so

$$\begin{aligned} P^{pnt}(0) &= \sum_{i=0}^{pnt-1} a^{(p^i-1)/(p-1)} = \sum_{j=0}^{p-1}\sum_{i=0}^{nt-1} a^{(p^{i+jnt}-1)/(p-1)} \\ &= \sum_{j=0}^{p-1}\sum_{i=0}^{nt-1} a^{(p^i-1)/(p-1)} = p\sum_{i=0}^{nt-1} a^{(p^i-1)/(p-1)} = 0. \end{aligned}$$

Since $pnt < p^n$ for $n > 2$, we conclude that $P(x)$ is not transitive on F if $n > 2$. For $n = 2$, we have $P^2(x) = a(ax^p + 1)^p + 1 = a^{p+1}x^{p^2} + a + 1 = a^{p+1}x + a + 1$. If $a^{p+1} \neq 1$, then $P^2(x)$ has a fixed point, while if $a^{p+1} = 1$, then $P^{2p}(0) = (1 + a)p = 0$. In either case, it follows that $P(x)$ is not transitive on F. □

5 The cycle structure of orbits

The cycle structure of orbits of a polynomial modulo an integer m is determined by that of its orbits modulo the prime powers dividing m. The following two propositions give an understanding of the cycle structure of orbits of affine maps modulo integers.

Proposition 5.1. Let $P(x)$ be a polynomial with integer coefficients and k, l be relatively prime integers such that $P(x)$ is a permutation polynomial modulo both k and l. Suppose that there exists an orbit of length r for $P(x)$ modulo k and there exists an orbit of length s for $P(x)$ modulo l. Then there exists an orbit of length $\mathrm{lcm}(r, s)$ for $P(x)$ modulo kl. Conversely, every orbit of $P(x)$ modulo kl has length $\mathrm{lcm}(r, s)$, where r is the length of some orbit of f modulo k, and s is the length of some orbit of f modulo l.

Proof. Let x and y be integers such that the $P(x)$-orbit of x modulo k has length r and the $P(x)$-orbit of y modulo l has length s. It follows from these assumptions that $P^r(x) = x \pmod k$ and $P^s(y) = y \pmod l$. By the Chinese remainder theorem, there exists z such that $z = x \pmod k$ and $z = y \pmod l$. Then $P^r(z) = z \pmod k$ and $P^s(z) = z \pmod l$, hence $P^{\mathrm{lcm}(r,s)}(z) = z \pmod{kl}$. Next, suppose that $P^t(z) = z \pmod{kl}$ for some $t \geq 1$. Then $P^t(x) = x \pmod k$ and $P^t(y) = y \pmod l$. It follows from Lemma 2.2 that $r|t$ and $s|t$, and so $\mathrm{lcm}(r, s)|t \Rightarrow t \geq \mathrm{lcm}(r, s)$. We have shown that $t = \mathrm{lcm}(r, s)$ is the smallest positive integer with $P^t(x) = x \pmod{kl}$, which implies that the $P(x)$-orbit of z modulo kl has length $\mathrm{lcm}(r, s)$.

For the converse, suppose that the orbit of an integer z modulo kl is t. Let r be the length of the $P(x)$-orbit of z modulo k, and let s be the length of the $P(x)$-orbit of z modulo l. It follows from the first part of this proof that $t = \mathrm{lcm}(r, s)$. This completes the proof. □

The order of a number a modulo m, denoted by $Ord(a, m)$, is the least positive integer k such that $a^k = 1 \pmod m$. We also set $Ord(a, 1) = 1$ and $\phi(1) = 1$, where ϕ is Euler's totient function.

