SQUARING GRAPHS MODULO $n$

In a recent Combinatorics seminar, David A. Jackson introduced the following family of directed graphs $\{\Gamma_n\}$: Let $n \in \mathbb{N}$. The vertex set is $V(\Gamma_n) = \mathbb{Z}/n\mathbb{Z}$. The directed edge $(x, y) \in E(\Gamma_n)$ if and only if $y = x^2$. We allow loops and double edges. In particular, for any $n$, the edges $(0, 0)$ and $(1, 1)$ belong to $E(\Gamma_n)$. As for double edges, $(2, 4)$ and $(4, 2)$ are both in $E(\Gamma_7)$.

$\Gamma_n$ consists of some number of connected components. In the seminar, it was proved that each component of $\Gamma_n$ contains a unique cycle. Here, we count a loop as a 1-cycle, and a directed pair of edges as a 2-cycle. There is a directed tree attached to each vertex in a given cycle.

These observations lead to a number of natural questions:

1. How many connected components does $\Gamma_n$ have?
2. What cycle lengths appear in $\Gamma_n$?
3. With what frequency does a particular cycle length appear in $\Gamma_n$?
4. Can we describe the structure of the trees attached to the cycles in $\Gamma_n$?
5. Given $k \in \mathbb{N}$, does there exist an $n$ so that $\Gamma_n$ has a $k$ cycle? If so, what is the smallest such $n$? What is the structure of all such $n$?

Our study attempts to provide satisfactory answers to these questions.

The first three questions are very closely related, and we give relatively complete answers to these. In particular, if we could provide an answer to each of these whenever $n$ is a prime power, then we would have a complete answer for general $n$. In addition, we do have some fairly explicit answers to these questions when $p$ is a prime power.

As for the last question, we are able to show that for any $k$, we can find infinitely many primes $p$ so that $\Gamma_p$ contains a cycle of length $k$. However, we do not know how to estimate the size of the smallest $n$ for which $\Gamma_n$ contains a $k$ cycle.

1. Definitions, Notations, and Basic Results

In a directed graph $G$, the **in-degree of vertex** $v$ is

$$d_-(v) = \# \{ u \in V(G) : (u, v) \in E(G) \}.$$ 

The **out-degree of vertex** $v$ is

$$d^+(v) = \# \{ u \in V(G) : (v, u) \in E(G) \}.$$ 

We say a directed graph is connected if the underlying undirected graph is connected. Likewise, the connected components of a directed graph are defined to be the connected components of the underlying undirected graph. We let $G^v$ denote the connected component of $G$ containing the vertex $v$. 
The directed cycle of length $k$ is denoted by $C_k$. The only word of caution with this definition is that we allow any $k \geq 1$. $C_1$ is the graph of a single vertex $x$ with the edge $(x,x)$. $C_2$ is the graph on vertices $x$ and $y$, with edges $(x,y)$ and $(y,x)$.

**Proposition 1.** Let $n \in \mathbb{N}$.

1. $d^+(x) = 1$ for all $x \in V(\Gamma_n)$.
2. Each connected component of $\Gamma_n$ contains exactly one directed cycle.

**Proof:** The first assertion is obvious. For the second assertion, let $x \in V(\Gamma_n)$. The orbit $x \mapsto x^2 \mapsto x^4 \mapsto x^8 \mapsto \cdots$ must be finite, showing that each connected component contains a directed cycle. One now uses $d^+(x) = 1$ for all $x$ to conclude there cannot be multiple cycles in same connected component. QED

Let $G$ be a graph and $\{H_g\}_{g \in V(G)}$ be a family of graphs. For each $g \in V(G)$, let $\sigma(g)$ be a fixed vertex in $H_g$. We define the product of $G$ and $\{H_g\}$ by $\sigma$,

$$G \times_\sigma \{H_g\}$$

as follows. The vertex set is the union $\bigcup_{g \in G} V(H_g)$. Edges come in two types. For fixed $g \in V(G)$, we have edges of the form $((g,h),(g,h'))$, where $(h,h') \in E(H_g)$. An induced edge from $G$ is of the form $((g,\sigma(g)),(g',\sigma(g')))$, where $(g,g') \in E(G)$. At each vertex of $G$, we place a graph $H_g$. There are edges internal to the $H_g$. There are also edges arising from $G$.

