Classification of quadratic iteration graphs

Kyle Miller
kmill@mit.edu

20 Nov 2010

Abstract

The basic theory of iteration graphs are explained, and quadratic iteration graphs of the form $f(x) = x^2 + c$ modulo prime p are classified for $c = 0$. As an application, the structure of the iteration graph for $f(x) = x^2$ is used to explain the operation of the Tonelli square root algorithm.

1 Introduction

The motivation for this paper is an attempt to understand the problem of computing square roots modulo a prime in polynomial time. Finding a deterministic polynomial time algorithm (with respect to $\lg p$) for this is currently an open problem, and the only algorithms which have been proven to run in polynomial time are randomized [Bach 155]. An example is the Tonelli square root algorithm, which uses a quadratic non-residue (that is, an integer which is not a square of anything modulo p) to transform the input into something which has a square root that is easy to compute. However, there are no known deterministic polynomial time algorithms which can generate quadratic nonresidues, so the Tonelli algorithm transforms one unsolved problem into another.

The distribution of quadratic nonresidues is favorable: exactly half of the numbers in the set $\{1, 2, \ldots, p-1\}$ are quadratic nonresidues, so we only expect to have to randomly select two elements from this set before finding a quadratic nonresidue.

The placement of the quadratic nonresidues, on the other hand, is more difficult to understand. With basic number theory, it can be shown that there must exist a quadratic nonresidue within the first $1 + \sqrt{p}$ positive integers [Niven, Theorem 3.9], but this only suggests an exponential time deterministic algorithm. However, assuming the Extended Riemann Hypothesis, which so far has eluded proof, this bound has been brought to $O(\lg^2 p)$ [Ankeny], which gives a way to find a quadratic nonresidue is deterministic polynomial time.

One way to attempt to understand both the problem of finding square roots and the problem of finding quadratic nonresidues is to study the function $f(x) = x^2$ modulo a prime, since quadratic nonresidues are those y such that $f(x) \not\equiv y \pmod{p}$ for all x. This suggests looking at the iteration graph for f, which is a graph whose vertices are the set of integers modulo p, and an edge $\overrightarrow{xy}$ exists in the graph if and only if $f(x) \equiv y \pmod{p}$.

There is a lot of structure in this type graph, and some of these iteration graphs modulo p are amenable to classification. And, it turns out that the structure of this graph reflects the principle behind the Tonelli algorithm.

In this paper, we will describe iteration graphs in more detail, restrict our attention to quadratic iteration graphs where f is of the form $f(x) = x^2 + c$, and classify some of such graphs. As an application, though, we will use these results to understand the Tonelli algorithm for square roots as an aid to gain intuition for the difficulties in determining quadratic nonresidues.

This discussion will require a better grounding in basic group theory and number theory than was covered in 18.310, so, for the benefit of the reader, we will review this background material.

2 Background material

In this section we will give an overview of background material from algebra and elementary number theory which we will use for the discussion of iteration graphs. We are covering this material in some depth because, for example, we need to be comfortable with the cosets of a group when we discuss the Tonelli algorithm, and we need a generalized version of Fermat's little theorem to classify certain iteration graphs.

We will not be following any book in particular, but the reader is invited to read [Artin] and [Niven] for more detail.

2.1 Group theory

A **group** G is a set with an associative binary operation $\cdot * \cdot : G \times G \to G$ which has an identity element 1 that satisfies $1 * a = a * 1 = a$ for all $a \in G$, and which has inverses: for every element $a \in G$ there is a $b \in G$ such that $a * b = b * a = 1$. When we think of the binary operation as being a kind of multiplication, we use juxtaposition, writing ab instead of $a * b$, the symbol 1 for the identity element, and a^{-1} for the inverse of a. In additive notation, where we use $+$ for the operation, we instead use the symbol 0 for the identity and write $-a$ for the inverse of a, which satisfy $a + 0 = 0 + a = a$ and $a + (-a) = 0$, respectively.

The **order** of G is the number of elements in G. In this paper, we will assume groups have finite order unless otherwise specified. We will also be using both additive and multiplicative groups; the notation we use will be clear from context.

A **subgroup** H of a group G is a subset of G which itself is a group when the binary operation of G is restricted to H (if such a restriction is possible, then we say H is **closed** under the binary operation). The **cyclic subgroup** generated by some element $x \in G$, denoted by $\langle x \rangle$, is all powers of x: $\dots, x^{-2}, x^{-1}, 1, x^1, x^2, \dots$, which clearly is a group. The **order** of an element $x \in G$ is the smallest positive integer ℓ such that $x^\ell = 1$. This terminology is justified by the following lemma:

Lemma 1. *The order of an element x of a group G is equal to the order of $\langle x \rangle$.*

Proof. First, we will prove the order of x exists. Since G is finite, the sequence $1, x, x^2, \dots$ must have at least one pair of terms which are equal. That is, there are integers s, t with $s > t$ such that $x^s = x^t$. Since G is a group, $x^{s-t} = 1$, and since $s - t$ is a positive integer, a smallest positive integer ℓ must exist. Now, $x^i = x^{i-\ell}x^\ell = x^{i-\ell}$ and $x^i = x^{i+\ell}x^{-\ell} = x^{i+\ell}$, so for any integer i there is a $0 \le j < \ell$ such that $x^i = x^j$, so $\langle x \rangle = \{1, x^2, x^3, \dots, x^{\ell-1}\}$. □

Let H be a subgroup of a group G. Given $a \in G$, a **coset** aH is the set

$$aH = \{ah \mid h \in H\}.$$

Lemma 2. *Let H be a subgroup of a group G. Each coset of H has the same order.*

Proof. Since every element $a \in G$ has an inverse, the map on G defined by $x \mapsto ax$ is a bijection with inverse $x \mapsto a^{-1}x$. Thus, H is in bijective correspondence with aH, and so $|H| = |aH|$ for all $a \in G$. Therefore, for any $a, b \in G$, $|aH| = |H| = |bH|$. □

A **partition** $\mathcal{A}$ of a set X is a collection of subsets such that $\cup_{A \in \mathcal{A}} A = X$ and all of the sets in the partition are disjoint. For instance, $\{\{1,2\},\{3\}\}$ is a partition of the set $\{1,2,3\}$.

Lemma 3. *Let H be a subgroup of a group G. Then the cosets of H partition G.*

Proof. First, we see every element a of G is contained in some coset of H, in particular $a \in aH$ since $1 \in H$ and $a = a1$. Next, we will show if, for $a, b \in H$, that if aH and bH have a nonempty intersection, then $aH = bH$. Let $x \in aH \cap bH$. Then $x = ah_1 = bh_2$, which means $a = bh_2h_1^{-1}$. Given an arbitrary element $ah_3 \in H$, $ah_3 = (bh_2h_1^{-1})h_3 = b(h_2h_1^{-1}h_3)$. Since H is a group, $h_2h_1^{-1}h_3 \in H$, so $ah_3 \in bH$. Since ah_3 was arbitrary, $aH \subset bH$. By symmetry, $aH \supset bH$, so $aH = bH$. Therefore, the union of the cosets of H is all of G, and the intersection of any two distinct cosets of H is nonempty, so the cosets of H partition G. □

These two lemmas prove the following theorem.