Proposition 5.2. Let $P(x) = ax + b$, p be a prime number such that $\gcd(a, p) = 1$, and $m \geq 1$. Let $t, r \leq m$ be the largest integers such that $p^t|b$ and $p^r|a - 1$.

i) If $r = 0$ or $t = m$, then there exists an orbit of length k for $P(x)$ modulo p^m if and only if there exists $0 \leq i \leq m$ such that $k = Ord(a, p^i)$. Moreover, the number of disjoint orbits of length k is

$$\frac{1}{k} \sum_{Ord(a,p^i)=k} \phi(p^i). \tag{5.1}$$

ii) If $r > \max\{0, t\}$ and $p > 2$, then every orbit of $P(x)$ modulo p^m has length p^{m-t}. The same conclusion holds if $p = 2$ and $r > \max\{1, t\}$.

iii) If $0 < r \leq t < m$ and $p > 2$, then $P(x)$ modulo p^m has $\phi(p^r)$ disjoint orbits of length p^s for $0 < s \leq m - r$, and it has p^r disjoint orbits of length 1. The same conclusion holds if $p = 2$ and $1 < r \leq t < m$.

iv) If $p = 2$ and $r = 1$, let $2 \leq h \leq m$ be the largest integer such that 2^h divides $a + 1$.

   a) If $t = 0$, then every orbit of $P(x)$ modulo 2^m has length $m - h + 1$.

   b) If $t > 0$ and $h < m$, then for every $k > 1$ there exists an orbit modulo 2^m of length k if and only if $k = 2^s$, where $0 < s \leq m - h$. Moreover, the number of orbits of length $k \geq 1$ is given by equation (5.1). In particular, there are exactly two orbits of length 1.

   c) If $t > 0$ and $m = h$, there are exactly two orbits of length 1 and all other orbits modulo 2^m have length 2.

Proof. i) Suppose $r = 0$, and let c be the multiplicative inverse of $a - 1$ modulo p^m. Via the conjugation $x \mapsto x - bc$, we note that $P(x) = ax + b$ is conjugated to $Q(x) = ax$. Therefore, the cycle structure of orbits of $P(x)$ is identical to the cycle structure of orbits of $Q(x) = ax$. Given $1 \leq x \leq p^m$, write $x = Ap^{m-i}$, where $\gcd(A, p) = 1$ and $0 \leq i \leq m$. Then the $Q(x)$-orbit of x has length $Ord(a, p^i)$. Given each i with $k = Ord(a, p^i)$, there are $\phi(p^i)$ choices for A, which yield $\phi(p^i)$ values for x with orbit length $Ord(a, p^i)$. Equation (5.1) then follows by summing over different values of $0 \leq i \leq m$ for which $k = Ord(a, p^i)$.

The same conclusion holds if $t = m$.

For the proofs of ii-iv, we let $b = Bp^t$, where $\gcd(p, B) = 1$ and $t < m$. Without loss of generality (via the conjugation $x \mapsto Bx$), we can assume $B = 1$ and so $b = p^t$. Suppose there exists $1 \leq x \leq p^m$ whose orbit has length i so that i is the least positive integer such that

$$P^i(x) - x = (a^i - 1)x + \frac{a^i - 1}{a - 1} p^t = 0 \pmod{p^m}. \tag{5.2}$$

Let $a - 1 = Ap^r$, $i = Ip^s$, and $x = Xp^u$, where $\gcd(A, p) = \gcd(I, p) = \gcd(X, p) = 1$.

For the proofs of ii-iii, suppose $r \geq 1$ and $p > 2$, or $p = 2$ and $r \geq 2$. We first show that the largest power of p dividing $(a^i - 1)/(a - 1)$ is p^s. By the Binomial Theorem, one has

$$\frac{a^i - 1}{a - 1} = \sum_{j=1}^{i} \binom{i}{j} (Ap^r)^{j-1} = i + \sum_{j=2}^{i} \frac{ip^{j-1}}{j!} K_j, \tag{5.3}$$

where $K_j \in \mathbb{Z}$. The largest power of p dividing $j!$ is smaller than p^{j-1} for $p > 2$ and $j \geq 2$, since

$$\sum_{l=1}^{\infty} \left\lfloor \frac{j}{p^l} \right\rfloor < \sum_{l=1}^{\infty} \frac{j}{p^l} \leq \frac{j}{p-1} \leq \frac{j}{2} \leq j-1, \tag{5.4}$$

for $p > 2$ and $j \geq 2$. It then follows from (5.3) that the largest power of p dividing $(a^i-1)/(a-1)$ is p^s if $p > 2$. If $p = 2$ and $r \geq 2$, then

$$\frac{a^{I2^s}-1}{a-1} = \frac{a^I-1}{a-1} \prod_{j=0}^{s-1} (a^{I2^j}+1) \tag{5.5}$$