**Proposition 2.** Given a connected component $\Gamma^x_n$ of $\Gamma_n$, there is a directed cycle $C_k$, for some $k$, and a family of trees $\{T_j\}_{j=1}^k$, so that

$$\Gamma^x_n \cong C_k \times_\sigma \{T_j\},$$

for some gluing map $\sigma$.

**Proof:** The previous proposition gives the existence of a unique cycle in $\Gamma^x_n$. Upon removing the edges in the cycle, we are left with a forest, each tree having its root at a vertex on the cycle. QED

This was trivial. Later we will show that in a given connected component, the attached trees are all isomorphic.

For $S \subset \mathbb{Z}/n\mathbb{Z}$ we write $\Gamma_n|_S$ to denote the subgraph of $\Gamma_n$ on the vertex set $S$. It is most natural to consider such subgraphs when $S$ is closed under squaring.

**Proposition 3.** Suppose $\mathbb{Z}/n\mathbb{Z} = S_1 \cup S_2 \cup \cdots \cup S_l$ is a disjoint union of $\mathbb{Z}/n\mathbb{Z}$ into subsets that are each closed under squaring, and let $C$ be a connected component of $\Gamma_n$. Then $C \subset \Gamma_n|_{S_j}$ for some $j$. 
Proof: $C$ contains a unique cycle, say generated by $z$. This cycle is clearly closed under squaring, so the cycle is contained in, say, $S_1$. Let $x$ be in $C$, but not in the cycle generated by $z$. Now, $x$ is in some $S_j$. Also, for some $k$, $x^{2^k} = z$. $S_j$ is closed under squaring, so $z \in S_j$. But $z \in S_1$, and the $S$’s defined a partitioning of $\mathbb{Z}/n\mathbb{Z}$. Therefore, $j = 1$, showing $x \in S_1$ for each $x$ in $C$. QED

When $S = U(n) = \mathbb{Z}/n\mathbb{Z}^*$, the group of units of $\mathbb{Z}/n\mathbb{Z}$, we will simply write $\Gamma_n^*$. We write $\Gamma_n^Z$ to denote $\Gamma_n|_{\mathbb{Z}/n\mathbb{Z}\setminus U(n)}$. It is easy to check that both $U(n)$ and $\mathbb{Z}/n\mathbb{Z}\setminus U(n)$ are closed under squaring.

The previous proposition yields the following useful corollary.

**Corollary 1.** For any $n \in \mathbb{N}$, the connected components of $\Gamma_n$ are partitioned into two classes:

$$\Gamma_n = \Gamma_n^* \cup \Gamma_n^Z.$$

This can be strengthened when $n$ has no repeated prime factors. We need some notation first. Suppose $n = ab$ where $(a,b) = 1$ and $b$ has no repeated prime factor. We may write

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}.$$ 

We let $M_b = \{0, b, 2b, \ldots\} = \mathbb{Z}/a\mathbb{Z} \oplus \{0\}$, the multiples of $b$. We let $M_b^* = (\mathbb{Z}/a\mathbb{Z})^* \oplus \{0\}$. $M_b^*$ is certainly closed under squaring. Now, suppose $(x,y) \in \mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/b\mathbb{Z}$ is not in $M_b^*$. Then either $x \notin U(a)$ or $y \neq 0$. Since $b$ has no repeated prime factors, $y \neq 0$ implies that $y^2 \neq 0$. Thus, we may assume $y = 0$. But in this case, $x \notin U(a)$, so $x$ has a zero divisor, and therefore $x^2$ does as well.

