FUNCTION DIGRAPHS OF QUADRATIC MAPS MODULO *p*

Christie L. Gilbert
8 Gerome Avenue, Burlington, NJ 08016 USA

Joseph D. Kolesar
4521 Birchwold Road, South Euclid, OH 44121 USA

Clifford A. Reiter
Department of Mathematics, Lafayette College, Easton, PA 18042 USA
E-mail: reiterc@lafayette.edu

John D. Storey
218 Sparrow Drive, Wake Forest, NC 27587 USA

1. INTRODUCTION

In this paper we will consider geometric representations of the iteration of quadratic polynomials modulo p. This is a discrete analogue of the classical quadratic Julia sets which have been the subject of much study [3,4]. In particular, let $\mathrm{fd}_m(\mathrm{u}(x))$ denote the function digraph which has $\mathbf{Z}_\mathrm{m}$ as vertices and edges of the form $(x,\mathrm{u}(x))$ where x is an element of $\mathbf{Z}_\mathrm{m}$. This digraph geometrically represents the function $\mathrm{u}(x)$ and paths correspond to iteration of $\mathrm{u}(x)$. The function digraphs resulting from squaring mod m, $\mathrm{fd}_m(x^2)$, have been studied when m is prime or has a primitive root [1,2,5,10]. In particular, the cycle and tree structures have been classified. In [8] these results were generalized from $\mathrm{fd}_p(x^2)$ to $\mathrm{fd}_p(x^k)$ and a correspondence between geometric subsets of the function digraph and subgroups of the group of units was established. Subsequently, most of the results were generalized to general moduli in [12].

The aim of our paper is to explore these same ideas for the iteration of general quadratic functions instead of powers. In other words, we will consider $\mathrm{fd}_p(a_0 + a_1x + a_2x^2)$ where $a_0, a_1 \in \mathbf{Z}_p$ and $a_2 \in \mathbf{Z}_p^*$. It is easy to enumerate the four function digraphs for $p = 2$ and so we will study the case when p is an odd prime. Although these digraphs do not contain nearly as much symmetry as the previously studied cases, it is possible to observe some aspects of their structure. Consider Figure 1 which shows the digraphs resulting from the iteration of x^2 and $x^2 + 1$ modulo 13. Each of those digraphs breaks into 3 components. In reading the digraphs note that the cycle contained in each component appears at the left and the cycles progress clockwise; that is $\mathrm{u}(x)$ appears below x, except for the lowest cycle element where $\mathrm{u}(x)$ appears at the top. For noncycle elements, $\mathrm{u}(x)$ appears to the left of x in accordance with the indicated tree structure. Notice that the trees associated with each cycle element are uniform for x^2 but not for $x^2 + 1$. While it seems very difficult to completely determine the tree and cycle structure without enumerating the entire digraph, we can determine various things about the structure.

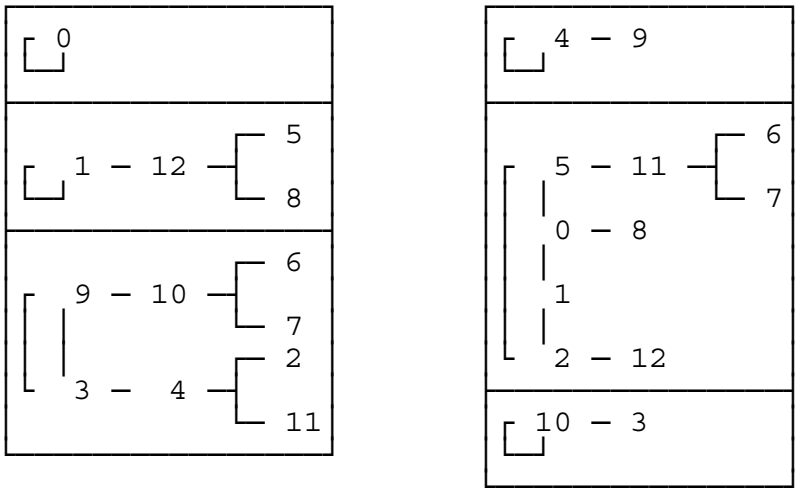

Figure 1. The function digraphs for x^2 and $x^2 + 1$ modulo 13.

In particular, basic results for general function digraphs are given in Section 2. There it is established that from the $p^2(p - 1)$ function digraphs there are at most p digraphs distinct up to isomorphism. In Section 3 we investigate what appear to be tight bounds on number of cycles of a given length. The occurrence of cycles containing exactly one and two elements is completely classified. In Section 4 we empirically compare these quadratic digraphs to "random" digraphs and this motivates our conjecture that there are exactly p distinct quadratic digraphs mod p except, remarkably, for $p = 17$. The quadratic function $x^2 - 2$ plays a special role in real dynamics [4] and in the theory of Mersenne primes [7, 9]. In Section 5 we investigate the corresponding family of function digraphs $\mathrm{fd}_p(x^2 - 2)$. The geometric form of these digraphs is very structured. We will see there are remarkable identities involving geometric position, addition and multiplication for these digraphs that lead to that rich structure.

2. BASIC RESULTS

We begin by discussing properties that are common to function digraphs on $\mathbf{Z}_m$, and then turn to our quadratic function digraphs.

Proposition 1: Let $\mathrm{u}:\mathbf{Z}_m \to \mathbf{Z}_m$ be a function.
(a) The out-degree of any vertex in $\mathrm{fd}_m(\mathrm{u}(x))$ is exactly one.
(b) The path in $\mathrm{fd}_m(\mathrm{u}(x))$ resulting from repeated iteration of any given element will eventually lead to a cycle.
(c) Every component of $\mathrm{fd}_m(\mathrm{u}(x))$ contains exactly one cycle.

Proof: (a) This follows from the fact that $\mathrm{u}(x)$ is a function.
(b) Since the function maps points in a finite set to a finite set, any path must eventually return to a previously visited vertex.
(c) If a component has more than one cycle, then somewhere on the undirected path connecting two cycles there would need to be a vertex with out-degree 2, contradicting (a). □

Theorem 2: The function digraphs $\mathrm{fd}_m(\mathrm{u}(x))$ and $\mathrm{fd}_m(\mathrm{v}(x))$ are isomorphic if and only if there exists a

permutation r such that $r^{-1} \circ u \circ r \equiv v \mod m$.

Proof: $(\Rightarrow)$ Let r denote an isomorphism between $fd_m(v(x))$ and $fd_m(u(x))$; r gives a bijection between the vertices. The isomorphism of edges implies that for all $x \in \mathbf{Z}_m$, the edge $(x,v(x))$ in $fd_m(v(x))$ is mapped by r to the edge $(r(x),u(r(x)))$ in $fd_m(u(x))$; hence, $u(r(x)) \equiv r(v(x)) \mod m$ which gives $r^{-1} \circ u \circ r \equiv v$.

$(\Leftarrow)$ Let r denote a permutation such that $r^{-1} \circ u \circ r \equiv v$. Now r gives a bijection between the vertices, hence we need to check this bijection respects the edges. Since $r^{-1} \circ u \circ r(x) \equiv v(x)$ for all $x \in \mathbf{Z}_m$, we have $u(r(x)) \equiv r(v(x))$ which is implies the edge $(x,v(x))$ in $fd_m(v(x))$ is mapped to the edge $(r(x),u(r(x)))$ in $fd_m(u(x))$ as required. □

Theorem 3: Let $m \geq 3$ be odd, and $\gcd(a_2, m) = 1$. The quadratic function digraph $fd_m(a_0 + a_1x + a_2x^2)$ is isomorphic to the function digraph of the canonical form quadratic $fd_m(x^2 + \gamma)$, where $\gamma = a_0a_2 + 2^{-1}a_1 - 2^{-2}a_1^2$.

Proof: First note that since m is odd, 2^{-1} exists and hence γ is well defined. Let $u(x)=a_0+a_1x+a_2x^2$, $v(x) = x^2 + \gamma$ and $r(x) = a_2^{-1}x - 2^{-1}a_1a_2^{-1}$. Note that a_2^{-1} is well defined since $\gamma(a_2, m) = 1$. By direct computation we can check $r^{-1} \circ u \circ r(x) \equiv v(x) \mod m$ as required. □

Corollary 4: Let $m \geq 3$ be odd. There are, up to isomorphism, at most m quadratic function digraphs modulo m with leading coefficient relatively prime to m.