We note that $a^{I2^j} + 1 = 2 \pmod 4$ for all $0 \leq j \leq s-1$. Moreover,

$$\frac{a^I-1}{a-1} = 1 + a + \cdots + a^{I-1} = I = 1 \pmod 2.$$

It then follows from (5.5) that the largest power of 2 dividing $(a^i-1)/(a-1)$ is 2^s. Therefore, there exists an integer V such that $(a^i-1)/(a-1) = Vp^s$ and $\gcd(V,p) = 1$. So $a^i - 1 = AVp^{s+r}$, and by substituting into (5.2), one has

$$p^s(AXp^{r+u} + p^t) = 0 \pmod{p^m}. \tag{5.6}$$

Since $i = Ip^s$ is the least integer such that (5.2) and equivalently (5.6) holds, we conclude that $I = 1$.

ii) If $r > t$, then it follows from (5.6) that $s + t = m$, and therefore every orbit has length p^{m-t}.

iii) If $r < t$, then for each s in the range $m - t < s \leq m - r$, let $u = m - r - s$ (and so $r + u = m - s < t$). It follows from (5.6) that the orbit of $x = Xp^u$ has length p^s, where $1 \leq X \leq p^{m-u}$ is coprime with p. The number of such $x = Xp^u$ is $\phi(p^{m-u}) = \phi(p^{r+s})$, and so the number of disjoint orbits of length p^s when $m - t < s \leq m - r$ is $\phi(p^{r+s})/p^s = \phi(p^r)$.

For s in the range $0 < s \leq m - t$, choose X such that the largest power of p dividing $AX + 1$ is p^{m-t-s}, and let $u = t - r$. It follows from (5.6) that the orbit of $x = Xp^u$ has length p^s. In this case, the number of allowable $x = Xp^u$ is given by the number of allowable X, which is $\phi(p^{r+s})$. Therefore, there are $\phi(p^r)$ orbits of length p^s in this case as well. Finally, it is easy to see that the number of orbits of length 1, i.e., solutions to $(a-1)x + b = 0$ is p^r.

If $r = t$, the orbit of every $x = Xp^u$ with $u > 0$ has length p^{m-r}. The number of such x is $\phi(p^m)$, and so the number of disjoint orbits of length p^{m-r} is $\phi(p^m)/p^{m-r} = \phi(p^t)$ in this case. On the other hand, the orbit of every x that is coprime with p is given by $p^s = p^{m-r-z}$, where $Ax + 1 = Tp^z$ and $\gcd(T,p) = 1$. For each $0 \leq z < m - r$ there are $\phi(p^{m-z})$ solutions x modulo p^m. Therefore, there are $\phi(p^r)$ disjoint orbits of length p^s for $0 < s \leq m - r$. Again for $s = 0$, there are p^r fixed points (orbits of length 1).

iv) Now, suppose $p = 2$, $r = 1$, and $s > 0$. Let $a = E2^h - 1$, $h \geq 2$, where E is odd. Then $a^i - 1 = P2^{h+s}$ and $(a^i-1)/(a-1) = Q2^{s+h-1}$ where P and Q are odd. Let also $x = X2^u$, X odd; rewrite equation (5.2) as

$$2^{s+h-1}(PX2^{u+1} + Q2^t) = 0 \pmod{2^m}. \tag{5.7}$$

a) If $t = 0$, it follows from (5.7) that $s + h - 1 = m$ or $s = m - h + 1$. Thus, every orbit has length $m - h + 1$.

b) If $u > t - 1$, it follows from (5.7) that $s + h - 1 + t = m$, and so $s = m - h - t + 1$.