This proves a simple lemma:

**Lemma 1.** Suppose $n = ab$ where $(a,b) = 1$ and $b$ has no repeated prime factor. Then $\Gamma_n$ partitions as

$$\Gamma_n = \Gamma_n|_{M_b^*} \cup \Gamma_n|_{\mathbb{Z}/n\mathbb{Z}\setminus M_b^*}.$$

Iteratively applying the lemma yields

**Corollary 2.** Suppose $n$ has no repeated prime factors. The partition of $\Gamma_n$ into connected components refines the partition

$$\Gamma_n \cong \bigcup_{d|n} \Gamma_d^*.$$

2. The Cycle Structure of $\Gamma_n$

We can give a fairly complete description of the cycle structure of $\Gamma_n$. Given $n \in \mathbb{N}$, we write

$$n = \prod_{p \in \mathcal{P}} p^{m_p},$$

where $m_p$ is the multiplicity of $p$ as a divisor of $n$. We therefore have
Proposition 4. Suppose \( n = a_1 a_2 \) where \((a_1, a_2) = 1\). Suppose \( \Gamma_{a_1} \) has a \( k \) cycle starting at \( x_1 \) and \( \Gamma_{a_2} \) has a \( k_2 \) cycle starting at \( x_2 \). Let \( k = \text{lcm}(k_1, k_2) \). Then \( \Gamma_{a_1 a_2} \) has a \( k \) cycle starting at \((x_1, x_2)\). Conversely, if \((x_1, x_2)\) generates a \( k \) cycle in \( \Gamma_{a_1 a_2} \), then \( x_1 \) generates a \( k_1 \) cycle in \( \Gamma_{a_1} \), \( x_2 \) generates a \( k_2 \) cycle in \( \Gamma_{a_2} \), and \( \text{lcm}(k_1, k_2) = k \).

Proof: We have

\[
x_1 \mapsto x_1^2 \mapsto \cdots \mapsto x_1^{2k_1} = x_1
\]

and

\[
x_2 \mapsto x_2^2 \mapsto \cdots \mapsto x_2^{2k_2} = x_2.
\]

We now show

\[
(x_1, x_2) \mapsto (x_1^2, x_2^2) \mapsto \cdots \mapsto (x_1^{2^l}, x_2^{2^l})
\]

is a cycle of length \( k \). First, write \( k = sk_1 \). Now,

\[
x_1^{2^l} = (x_1^{2k_1})^{(2^l)/2} = x_1^{(2^{k_1})^{l-1}} = \cdots = x_1.
\]

Similarly for \( x_2 \). Thus,

\[
(x_1, x_2)^{2^l} = (x_1, x_2).
\]

Furthermore, suppose \( 0 < t \leq k \) and suppose

\[
(x_1, x_2)^t = (x_1, x_2).
\]

As \( x_1^t = x_1 \), we must have \( k_1|t \). Similarly, \( k_2|t \). Thus, \( \text{lcm}(k_1, k_2)|t \). So, the orbit of \((x_1, x_2)\) has length \( \text{lcm}(k_1, k_2) \).

Now we prove the converse:

\[
(x_1, x_2) \mapsto (x_1^2, x_2^2) \mapsto \cdots \mapsto (x_1^{2^k}, x_2^{2^k}) = (x_1, x_2)
\]

implies that \( x_1^{2^k} = x_1 \) and \( x_2^{2^k} = x_2 \). Let \( k_1 \) and \( k_2 \) be the smallest positive integers so that \( x_1^{2k_1} = x_1 \) and \( x_2^{2k_2} = x_2 \). Then, \( k_1|k \) and \( k_2|k \). Furthermore, if \( \text{lcm}(k_1, k_2) = l < k \), then we would obtain a shorter cycle on \((x_1, x_2)\), contrary to assumption. QED

If \( x \in \Gamma_n \) is contained in a \( k \) cycle, we write \( k_n(x) = k \). If \( x \in \Gamma_n \) is not in a cycle, we let \( k_n(x) = \infty \). The above proposition may be written as follows,

\[
k_{a_1 a_2}((x_1, x_2)) = \text{lcm} (k_{a_1}(x_1), k_{a_2}(x_2)).
\]

where \( x \in \mathbb{Z}/a_1 a_2 \mathbb{Z} \) is identified with \((x_1, x_2) \in \mathbb{Z}/a_1 \mathbb{Z} \oplus \mathbb{Z}/a_2 \mathbb{Z} \).

This gives a simple corollary:

Let \( \text{Cyc} (\Gamma_n) \) denote the set of lengths of cycles that appear in \( \Gamma_n \).