Proof: By Theorem 3, every quadratic function digraph with $\gcd(a_2, m) = 1$ in $\mathbf{Z}_m$ is isomorphic to that of a quadratic in the canonical form $x^2 + \gamma$. Since there are m distinct quadratics in the canonical form, up to isomorphism, there are no more than m quadratic function digraphs mod m with leading coefficient relatively prime to m. □

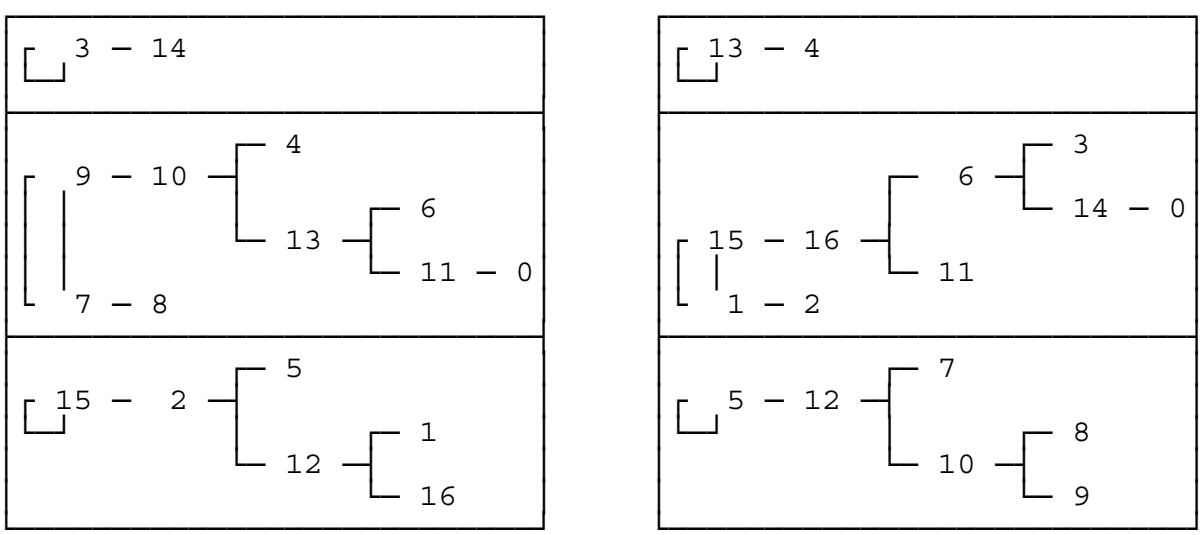

Figure 2. The function digraph $fd_{17}(x^2 + 11)$ is isomorphic to $fd_{17}(x^2 + 14)$.

The proviso on leading coefficients is necessary. For example, when $m = 4$ the eight polynomials x^2, $x^2 + 1$, $2x^2$, $2x^2 + x$, $2x^2 + 2x$, $2x^2 + 3x$, $2x^2 + x + 1$, $2x^2 + 3x + 1$ all have nonisomorphic function digraphs. Our interest lies primarily with odd prime moduli. Of course Theorem 3 and Corollary 4 hold for odd prime moduli, p. Hereafter in the paper we will let p denote an odd prime.

There is a situation when, up to isomorphism, there are fewer than p quadratic function digraphs mod p. Figure 2 shows two canonical form function digraphs that are isomorphic mod 17. However, we conjecture this is the only example where there are fewer than p quadratic function digraphs; this will be discussed further in Section 4 after we have established certain facts about arbitrary digraphs that satisfy the conclusion of the next theorem. This theorem is the first that requires the modulus to be an odd prime.

Theorem 5: Let $\mathrm{u}(x)$ be a quadratic function modulo p. In the function digraph $\mathrm{fd}_p(\mathrm{u}(x))$ there are exactly $(p-1)/2$ vertices of in-degree 0, one vertex of in-degree 1, and $(p-1)/2$ vertices of in-degree 2.

Proof: There are $(p-1)/2$ quadratic residues and nonresidues mod p. Note that we need only consider the digraphs of quadratics in canonical form. In order to determine the in-degree of a vertex y we need to know the number of solutions x to $y \equiv x^2 + \gamma$. Note that a vertex has in-degree 2 if and only if $y - \gamma$ is a quadratic residue, it has in-degree 0 if and only if $y - \gamma$ is a quadratic nonresidue, and it has in-degree 1 if and only if $y - \gamma \equiv 0$. Thus, there are exactly $(p-1)/2$ vertices of in-degree 0, 1 vertex of in-degree 1, and $(p-1)/2$ vertices of in-degree 2. □

3. CYCLES

Notice that each element in an n-cycle of $\mathrm{fd}_p(\mathrm{u}(x))$ must be a solution to the congruence $\mathrm{u}^n(x) \equiv x \mod p$, where $\mathrm{u}^n(x)$ denotes the composition of the function $\mathrm{u}(x)$ with itself n times. In contrast, we will use $\mathrm{u}(x)^n$ to denote the nth power of the function $\mathrm{u}(x)$. Since the congruence $\mathrm{u}^n(x) \equiv x$ has degree 2^n when $\mathrm{u}(x)$ is quadratic, it is a standard result that there can be at most 2^n solutions since the modulus is prime [11]. Thus, there are at most $2^n/n$ cycles of length n. It turns out that we can establish a better bound on the number of cycles of length n when $n = p^e$ as we will see in Corollary 8. A heuristic argument suggest this bound works for general n and empirical evidence indicates the bound is tight. In order to establish the bound we use the following lemma and theorem. We will then consider our heuristic and empirical evidence and finish this section by classifying the number of one and two cycles that appear.

Lemma 6: Let $\mathrm{v}(x) = x^2 + \gamma$, $\gamma \in \mathbf{R}$ and $\mathrm{P}_n(x) = \mathrm{v}^n(x) - x$. Then $\mathrm{P}_n(x)$ divides $\mathrm{P}_{kn}(x)$ as a polynomial in $\mathbf{R}[x]$. Moreover, the quotient is in $\mathbf{Z}[x]$ if $\gamma \in \mathbf{Z}$.

Proof: Since both $\mathrm{P}_n(x)$ and $\mathrm{P}_{kn}(x)$ are monic it suffices to show that every complex root of $\mathrm{P}_n(x)$ is also a root of $\mathrm{P}_{kn}(x)$ with at least as high a multiplicity. Note that if x_0 is a root of $\mathrm{P}_n(x)$ then $\mathrm{v}^n(x_0) = x_0$ and hence $\mathrm{v}^{kn}(x_0) = x_0$ which implies x_0 is a root of $\mathrm{P}_{kn}(x)$; this takes care of the single roots. Note x_0 is a root of $\mathrm{P}_n(x)$ of multiplicity m if and only if it is a root of $\mathrm{P}_n(x)$ and a root of the derivative of $\mathrm{P}_n(x)$ with multiplicity m-1. Using the chain rule repeatedly and the fact that

$\mathrm{v}'(x) = 2x$ we see that

$$\mathrm{P}'_n(x) = 2^n \mathrm{v}^{n-1}(x)\mathrm{v}^{n-2}(x)\ldots\mathrm{v}(x)x - 1$$

and hence

$$\mathrm{P}'_{kn}(x) = 2^{kn}\mathrm{v}^{kn-1}(x)\mathrm{v}^{kn-2}(x)\ldots\mathrm{v}(x)x - 1.$$

Now we want to consider the derivative $\mathrm{P}'_{kn}(x)$ modulo $\mathrm{P}_n(x)$. Note that by definition $\mathrm{v}^n(x) \equiv x \bmod \mathrm{P}_n(x)$ and hence $\mathrm{v}^{jn+i}(x) \equiv \mathrm{v}^i(x) \bmod \mathrm{P}_n(x)$ so that

$$\mathrm{P}'_{kn}(x) \equiv (2^n \mathrm{v}^{n-1}(x)\mathrm{v}^{n-2}(x)\ldots\mathrm{v}(x)x)^k - 1 \mod \mathrm{P}_n(x).$$

If we let $\mathrm{w}(x) = 2^n \mathrm{v}^{n-1}(x)\mathrm{v}^{n-2}(x)\ldots\mathrm{v}(x)x$ then $\mathrm{P}'_n(x) = \mathrm{w}(x) - 1$ and

$\mathrm{P}'_{kn}(x) \equiv \mathrm{w}(x)^k - 1 = (w(x)-1)\left(w(x)^{k-1} + w(x)^{k-2} + \ldots + w(x) + 1\right) = \mathrm{P}'_n(x)\left(w(x)^{k-1} + \ldots + 1\right) \bmod \mathrm{P}_n(x).$

Now suppose x_0 is a root of $\mathrm{P}_n(x)$ of multiplicity *m* and hence is also a root of $\mathrm{P}'_n(x)$ of multiplicity *m*-1. By the above, it is also a root of $\mathrm{P}'_{kn}(x)$ of multiplicity *m*-1 and hence is a root of $\mathrm{P}_{kn}(x)$ of multiplicity *m*. Thus $\mathrm{P}_n(x)$ divides $\mathrm{P}_{kn}(x)$.

