DIGRAPHS FROM POWERS MODULO *p*

Caroline Lucheta
Box 1121 GCC, 100 Campus Drive, Grove City PA 16127 USA
Eli Miller
PO Box 410, Sumneytown, PA 18084 USA
Clifford Reiter
Department of Mathematics, Lafayette College, Easton, PA 18042 USA

1. Introduction

Given any function f defined modulo m, we can consider the digraph that has the residues modulo m as vertices and a directed edge (a, b) if and only if $f(a) \equiv b \pmod{m}$. The digraph associated with squaring modulo p, a prime, has been studied in [1]. In that paper the cycle lengths and the number of cycles appearing were characterized. The structure of the trees attached to cycle elements was also completely described. Our paper will generalize those results to the digraph associated with the function x^k modulo a prime p with k any positive integer. Since zero is in an isolated cycle for all p and k, we will consider the digraph generated by the non-zero reduced residues. We will let G_p^k denote the digraph on the non-zero residues modulo p with edges given by $x^k \pmod{p}$. Hence, the vertex set of G_p^k is equal to Z_p^*. For example, G_{53}^3 is shown in Figure 1 and G_{41}^4 is shown in Figure 2. Note that when $p = 2$, G_p^k consists of the vertex 1 in a loop. Thus, we need only consider G_p^k when p is an odd prime. We will use p to denote an odd prime throughout this paper.

Elementary results about these digraphs are described in Section 2. In particular, we see each component contains a single cycle and we can determine when there are non-cycle vertices. Section 3 characterizes the cycle lengths that appear. Section 4 explores the relationship of geometric subsets of the digraph to subgroups of the group of units mod p. Section 5 considers some special cases where long cycles occur. Section 6 returns to the basic structure of the digraph and shows that all the forests appearing must be isomorphic and characterizes their heights. Section 7 explores the simplifications of the structures that appear when k is prime.

We begin by enumerating six well known elementary theorems which will be used. Proofs can be found in many standard texts.

Theorem 1: If a _ 0, there are 0 or gcd(k, p - 1) solutions to $x^k \equiv a \pmod{p}$.
Proof: See [2,47]. □

Theorem 2: If d is a positive integer such that $d \mid p - 1$, then there are exactly $\varphi(d)$ incongruent residues of order d modulo p.
Proof: See [2,48]. □

Theorem 3: If n is a positive integer, then $\sum_{d\_n,d>0} \phi(d) = n$.

Proof: See [4,83]. □

Theorem 4: If a is an integer such that gcd(a, m) = 1 and i is a positive integer, then

$$\mathrm{ord}_m\ a^i = \frac{\mathrm{ord}_m\ a}{\gcd(i,\ \mathrm{ord}_m\ a)}.$$

Proof: See [4,132]. □

Theorem 5: A primitive root modulo m exists if and only if m is of the form 2, 4, p^n, or $2p^n$ where p is an odd prime.
Proof: See [2,49]. □

Theorem 6: If a and b are elements of Z_p^* such that $\alpha = \mathrm{ord}_p\, a$, $\beta = \mathrm{ord}_p\, b$, and $\gcd(\alpha, \beta) = 1$, then $\mathrm{ord}_p\, ab = \alpha\beta$.
Proof: See [3,46]. □

2. Basic Properties

The following lemmas are easy to prove but fundamental to the understanding of the digraph structure of G_p^k. We will see that for all G_p^k, each graph component contains a unique cycle which may have forest structures attached to it.

Lemma 7: The outdegree of any vertex in G_p^k is one.
Proof: The function x^k (mod p) maps the vertex a to a^k and only a^k. □

Lemma 8: Given any element in G_p^k, repeated iteration of x^k (mod p) will eventually lead to a cycle.
Proof: Because there are p - 1 vertices in G_p^k, iterating x^k (mod p) must eventually produce a repeated value. □

Lemma 9: Every component of G_p^k contains exactly one cycle.
Proof: Suppose a component has more than one cycle; then somewhere along the undirected path connecting any two cycles there exists a vertex with outdegree at least 2, which is impossible. □

Lemma 10: The set of non-cycle vertices leading to a fixed cycle vertex forms a forest.
Proof: Since each component contains exactly one cycle, the vertices leading to a cycle vertex cannot contain a cycle; thus they are a forest. □

Lemma 11: The indegree of any vertex in G_p^k is 0 or $\gcd(k, p - 1)$.
Proof: This result is an immediate application of Theorem 1. □

Lemma 12: Every component of G_p^k is cyclical if and only if $\gcd(k, p - 1) = 1$.
Proof: (⇒) If all digraph components are cyclical both the indegree and outdegree are one, which implies from Lemma 11 that $\gcd(k, p - 1) = 1$.