Corollary 3. If \((a_1, a_2) = 1\) then

\[
\text{Cyc} (\Gamma_{a_1 a_2}) = \text{lcm} (\text{Cyc} (\Gamma_{a_1}), \text{Cyc} (\Gamma_{a_2})).
\]
This can be strengthened. Not only do the sizes of cycles in $\Gamma_{a_1}$ and $\Gamma_{a_2}$ relate to those in $\Gamma_{a_1a_2}$, but so do their frequencies. Consider the “cycle frequency function” $f(\cdot; n) : \mathbb{N} \to \mathbb{N} \cup \{0\}$, where $f(j; n)$ denotes the number of cycles of length $j$ in $\Gamma_n$.

**Corollary 4.** If $(a_1, a_2) = 1$ and $k \in \mathbb{N}$, then

$$f(k; a_1a_2) = \sum_{\substack{k_1|k, k_2|k \\text{lcm}(k_1, k_2)=k}} \frac{k_1k_2}{k} f(k_1; a_1)f(k_2; a_2)$$

We have a $k_1$ cycle in $\Gamma_{a_1}$ and a $k_2$ cycle in $\Gamma_{a_2}$. The vertices give us $k_1k_2$ vertices. These vertices are divided into cycles of length $\text{lcm}(k_1, k_2)$. Therefore, the $k_1k_2$ vertices give $\frac{k_1k_2}{\text{lcm}(k_1, k_2)}$ different cycles.

As an example, $\Gamma_7$ has two 1-cycles and a single 2-cycle, $\Gamma_{11}$ has two 1-cycles and a single 4-cycle. Thus, we should expect $\Gamma_{77}$ to contain cycles of lengths 1, 2, and 4. Furthermore, their frequencies are given below:

$$f(1; 77) = \sum_{\substack{k_1|1, k_2|1 \\text{lcm}(k_1, k_2)=1}} \frac{k_1k_2}{1} f(k_1; 7)f(k_2; 11) = f(1; 7)f(1; 11) = 2 \cdot 2 = 4;$$

$$f(2; 77) = \frac{2 \cdot 1}{2} f(2; 7)f(1; 11) = 2;$$

$$f(4; 77) = \frac{1 \cdot 4}{4} f(1; 7)f(4; 11) + \frac{2 \cdot 4}{4} f(2; 7)f(4; 11) = 2 + 2 = 4.$$ 

It may be more natural to consider $g(\cdot; n) : \mathbb{N} \to \mathbb{N} \cup \{0\}$, where $g(j; n)$ denotes the number of vertices contained in cycles of length $j$ in $\Gamma_n$. Thus, $g(j; n) = jf(j; n)$.

The most recent corollary becomes

**Corollary 5.** If $(a_1, a_2) = 1$ and $k \in \mathbb{N}$, then

$$g(k; a_1a_2) = \sum_{\substack{k_1|k, k_2|k \\text{lcm}(k_1, k_2)=k}} g(k_1; a_1)g(k_2; a_2)$$

We also obtain an expression for the total number of connected components in $\Gamma_{a_1a_2}$. First, the number of connected components in $\Gamma_n$ is

$$\sum_{k=1}^{\infty} f(k; n).$$

**Corollary 6.** The number of connected components in $\Gamma_{a_1a_2}$ is equal to

$$\sum_{k=1}^{\infty} f(k; a_1a_2) = \sum_{k_1, k_2} \gcd(k_1, k_2)f(k_1; a_1)f(k_2; a_2).$$
The above discussion shows that understanding the cycle behavior of $\Gamma_n$ can be reduced to understanding the cycle behavior of $\Gamma_{p^a}$, where $p$ is a prime and $a \in \mathbb{N}$. To do this, we use the decomposition

$$\Gamma_{p^a} = \Gamma_p^a \cup \Gamma_{p^a}^Z.$$  

Suppose, then, that $x \in \mathbb{Z}/p^a\mathbb{Z} \setminus U(p^a)$. Then $x$ is a multiple of $p$, say $x = py$. Then $x^{2^s} = p^{2^s}y^{2^s}$, so the orbit of $x$ contains 0. Thus, the cycles in $\Gamma_{p^a}$ come in two varieties. First, there is the cycle based at 0. Then there are the cycles arising from $\Gamma_{p^a}^Z$.