In order to see that the quotient is in $\mathbf{Z}[x]$ if $\gamma \in \mathbf{Z}$, consider the following. Since $\mathrm{P}_n(x) \in \mathbf{Z}[x]$ is monic of degree 2^n we can write $\mathrm{P}_n(x) = b_0 + b_1 x + \ldots + b_{2^n-1}x^{2^n-1} + x^{2^n}$ where $b_i \in \mathbf{Z}$. Since $\mathrm{P}_{kn}(x) \in \mathbf{Z}[x]$ is also monic, we can also write the quotient in the form $\mathrm{f}(x) = a_0 + a_1 x + \ldots + a_{K-1}x^{K-1} + x^K$ where $K = 2^{kn} - 2^n$ is the degree of the quotient. Suppose $\mathrm{f}(x) \notin \mathbf{Z}[x]$. Let *m* be the largest integer such that $a_m \notin \mathbf{Z}$. Now the coefficient of x^{2^n+m} in the product $\mathrm{P}_{kn}(x) = \mathrm{P}_n(x)\,\mathrm{f}(x)$ is a finite sum of the form $a_m + a_{m+1}b_{2^n-1} + a_{m+2}b_{2^n-2} + \ldots$. This coefficient is an integer since $\mathrm{P}_{kn}(x) \in \mathbf{Z}[x]$ and each factor in the second and higher terms of the finite sum are integers; thus a_m is also an integer which contradicts $a_m \notin \mathbf{Z}$ and proves the claim. □

The elements $x_0 \in \mathbf{R}$ such that $\mathrm{v}^n(x_0) = x_0$ are said to be cyclic of period *n*. Any root of $\mathrm{P}_n(x)$ is a cycle element of period *n*. Any root of $\mathrm{P}_n(x)$ which is of period *n* and not of any shorter period is said to be of *prime period n*. Any complex root with non-prime period *n* will be a root of some $\mathrm{P}_d(x)$ where *d* divides *n* though it is possible that $\mathrm{P}_n(x)$ does not have roots of prime period *n*. For example, when $\gamma = -3/4$, then $\mathrm{P}_1(x) = (x+1/2)(x-3/2)$ and $\mathrm{P}_2(x) = (x+1/2)^3(x-3/2)$ which has no new roots; hence there are no points of prime period 2 for this γ.

The following theorem and conjecture involve a factorization similar to the classical factorization of $x^n - 1$ in terms of cyclotomic polynomials [10], yet it is quite different in that $\mathrm{P}_n(x) = \mathrm{v}^n(x) - x$ involves function iteration, not ordinary powers.

Theorem 7: Let $\mathrm{P}_n(x) = \mathrm{v}^n(x) - x$ be as above and let $n = q^k$ be a power of a prime. Also let $\mathrm{Q}_1(x) = \mathrm{P}_1(x)$ and $\mathrm{Q}_n(x) = \dfrac{\mathrm{P}_n(x)}{\prod_{d|n, d<n} \mathrm{Q}_d(x)}$ 5, then $\mathrm{Q}_n(x)$ is a polynomial in $\mathbf{R}[x]$ for $\gamma \in \mathbf{R}$ and it is in $\mathbf{Z}[x]$ for $\gamma \in \mathbf{Z}$.

Proof: Since $n = q^k$ is a power of a prime this is easy to check that

$$\mathrm{Q}_n(x) = \mathrm{Q}_{q^k}(x) = \frac{\mathrm{P}_{q^k}(x)}{\mathrm{Q}_{q^{k-1}}(x)\mathrm{Q}_{q^{k-2}}(x)\ldots\mathrm{Q}_q(x)\mathrm{Q}_1(x)} = \frac{\mathrm{P}_{q^k}(x)}{\mathrm{P}_{q^{k-1}}(x)}$$

which is a polynomial by Lemma 6. The remark about the quotient being in in $\mathbf{Z}[x]$ for $\gamma \in \mathbf{Z}$ follows as in the previous Lemma. □

We conjecture that this property holds for general n.

Conjecture A: Let $\mathrm{P}_n(x) = \mathrm{v}^n(x) - x$ be as above and let $\mathrm{Q}_1(x) = \mathrm{P}_1(x)$ and $\mathrm{Q}_n(x) = \dfrac{\mathrm{P}_n(x)}{\prod_{d|n, d<n} \mathrm{Q}_d(x)}$, then $\mathrm{Q}_n(x)$ is a polynomial in $\mathbf{R}[x]$ for $\gamma \in \mathbf{R}$ and it is in $\mathbf{Z}[x]$ for $\gamma \in \mathbf{Z}$.

Consider the following heuristic argument in favor of the conjecture. Solving for $\mathrm{P}_n(x)$, we see that $\mathrm{P}_n(x) = \prod_{d|n} \mathrm{Q}_d(x)$. We can obtain a sum over the divisors of n by taking logarithms and then we can apply the Möbius Inversion formula. On rewriting the result as a product, we see that $\mathrm{Q}_n(x) = \prod_{d|n} \mathrm{P}_d(x)^{\mu(n/d)}$ where $\mu(n)$ is the Möbius function. In the case when $n = q_1^{k_1} q_2^{k_2}$ is the product of powers of two primes, this amounts to $\mathrm{Q}_n(x) = \mathrm{Q}_{q_1^{k_1} q_2^{k_2}}(x) = \dfrac{\mathrm{P}_n(x)\,\mathrm{P}_{\frac{n}{q_1 q_2}}(x)}{\mathrm{P}_{\frac{n}{q_1}}(x)\,\mathrm{P}_{\frac{n}{q_2}}(x)}$. Now if $\mathrm{P}_{\frac{n}{q_1}}(x)$ and $\mathrm{P}_{\frac{n}{q_2}}(x)$ have no roots in common, then all their roots with all their multiplicity are also roots of $\mathrm{P}_n(x)$, and hence $\mathrm{Q}_n(x)$ is a polynomial. If they have a common root x_0 and it is a single root of at least one factor of the denominator, then the factor with the higher multiplicity divides $\mathrm{P}_n(x)$ by Lemma 6. Since x_0 is a root of $\mathrm{P}_{\frac{n}{q_1}}(x)$ and $\mathrm{P}_{\frac{n}{q_2}}(x)$ then it has period $\dfrac{n}{q_1}$ and also has period $\dfrac{n}{q_2}$; hence it has period $\gcd\left(\dfrac{n}{q_1}, \dfrac{n}{q_1}\right) = \dfrac{n}{q_1 q_2}$. That is, it is a root of $\mathrm{P}_{\frac{n}{q_1 q_2}}(x)$. Thus, the factors arising from the root x_0 will cancel except possibly some factors in the numerator. So long as common roots of factors appearing in the denominator do not have common multiplicity over 1, this argument would generalize to any number of prime factors. We expect that for a generic choice of γ, the roots of $\mathrm{P}_n(x)$ would all be single roots. Thus common multiplicity would be one and hence the above argument would work. However, once the result is true for some generic γ, it should be true for the formal parameter γ as well.

We can formally compute $\mathrm{Q}_n(x)$ for small n. Notice that these are polynomials in x and γ.

$\mathrm{Q}_1(x) = x^2 - x + \gamma,$

$\mathrm{Q}_2(x) = x^2 + x + \gamma + 1,$

$\mathrm{Q}_3(x) = x^6 + x^5 + (1+3\gamma)\,x^4 + (1+2\gamma)\,x^3 + (1+3\gamma+3\gamma^2)\,x^2 + (1+\gamma)^2\,x + \gamma^3 + 2\gamma^2 + \gamma + 1,$

$\mathrm{Q}_4(x) = x^{12} + 6\gamma\,x^{10} + x^9 + (15\gamma^2 + 3\gamma)\,x^8 + \ldots + (2\gamma + \gamma^2 + 2\gamma^3 + \gamma^4)x + (1 + 2\gamma^2 + 3\gamma^3 + 3\gamma^4 + 3\gamma^5 + \gamma^6).$

Using symbolic manipulation software we have verified that $\mathrm{Q}_6(x)$ is a formal polynomial in x and □

Corollary 8: Let u(x) be a quadratic function and let $n = q^k$ be a power of a prime. In $\mathrm{fd}_p(\mathrm{u}(x))$ the number of cycles of length n is less than or equal to $\dfrac{1}{n}\deg(\mathrm{Q}_n(x)) = \dfrac{1}{n}\left(2^n - \sum_{d|n, d<n} \deg(\mathrm{Q}_d(x))\right)$.

Proof: The number of elements with prime period n is less than or equal to the degree of $\mathrm{Q}_n(x)$ which can be computed recursively from its definition given in Theorem 7. □

cycle length	bound on repetitions	odd prime p
1	2	3
2	1	7
3	2	29
4	3	31
5	6	311
6	9	127
7	18	509
8	30	1,021
9	56	3,067
10	99	4,093
11	186	36,847
12	335	8,191

Table 1. Minimal odd prime p such that the function digraph $\mathrm{fd}_p(x^2)$ achieves the maximal repetition of cycle lengths.