(⇐) Conversely, if $\gcd(k, p - 1) = 1$ the indegree of every vertex is 0 or 1. If some component were not cyclical there would exist a cycle vertex with indegree ≥ 2, a contradiction. □

For example, each component of G_{53}^{3} is cyclical since gcd(3, 52) = 1; this is apparent in Figure 1. Likewise, G_{41}^{4} has vertices outside the cycles because gcd(4, 40) = 4 (see Figure 2). We will refer to a *child* of a vertex a as a vertex v that satisfies the equation $v^k \equiv a \pmod{p}$. These are the predecessors of a in G_p^k. Note that our child vertices are children in the sense of the forest structure but not in the standard sense of direction. Predecessors that are not in a cycle will be called *non-cycle* children. For example, in G_{41}^{4}, 37 has the three non-cycle children 8, 31 and 33.

Lemma 13: Any cycle vertex, c, has gcd(k, p - 1) - 1 non-cycle children.
Proof: From Lemma 11, the indegree of c is 0 or gcd(k, p - 1). Since c is a cycle vertex, the indegree is not zero but gcd(k, p - 1). The number of non-cycle children is gcd(k, p - 1) - 1. □

Above we saw some of the basic results about G_p^k. Notice that if we fix k and vary p the number of vertices changes and infinitely many different digraphs result. However, the next theorem shows that if p is fixed, only finitely many distinct digraphs result as k varies.

Theorem 14: $k_1 \equiv k_2 \pmod{p - 1}$ if and only if $G_p^{k_1} = G_p^{k_2}$.
Proof: (⇒) Suppose $k_1 \equiv k_2 \pmod{p - 1}$ and without loss of generality $k_1 \geq k_2$. If a is any vertex in the reduced residue set, $\text{ord}_p\, a \mid (p - 1) \mid (k_1 - k_2)$, so $a^{k_1 - k_2} \equiv 1$ implies $a^{k_1} \equiv a^{k_2} (\text{mod } p)$. Hence, $G_p^{k_1} = G_p^{k_2}$.

(⇐) Suppose $G_p^{k_1} = G_p^{k_2}$, and assume $k_1 \geq k_2$. Then $a^{k_1} \equiv a^{k_2} (\text{mod } p)$ implies $\text{ord}_p\, a \mid (k_1 - k_2)$ for all a in G_p. So $(p - 1) \mid (k_1 - k_2)$, and the conclusion follows. □

The 12 different digraphs for G_{13}^{k} are shown in Figure 3. Notice that some have only cycles and some have forest structures. Also notice that this theorem gives a condition for equality of digraphs, but does not settle the question of when two digraphs can be *isomorphic* for different values of k. Note that G_{11}^{2} *ne* G_{11}^{8} but $G_{11}^{2} \approx G_{11}^{8}$.

3. Characterizing Cycles

When considering the cycle structure of G_p^k it is convenient to factor p - 1 as wt where t is the largest factor of p - 1 relatively prime to k. So gcd(k, t) = 1 and gcd(w, t) = 1. For example, if p = 41 and k = 6, then $p - 1 = 2^3 5$, so w = 8 and t = 5. Similarly if p = 47 and k = 4 then w = 2 and t = 23; also if p = 19 and k = 6 then w = 18 and t = 1. In all the theorems below we will be considering the digraph G_p^k with $p - 1 = wt$ as described.

Theorem 15: The vertex c is a cycle vertex if and only if $\text{ord}_p\, c \mid t$.
Proof: (⇒) Since c is in a cycle there exists some $x \geq 1$ such that $c^{k^x} \equiv c$ and thus $c^{k^x - 1} \equiv 1 (\text{mod } p)$. Hence, $\text{ord}_p\, c \mid k^x - 1$, which implies that gcd(ord$_p\, c$, k) = 1, so gcd(ord$_p\, c$, w) = 1 also. We know $\text{ord}_p\, c \mid p - 1 = wt$, and so ord$_p\, c$ must divide t.

(⇐) Suppose $c \in G_p^k$ and $\text{ord}_p\, c \mid t$; therefore, gcd(ord$_p\, c$, k) = 1. On repeated iteration, c

must eventually end up in a cycle. If y is the number of steps to reach the cycle and x is the cycle length, then $c^{k^y(k^x-1)} \equiv 1 (\bmod\ p)$. Therefore, $\text{ord}_p\, c \mid k^y(k^x - 1)$, but since $\gcd(\text{ord}_p\, c, k) = 1$, $\text{ord}_p\, c \mid k^x - 1$. Hence, $c^{k^x} \equiv c (\bmod\ p)$ which implies that c is a cycle vertex. □

Corollary 16: There are t vertices in cycles.
Proof: From Theorem 15, the total number of cycle vertices is $\sum_{d \mid t} \text{N(d)}$ where N(d) is the number of elements of order d (mod p). Theorems 2 and 3 imply that this is t. □

Theorem 17: Vertices in the same cycle have the same order (mod p).
Proof: Assume a and b are in the same cycle. Hence, there exists an e such that $a^e \equiv b$ (mod p). Let $\alpha = \text{ord}_p\, a$ and $\beta = \text{ord}_p\, b$. It follows that $b^\alpha \equiv a^{e\alpha} \equiv 1$ (mod p) and thus $\beta \mid \alpha$. Similarly, $\alpha \mid \beta$ and hence the orders are equal. □

Theorem 17 shows that the order (mod p) of vertices in the same cycle are equal. Hence, the notion of the *order of a cycle* is well-defined. We now look at the relationship between the order of a cycle and its length.