The description of the cycles in $\Gamma_{p^a}^*$ is no more difficult than the description of the cycles in $\Gamma_{p^a}^*$, so we will proceed with general $n$. Given $n$, we let $S_2(n)$ denote the 2-Sylow subgroup of $U(n)$, and we let $T_2(n)$ denote the corresponding complement. Thus, we write

$$U(n) = \bigoplus_p G_p$$

where each $G_p$ is a $p$-group. $S_2(n)$ thus corresponds to $G_2$ whereas $T_2(n)$ corresponds to $\bigoplus_{p \neq 2} G_p$.

We let $t_2(n)$ denote the cardinality of $T_2(n)$. For $x \in U(n)$ we let $o_n(x)$ denote the (multiplicative) order of $x$. $o_n(x)$ is odd if and only if $x \in T_2(n)$. For $a$ an odd integer, we let $\sigma(a) = \sigma_2(a)$ denote the multiplicative order of 2 modulo $a$. If $a$ is even, we adopt the convention that $\sigma(a) = \infty$.

**Proposition 5.** Suppose $x \in \Gamma_n^*$. Then

$$k_n(x) = \sigma_2(o_n(x)).$$

**Proof:** $\sigma_2(o_n(x)) = \infty$ if and only if $o_n(x)$ is even if and only if $x$ is not contained in $T_2(n)$ if and only if $x$ is not contained in a cycle, thus $k_n(x) = \infty$. We therefore restrict attention to $x \in T_2(n)$, i.e., $x$ in a cycle.

Let $k$ denote the length of the cycle generated by $x$. Then

$$x \mapsto x^2 \mapsto \cdots \mapsto x^{2^k} = x.$$  

Therefore, $2^k - 1$ divides the order of $x$ in $U(n)$. Thus,

$$2^k \equiv 1 \mod o_n(x).$$

But then $k$ must be a multiple of the order of 2 in $\mathbb{Z}/o_n(x)\mathbb{Z}$, $\sigma_2(o_n(x))|k_n(x)$, and in particular $\sigma_2(o_n(x)) \leq k_n(x)$. Now consider the path

$$x \mapsto x^2 \mapsto \cdots \mapsto x^{2^{\sigma_2(o_n(x))}}.$$  

By definition, $2^{\sigma_2(o_n(x))} \equiv 1 \mod o_n(x)$. Therefore, $x^{2^{\sigma_2(o_n(x))}} = x$, showing that $k_n(x) \leq \sigma_2(o_n(x))$. We conclude $k_n(x) = \sigma_2(o_n(x))$. QED
Now, assuming that $n$ is a power of prime gives us a bit more information in the above. Namely, for $n = p^a$, $p$ prime and not equal to 2, then $U(p^a) \cong \mathbb{Z}/(p - 1)p^{a-1}\mathbb{Z}$, and therefore $T_2(p^a)$ is a cyclic group of order $t_2(p)p^{a-1}$.

Given $n \in \mathbb{N}$, we let $\kappa(n)$ denote the length of the longest cycle in $\Gamma_n$. Given $m \in \mathbb{N}$, we write

$\text{Div}(m) = \{d \in \mathbb{N} : d|m\}$.

Lemma 2. $\kappa(p^a) = \sigma_2(t_2(p)p^{a-1})$.

Proof: $T_2(p^a)$ is a cyclic group of order $t_2(p)p^{a-1}$. Let $x$ be a generator of this cyclic group. Apply the above proposition with $x$. QED

Lemma 3. If $a|b$ then $\sigma_2(a)|\sigma_2(b)$.

Proof: Let $s = \sigma_2(b)$. So $2^s \equiv 1 \mod b$, and $s$ is the smallest such positive integer. But $a|b$ implies that $2^s \equiv 1 \mod a$. Therefore, $\sigma_2(a)|s$. QED

Proposition 6. Given $n \in \mathbb{N}$,

$\text{Cyc}(\Gamma_n) \subset \text{Div}(\kappa(n))$.