Of course, if Conjecture A is true we would have also established Corollary 8 for general n. Hence we have the following conjecture.

Conjecture B: Let $\mathrm{u}(x)$ be a quadratic function and let n be a positive integer. In $\mathrm{fd}_p(\mathrm{u}(x))$ the number of cycles of length n is less than or equal to $\frac{1}{n}\deg(Q_n(x)) = \frac{1}{n}\left(2^n - \sum_{d|n, d<n} \deg(Q_d(x))\right)$.

Note that the bounds given in the corollary and conjecture may be ugly in the sense that they are recursively defined, but they are easy to compute. Table 1 gives some examples illustrating primes where these bounds are achieved. Notice the bounds seem to be tight even though they get large. It seems remarkable that the theoretic bound on 11-cycles is 186 occurrences and this happens for a relatively small prime. The fact that these bounds are indeed the maximal number of occurrences we found for some additional cases where n is not a prime power provides additional evidence for the correctness of Conjecture A and Conjecture B. It is also interesting to compare these bounds which are computed algebraically here with the number of orbits of prime period arising from the genealogy of periodic points in classical real dynamics [3]. The next theorems allow us to determine when there are 1-cycles and 2-cycles.

Theorem 9: The number of 1-cycles in $fd_p(x^2 + \gamma)$ is $1+\left(\frac{2^{-2}-\gamma}{p}\right)$.

Proof: Recall that since p is an odd prime, 2^{-1} exists modulo p. By completing the square of $Q_1(x) = x^2 - x + \gamma \equiv 0$, we have $(x - 2^{-1})^2 \equiv 2^{-2} - \gamma$. Thus $fd_p(x^2 + \gamma)$ has two, one or zero 1-cycles if and only if $2^{-2} - \gamma$ is a quadratic residue, 0 or a nonresidue respectively. □

Theorem 10: There is exactly one 2-cycle in $fd_p(x^2 + \gamma)$ iff $\left(\frac{2^{-2}-\gamma-1}{p}\right) = 1$.

Proof: Notice that if $Q_2(x)$ has a repeated root mod p, the root is a 1-cycle; moreover, if $Q_1(x)$ and $Q_2(x)$ have a shared root, then $Q_2(x)-Q_1(x) = 2x + 1 \equiv 0$ from which we see $x \equiv -2^{-1}$ is the only possible shared root. In such a case the other root of $Q_2(x)$ must be a 1-cycle, hence both roots must be -2^{-1}. Thus, the function digraph $fd_p(x^2 + \gamma)$ has exactly one 2-cycle if and only if $Q_2(x) = x^2 + x + \gamma + 1 \equiv 0$ has two distinct solutions in $\mathbf{Z}_p$. Completing the square in that congruence yields $(x + 2^{-1})^2 \equiv 2^{-2} - \gamma - 1$ which has two distinct solutions in $\mathbf{Z}_p$ if and only if $2^{-2} - \gamma - 1$ is a quadratic residue mod p. □

4. RANDOM QUASIQUADRATIC DIGRAPHS

We have seen that it is difficult to predict the structure of $fd_p(u(x))$ for quadratic functions $u(x)$, yet we have been able to give some restrictions on the behavior of these function digraphs. In this section we will compare the structure of the quadratic function digraphs $fd_p(u(x))$ with those of "random" functions whose function digraphs have the same number of vertices with in-degree 0, 1 and 2 as have the quadratic function digraphs. In particular, we will call a function $q:\mathbf{Z}_p \to \mathbf{Z}_p$ *quasiquadratic* if it is 2-to-1 for all of its domain except that it is 1-to-1 for one element of its domain. For example, Figure 3 shows a randomly chosen quasiquadratic function digraph on $\mathbf{Z}_{17}$. Notice it has the same random appearance of the quadratic function digraphs modulo 17 but it has two 2-cycles, which is impossible for a quadratic function digraph by Corollary 8.

We begin our investigation by counting the number of quasiquadratic functions.

Theorem 11: Given a prime modulus $p \geq 3$,

(a) the number of quasiquadratic functions is $\frac{p+1}{2}\binom{p}{\frac{p+1}{2}}\binom{p}{2\ 2 \ldots 2\ 2\ 1}$ and

(b) the number of quasiquadratic digraphs that are nonisomorphic is $\binom{p}{\frac{p+1}{2}}$.

Proof: (a) There are $\binom{p}{\frac{p+1}{2}}$ ways to choose the $\frac{p+1}{2}$ range elements of the quasiquadratic functions and there are $\frac{p+1}{2}\binom{p}{2\ 2 \ldots 2\ 2\ 1}$ permutations that would result in distinct rearrangements since the multinomial $\binom{p}{2\ 2 \ldots 2\ 2\ 1}$ gives the number of ways to partition p elements into classes of size 2,2,...2,1 and there are $\frac{p+1}{2}$ ways to position the 1.

(b) An isomorphism between quasiquadratic digraphs must map each pair of the range of the first digraph to a pair in the range of the second digraph; the isomorphism must also map the singleton of the range of the first digraph to the singleton in the range of the second digraph. Since there are $\binom{p}{2\ 2 \ldots 2\ 2\ 1}$

0 -> 7	1 — 10
1 -> 1	
2 -> 6	6 — 2
3 -> 15	4 — 15 — 3
4 -> 6	9 — 11 — 8
5 -> 13	14
6 -> 4	13 — 5
7 -> 12	16
8 -> 11	12
9 -> 15	7 — 0
10 -> 1	
11 -> 9	
12 -> 7	
13 -> 9	
14 -> 11	
15 -> 4	
16 -> 13	

Figure 3. A random quasiquadratic function and its digraph which contains two 2-cycles.

ways to pick the pairs and singleton and $\frac{p+1}{2}$ ways to place the singleton, there are $\frac{p+1}{2}\binom{p}{2\ 2 \ldots 2\ 2\ 1}$ such permutations. Dividing this into the total number of quasiquadratic digraphs we see the number of quasiquadratic digraphs that are nonisomorphic is $\binom{p}{\frac{p+1}{2}}$.

Notice that we really only used the fact that the modulus is odd, not that it is prime. □

We can easily generate random quasiquadratic digraphs and compare their structure with the structure of quadratic digraphs. Figure 4 shows the frequency that cycles of specified length appear in 10,000 random choices of quasiquadratic digraphs modulo 1009. These quasiquadratic frequencies are shown with the connected lines. The isolated points show the same information for the 1009 quadratic function digraphs. Likewise, Figure 5 shows the average frequency that specified numbers of components occur for quasiquadratic and quadratic function digraphs modulo 1009. While the fits are

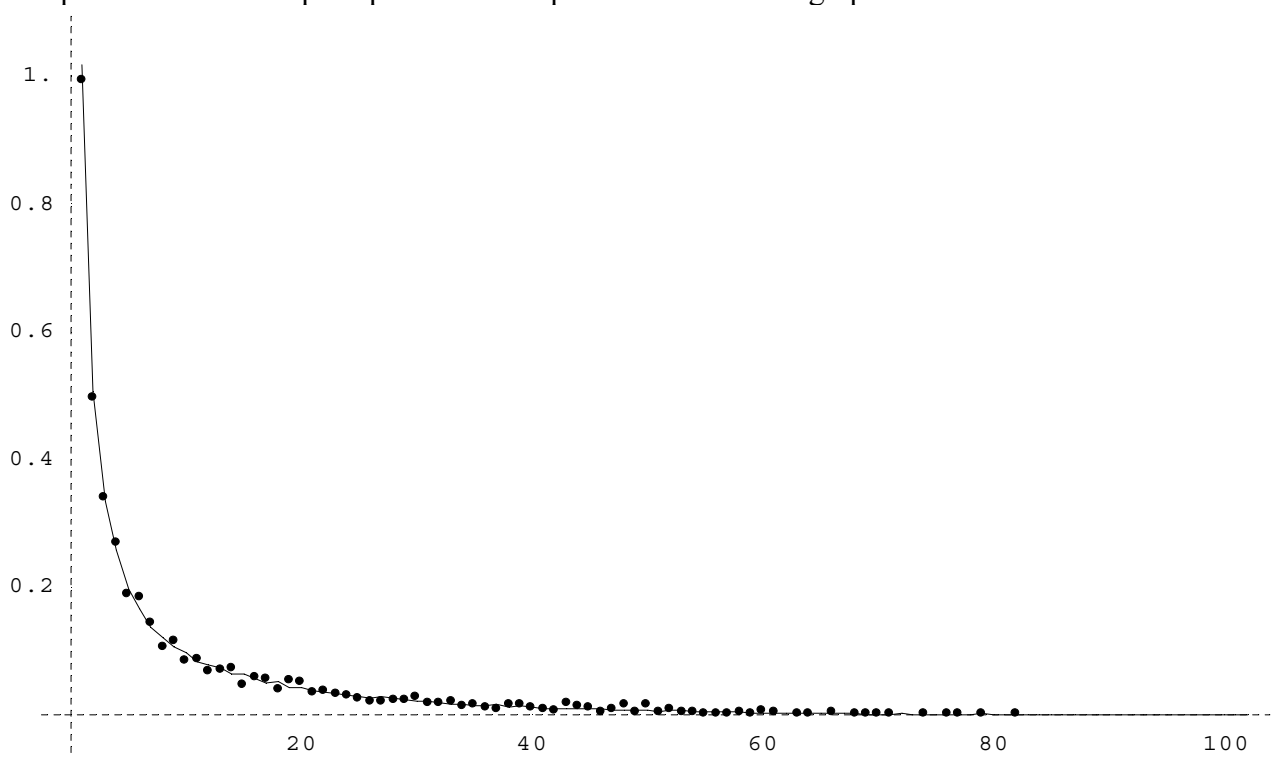

Figure 4. The average frequency of cycle lengths for quadratic and quasiquadratic digraphs modulo 1009