If $0 \leq u < t - 1$, it follows from (5.7) that $s + h - 1 + u + 1 = m$, and so $s = m - h - u$. Therefore, for every s in the range $m - h \geq s > m - h - t + 1$, there exists an orbit of length 2^s.

If $u = t - 1$, then one can arrange for $PX + Q = 2^\alpha \pmod{2^m}$, where $\alpha \geq 1$ is arbitrary. It then follows again from (5.7) that $s + h - 1 + t + \alpha = m$, and so $s = m - h - t + 1 - \alpha$, or $0 < s \leq m - h - t$.

Combining these, we conclude that for every $0 < s \leq m - h$, there exists at least one orbit of length 2^s.

In addition, in this case, $P(x)$ can be conjugated to $Q(x) = ax$ via $x \mapsto x - \beta$, where β is such that

$$(a - 1)\beta = 2^t \pmod{2^m}.$$

Equation (5.1) then follows from the proof of (i).

It remains to discuss orbits of length 1. Suppose x is a fixed point of $P(x)$ i.e.,

$$(E2^h - 2)x + 2^t = 0 \pmod{2^m}.$$

If $t > 0$, then there are exactly two fixed points given by $x = -2^{t-1}c$ and $x = -2^{t-1}c + 2^{m-1}$, where c is the multiplicative inverse of $(E2^{h-1} - 1)$ modulo 2^m.

c) We have that there are exactly two orbits of length 1 for the same reasoning as above. The rest of the orbits have length 2 because if $m = h$, then $P(x) = -x + b$ and so, $P(P(x)) = x$. □

References

[1] Desjardins, D. L., & Zieve, M. E. *On the structure of polynomial mappings modulo an odd prime power*, `Arxiv.math/013046v1`.

[2] Dickson, L. E. (1901) *Linear Groups, with an exposition of the Galois field theory*, Published by Leipzig B.G. tuebner.

[3] Dickson, L. E. (1896–97) Analytic representation of substitutions, *Ann. of Math.,* v. 11, 65–120.

[4] Mullen, G. L., & Mummert, C. (2004) *Finite Fields and Applications*, AMS.

[5] Gouvêa, F.Q. (1993) *p-adic Numbers*, Springer-Verlag Berlin Heidelberg.

[6] Gupta, I., Narain, L., & Madhavan, C. E. V. (2003) Cryptological Applications of Permutation Polynomials, *Electron. Notes Discrete Math.*, 15, 91.

[7] Kedlaya, K., & Ng, L. (2015) *Solutions to the 73rd William Lowell Putnam Mathematical Competition*, `http://kskedlaya.org/putnam-archive/2012s.pdf`, Last visited: August 14, 2015.

[8] Laigle-Chapuy, Y. (2007) Permutation polynomials and applications to coding theory, *Finite Fields Appl.*, 13(1), 58–70.

[9] Larin, M. V. (2002) Transitive polynomial transformations of residue rings, *Discrete Math. Appl.*, 12(2), 127–10.

[10] Li, S. *Permutation Polynomials modulo* m, `Arxiv.math/0509523v6`.

[11] Lidl, R., & Mullen, G. L. (1988) When does a polynomial over a finite field permute the elements of the field? *Amer. Math. Monthly*, 95(3), 243–246.

[12] Lidl, R., & Mullen, G. L. (1993) When does a polynomial over a finite field permute the elements of the field? II, *Amer. Math. Monthly*, 100(1), 71–74.

[13] Lidl, R., & Müller, W. B. (1984) Permutation polynomials in RSA-Cryptosystems, In *D. Chaum (Ed.), Advances in Cryptology*, Springer US, 293–301.

[14] Mollin, R. A. (2011) *Algebraic Number Theory*, 2nd Ed., CRC Press.

[15] Rivest, R. L. (2001) Permutation Polynomials Modulo 2^w, *Finite Fields Appl.*, 7, 287–292.

[16] Rivest, R. L., Robshaw, M. J. B., Sidney, R., & Yin, Y. L. *The RC6 block cipher*, `http://people.csail.mit.edu/rivest/Rc6.pdf`, Last visited: June 2016.