Theorem 18: Let x be the length of a cycle of order d (mod p), then $k^x - 1$ is the smallest number of the form $k^n - 1$ divisible by d.
Proof: Let c be a vertex in the cycle. Since the cycle is of length x, $c^{k^x-1} \equiv 1 (\bmod\ p)$. It follows that $d = \text{ord}_p\, c$ divides $k^x - 1$. If $\text{ord}_p\, c \mid k^s - 1$ for some $s < x$, then $c^{k^s} \equiv c$, a contradiction. □

Theorem 18 shows that the length of a cycle depends entirely on its order. If we let l(d) denote the *length of cycles* with order d, we get the following theorem.

Theorem 19: Let a, b and d be orders of cycles. Then :

(i) $\text{l}(d) = \text{ord}_d\, k$.

(ii) There are $\varphi(d) / \text{l}(d)$ cycles of order d.

(iii) $\text{l}(\text{lcm}(a, b)) = \text{lcm}(\text{l}(a), \text{l}(b))$.

(iv) The longest cycle length in G_p^k is $\text{l}(t) = \text{ord}_t\, k$.

Proof: (i) By Theorem 18, $\text{l}(d) = \min\{n : d \mid k^n - 1\}$, hence $\text{l}(d) = \text{ord}_d\, k$.

(ii) By Theorem 2, there are $\varphi(d)$ elements of order d, and there are l(d) in each cycle by (i), hence the result.

(iii.a) By (i), $k^{\text{l}(a)} \equiv 1$ (mod a) and $k^{\text{l}(b)} \equiv 1$ (mod b), thus $k^{\text{lcm}(\text{l}(a),\, \text{l}(b))} \equiv 1$ (mod a) and $k^{\text{lcm}(\text{l}(a),\, \text{l}(b))} \equiv 1$ (mod b). It follows that $k^{\text{lcm}(\text{l}(a),\, \text{l}(b))} \equiv 1$ (mod lcm(a, b)). So, $\text{l}(\text{lcm}(a, b)) \mid \text{lcm}(\text{l}(a), \text{l}(b))$.

(iii.b) We know $k^{\text{l}(\text{lcm}(a,\, b))} \equiv 1$ (mod lcm(a, b)). So $k^{\text{l}(\text{lcm}(a,\, b))} \equiv 1$ (mod a) and $k^{\text{l}(\text{lcm}(a,\, b))} \equiv 1$ (mod b). Thus, $\text{l}(a) \mid \text{l}(\text{lcm}(a, b))$ and $\text{l}(b) \mid \text{l}(\text{lcm}(a, b))$ which implies that $\text{lcm}(\text{l}(a), \text{l}(b)) \mid \text{l}(\text{lcm}(a, b))$. Putting (iii.a) and (iii.b) together gives $\text{l}(\text{lcm}(a, b)) = \text{lcm}(\text{l}(a), \text{l}(b))$.

(iv) All orders of cycles divide t and if $d \mid t$ then $\text{l}(t) = \text{l}(\text{lcm}(t, d)) = \text{lcm}(\text{l}(t),\text{l}(d))$ which implies $\text{l}(d) \mid \text{l}(t)$. Thus, l($t$) is the maximal cycle length. □

We are now in a position to identify the number of cycles of every length appearing in the digraph of G_p^k. For example, consider G_{53}^3 (Figure 1); in this case $p - 1 = 52$ so $w = 1$ and $t = 52$.

The possible orders of the cycle elements are the divisors of *t*: 1, 2, 4, 13, 26, and 52. There are φ(52) = 24 elements of order 52, and these 24 elements are in cycles of length l(52) = ord_{52} 3 = 6, contributing four cycles of length 6. Similarly, the elements of order 26 appear in 4 cycles of length 3; and those of order 13 are in 4 cycles of length 3. There are 2 elements of order 4 in one cycle and two cycles of length one with orders 1 and 2. Table 1 gives some details about cycles in G_p^k for selected *p* and *k*.