Theorem 4 (Counting theorem)**.** *Let k be the number of distinct cosets of a subgroup H of a group G. Then*

$$k\,|H| = |G|\,.$$

*We call k the **index** of H in G.* □

Corollary 5 (Lagrange's theorem)**.** *If H is a subgroup of a group G, then the order of H divides the order of G.* □

This corollary gives a convenient number n so that $a^n = 1$ for all $a \in G$:

Corollary 6. *Let G be a group and n its order. Then $a^n = 1$ for all $a \in G$.*

Proof. Let $a \in G$. By Lagrange's theorem, the order of $\langle a \rangle$ divides the order of G, and since the order of $\langle a \rangle$ equals the order of a, the order of a divides the order of G. Thus, $k\ell = n$ for some integer k. We see $a^n = a^{k\ell} = (a^\ell)^k = 1^k = 1$. □

2.2 Elementary number theory

This section reviews notions from elementary number theory. Some of this material was mentioned in 18.310. However, our treatment of the material is different enough so the author thought it would be profitable to mention it again.

If x, y, and n are integers, then x and y are said to be **congruent modulo** n if n divides $x - y$. This relation is denoted by $x \equiv y \pmod{n}$.

We will show congruence is an equivalence relation. This relation is reflexive since 0 is divisible by any n, so n divides $x - x$. This relation is also transitive since if $x \equiv y$ and $y \equiv z$ modulo n, then $k_1 n = x - y$ and $k_2 n = y - z$ for some integers k_1 and k_2, so $y = x - k_1 n$, which means

$k_2n = (x - k_1n) - z$, thus $(k_1 + k_2)n = x - z$. Therefore, $x \equiv z \pmod{n}$. Next, we will show congruency respects addition and multiplication.

If $x_1 \equiv x_2$ and $y_1 \equiv y_2$ modulo n, then $x_1 + y_1 \equiv x_2 + y_2$ modulo n. This is because, by the hypotheses, $k_xn = x_1 - x_2$ and $k_yn = y_1 - y_2$ for some integers k_x, k_y, so $(k_x + k_y)n = (x_1 + y_1) - (x_2 + y_2)$, and therefore $x_1 + y_2 \equiv x_2 + y_2 \pmod{n}$.

Also, if $x_1 \equiv x_2$ and $y_1 \equiv y_2$ modulo n, then $x_1y_1 \equiv x_2y_2 \pmod{n}$. By the hypotheses, there are integers k_x, k_y so $k_xn = x_1 - x_2$ and $k_yn = y_1 - y_2$. Then $(x_1k_y + y_2k_x)n = x_1(y_1 - y_2) + y_2(x_1 - x_2) = x_1y_1 - x_2y_2$, and thus $x_1y_1 \equiv x_2y_2 \pmod{n}$.

We can take this equivalence relation of congruence and find representative elements so that it is easier to work with. Let $\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}$. We claim every integer x is congruent to exactly one element of $\mathbb{Z}_n$ modulo n. By the division algorithm, $x = qn + r$ uniquely for some integers q and r where $0 \leq r < n$. Thus, $qn = x - r$, and so $x \equiv r \pmod{n}$. Therefore x is congruent to some unique $r \in \mathbb{Z}_n$.

The previous three results imply that we can let $\mathbb{Z}_n$ inherit the operations of addition and multiplication in $\mathbb{Z}$ by taking the result of the operation and finding the unique element of $\mathbb{Z}_n$ to which it is congruent. This means $\mathbb{Z}_n$ has associative and commutative addition and binary operations which respect the distributive law, and which have identities 0 and 1, respectively, and addition has inverses.

Under some circumstances, multiplication also has inverses. By the Euclidean algorithm for computing the greatest common denominator of two integers x and y, there exist integers s and t so that $\gcd(x, y) = sx + ty$. We will use this fact to prove the following lemma:

Lemma 7. *An element $a \in \mathbb{Z}_n$ has a multiplicative inverse if and only if* $\gcd(a, n) = 1$.

Proof. Assume $\gcd(a, n) = 1$. Then there are integers s, t so that $sa + tn = 1$, which means $tn = 1 - sa$, so $1 \equiv sa \pmod{n}$. Therefore s is the multiplicative inverse of a.

Now, assume $a \in \mathbb{Z}_n$ has a multiplicative inverse $s \in \mathbb{Z}_n$. Then $as \equiv 1 \pmod{n}$, which implies $as - 1 = kn$ for some integer k, and so $1 = as - kn$. Since the greatest common denominator of two numbers divides any integer linear combination of the numbers (a fact utilized by the Euclidean algorithm), $\gcd(a, n) = 1$. □

This lemma justifies the definition of the **multiplicative group modulo** n to be all of the elements a of $\mathbb{Z}_n$ such that $\gcd(a, n) = 1$. We denote this set by $\mathbb{Z}_n^*$. It is clear that this set is indeed a group as multiplication is associative, there is an identity 1, multiplication is closed since, if both $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(ab, n) = 1$, and every element has an inverse: $\gcd(a, n) = 1$ means $1 = sa + tn$ for some integers s, t, so $1 = as + tn$, thus $\gcd(s, n) = 1$, where s is the inverse of a modulo n, and this has a representative in $\mathbb{Z}_n^*$.

The order of this group is denoted by $\varphi(n) = |\mathbb{Z}_n^*|$. It is called the **totient function.** For prime numbers p, $\varphi(p) = p - 1$ because every element $i \in \mathbb{Z}_p$ but $i = 0$ has $\gcd(i, p) = 1$. Thus, $\mathbb{Z}_p^*$ is $\mathbb{Z}_p$ without 0.

The following theorem is a special case of Corollary 6, and a generalization of Fermat's little theorem which appeared in class:

Theorem 8 (Euler's theorem)**.** *For any $x \in \mathbb{Z}_n^*$,*

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

□

We will run into the need to solve equations of the form $ax \equiv b \pmod{n}$. These linear equations in general do not have a unique solution.