not perfect, they are remarkably good and this provides empirical support for the heuristic view that the quadratic function digraphs are nearly "random".

In Section 2 we noted an example of quadratic function digraphs in canonical form that are isomorphic: $fd_{17}(x^2 + 11) \square fd_{17}(x^2 + 14)$. If we assume that the p quadratic function digraphs are randomly distributed over the quasiquadratic function digraphs, then we can estimate the expected number of pairs of quadratic function digraphs that will be isomorphic by multiplying the number of pairs $\binom{p}{2}$ by the reciprocal of the number of distinct quasiquadratic functions digraphs. Table 2 shows the

expected number of isomorphic pairs implied by that estimate. One might choose to use $\binom{p-2}{2}$ instead of $\binom{p}{2}$ since $fd_p(x^2)$ and $fd_p(x^2 - 2)$ are special; see [8] and Section 5 respectively, for how those digraphs are special. Using $\binom{p-2}{2}$ would reduce the expected numbers, especially for small p. However, the main point is that these expected numbers approach 0 very quickly since the number of pairs is quadratic but the number of quasiquadratic functions is exponential in p. Hence we make the following conjecture.

Conjecture C: Quadratic Digraph Isomorphism Conjecture. The only occurrence of isomorphic quadratic function digraphs in canonical form is $fd_{17}(x^2 + 11) \cong fd_{17}(x^2 + 14)$.

In addition to the heuristic argument in favor of this conjecture given above, we have computationally verified the conjecture for all primes up to 1009.

p	Expected isomorphisms
3	1.0
5	1.0
7	0.6
11	0.119
13	0.0455
17	0.00559
19	0.00185
23	0.000187
29	0.00000523
31	0.00000154

Table 2. The expected number of isomorphic quadratic function digraphs for small odd primes.

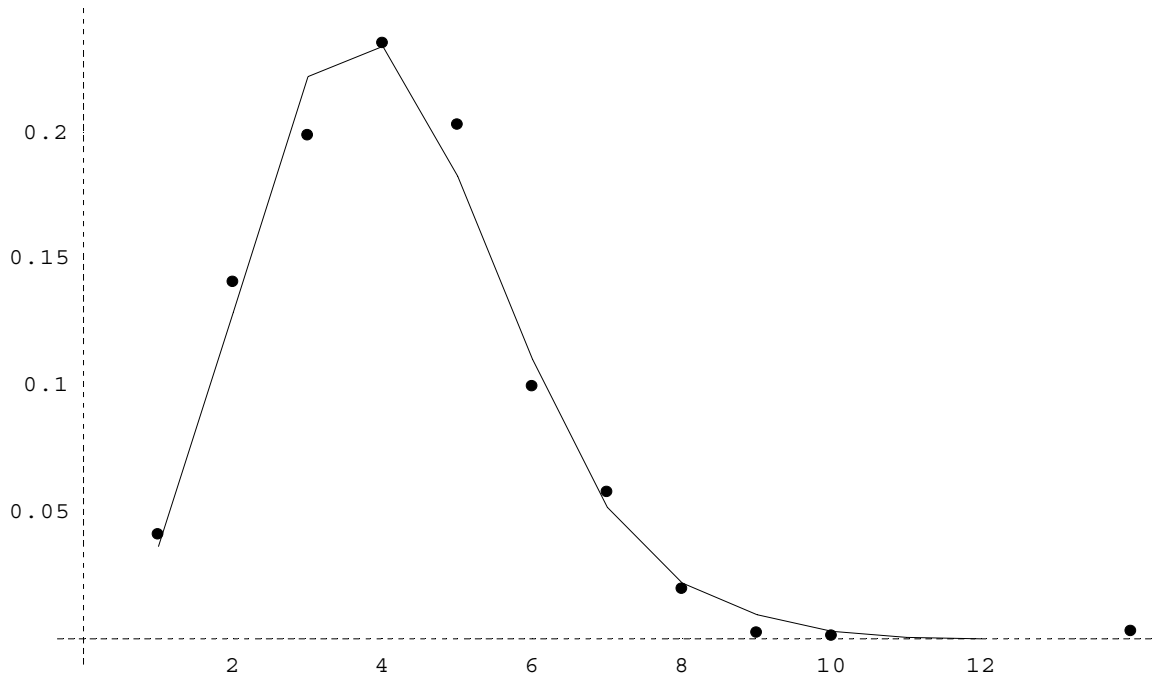

Figure 5. The average number of components for quadratic and quasiquadratic digraphs modulo 1009

5. FUNCTION DIGRAPHS $\mathbf{fd}_p(x^2 - 2)$

In classical dynamics the dynamics of the function $x^2 - 2$ are special [4] because the Julia set is unusually simple. A similar statement can be made in the theory of numbers where iteration of this function plays a role in whether Mersenne numbers $p = 2^{q-1} - 1$ are prime [7, 9]. We investigate the family of function digraphs $\mathrm{fd}_p(x^2 - 2)$ for general odd prime modulus which has far more structure than typical quadratic function digraphs. This structure seems to be as deep as, but more complicated than the structure of $\mathrm{fd}_p(x^2)$. Indeed, we will see that the identities we use involve both multiplication and addition. Figure 6 shows $\mathrm{fd}_{239}(x^2 - 2)$. This example is rather large but serves to illustrate all the properties that we want to observe without requiring several examples. We see that all the cycle elements have one leaf or a binary tree attached. The non-leaf trees all have the same depth and are isomorphic except for one vertex of in-degree one. Our goal in this section is to show that those claims are true in general. Also notice that the cycle lengths seem to have some coherence. Readers who would like to see examples of the remarkable arithmetic/structure identities before considering the general theory may preview the examples that follow Theorem 19.

In this section we will let $s(x) = x^2 - 2$. The *level* of a vertex x measured from its cycle is given by the smallest k such that $s^k(x)$ is a cycle element. Thus, cycle elements are at level 0. Components with at least one vertex at level 2 are called *branched components*. Other components are called *stumpy components*. We say that two distinct vertices M and N are *k-ancestors* if k is the smallest positive integer such that $s^k(M) = s^k(N)$. For example, M and N are 1-ancestors if and only if $M = -N$ and they are 2-ancestors if and only if $s(M) = -s(N)$; namely, $M^2 - 2 = 2 - N^2$.