4. Subgroups of Z_p^* in G_p^k

We now consider orders of elements throughout G_p^k. We will be able to associate elements of various orders with subgroups of Z_p^*, which allows for the identification of certain

k	2			3			4			5			6		
p	*d*	l(*d*)	#	*d*	l(*d*)	#	*d*	l(*d*)	#	*d*	l(*d*)	#	*d*	l(*d*)	#
41	1 5	1 4	1 1	1 2 4 5 8 10 20 40	1 1 2 4 2 4 4 4	1 1 1 1 2 1 2 4	1 5	1 2	1 2	1 2 4 8	1 1 1 2	1 1 2 2	1 5	1 1	1 4
43	1 3 7 21	1 2 3 6	1 1 2 2	1 2 7 14	1 1 6 6	1 1 1 1	1 3 7 21	1 1 3 3	1 2 2 4	1 2 3 6 7 14 21 42	1 1 2 2 6 6 6 6	1 1 1 1 1 1 2 2	1 7	1 2	1 3
47	1 23	1 11	1 2	1 2 23 46	1 1 11 11	1 1 2 2	1 23	1 11	1 2	1 2 23 46	1 1 22 22	1 1 1 1	1 23	1 11	1 2
53	1 13	1 12	1 1	1 2 4 13 26 52	1 1 2 3 3 6	1 1 1 4 4 4	1 13	1 6	1 2	1 2 4 13 26 52	1 1 1 4 4 4	1 1 2 3 3 6	1 13	1 12	1 1

Table 1: Cycle lengths in G_p^k.

subgroups of Z_p^* with geometric subsets of the digraph. In later sections we will return to characterizing the cycle and forest structure of these digraphs.

Lemma 20: If H_d is the set of residues with orders dividing d, with $d \geq 1$, then H_d is a cyclic subgroup of Z_p^*.

Proof: Since Z_p^* is a finite cyclic group, we need only show that H_d is non-empty and closed under multiplication. Clearly H_d is not empty because it has the identity. To show closure suppose that a, $b \in H_d$ and let $\alpha = \text{ord}_p\, a$, and $\beta = \text{ord}_p\, b$. Since $(ab)^{\text{lcm}(\alpha,\, \beta)} \equiv 1 \pmod{p}$, $\text{ord}_p\, ab$ divides $\text{lcm}(\alpha, \beta)$ which in turn divides d. Therefore, H_d is a subgroup of Z_p^*. □

For instance, if we consider the group Z_{41}^*, the elements of order 1 and 2 form the subgroup H_2 while H_{10} contains those elements of order 1, 2, 5 and 10.

We will now introduce a notation for the forest originating from any given cycle vertex. Let F_c^n represent the set of vertices in the n^{th} level of the forest originating from the cycle vertex c. Of course, F_c^n depends on G_p^k. For example, in G_{41}^4 (Figure 2), $F_{16}^1 = \{2, 23, 39\}$ and $F_{16}^2 = \{7, 19, 22, 34\}$. Similarly, F^n refers to the vertices in the n^{th} level of all forests and F_c refers to all forest vertices associated with the cycle vertex c at all levels $n \geq 1$. Note that the cycle vertices are not a part of the forests but for convenience we will denote the set of cycle elements by F^0 and also $F_c^0 = \{c\}$ but $c \notin F_c$.

The next theorem and corollary explain the subgroup structures present in the digraphs. First it will be shown that the order of an element is constrained by its height in the forest structure.

Theorem 21: Let $a \in F_c$ and $\text{ord}_p\, c = d \mid t$. Then $\text{ord}_p\, a \mid k^h d$ if and only if $a \in F_c$ where $x \leq h$.

Proof: ($\Rightarrow$) Suppose $\text{ord}_p\, a \mid k^h d$. Then $(a^{k^h})^d \equiv 1 \pmod{p}$. Now using Theorem 4,

$$1 = \text{ord}_p\, 1 = \text{ord}_p\, (a^{k^h})^d = \frac{\text{ord}_p\, a^{k^h}}{\gcd(d,\ \text{ord}_p\, a^{k^h})}$$

Because $\gcd(d, \text{ord}_p\, a^{k^h}) = \text{ord}_p\, a^{k^h}$, $\text{ord}_p\, a^{k^h}$ divides d which divides t. From Theorem 15, a^{k^h} must be a cycle element, and hence $a \in F_c$ where $x \leq h$.

($\Leftarrow$) If $a \in F_c$ and $x \leq h$, then a^{k^x} is a cycle element of order d. Furthermore, $d = \text{ord}_p\, a^{k^x} = \dfrac{\text{ord}_p\, a}{\gcd(k^x,\ \text{ord}_p\, a)}$, hence $d \cdot \gcd(k^x, \text{ord}_p\, a) = \text{ord}_p\, a$ and thus $\text{ord}_p\, a \mid d \cdot k^x \mid d \cdot k^h$.

□

From the Theorem 21 it can be ascertained that various sets of digraph structures form subgroups of Z_p^*, as stated in the next corollary.

Corollary 22: For all d dividing t and all h, $\bigcup_{\substack{0 \le x \le h \\ \mathrm{ord}_p\, c \mid d}} \mathrm{F}_c^x$ is a subgroup of Z_p^*, namely $\mathrm{H}_{k^h d}$.