Lemma 9. *Let a, b, n be integers with n positive. If $\gcd(a, n)$ divides b, then $ax \equiv b \pmod{n}$ has exactly $\gcd(a, n)$ solutions x. Otherwise, the equation has no solutions.*

Proof. Let $g = \gcd(a, n)$. Assume g divides b. The congruence $ax \equiv b \pmod{n}$ is equivalent to $kn = ax - b$ for some integer k. Since g divides a, b, and n, we have $k\frac{n}{g} = \frac{a}{g}x - \frac{b}{g}$. Thus,

$$\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{n}{g}}.$$

Now, we note that $\frac{a}{g}$ has no common divisors with n since the common divisors between a and n have been removed from a, so $\gcd(\frac{a}{g}, n) = 1$. This implies there are integers c and d such that $1 = c\frac{a}{g} + dn$. Thus, $1 \equiv c\frac{a}{g} \pmod{\frac{n}{g}}$ since dn is divisible by $\frac{n}{g}$. Therefore c is an inverse so that

$$x \equiv \frac{bc}{g} \pmod{\frac{n}{g}},$$

and this implies $x = \frac{bc}{g} + \frac{mn}{g}$ for some integer m. Since $\frac{ca}{g} = 1 - dn$, first multiplying by a,

$$ax = \frac{abc}{g} + \frac{amn}{g} = b(1 - dn) + \frac{amn}{g}.$$

Because g divides a, n divides $\frac{n}{g}$. Consequentially, $ax \equiv b \pmod{n}$ no matter the choice of m. It is clear that $0 \leq m < g$ represents all incongruous solutions to the equation, so there are g solutions to the equation.

Now, assume g does not divide b. Since g divides n, any solutions to $ax \equiv b \pmod{n}$ will also be solutions to $ax \equiv b \pmod{g}$. We note that $b \not\equiv 0 \pmod{g}$, but, since g divides a, $ax \equiv 0 \pmod{g}$, so $0 \equiv b \pmod{g}$, which is a contradiction. Thus, there are no solutions to the equation. □

2.2.1 Primitive roots

We will leave the following theorem without proof since it requires some more advanced techniques. The reader is invited to read [Artin, Theorem 15.7.3(c)], which uses the structure theorem for abelian groups [Artin, Theorem 14.7.3].

Theorem 10. *The multiplicative group $\mathbb{Z}_n^*$ is cyclic. In other words, there exists an element $\omega \in \mathbb{Z}_n^*$ such that for every $x \in \mathbb{Z}_n^*$, there is an integer i so $x \equiv \omega^i \pmod{n}$.* □

This ω is called a **primitive root modulo** n. As an example, 3 is a primitive root modulo 7:

i	1	2	3	4	5	6
3^i	3	2	6	4	5	1

Theorem 11. *Let d be a divisor of the order of $\mathbb{Z}_p^*$, where p is prime. The number of elements of order d in $\mathbb{Z}_p^*$ is $\varphi(d)$.*

Proof. Let ω be a primitive root modulo p and let d be a divisor of $\mathbb{Z}_p^*$. If x is such that $x^d \equiv 1 \pmod{p}$, then, since $x \equiv \omega^\ell \pmod{p}$ for some $0 \le \ell < p-1$, we have $\omega^{d\ell} \equiv 1 \pmod{p}$. By Euler's theorem, then $d\ell \equiv 0 \pmod{p-1}$. Because d divides $p-1$, we have that ℓ is divisible by $\frac{p-1}{d}$. So, $\ell = k\frac{p-1}{d}$ for some $0 \le k < d$, since $0 \le \ell < p-1$. Assume that $\gcd(k,d) \ne 1$, and let $d' = \frac{d}{\gcd(k,d)}$, which means $d' < d$. We see that

$$x^{d'} \equiv \omega^{\ell d'} \equiv \omega^{\frac{kd'(p-1)}{d}} \equiv \omega^{\frac{kd(p-1)}{\gcd(k,d)d}} \equiv \left(\omega^{p-1}\right)^{\frac{k}{\gcd(k,d)}} \pmod{p}.$$

And, because k is divisible by $\gcd(k,d)$, we conclude that $x^{d'} \equiv 1 \pmod{p}$, contradicting the fact that d is the order of x. This shows there are at most $\varphi(d)$ elements of order d.

Now, let $0 \le k < d$ be such that $\gcd(k,d) = 1$, and assume there is a $0 < d' < d$ such that $x^{d'} \equiv 1 \pmod{p}$. Then, $\ell d \equiv \ell d' \equiv 0 \pmod{p-1}$. Since $\ell = k\frac{p-1}{d}$, we have $k(p-1) \equiv \frac{kd'(p-1)}{d} \pmod{p-1}$. Because $k(p-1) \equiv 0 \pmod{p-1}$, and $\gcd(k,d) = 1$, we have $\frac{d'(p-1)}{d} \equiv 0 \pmod{p-1}$. But, $d' < d$, so this is an impossibility. Thus, there is no such d'. This concludes the proof that there are exactly $\varphi(d)$ elements of order d. □

2.2.2 Quadratic residues

A **quadratic residue** x modulo n is an element such that there is a y so $x \equiv y^2 \pmod{n}$. From this point forward, we will assume that $n = p$ for some prime p.

Detecting whether x is a quadratic residue modulo prime p, where $p > 2$, involves the following observation. Let ω be a primitive root modulo p. Then there is an integer i so that $\omega^i \equiv x \pmod{p}$. If i is even, $i = 2k$ for some k, so $x^{\frac{p-1}{2}} \equiv \omega^{\frac{i(p-1)}{2}} \equiv \omega^{k(p-1)} \equiv (\omega^{p-1})^k \equiv 1 \pmod{p}$. However, if i is odd, then $i = 2k+1$ for some k, which means $x^{\frac{p-1}{2}} \equiv \omega^{\frac{i(p-1)}{2}} \equiv \omega^{k(p-1)+\frac{p-1}{2}} \equiv \omega^{\frac{p-1}{2}} \pmod{p}$. But, since $\frac{p-1}{2} < p-1$, this is not congruent to 1 modulo p. This proves the following theorem:

Theorem 12. *Let $p > 2$ be prime and $x \in \mathbb{Z}_p^*$. Then x is a quadratic residue if and only if $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.* □

Like linear equations in Lemma 9, we will have the need to know how many solutions to $x^2 \equiv c \pmod{p}$ there are, for some integer c. If $p = 2$, then only $0^2 = 0$ and $1^2 = 1$, so we may assume $p > 2$.

Lemma 13. *Let $p > 2$ be prime and $c \in \mathbb{Z}_p$. Then, the number of solutions to $x^2 \equiv c \pmod{p}$ is*

- *zero if c is not a quadratic residue,*
- *one if $c = 0$,*
- *and two if c is a quadratic residue.*

Proof. If c is not a quadratic residue, then there are zero solutions by definition.

If $c = 0$, then we are trying to find an element so $x^2 \equiv 0 \pmod{p}$, which is to say, find an integer x so that p divides x^2. Assume x is such that p divides x^2. Then, since p is prime (which means if p divides ab then either p divides a or p divides b), p divides x. Thus $x \equiv 0 \pmod{p}$. This gives exactly one solution.