Our first lemma in this section shows that multiplying two 2-ancestors gives a nearby vertex. We think of this theorem as giving enough structure to the digraphs so that we can establish a base case for our eventual induction. It also establishes enough structure so that in the subsequent lemma we can

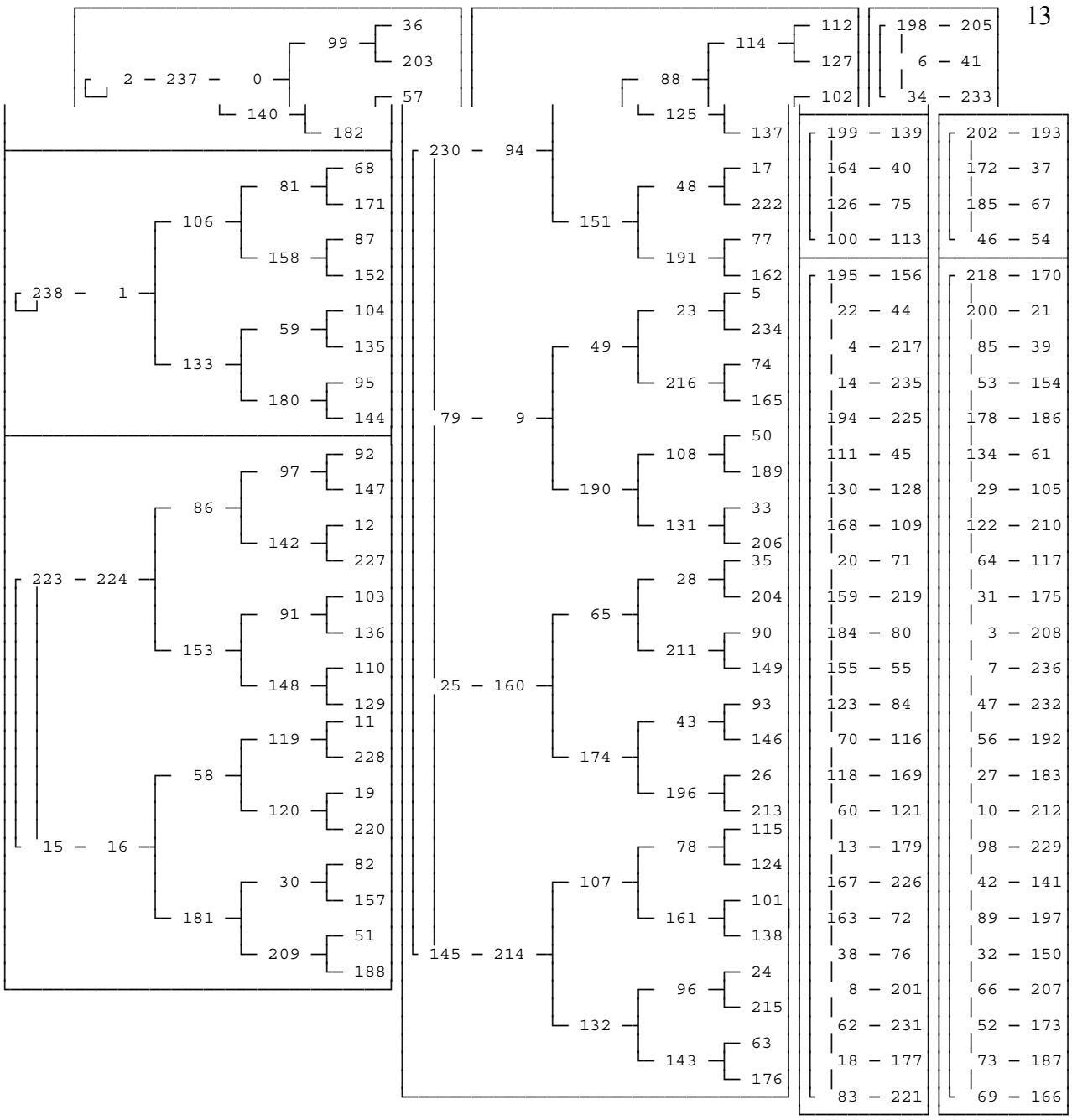

Figure 6. The function digraph $fd_{239}(x^2 - 2)$.

discuss leaves, cycles and distinguish two fundamentally different types of digraph components: those that reach level two and those that do not.

Lemma 12: If M and N are 2-ancestors in $fd_p(s(x))$ then MN and $s(M)$ are 2-ancestors and MN and $s(N)$ are 2-ancestors as well.

Proof: Since M and N are 2-ancestors, $s(M) = - s(N)$ so $M^2 - 2 = 2 - N^2$ and hence $N^2 = 4 - M^2$. Now $s^2(M) = M^4 - 4M^2 + 2 = 2 - M^2(4 - M^2) = 2 - (MN)^2 = - s(MN)$. Thus, MN and $s(M)$ are 2-

ancestors and by symmetry so are MN and s(N). □

As an aside, we notice that if we try to generalize this to $\mathrm{v}(x) = x^2 + \gamma$, we see that M and N are 2-ancestors means $M^2 + \gamma = -\gamma - N^2$ and hence $-2\gamma = N^2 + M^2$. Thus,

$$\mathrm{v}^2(M) = M^4 + 2\gamma M^2 + \gamma^2 + \gamma = M^4 + (-N^2 - M^2) M^2 + \gamma^2 + \gamma = -\mathrm{v}(MN) + \gamma^2 + 2\gamma$$

and hence $\mathrm{v}^2(M) = -\mathrm{v}(MN)$ if an only if $\gamma^2 + 2\gamma = 0$. This gives the special cases $\gamma = 0, -2$ mentioned in Section 4.

We will refer to Figure 6 to provide an illustration of Lemma 12 in $\mathrm{fd}_{239}(\mathrm{s}(x))$. Notice that M=230 and N=65 are 2-ancestors appearing in the component of $\mathrm{fd}_{239}(\mathrm{s}(x))$ that has a 4-cycle. We see that s(M)=s(230)=79 while $MN = 230 * 65 \equiv 132 \mod 239$. We can observe that 79 and 132 are also 2-ancestors.

If x is a noncycle element we define the *tree leading to x* to be the union of all paths leading to x. More precisely, the tree leading to x is $\left\{ y \in \mathbf{Z}_p \,|\, s^k(y) = x \text{ for some } k \geq 0 \right\}$. Notice that for each p, the function digraph $\mathrm{fd}_p(\mathrm{s}(x))$ contains a component where 0 maps to -2 which maps to 2 and where 2 maps back onto itself. The vertex $x = -2$ is the single vertex of in-degree 1 and it is at level one. Therefore, all cycle elements have in-degree 2. Thus, each cycle element has a unique noncycle parent. If c is a cycle element we define the *tree associated with c* to be the tree leading to the noncycle parent of c. In particular, x is an element of the tree leading to x but c is not an element of the tree associated with c.

A vertex $x \neq -2$ has parents if and only if there are two solutions y to $y^2 - 2 = x$ and this occurs exactly when the Legendre symbol $\left(\frac{2+x}{p}\right) = 1$. In particular, the tree leading to 0 contains more than the vertex 0 if and only if $p = 1, 7 \mod 8$ since those are the cases when 2 is a quadratic residue. We call this component the 0-component. Eventually we will see the existence and depth of the tree leading to 0 influences the structure of the branched components.

We say a tree is a *complete binary tree up to level k* if the tree has a root and each vertex at level less than k from the root has exactly two parents.

The next lemma describes the structure of the components up to level 2 which gives a starting point for our structure theorem.

Lemma 13: In $\mathrm{fd}_p(\mathrm{s}(x))$,
(a) The tree associated with a cycle element in a stumpy component consists of one leaf at level one.
(b) The tree associated with a cycle element in a branched component, except the vertex 2, is a tree structure that is a complete binary tree up to level 2.

Proof: Recall that -2 is the only vertex of in-degree one and it is not a cycle element. Thus, every cycle element has in-degree 2.

(a) By definition, stumpy components cannot have any elements at level 2 or higher and we have noted every cycle element in a stumpy component will have in-degree 2; this gives the result.

(b) We know that each cycle element has a single noncycle parent. By definition, in every branched component there is some vertex M at level 2. Let N be the cycle element such that M and N are 2-ancestors. Lemma 12 implies that MN is at level 2 leading to the cycle element after $\mathrm{s}^2(M)$. Repeating the process on MN and proceeding around the entire cycle implies there is a vertex at level 2 in the tree associated with every cycle element. Since the in-degree of all the level 1 vertices must be 2, except for at -2 in the 0-component, we see the trees associated with such a cycle element from a

branched component must be a complete binary tree up to level 2. □

We now show that in the branched components any vertex has parents if and only if its additive inverse has parents. We already noted that ±2 both have parents.

Lemma 14: If x is a vertex other than ±2 in a branched component then x has parents if and only if $-x$ has parents. That is, $\left(\frac{2+x}{p}\right) = \left(\frac{2-x}{p}\right)$.

Proof: We have seen this is true for levels 0 and 1 since all such vertices have parents (Lemma 13 b) and it is trivially true for x=0. Suppose this lemma is not true in general. Suppose x is a vertex at the lowest level such that $\left(\frac{2+x}{p}\right) \neq \left(\frac{2-x}{p}\right)$. Now $\left(\frac{2+x}{p}\right)\left(\frac{2-x}{p}\right) = \left(\frac{4-x^2}{p}\right) = \left(\frac{2-s(x)}{p}\right)$. Since s($x$) is at a lower level, the result is true for s(x) hence $\left(\frac{2-s(x)}{p}\right) = \left(\frac{2+s(x)}{p}\right) = \left(\frac{x^2}{p}\right) = 1$ so $\left(\frac{2+x}{p}\right) = \left(\frac{2-x}{p}\right)$ 9 which contradicts the supposition and completes the proof. □

Note that if any vertex x appears at level 3 or higher then s(x) and -s(x) will both have parents and hence we get at least 4 vertices at the level of x.