Proof: The union over all c such that $\mathrm{ord}_p\, c \mid d$ and over all $x \le h$, contains all $a \in Z_p^*$ such that $\mathrm{ord}_p\, a \mid k^h d$ by Theorem 21. This is the subgroup $\mathrm{H}_{k^h d}$ of Z_p^* by Lemma 20. □

Thus, the union of cycle vertices with orders dividing a fixed d and vertices in their associated forest structures up to a fixed height form a subgroup of Z_p^*. In particular, if $d = 1$, all the vertices in F_1 up to any fixed level (along with 1) form a subgroup. On the other extreme, if $d = t$, all the vertices in all the components up to a fixed height form subgroups. Examining the digraph of G_{41}^4 (Figure 2) one finds the following subgroups :

$d = 1, h = 0$: $\mathrm{F}_1^0 = \{1\} = \mathrm{H}_1$.

$d = 1, h = 1$: F_1^0 union $\mathrm{F}_1^1 = \{1, 9, 32, 40\} = \mathrm{H}_4$.

$d = 1, h = 2$: F_1^0 union F_1^1 union $\mathrm{F}_1^2 = \{1, 3, 9, 14, 27, 32, 38, 40\} = \mathrm{H}_8$.

$d = 5, h = 0$: $\mathrm{F}^0 = \{1, 10, 16, 18, 37\} = \mathrm{H}_5$.

$d = 5, h = 1$: F^0 union $\mathrm{F}^1 = \{1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40\} = \mathrm{H}_{20}$.

$d = 5, h = 2$: F^0 union F^1 union $\mathrm{F}^2 = \{1, \ldots, 40\} = Z_{41}^* = \mathrm{H}_{40}$.

Lemma 23: The product of a forest element and a cycle element is a forest element.
Proof: The cycle elements of G_p^k form a closed multiplicative subgroup of Z_p^*; hence, the product of a forest element and a cycle element must be a forest element. □

These algebraic properties imply that the highest level of the digraph, which will be referred to as the *canopy*, must contain at least half of the vertices. For example, in G_{41}^4 (Figure 2) the canopy is F^2.

Corollary 24: If h_0 is the maximal height attained by the forest elements in G_p^k then $|\mathrm{F}^{h_0}| \ge \frac{p-1}{2}$.

Proof: (i) If $h_0 = 0$ then all vertices are in cycles, so $|\mathrm{F}^0| = p - 1 \ge \frac{p-1}{2}$.

(ii) If $h_0 \ge 1$, then from Corollary 22, $\mathrm{H}_{k^{h_0-1}t} = \underset{0 \le n \le h_0 - 1}{\mathrm{union}} \mathrm{F}^n$ is a proper subgroup of Z_p^*. The number of elements in $\mathrm{H}_{k^{h_0-1}t}$ must be a proper divisor of $|Z_p^*| = p - 1$. Because the largest proper divisor of $p - 1$ is $(p - 1) / 2$ there are at least $(p - 1) / 2$ vertices remaining in the canopy. □

5. Occurrence of Long Cycles

Control over the lengths of cycles is highly desirable. This is essential for applications to pseudo-random number generation and data encryption. The first theorem below provides an upper bound for the cycle lengths appearing in G_p^k. Special cases where long cycles can be guaranteed are then considered.

Theorem 25: Let $p > 5$ be prime. Then the length of the longest cycle in G_p^k is less than or equal to $(p - 3) / 2$.

Proof: Consider two cases depending on $\gcd(k, p - 1)$.

(i) Suppose $\gcd(k, p - 1) \neq 1$. By Lemma 12, G_p^k is not entirely cyclical and by Theorem 24, it has a forest structure with at least $(p - 1) / 2$ vertices in the canopy. So, there are at most $(p - 1) / 2$ vertices in cycles. Since $p > 5$, we know we are not interested in longest cycles of length 1, and since 1 is in a loop, it is not part of any longest cycle of interest, hence the maximal length cannot exceed $\frac{p - 1}{2} - 1 = \frac{p - 3}{2}$.

(ii) Suppose $\gcd(k, p - 1) = 1$; thus G_p^k consists entirely of cycles. From Theorem 19, the longest cycle length is associated with the elements of order $t = p - 1$ which can be factored as $2^s\tau$, where $s \geq 1$ and τ is odd.

(a) If $\tau \neq 1$, then the number of elements of order $p - 1$ is $\varphi(p - 1) = \varphi(2^s\tau) = 2^{s-1}\varphi(\tau) < 2^{s-1}\tau = \frac{p - 1}{2}$. Now since $\varphi(p - 1)$ is an integer, $\varphi(p - 1) \leq \frac{p - 3}{2}$. Hence, even if all elements of order $p - 1$ were together in one cycle, the length could not exceed $(p - 3) / 2$.