On the other hand, if c is a quadratic residue, then we have seen that $c \equiv \omega^{2k} \pmod{p}$ for some integer k, where ω is a primitive root modulo p. Let x be an arbitrary element of $\mathbb{Z}_p^*$, thus $x \equiv \omega^i \pmod{p}$ for some integer i. Because $x^2 \equiv c \pmod{p}$, $x^2 \equiv \omega^{2i} \equiv \omega^{2k} \pmod{p}$. Since $\omega^{p-1} \equiv 1 \pmod{p}$, and since this is the smallest positive exponent such that this is true, this equation is equivalent to $2i \equiv 2k \pmod{p-1}$. By lemma 9, since 2 divides $2k$, and $\gcd(2, p-1) = 2$, there are exactly two solutions i, which results in exactly two solutions x. □

3 Iteration graphs

Examining an iteration graph for a function $f : V \to V$ which maps a set V into itself is a way to study the behavior of iterative application of the function. That is, an iteration graph simultaneously shows the shape of the sequences $x, f(x), f(f(x)), \ldots, f^{(n)}(x), \ldots$, for all $x \in V$.

Definition 14. *The* ***iteration graph*** *of a function $f : V \to V$ is a directed graph G which allows self-loops, with V as its set of vertices, and, for all $a, b \in V$, G has edge $\overrightarrow{ab}$ if and only if $f(a) = b$.*

For the purpose of this paper, we will restrict our attention to sets V with finitely many elements as we will generally be looking at $V = \mathbb{Z}_p$.

A **walk** on a graph G is a sequence of vertices $x_1, x_2, \ldots$ such that $\overrightarrow{x_i x_{i+1}}$ is an edge in G for every i.

Because f is a function, a basic property of iteration graphs is that every vertex has exactly one out-edge. We see, then, that walks in G and iteration sequences of f are equivalent concepts: a walk of length n starting from $x \in V$ gives a unique iteration sequence $x, f(x), \ldots, f^{(n)}(x)$, and there is only one walk which follows the elements of this iteration sequence as each vertex has exactly one out-edge.

It is clear that there is an infinite walk starting from every $x \in V$, namely

$$x, f(x), \ldots, f^{(n)}(x), \ldots,$$

and, since V has finitely many elements, this walk cannot continue visiting unvisited vertices forever, so there are integers n, m with $n < m$ so that $f^{(n)}(x) = f^{(m)}(x)$. Since each vertex has exactly one out-edge, it is clear that there is some integer $s > 0$ such that $f^{(n)}(x) = f^{(n+s)}(x)$. Thus, the infinite walk starting from any vertex in G will enter a cycle. This justifies the following definitions:

Definition 15. *A vertex x in an iteration graph G is called* ***cyclic*** *if $f^{(m)}(x) = x$ for some positive integer m, and the smallest such m is called the* ***period*** *of x. If x is cyclic, the set $\{x, f(x), \ldots, f^{(n)}(x), \ldots\}$ is called a* ***cycle*** *of G, and the* ***period*** *of a cycle is its cardinality.*

By the equivalence of walks and iteration sequences, the period of a cyclic element x and the period of its corresponding cycle are equal. Also, every element of this cycle necessarily generates the same cycle, so all elements of a cycle have the same period.

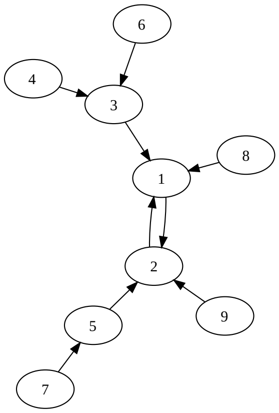
Definition 16. *The* ***preperiod*** *of a vertex x in an iteration graph G is the minimal non-negative integer m such that $f^{(m)}(x)$ is cyclic.*

If x is cyclic, then the preperiod is zero, and if x isn't cyclic, then the preperiod is a positive integer.

The **trees** of an iteration graph G are the disconnected subgraphs after removing cyclic vertices. Since each vertex has exactly one out-edge, each tree is attached to exactly one vertex of some cycle.

The following is an example of an iteration graph and its corresponding function f on the set $\{1, \ldots, 9\}$:

x	1	2	3	4	5	6	7	8	9
$f(x)$	2	1	1	3	2	3	5	1	2



Elements 1 and 2 are cyclic of period two, and they form a cycle. The preperiod of 7 is two, and the preperiod of 5 is one. The trees of this iteration graph are the subgraphs with the vertices $\{3, 4, 6\}$, $\{8\}$, $\{9\}$, and $\{5, 7\}$.

3.1 Quadratic iteration graphs

A **quadratic iteration graph** is an iteration graph generated by a quadratic function $f(x) = ax^2 + bx + c$ on $\mathbb{Z}_p$ for prime p, but we will restrict our attention to f of the form $f(x) = x^2 + c$.

Basic properties of these graphs are that each vertex $y \in \mathbb{Z}_p$ has zero, one, or two in-edges, since there is an edge $\overrightarrow{xy}$ if and only if $f(x) = y$, which is equivalent to $x^2 \equiv y - c \pmod{p}$, and the number of in-edges follows from Theorem 12 and Lemma 13:

- Exactly one vertex has only one in-edge;
- $\frac{p-1}{2}$ vertices have no in-edges;
- And $\frac{p-1}{2}$ edges have two in-edges.

It turns out that there is very regular structure when $c = 0$ or $c = -2$, and for other c, the graphs experimentally appear random in general.

A non-rigorous justification for this is the following. Let us take the quadratic map $x \mapsto x^2 + c$ to be over $\mathbb{C}$ instead of $\mathbb{Z}_p$, as it is also a field. If $c = 0$, then points on the unit disc are mapped into the unit disc, points outside are mapped to points with larger magnitude, and points inside are mapped to points with lesser magnitude. Thus, the unit disc is the set of points which do not diverge after iteration by the map. If we instead take $c = -2$, then real points a so $-2 \leq a \leq 2$ are mapped back into this line segment. Points off this line segment are mapped farther away from the line segment, and so iteration diverges. However, if c is neither of these, then the situation is much more complicated. The set of points for which the iteration does not diverge is a kind of Julia set. For almost every c not equal to -2 or 0, this set is a fractal (and it is an open question if every such c is a fractal) [Weisstein].

3.1.1 Classification of quadratic iteration graphs when $c = 0$

To classify these graphs, we will describe the structure of the cycles and of the trees. For the following, we assume p is a prime integer greater than 3, for if $p = 2$ the graph is very simple: two vertices, each with a self loop. Our main theorem is the following:

Theorem 17. *Let $p \geq 3$ be a prime number and $f(x) = x^2$, and let Q and ℓ be so $p - 1 = 2^\ell Q$ with Q odd. The iteration graph G for f on $\mathbb{Z}_p$ has*

- *a self loop at* 0*;*
- *for each divisor d of Q, $\frac{\varphi(d)}{n}$ cycles with period n, where n is the order of* 2 *modulo d (that is, the minimal integer n such that $2^n \equiv 1 \pmod{d}$);*
- *for each nonzero cyclic element x, there is one complete binary tree of ℓ levels attached to x.*

A corollary to this is that the number of cyclic elements is Q. For, let x be the number of cyclic elements. There is a tree of ℓ levels attached to each cyclic element, and each tree has $2^\ell - 1$ elements. We then have $p - 1 = (2^\ell - 1)x + x = 2^\ell x$, and therefore $x = Q$.