We already know that 2 is a 1-cycle element and -2 is a nonleaf leading to that cycle. Thus ±2 are nonleaves in a branched component. The next theorem shows that we can use the two Legendre symbols from Lemma 14 to classify all the other vertices into four geometric classes.

Theorem 15: Suppose x is a vertex other than ±2 in $fd_p(s(x))$.

(a) If $\left(\frac{2+x}{p}\right) = 1$ and $\left(\frac{2-x}{p}\right) = 1$ then x is a nonleaf in a branched component.

(b) If $\left(\frac{2+x}{p}\right) = 1$ and $\left(\frac{2-x}{p}\right) = -1$ then x is a cycle element in a stumpy component.

(c) If $\left(\frac{2+x}{p}\right) = -1$ and $\left(\frac{2-x}{p}\right) = 1$ then x is a leaf in a stumpy component.

(d) If $\left(\frac{2+x}{p}\right) = -1$ and $\left(\frac{2-x}{p}\right) = -1$ then x is a leaf in a branched component.

Proof: Lemma 14 showed that the vertices in the branched components have equal Legendre symbols. We saw that for $x \neq -2$, $\left(\frac{2+x}{p}\right) = 1$ if and only if x has parents; hence $\left(\frac{2+x}{p}\right) = -1$ if and only if x is a leaf. Checking the Legendre symbol values for the leaf and nonleaf positions gives the results. □

In order to count the actual number of vertices in each of the geometric classes, we use the following results on sums of the Jacobi symbol on quadratic forms.

Lemma 16:

(a) Let $p > 2$ and $a^2 - 4b \neq 0 \bmod p$, then $\sum_{x=1}^{p}\left(\frac{x^2+ax+b}{p}\right) = -1$.

(b) Let $p > 2$, then $\sum_{x=1}^{p}\left(\frac{4-x^2}{p}\right) = -1\left(\frac{-1}{p}\right)$.

Proof: Part (a) is Theorem 8.2 in Hua [6] and (b) is $\left(\frac{-1}{p}\right)$ times a special case. □

Theorem 17: In the function digraph $\mathrm{fd}_p(\mathrm{s}(x))$

(a) the total number of nonleaf vertices in the branched components is $1+\frac{1}{4}\left(p-\left(\frac{-1}{p}\right)\right)$

(b) the total number of cycle vertices in the stumpy components is $\frac{1}{4}\left(p-2+\left(\frac{-1}{p}\right)\right)$

(c) the total number of leaf vertices in the stumpy components is $\frac{1}{4}\left(p-2+\left(\frac{-1}{p}\right)\right)$

(d) the total number of leaf vertices in the branched components is $\frac{1}{4}\left(p-\left(\frac{-1}{p}\right)\right)$

Proof: First consider (d). The total number of leaf vertices in the branched components is $\frac{1}{4}\sum_{x=1}^{p}\left(1-\left(\frac{2+x}{p}\right)\right)\left(1-\left(\frac{2-x}{p}\right)\right)$ where we take care to notice that the terms are zero for $x = \pm 2$ and those vertices are not leaves. Expanding, we see $\frac{1}{4}\sum_{x=1}^{p}\left(1-\left(\frac{2+x}{p}\right)-\left(\frac{2-x}{p}\right)+\left(\frac{4-x^2}{p}\right)\right) =$ $\frac{1}{4}\left(p-\left(\frac{-1}{p}\right)\right)$ where we use Theorem 16(b) and the fact that $\sum_{x=1}^{p}\left(\frac{x}{p}\right) = 0$. Next consider (a). The total number of nonleaf vertices in the branched components is $1+\frac{1}{4}\sum_{x=1}^{p}\left(1+\left(\frac{2+x}{p}\right)\right)\left(1+\left(\frac{2-x}{p}\right)\right)$ where we take care to notice that the terms of the sum are 2 for $x = \pm 2$ and those vertices are not leaves hence we need to add 1 to get the correct count. Expanding as above gives the desired result. We can handle (b) and (c) in a similar way or note that we already know from Lemma 13(a) that these numbers must be equal and hence are half of the vertices not accounted for in (a) and (d). □

For example, consider $p = 239$. Since $\left(\frac{-1}{239}\right) = -1$ we see that by Theorem 17 (d) that the number of leaves in the branched components is $\frac{1}{4}(239 - -1) = 60$.

The next lemma gives a technical identity that provides the key inductive step in the theorem that follows the lemma. Informally speaking, it shows that we can follow a chain of sums of paths multiplied by inverses of elements in the tree leading to 0 to get a path in the "next" tree of the appropriate size.

Lemma 18: Suppose r, $\mathrm{s}(r)$ and $\mathrm{s}^2(r)$ are nonzero elements in $\mathrm{fd}_p(\mathrm{s}(x))$. If $\frac{1}{\mathrm{s}(r)}\big(\mathrm{s}(M)+\mathrm{s}(N)\big)$ is a parent of $\frac{1}{\mathrm{s}^2(r)}\big(\mathrm{s}^2(M)+\mathrm{s}^2(N)\big)$ then either $\frac{1}{r}(M+N)$ or $\frac{1}{r}(M-N)$ is a parent of $\frac{1}{\mathrm{s}(r)}\big(\mathrm{s}(M)+\mathrm{s}(N)\big)$ 10.

Proof: Notice that a vertex x is a parent of y if and only if $\mathrm{s}(x) - y$ is zero. Direct computation verifies that

$$r^4\left(\mathrm{s}\left(\frac{1}{r}(M+N)\right) - \frac{1}{\mathrm{s}(r)}\big(\mathrm{s}(M)+\mathrm{s}(N)\big)\right)\left(\mathrm{s}\left(\frac{1}{r}(M-N)\right) - \frac{1}{\mathrm{s}(r)}\big(\mathrm{s}(M)+\mathrm{s}(N)\big)\right)$$

is

$$\frac{4\big(M^2+2MN+N^2-4r^2-MNr^2+r^4\big)\big(M^2-2MN+N^2-4r^2+MNr^2+r^4\big)}{\mathrm{s}(r)^2}$$

which identical to

$$-2\,\mathrm{s}^2(r)\left(\mathrm{s}\left(\frac{1}{\mathrm{s}(r)}\big(\mathrm{s}(M)+\mathrm{s}(N)\big)\right) - \frac{1}{\mathrm{s}^2(r)}\big(\mathrm{s}^2(M)+\mathrm{s}^2(N)\big)\right).$$

Now the last expression is zero by the hypothesis and hence one of the factors of the first expression is zero. This gives the claim. □

Lemma 12 gave a multiplicative relationship between vertices that were 2-ancestors. The following result involves both addition of k-ancestors and multiplication by inverses of tree elements in the 0-component. This connects the existence of tree elements in the 0-component to the existence of vertices with higher ancestory.

Theorem 19: If M and N are k-ancestors in $\mathrm{fd}_p(\mathrm{s}(x))$ for some $k \geq 2$ and if r is a predecessor of 0 such that $\mathrm{s}^{k-1}(r) = 0$ then M and something of the form $\frac{1}{r}(M+N')$ are k+1-ancestors where N' is a vertex such that N' and M are k-ancestors. Moreover, if M is at level k+2 or higher, then there are 2^k vertices that are k+1-ancestors with M.

Proof: Proceed by induction on k. When $k = 2$ we claim that $\frac{1}{r}(M+N)$ is a 3-ancestor of M. We are assuming $\mathrm{s}(r) = 0$ and hence $r^2 = 2$; from Lemma 12 we saw MN is a 2-ancestor of $\mathrm{s}(M)$ and hence we need only show $\mathrm{s}(\frac{1}{r}(M+N)) = MN$. Notice that

$$\mathrm{s}(\tfrac{1}{r}(M+N)) = \frac{1}{r^2}(M^2+2MN+N^2) - 2 = MN + \frac{1}{2}(M^2+N^2-4) = MN$$

where the last equality holds since M and N are 2-ancestors implies that $M^2 + N^2 = 4$. Also, if M is at

level 4 or higher we know that $\frac{1}{r}(M+N)$ is also at level 4 or higher since $s^3(M)$ is not a cycle element. Thus, $\frac{1}{r}(M+N)$ is its own "0-ancestor", it has one 1-ancestor (its additive inverse), and two 2-ancestors from the reasoning in the remark after Lemma 14. All of those are 3-ancestors of *M* and hence we have four 3-ancestors of *M*.