(b) If $\tau = 1$, then $p = 2^s + 1$ is a Fermat prime larger than 5, so $s > 1$. By Theorem 19 the length of the longest cycle is $l(t) = l(2^s) = \mathrm{ord}_{2^s}\, k$. However, $Z_{2^s}^*$ does not have a primitive root for $s > 1$ (Theorem 5). Thus, $\mathrm{ord}_{2^s}\, k < \phi(2^s) = \frac{p-1}{2}$ and hence $l(t) \leq \frac{p - 3}{2}$ in this case as well. □

While this theorem gives an upper bound for the cycle lengths in G_p^k, it does not specify whether this bound is ever attained. The next theorem shows that for Sophie Germain primes these maximal cycle lengths can be attained.

Theorem 26: Let $p = 2q + 1$ where q is an odd Sophie Germain prime. If k is a primitive root mod q, then G_p^k contains a cycle of length $(p - 3) / 2$.

Proof: Because $\gcd(k, q) = 1$ and $q \mid t$, the elements with order q are in cycles of length $\mathrm{ord}_q\, k = q - 1 = (p - 3) / 2$. □

Corollary 27: Let $p = 2q + 1$ where q is an odd Sophie Germain prime. If k is an odd primitive root mod q, then G_p^k contains two cycles of length $(p - 3) / 2$.

Proof: Since k is odd, $t = 2q$ and the graph is entirely cyclical. The elements of order q are in a cycle of length $\mathrm{ord}_q\, k = q - 1 = (p - 3) / 2$. The elements of order $t = 2q$ are, by Theorem 19, in the longest cycles of the digraphs. So the elements of order $2q$ are also in a cycle of length $(p - 3) / 2$. □

For example, consider G_{23}^2 (Figure 4); $p = 23 = 2(11) + 1$, and 2 is a primitive root mod 11. As expected, G_{23}^2 contains one cycle of length 10. Corollary 27 is illustrated by G_{47}^5 where $p = 47 = 2(23) + 1$, 5 is a primitive root mod 23, and the digraph has two cycles of length 22.

Given a prime of the form $2q + 1$, where k is a primitive root mod q, it is simple to iterate through a cycle of length $(p - 3) / 2$. Any residue between 2 and $p - 2$ is either in a long cycle or is one step away. Beginning with any such residue we can iterate $x^k \pmod p$ to produce $(p - 3) / 2$ incongruent values. For example, consider the prime $9887 = 2(4943) + 1$ where 4943 is also prime. Since 7 is a primitive root of 4943, iteration of x^7 (mod 9887) beginning with any x from 2 to 9885 will yield 4942 incongruent values.

6. Characterizing Forests

Having completely characterized the cycles for the digraph generated by $x^k \pmod p$ we turn our attention to characterizing the noncyclical elements of G_p^k. In each of our examples, we notice that the forests in any particular digraph are isomorphic. This turns out to be true in general and will be proved by constructing a one-to-one correspondence between F_1 and F_c. The next lemma gives the essence of how the correspondence will be constructed.

Lemma 28: If $a \in \mathrm{F}_1^\mathrm{h}$ and c is a cycle vertex, then $ac \in \mathrm{F}^\mathrm{h}_{\mathrm{c}^{\mathrm{k}^\mathrm{h}}}$.

Proof: Using Lemma 23, it follows immediately that $ac \notin \mathrm{F}^0$. Furthermore, $(ac)^{k^h} \equiv c^{k^h} (\bmod\ p)$ is a cycle element but $(ac)^{k^{h-1}}$ is a forest element, which implies that $ac \in \mathrm{F}^\mathrm{h}_{\mathrm{c}^{\mathrm{k}^\mathrm{h}}}$. □

Theorem 29: Let c be a cycle element, then $\mathrm{F}_1 \approx \mathrm{F}_c$.

Proof: (i) First we show there exists a 1-1 correspondence between the vertices of F_1^h and $\mathrm{F}_\mathrm{c}^\mathrm{h}$ for all heights h, and hence between F_1 and F_c. Let h be fixed and let c_h denote the unique *cycle* element such that $c_h^{k^h} \equiv c (\bmod\ p)$. Define $f_h : \mathrm{F}_1^\mathrm{h} \rightarrow \mathrm{F}_\mathrm{c}^\mathrm{h}$ by $f_h(a) \equiv a \cdot c_h \pmod p$.