Before proving the theorem, we will look at some example graphs to see that it makes sense. Figure 1 has iteration graphs for primes 7, 17, 19, and 601. By the main theorem, we see that each has a self loop at zero. We can continue the analysis:

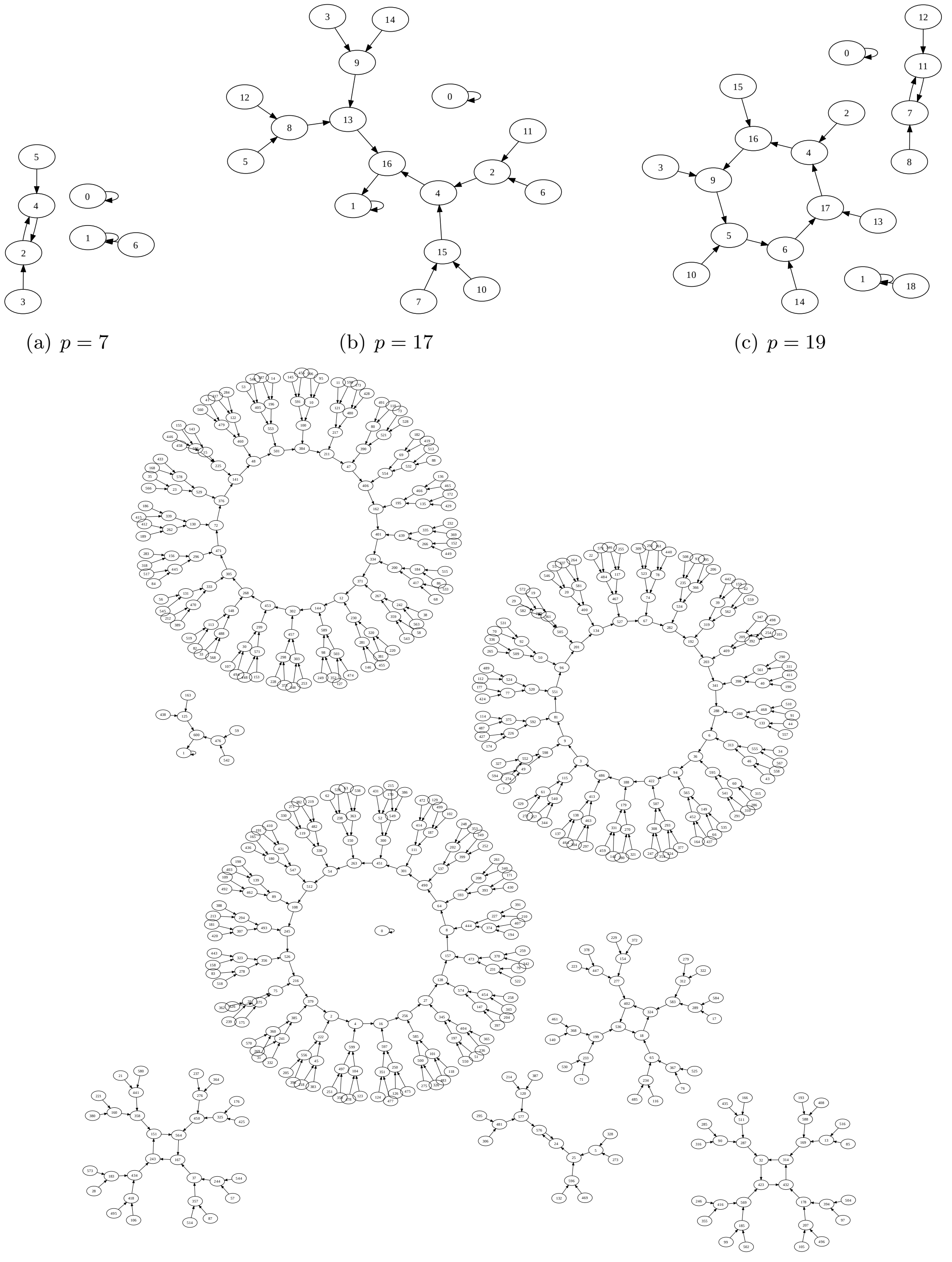
- $7 - 1 = 2^1 \cdot 3$. So we expect trees of one level attached to each nonzero cyclic element, which is what we see. The divisors of 3 are 1 and 3. The order of 2 modulo these divisors is 1 and 2, respectively. Thus, there is $\varphi(1)/1 = 1$ cycles of period 1 and $\varphi(3)/2 = 1$ cycle of period 2.
- $17 - 1 = 2^4 \cdot 1$. We expect trees with 4 levels. Since only 1 divides 1, there is $\varphi(1)/1 = 1$ cycle of period 1.
- $19 - 1 = 2^1 \cdot 9$. The trees in this case have only one level each. The divisors of 9 are 1, 3, and 9, and the order of two in each case is 1, 2, and 6, respectively. This gives $\varphi(1)/1 = 1$ cycle of period 1, $\varphi(3)/2 = 1$ cycle of period 2, and $\varphi(9)/6 = 1$ cycle of period 6.
- $601 = 2^3 \cdot 75$. Thus, the trees have three levels each. We can construct a table to aid in the computation:

(divisor of 75) d	1	3	5	15	25	75
(order of 2 modulo d) i	1	2	4	4	20	20
$\varphi(d)/i$	1	1	1	2	1	2

  Thus, there is one cycle of period 1, one cycle of period 2, one cycle of period 4, two more cycles of period 4, one cycle of period 20, and two more cycles of period 20.

Note that different divisors may give cycles of the same order. For instance, there is a multiplicity of period 20 cycles when $p = 601$. In general, if one were expecting a cycle of order $\varphi(d)$ for some divisor d, the cycle may "split" depending on the order of 2 modulo d.

We now prove the theorem.



(a) $p = 7$

(b) $p = 17$

(c) $p = 19$

(d) $p = 601$

Figure 1: Iteration graphs for $f(x) = x^2$ with various moduli.

Proof. We see $0^2 = 0$, so there is a self loop at 0. Since, modulo the prime p, $x^2 = 0$ only has the solution $x = 0$, the self loop at 0 is disconnected from the rest of the iteration graph. Thus, we may restrict our attention to $\mathbb{Z}_p^*$, which is $\mathbb{Z}_p$ without 0.

The following lemma will aid in determining which elements are cyclic.