When $k = 3$, we know that *M* and *N* are 3-ancestors means s(*M*) and s(*N*) are 2-ancestors. By the the k=2 induction step, we can assume that s(*M*) has a 3-ancestor of the form $\frac{1}{s(r)}(s(M)+s(N))$. Now we need to show $s(\frac{1}{r}(M+N)) = \frac{1}{s(r)}(s(M)+s(N))$ or $s(\frac{1}{r}(M-N)) = \frac{1}{s(r)}(s(M)+s(N))$. First note that *M* and *N* are 3-ancestors if and only if $s^2(M) = -s^2(N)$ which is if and only if $M^4 - 4M^2 + 4 - 4N^2 + N^4 = 0$. Now direct computation using the fact that $r^4 = 4r^2 - 2$ 15 shows that:

$$\left(s(\frac{1}{r}(M+N)) - \frac{1}{s(r)}(s(M)+s(N))\right)\left(s(\frac{1}{r}(M-N)) - \frac{1}{s(r)}(s(M)+s(N))\right)$$

$$= \frac{4}{r^4 s(r)^2}(M^4 - 4M^2 + 4 - 4N^2 + N^4)$$

which is zero since *M* and *N* are 3-ancestors. Hence one of the two conditions required must hold. Thus we have found a 4-ancestor $A = \frac{1}{r}(M \pm N)$ of *M* and we can rename *N* if desired to avoid the minus sign. Now suppose *M* is at level at least k+2. We see *A* must be at the same level since $s^{k+1}(M)$ is not a cycle element. We know that *A* is its own "0-ancestor", it has one 1-ancestor, two 2-ancestors, and four 3-ancestors by induction. All of those are 4-ancestors of *M* and hence *M* has eight 4-ancestors.

Now suppose we have shown the theorem up to k-1 and want to show it for k. By renaming *N* if need be (to avoid minus signs) we can assume that s(*M*) and $\frac{1}{s(r)}(s(M)+s(N))$ are k-ancestors and $s^2(M)$ and $\frac{1}{s^2(r)}(s^2(M)+s^2(N))$ are k-1-ancestors with $s\left(\frac{1}{s(r)}(s(M)+s(N))\right) = \frac{1}{s^2(r)}(s^2(M)+s^2(N))$. We can now apply Lemma 18 to get a k+1 ancestor of *M* of the desired form. When *M* is at level at least k+2, using the induction steps to complete the tree surrounding this new vertex gives the desired 2^k vertices which are k+1-ancestors with *M*. □

We will refer to Figure 6 to provide some illustrations of this theorem in $fd_{239}(s(x))$. Notice that s(99) = 0 and the multiplicative inverse of $r = 99$ is 169. Now $M = 112$ and $N = 102$ are 2-ancestors appearing at level 4 in the branched component containing a 4-cycle. Note $\frac{1}{r}(M+N) = 169(112+102) = 77$ which is a 3-ancestor with *M*. Also, 65, which appears at level 2, and

230, which is a cycle element, are 2-ancestors. Note $\frac{1}{r}(M+N) = 169(230+65) = 143$ is at level 3 in the next tree; hence 65 and 143 are 3-ancestors. Also $s^2(36) = 0$ and the multiplicative inverse of $r = 36$ is 166. Therefore we are able to lift to level 4 via $\frac{1}{r}(M+N) = 166(230+143) = 17$; hence 17 and 143 are 4-ancestors18.

Notice we are able to use Theorem 19 to find elements at the same level in a tree associated with a cycle element and we also are able to use the theorem to find elements at a higher level in the next tree associated with a cycle element having more distant ancestry. Thus it can be used both to complete trees and to lift levels. We put these ideas together in our main theorem about the tree structure in $\mathrm{fd}_p(\mathrm{s}(x))$.

Theorem 20: The tree leading to any vertex at level 2 in $\mathrm{fd}_p(\mathrm{s}(x))$ is a complete binary tree and is isomorphic to the tree leading to the vertex 0.

Proof: Suppose the leaves in the 0-component reach level d. Then if r is such a leaf in that component, $\mathrm{s}^{d-2}(r) = 0$. Now if $d \geq 3$ we can use Theorem 19 on vertices at height 2 with a cycle element that gives a 2-ancestor to produce a 3-ancestor at level 3. If $d \geq 4$ we can use this vertex and a cycle vertex to get a vertex at level 4. We can repeat this d - 2 times resulting in a vertex at height d. We can then use Theorem 19 and the vertices at height d to see that all the trees in the branched components are complete binary trees from level 2 up to height d.

Lastly, we need to show that if any component has reached level d+1, then we can reverse the identity used to raise to level d + 1 (in Lemma 18) to solve for an r that leads to 0 in one more step, contradicting our choice of d. In particular, we can assume that r is at level d in the tree leading to 0 and that there is vertex R at level d+1 in some other branched component. By the induction to level d we know the trees to level d are complete, in fact, trees rooted to depth d or less from any vertex are complete. Now s(R) is at level d and the trees are complete to that level. Thus, s(R) must be obtainable from the process of lifting described in Theorem 19. In particular, we can find a cycle vertex M and a vertex N at level d so that s(M) and s(N) are d-ancestors lifting to s(R). That is,

$$\frac{1}{r}(\mathrm{s}(M) + \mathrm{s}(N)) = \mathrm{s}(R), \qquad (*)$$

and

$$\frac{1}{\mathrm{s}(r)}(\mathrm{s}^2(M) + \mathrm{s}^2(N)) = \mathrm{s}^2(R)$$

and from that it follows that

$$\mathrm{s}\left(\frac{1}{r}(\mathrm{s}(M) + \mathrm{s}(N))\right) = \frac{1}{\mathrm{s}(r)}(\mathrm{s}^2(M) + \mathrm{s}^2(N)).$$

We need only show that $\mathrm{s}(\frac{1}{R}(M+N)) = r$ or $\mathrm{s}(\frac{1}{R}(M-N)) = r$ to show that the tree leading to 0 rises to level d + 1. Now an identity similar to that appearing in Lemma 18 is

$$\mathrm{s}\left(\frac{1}{r}(\mathrm{s}(M) + \mathrm{s}(N))\right) - \frac{1}{\mathrm{s}(r)}(\mathrm{s}^2(M) + \mathrm{s}^2(N))$$
$$= \frac{2}{r^2\mathrm{s}(r)}(4 - M^2 - N^2 - rMN - r^2)(-4 + M^2 + N^2 - rMN + r^2).$$

We noted above that the left hand side must be zero. If we assume the first factor of the right hand side is zero and simplify using (*) we get $s(\frac{1}{R}(M + N)) = r$ and the other possibility arises from the other factor. In this way we see all the trees in branched components have the same height which completes the proof. □

Notice that knowing that the trees are uniform complete binary trees along with knowledge of the number of leaves in the branched components now allows us to compute the number of branched cycle elements, c, and the depth, d, of the trees. For example, when $p = 239$ we checked that there are 60 leaves in the branched components. Since there are $2c - 1$ trees associated with level 2 vertices each of which will have 2^{d-2} leaves we see $(2c-1)2^{d-2} = 60 = 15(2^2)$; by equating the odd factors and powers of two we see $2c - 1 = 15$ and $2^{d-2} = 2^2$ so $c = 8$ and $d = 4$ which is correct.

ACKNOWLEDGMENT

This work was supported in part by NSF-REU grant DMS-9424098. The generous advice of an anonymous referee was extremely helpful and much appreciated.

REFERENCES

1. E. L. Blanton, Jr., S. P. Hurd, and J. S. McCranie. "On A Digraph Defined By Squaring Modulo *n*." *The Fibonacci Quarterly* **30.4** (1992):322-334.
2. E. L. Blanton, Jr., S. P. Hurd, and J. S. McCranie. "On The Digraph Defined By Squaring mod *m*, when *m* has Primitive Roots." *Congressus Numerantium* **82** (1991):167-177.
3. R. L. Devaney. *An Introduction to Chaotic Dynamical Systems.* Reading, MA:Addison-Wesley, 1987.
4. R. L. Devaney. *A First Course in Chaotic Dynamical Systems.* Reading, MA:Addison-Wesley, 1992.
5. A. Flores. "Geometry Of Numeric Iterations." *PRIMUS* **4.1** (1994):29-38.
6. Hua L. K. *Introduction to Number Theory.* Berlin: Springer-Verlag, 1982.
7. S. Kravitz, "The Lucas-Lehmer Test for Mersenne Numbers", *The Fibonacci Quarterly* **8.1** (1970): 1-3.
8. C. Lucheta, E. Miller, and C. Reiter. "Digraphs From Powers Modulo *p*," *The Fibonacci Quarterly* **34.3** (1996):226-239.
9. H. Riesel. *Prime Numbers and Computer Methods for Factorization*. Boston: Birkhäuser, 1985.
10. T. D. Rogers. "The Graph Of The Square Mapping On The Prime Fields." *Discrete Mathematics* **148** (1996):317-324.
11. J. Strayer. *Elementary Number Theory.* Boston: PWS Publishing Co., 1994.
12. B. Wilson. "Power Digraphs Modulo *p*." *The Fibonacci Quarterly* **36.3** (1998):229-239.

AMS Classification Numbers: 05C20, 11B50.