First we check that f_h is one-to-one and onto. Let $b \in \mathrm{F}_\mathrm{c}^\mathrm{h}$. Then $(b \bullet c_h^{-1})^{k^h} \equiv b^{k^h} (c_h^{k^h})^{-1} \equiv c \bullet c^{-1} \equiv 1 \in \mathrm{F}_1^0$ and $(b \bullet c_h^{-1})^{k^{h-1}} \notin \mathrm{F}^0$ because $b^{k^{h-1}} \notin \mathrm{F}^0$ and $c_h^{-k^{h-1}} \in \mathrm{F}^0$. It follows that $b \bullet c_h^{-1} \in \mathrm{F}_1^\mathrm{h}$. Furthermore, $f_h(b \bullet c_h^{-1}) \equiv b \bullet c_h^{-1} \bullet c_h \equiv b (\bmod\ p)$ so f_h is onto $\mathrm{F}_\mathrm{c}^\mathrm{h}$. Suppose $f_h(a_1) \equiv f_h(a_2) \pmod p$ for $a_1, a_2 \in \mathrm{F}_1^\mathrm{h}$. Then $a_1 \cdot c_h \equiv a_2 \cdot c_h$ implies $a_1 \equiv a_2 \pmod p$. Thus, f_h is one-to-one.

(ii) It remains to be shown that there exists a 1-1 correspondence between the edges of F_1 and F_c. We want to define $g : \mathrm{E}(\mathrm{F}_1) \rightarrow \mathrm{E}(\mathrm{F}_\mathrm{c})$ by $g(a, a^k) = (f_h(a), f_{h\text{-}1}(a^k))$ where h is the height of a in F_1. If $(f_h(a), f_{h\text{-}1}(a^k))$ is in fact in $\mathrm{E}(\mathrm{F}_c)$, then g will inherit the 1-1 and onto properties from f_h and $f_{h\text{-}1}$. We have an edge $(f_h(a), f_{h\text{-}1}(a^k))$ if and only if $(f_h(a))^k \equiv f_{h\text{-}1}(a^k) \pmod p$. Now $f_h(a) \equiv a \cdot c_h \pmod p$ where $c_h^{k^h} \equiv c$ and $f_{h\text{-}1}(a) \equiv a \cdot c_{h\text{-}1} \pmod p$ where $c_{h-1}^{k^{h-1}} \equiv c (\bmod\ p)$; thus $c_h^{k^h} \equiv c \textit{ implies} (c_h^k)^{k^{h-1}} \equiv c (\bmod\ p)$. By the uniqueness of c_h, $c_{h-1} \equiv c_h^k$ and $f_{h-1}(a) \equiv a \bullet c_h^k (\bmod\ p)$. Now $(f_h(a))^k \equiv (a \cdot c_h)^k \equiv a^k \bullet c_h^k \equiv f_{h\text{-}1}(a^k) \pmod p$. Hence, $(f_h(a), f_{h\text{-}1}(a^k)) \in \mathrm{E}(\mathrm{F}_c)$ and by the argument above, the edges and vertices are in 1-1 correspondence, so $\mathrm{F}_1 \approx \mathrm{F}_\mathrm{c}$. □

There is another property of this mapping that can be addressed. Considering $a \in \mathrm{F}_1$ and $c \in \mathrm{F}^0$, the order of the element $ac \pmod p$ will be $(\mathrm{ord}_p\, a)(\mathrm{ord}_p\, c)$. That is, the isomorphism "preserves" orders between F_1 and F_c in that the orders of corresponding elements in F_c are multiplied by the order of *c*.

Theorem 30: If $a \in F_1$ and $b \in F_c$ with c_h the cycle element such that $b \equiv a \cdot c_h \pmod{p}$, then $\text{ord}_p\, b = (\text{ord}_p\, a)(\text{ord}_p\, c)$.
Proof: By Theorem 21, $\text{ord}_p\, a \mid k^h$ and thus $\gcd(\text{ord}_p\, a, t) = 1$. By Theorem 15, $\text{ord}_p\, c = \text{ord}_p\, c_h \mid t$, hence $\gcd(\text{ord}_p\, a, \text{ord}_p\, \text{c}) = 1$ and applying Theorem 6 gives the desired result. □

Some examples of the isomorphism described in Theorem 29 and Theorem 30 can be seen in Table 2.

a	*c*	*ac*	$\text{ord}_p\, a$	$\text{ord}_p\, c$	$\text{ord}_p\, ac$
1	10	10	1	5	5
9	37	5	4	5	20
3	10	30	8	5	40

Table 2: Some orders and products in G_{41}^{4}.

Finally, we prove a result that determines the height of the forests:

Theorem 31: If h_0 is the minimal *h* such that $p - 1 \mid k^h t$, then h_0 is the height of the forests in G_p^k.
Proof: (i) If $\gcd(k, p - 1) = 1$, then all the vertices are in cycles and hence $h_0 = 0$.