Lemma 18. *Let x be an element of $\mathbb{Z}_p^*$ with order d. If d is odd, then x^2 has order d. Otherwise, if d is even, then x^2 has order $\frac{d}{2}$.*

Proof. Let $x \in \mathbb{Z}_p^*$ be an element with order d. Looking at the exponents of elements in $\langle x \rangle$, we see that $x^i \equiv x^j \pmod p$ for integers i, j if and only if $i \equiv j \pmod d$, since $x^d \equiv 1 \pmod p$ gives us a congruence relation on exponents. We see that $\left\langle x^2 \right\rangle$ is a subgroup of $\langle x \rangle$, and elements of $\left\langle x^2 \right\rangle$ are of the form x^{2i} for some integer i. Thus, the element x of $\langle x \rangle$ is an element of $\left\langle x^2 \right\rangle$ if and only if $1 \equiv 2j \pmod d$ for some integer j.

If d is odd, then $\gcd(2, d) = 1$, which divides 1. Thus, by lemma 9, then there is exactly one j which satisfies this, so $\langle x \rangle = \left\langle x^2 \right\rangle$, and therefore x^2 has degree d.

However, if d is even, $\gcd(2, d) = 2$, which does not divide 1, and by the same lemma, there are no solutions, so $x \notin \left\langle x^2 \right\rangle$. Since $x^{2j} \in \left\langle x^2 \right\rangle$ for all integers j, we can conclude the order of $\left\langle x^2 \right\rangle$ is half the order of $\langle x \rangle$. □

From this lemma, it follows that the iteration sequence of f on an element x of even order will stabilize to elements of only odd order, so the sequence never returns to x, and thus x is not cyclic, and instead is a vertex of the trees of G.

Lemma 19. *An element $x \in \mathbb{Z}_p^*$ is cyclic if and only if its order d divides Q.*

Proof. Assume $x \in \mathbb{Z}_p^*$ has an order d which divides Q. Since d is odd, 2 is an element of $\mathbb{Z}_d^*$, so there is some r such that $2^r \equiv 1 \pmod d$. We claim that $x^{2^r} \equiv x \pmod p$. By Euler's theorem, since $x^d \equiv 1 \pmod p$, since $2^r \equiv 1 \pmod d$, and since d divides $\varphi(p)$, we have $x^{2^r} \equiv x^1 \equiv x \pmod p$. Thus, $f^{(r)}(x) = x$.

Now, assume $x \in \mathbb{Z}_p^*$ has an order d which does not divide Q. Then, since d divides $p - 1$, d must be even. By the previous lemma, x is not cyclic. □

We know there exists an n so that $f^{(n)}(x) = x$ for x whose order divides Q, and the following lemma gives the minimal such n.

Lemma 20. *Let $x \in \mathbb{Z}_p^*$ be order d and cyclic. Then its period is the order of 2 modulo d.*

Proof. The iteration sequence of x is $x, x^2, x^{2^2}, x^{2^3}, \ldots, x^{2^i}, \ldots$. Since x has order d, we may instead look at the following sequence modulo d: $1, 2, 2^2, \ldots, 2^i, \ldots$, because elements from this sequence are the exponents of x. The first i such that $2^i \equiv 1 \pmod d$ is the period of x. It is also the order of 2 modulo d. □

By the previous lemma, all elements of odd order d have a period of n, where n is the order of 2 modulo d. By Theorem 11, there are $\varphi(d)$ elements of order d, modulo p. Therefore, there are $\varphi(d)/n$ cycles of period n.

The following lemma will aid us in showing the structure of the trees.

Lemma 21. *The preperiod of a quadratic nonresidue is ℓ.*

Proof. First, we will show quadratic residues modulo $p = 2^\ell Q + 1$ have orders which are divisible by 2^ℓ. Let $x \in \mathbb{Z}_p^*$ be a quadratic nonresidue. Then, by Theorem 12, $x^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. This means the order d of x divides $p-1$ but not $\frac{p-1}{2}$, so 2^ℓ divides d.

By induction, we will show the preperiod of an element x with order $2^i q$, where q is odd, is i. First, if $i = 0$, then the order is odd, so x is cyclic, and has preperiod $i = 0$. Next, suppose elements with order $2^{i-1}u$ with odd u have preperiod $i - 1$. By Lemma 18, x^2 has the order $2^{i-1}q$, which has preperiod $i - 1$. Therefore, x has preperiod $1 + (i - 1) = i$.

Since the order of a quadratic nonresidue x is $2^\ell q$, where q is odd, we conclude the preperiod of x is ℓ. □

We will now show that there is a complete binary tree of ℓ levels attached to cyclic elements.

If x is cyclic, then it has two square roots because it is not 0. We will show x has exactly one non-cyclic square root. At least one square root must be cyclic, for, if neither are, then they are in the trees, which means that iterated squaring on x will never reach x, a contradiction. If both square roots are cyclic, then iterated squaring of x will reach one of the square roots, which means the other square root is not cyclic, a contradiction. Therefore, cyclic elements have exactly one cyclic square root and one non-cyclic square root.

Let y be the non-cyclic square root of cyclic x. Then, by Lemma 18, since y^2 must have odd order x, the order of y is twice that of the order of x.

We will proceed by induction. Let $\{y_1, y_2, \ldots, y_2^n\}$ be the elements on the nth level of the tree attached to x, each of order $2^n q$, for some odd q. The base case is $\{y\}$, being the first level of the tree, having order $2q$, where q is the order of x.

If an element $a \in \mathbb{Z}_p^*$ has even order d, then a^2 has order $\frac{1}{2}d$. Thus, if $a \in \mathbb{Z}_p^*$ has even order, and is a quadratic residue, then its two square roots have order $2d$. The square roots are distinct because of the single out-vertex property. Then, we have a new level $\{y_{11}, y_{12}, \ldots, y_{2^n1}, y_{2^n2}\}$, where y_{i1} and y_{i2} are the square roots of y_i, and each of these elements has order $2^{n+1}q$.

By Lemma 21, this process will eventually stop with ℓ levels. Since each level of the tree is filled, and each quadratic residue in the tree has two in-vertices, the tree is a complete binary tree.

This concludes the proof of the theorem. □

3.1.2 Classification of quadratic iteration graphs when $c = -2$

This section is conjecture supported by examining the iteration graphs of about one-thousand primes and consulting the On-Line Encyclopedia of Integer Sequences. It is included to show that, as predicted by the non-rigorous Julia set argument, there is regular structure when $c = -2$.

Conjecture 22. *Let $p \geq 3$ be a prime number and $f(x) = x^2 - 2$. Let ℓ be one less than the order of 2 modulo $p^2 - 1$. The iteration graph for f on $\mathbb{Z}_p$ is the following:*

- *There are three classes of trees: trees with one level, a binary tree with ℓ levels, and complete binary trees with ℓ levels.*
- *Let $\sigma_1 = \left\lfloor \frac{p}{4} \right\rfloor$. This is the number of cyclic elements with a tree of one level attached.*
- *σ_2 is the number of cyclic elements with a complete binary tree of ℓ levels attached.*
- *Attached to the element -2 (which is cyclic), is a tree which is a complete binary tree of $\ell - 1$ levels attached at its root to a single element.*

- *The relation $p = 2\sigma_1 + 2^{\ell-1} + 1 + 2^\ell(\sigma_\ell)$ is satisfied.*

This conjecture does not constrain the entire structure of these graphs: the periods of the cyclic elements are not known. Examples of iteration graphs are in Figure 2.