(ii) If $\gcd(k, p - 1) \neq 1$, then $h_0 \geq 1$. Let *a* be a vertex of order $p - 1$. From Theorem 21 *a* must be at height h_0 because $\text{ord}_p\ a \mid k^{h_0} t$ but $\text{ord}_p\ a \_ k^{h_0 - 1} t$. There are no vertices at a greater height since for any vertex *b* in G_p^k, $\text{ord}_p\ b \mid p - 1 \mid k^{h_0} t$ and thus *b* is at level h_0 or lower in G_p^k. □

For example, in G_{41}^{4} we see that $t = 5$ and $41 - 1 = 40 \mid 4^2 5$ which implies that the height of the forest is 2. This value is apparent in Figure 2.

7. Prime Exponents

In the special case where the exponents are prime, many of our results simplify. In particular, while we were able to prove that the forest structures were isomorphic with a general exponent *k*, we can completely characterize that structure if the exponent is prime. We will consider the digraph associated with a prime exponent *q*, letting $p - 1 = q^s t$ where *t* is relatively prime to *q*.

Corollary 32: The indegree of a vertex in G_p^q is $\begin{cases} \mathit{0\ or\ q} & \text{if } p \equiv 1 \pmod{q} \\ 1 & \text{otherwise} \end{cases}$.
Proof: This follows from Lemma 11 and Lemma 12 with $k = q$. □

Thus all the digraph components are cyclical if and only if $p \_ 1 \pmod{p}$.

Corollary 33: Any cycle vertex has $q - 1$ non-cycle children.
Proof: This follows from Lemma 13. □

Theorem 34: If $p \equiv 1 \pmod{q}$, the q - 1 non-cycle children of each cycle element are roots of complete q-nary trees.

Proof: Since the t forests in G_p^q are isomorphic and there are $q^s t$ elements in the digraph, $|F_1| = q^s - 1$. Furthermore, Theorem 31 states that the height of F_1 is s. If F_1 is not composed of q - 1 complete q-nary trees, there exists a vertex that has indegree 0 but is not at height s. This would imply that $|F_1| < q^s - 1$, a contradiction. Since all the forests are isomorphic to F_1, and F_1 consists of complete q-nary trees, all the forests in G_p^q are complete q-nary trees as well. □

As an example, consider F_1 in the digraph G_{109}^3, as shown in Figure 5. Since $109 - 1 = 3^3(4)$, and $45^3 \equiv 63^3 \equiv 1 \pmod{109}$, 45 and 63 are roots of complete ternary trees with height $3 - 1 = 2$.

When the exponent is prime we can also say more about the orders of elements in the digraph G_p^q.

Theorem 35: A vertex $a \in F_1$ if and only if $\text{ord}_p\, a = q^h$.

Proof: Consider Theorem 21 with $k = q$ and $c = 1$, and hence $d = 1$. Then $\text{ord}_p\, a \mid q^h$ if and only if $a \in F_1^x$ for $x \leq h$. Having elements of order q^h in a level x less than h would imply that $q^h \mid q^x$ where $x < h$, a contradiction. □

Returning to G_{109}^3 (Figure 5), one can check that the orders of 3, 9, and 27, correspond to F_1^1, F_1^2, and F_1^3.

Corollary 36: If $a \in F_c^h$ then $\text{ord}_p\, a = q^h \cdot \text{ord}_p\, c$.

Proof: Theorem 35 and the multiplying principle of Theorem 30 give the desired result. □

Conclusions

We have seen that many of the features of the digraph G_p^k can be determined in terms of properties of p and k. In particular, we have seen that the digraphs break up into components with exactly one cycle per component and that the forest structures associated with each cycle vertex throughout the digraph are isomorphic. The cycle lengths depend on the orders of the elements; we can also determine the heights of the forests. In special cases long cycles can be found and complete q-nary trees can be guaranteed.

While we have found a very rich structure for the digraphs associated with x^k mod p, it is natural to ask what other digraphs arising from functions such as these have a rich structure. The function x^k mod m, where m is not prime will have a much different digraph since 0 will not necessarily be in a trivial cycle and primitive roots may not exist. On the other hand, looking at x^k in a finite field where 0 must be trivial and primitive roots always exist ought to lead to a theory like that seen in this paper. Digraphs from functions such as $x^k + 1$ mod p will be difficult to handle because we can not lean on the theory of orders of elements as in this paper. It would be interesting to know what kind of control on the digraphs can obtained in such cases.

Acknowledgement

This work was supported in part by NSF-REU grant DMS-9300555.

References

[1] Earle L. Blanton, Jr., Spencer P. Hurd, and Judson S. McCranie, "On a Digraph Defined by Squaring Modulo n", *The Fibonacci Quarterly* 30.4 (1992) 322-334.

[2] Hua Loo Keng, *Introduction to Number Theory*, translated by Peter Shiu, Berlin: Springer-Verlag, 1982.

[3] Nathan Jacobson, *Basic Algebra I*, San Francisco: W.H. Freeman and Co., 1974.

[4] James Strayer, *Elementary Number Theory*, Boston: PWS Publishing Co., 1994.

AMS Classification Numbers: 05C20, 11B50.

*****