4 Tonelli algorithm

The Tonelli algorithm is a randomized algorithm for finding a square root of a quadratic residue modulo a prime p in polynomial time, with respect to $\lg p$. The algorithm is described in [Bach 156]. We will explain the algorithm in this paper using some language of quadratic iteration graphs. We will omit a formal analysis of the running time of the algorithm, since the analysis is not the purpose of this paper. Fixing a prime $p > 2$, let ℓ and Q be such that $p - 1 = 2^\ell Q$ with odd Q.

First, we note that if $x \in \mathbb{Z}_p^*$ is cyclic, then it is relatively straightforward to compute a square root. In fact, $y = x^{\frac{Q+1}{2}}$ is a square root. Checking this, we note that since x is cyclic, it has an order q which divides Q, so we see that $y^2 \equiv x^{Q+1} \equiv x^Q x \equiv x \pmod p$. We also see y is easily computable for two reasons: $Q + 1$ is even (thus $\frac{Q+1}{2}$ is an integer), and there is a polynomial time exponentiation algorithm (which was covered in 18.310).

There is no known procedure which is as simple for computing the square root of a general element of $\mathbb{Z}_p^*$. However, we may use tricks from group theory to turn the general square root problem into the simple computation outlined above. For the remainder of the discussion, assume $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ is defined to be $f(x) = x^2$ (we may ignore 0 since only $x = 0$ satisfies $f(x) = 0$).

An overview of the Tonelli algorithm is, given a quadratic residue $x \in \mathbb{Z}_p^*$ and a quadratic nonresidue g, we find an even exponent k so that $g^k x$ is cyclic. Cyclic elements have easily calculable square roots, so let a square root of $g^k x$ be a. Then, $ag^{-\frac{1}{2}k}$ is a square root of x since $(ag^{-\frac{1}{2}k})^2 = a^2 g^{-k} = (g^k x)g^{-k} = x$.

We claim that we can find a sequence of subgroups

$$H_0 \subset H_1 \subset \ldots \subset H_\ell$$

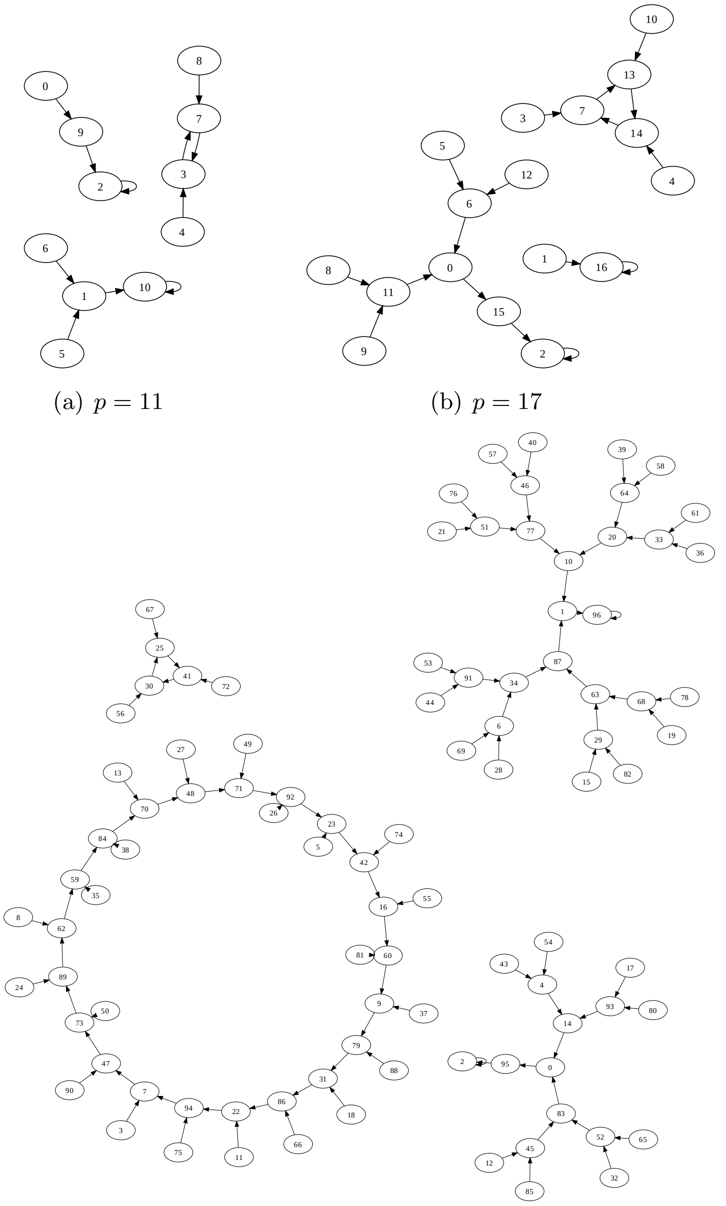
where H_0 is the set of cyclic elements, $H_\ell = \mathbb{Z}_p^*$, and the index of H_i in H_{i+1} is two, for all $0 \le i < \ell$. This requirement on index means that $2\,|H_i| = |H_{i+1}|$ for all $0 \le i < \ell$, which implies $|H_i| = 2^i Q$, since the number of cyclic elements is Q.

We will prove this by constructing these subgroups. Let $H_\ell = \mathbb{Z}_p^*$, and for each $0 \le i < \ell$, let $H_i = f(H_{i+1})$ (and by this we mean $H_i = \{f(x) \mid x \in H_{i+1}\}$). We now need to prove that the H_i are, in fact, subgroups of $\mathbb{Z}_p^*$. Clearly, H_ℓ is a subgroup of $\mathbb{Z}_p^*$ since $H_\ell = \mathbb{Z}_p^*$. We will proceed by induction. Let i be so $0 \le i < \ell$, and assume H_j is a subgroup of $\mathbb{Z}_p^*$ for all $i < j \le \ell$. Since $1 \in H_{i+1}$ and $f(1) = 1$, H_i has an identity. Letting $y_1, y_2 \in H_i$, we will show $y_1 y_2 \in H_i$. There are x_1 and x_2 so $f(x_1) = y_1$ and $f(x_2) = y_2$. Since H_{i+1} is closed under its operation, $x_1 x_2 \in H_{i+1}$, so $f(x_1 x_2) \in H_i$. And,

$$f(x_1 x_2) = (x_1 x_2)^2 = x_1^2 x_2^2 = f(x_1) f(x_2) = y_1 y_2 \in H_i.$$

Thus, H_i is closed under its binary operation. Finally, H_i has inverses. Let $y \in H_i$ and x be so $f(x) = y$. We claim $f(x^{-1})$ is an inverse of y. We see

$$y f(x^{-1}) = x^2 (x^{-1})^2 = (x x^{-1})^2 = 1^2 = 1.$$



(a) $p = 11$

(b) $p = 17$

(c) $p = 97$

Figure 2: Iteration graphs for $f(x) = x^2 - 2$ with various moduli.

Therefore, H_i is a subgroup of H_{i+1}, and likewise a subgroup of $\mathbb{Z}_p^*$. This completes the induction.

This subgroup structure is very closely related to the iteration graph of p when $c = 0$. In fact, H_0 is the union of all the cycles in the graph, and each H_i is the union of all the ith levels of the trees along with the elements of H_{i-1}. As a concrete example, for $p = 19$,

$$\begin{aligned} H_0 &= \{1, 4, 5, 6, 7, 9, 11, 16, 17\} \\ H_1 &= H_0 \cup \{2, 3, 8, 10, 12, 13, 14, 15, 18\}, \end{aligned}$$

and for $p = 17$,

$$\begin{aligned} H_0 &= \{1\} \\ H_1 &= H_0 \cup \{16\} \\ H_2 &= H_1 \cup \{4, 13\} \\ H_3 &= H_2 \cup \{2, 8, 9, 15\} \\ H_4 &= H_3 \cup \{3, 5, 6, 7, 10, 11, 12, 14\}. \end{aligned}$$

This follows from the fact that H_0 consists of all the cyclic elements, and H_i is the set of elements of $\mathbb{Z}_p^*$ with an out-edge which leads into H_{i-1}, for $0 < i \leq \ell$. Another way of looking at the Tonelli algorithm is that it finds a g^k such that, if x is in the trees, then $g^k x$ is in some cycle. The procedure for finding this k involves bringing x toward a cycle level by level.

From this relation between the subgroups and the quadratic iteration graph, we see that the elements of H_i which are not in H_{i-1} have preperiod i. This is an important fact for the following lemma.

Lemma 23. *Let g be a quadratic nonresidue in $\mathbb{Z}_p^*$. If $x \in H_{i+1}$, for $0 \leq i < \ell - 1$, then there is some even exponent k so $g^k x \in H_i$.*

Note that this intentionally does not handle the case when $x \in H_\ell$. Because x is a quadratic residue, we are guaranteed $x \in H_{\ell-1}$.

Proof. Say x is in H_i already. Then, letting $k = 0$, we trivially have $g^k x \in H_i$.

Otherwise, say $x \notin H_i$. We claim that xH_i is not H_i. If it were, then since $1 \in H_i$, $x \in xH_i$, which implies $x \in H_i$, a contradiction. Now, because H_i has index two in H_{i+1}, we have shown that H_i and xH_i are the only two cosets of H_i in H_{i+1}.

We claim that, if $k = 2^{\ell-i-1}$, then g^k is in H_{i+1} and not in H_i. Since g has a preperiod of ℓ, if $0 \leq m \leq \ell$, then $f^{(m)}(g)$ has preperiod $\ell - m$, which is to say $f^{(m)}(g)$ is in $H_{\ell-m}$ but not $H_{\ell-m-1}$. Thus, if $m = \ell - i - 1$, $f^{(\ell-i-1)}(g)$ is in H_{i+1} but not H_i. And, $f^{(\ell-i-1)}(g) = g^k$.

Say $y \in xH_i$. Then $y = xh$ for some $h \in H_i$, which means $xy = x^2 h$. For sake of contradiction, assume $x^2 h \in xH_i$. Then there is an h' so $x^2 h = xh'$, which implies $x = h'h^{-1}$. But, since H_i is a group, this implies $x \in H_i$, a contradiction.

Since g^k is in H_{i+1} but not in H_i, we have that g^k is an element of xH_i, so $g^k x$ is an element of H_i.

And, because $i < \ell - 1$, k is divisible by two. Thus, we have the required even k. □

In more detail, the Tonelli algorithm, then, is that we take some $x \in \mathbb{Z}_p^*$ and check if $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ to see if it is a quadratic residue by Theorem 12. If it is, then $x \in H_{\ell-1}$, and we can iteratively apply Lemma 23. We start with $x_{\ell-1} = x$. For each $0 \leq i < \ell - 1$, we let k_i be the even number such that $x_i = g^{k_i} x_{i+1} \in H_i$. This gives a sequence of even $k_{\ell-2}, k_{\ell-1}, \ldots, k_0$ so that $(g^{k_{\ell-2}} g^{k_{\ell-1}} \cdots g^{k_0})x$ is cyclic. Then, letting $k = k_{\ell-2} \ldots + k_0$, if a is a square root of the cyclic $g^k x$, then $ag^{-\frac{1}{2}k}$ is a square root of x modulo p.

The main difficulty with this algorithm, however, is in finding a quadratic nonresidue, which is a representative element of $H_\ell - H_{\ell-1}$. As we've seen, no part of the described algorithm has used random choices; this is the part which makes the algorithm randomized. If we examine the structure of the iteration graph, we see that the quadratic nonresidues are the leaves of the trees, which means that they are not in H_i for $i < \ell$.

However, since H_i is a group, no multiplication operation can generate a quadratic nonresidue, which are all outside of H_i, so we are either left with having to use the addition operation (and the means of doing so are unclear), or coming up with something else entirely (such as using non-field properties of $\mathbb{Z}_p$).

5 Conclusion

The study of quadratic iteration graphs shows us that squares modulo a prime have a very nice structure. But, going the other way and finding square roots is difficult. Intuitively, this is because the levels of the trees form a subgroup structure on $\mathbb{Z}_p^*$, and multiplicative operations within the ith level of the cycles cannot leave these levels. And, we see that finding square roots of non-cyclic elements and quadratic nonresidues are intimately connected: if one can find arbitrary square roots of non-cyclic elements in polynomial time with respect to $\lg p$, then iterative application of the algorithm ultimately leads to a quadratic nonresidue in polynomial time, since $\ell \approx \lg p$. And, if one has a method of finding quadratic nonresidues in polynomial time, then the Tonelli algorithm described above gives a way of computing square roots in polynomial time.

6 References

Ankeny, N. C. The Least Quadratic Non Residue. The Annals of Mathematics. Vol. 55, No. 1. 1952. pp. 65-72.

Artin, Michael. "Algebra." 2nd ed.

Bach, Eric and Jeffrey Shallit. "Algorithmic number theory. Volume 1. Efficient algorithms."

Niven, Ivan and Herbert S. Zuckerman. "An introduction to the theory of numbers." 5th ed.

Weisstein, Eric W. "Julia Set." From MathWorld–A Wolfram Web Resource.
http://mathworld.wolfram.com/JuliaSet.html