Proof: First, suppose $n = p^a$ for some prime $p$, and suppose $x$ is a cycle in $\Gamma_{p^a}$. Therefore, $x \in T_2(p^a)$ and so $o_{p^a}(x)|t_2(p^a)$. Therefore, $\sigma_2(o_{p^a}(x))|\sigma_2(t_2(p^a))$. That is, $\sigma_2(o_{p^a}(x)) \in \text{Div}(\kappa(n))$.

Now, suppose the proposition is known to be true for $\Gamma_{a_1}$ and $\Gamma_{a_2}$, where $(a_1, a_2) = 1$. Previous propositions show that $\kappa(a_1a_2) = \text{lcm}(\kappa(a_1), \kappa(a_2))$, and

$\text{Cyc}(\Gamma_{a_1a_2}) = \text{lcm}(\text{Cyc}(\Gamma_{a_1}), \text{Cyc}(\Gamma_{a_2}))$.

Now, let $k \in \text{Cyc}(\Gamma_{a_1a_2})$. There exist $x_1$ and $x_2$ in their respective $\Gamma$’s, with cycles of lengths $k_1$ and $k_2$ respectively, where $\text{lcm}(k_1, k_2) = k$. Now, $k_1|\kappa(a_1)$ and $k_2|\kappa(a_2)$. Therefore, $\text{lcm}(k_1, k_2)|\text{lcm}(\kappa(a_1), \kappa(a_2))$.

These two cases inductively prove the proposition. QED

Typically, $\text{Cyc}(\Gamma_n)$ is a proper subset of $\text{Div}(\kappa(n))$. I do not know how to classify which divisors of $\kappa(n)$ belong to $\text{Cyc}(\Gamma_n)$.

Next, we prove that there are no forbidden cycle lengths. Specifically, we prove

Theorem 1. Let $k \in \mathbb{N}$. There exist infinitely many primes $p$ so that $k \in \text{Cyc}(\Gamma_p)$.

Proof: The proof is in two steps. First, we show that $\sigma_2$ maps the odd integers onto $\mathbb{N}$. This follows from direct calculation:

$\sigma_2(2^k - 1) = k$. 

Let $a_k$ denote some odd integer satisfying $\sigma_2(a_k) = k$. (For practical purposes, $2^k - 1$ grows too fast. We just use $2^k - 1$ to give a simple argument that such an $a_k$ always exists. Usually, one can find much smaller $a_k$'s.)

Now, from one of the above propositions, it is enough to show there is a prime $p$ and an $x \in \Gamma_p^*$ so that

$$o_p(x) = a_k.$$  

For then,

$$k_p(x) = \sigma_2(o_p(x)) = \sigma_2(a_k) = k.$$  

Dirichlet's Theorem on primes in arithmetic progressions guarantees the existence of infinitely many primes $p$ satisfying

$$p \equiv 1 \mod a_k.$$  

Thus, $p - 1 = ma_k$ for some integer $m$. Write $m = 2^s t$ where $t$ is odd. Then $p - 1 = 2^s (t a_k)$, and so $t_2(p) = t a_k$. Let $y$ be a generator of $T_2(p)$, and let $x = y^t$. Then the order of $x$, as an element of $T_2(p)$ is $a_k$. This is the same as the order of $x$ viewed as an element of $U(n)$, so $o_p(x) = a_k$. QED

3. The Tree Structure of $\Gamma_n$  

At each vertex $x \in \Gamma_n$ which is contained in a cycle, there is a directed tree with root at $x$. We let $\tau(x; n)$ denote this tree. If $y \in \tau(x; n)$, the depth of $y$ in $\tau(x; n)$ is the natural number $k$ so that $y^{2^k} = x$. We say $x$ has depth 0 in $\tau(x; n)$.

Similar to the cycle structure, we can describe the tree structure of $\Gamma_n$ in terms of the structures of $\Gamma_{p^a}$ for the maximal prime power divisors of $\Gamma_{p^a}$. The description, however, is a bit more complicated, in that the cycle structure of $\Gamma_n$ only depended on the cycle structure of the $\Gamma_{p^a}$'s, whereas the tree structure of $\Gamma_n$ depends on the tree and cycle structures in the $\Gamma_{p^a}$'s.

**Proposition 7.** For $x \in T_2(n)$, $\tau(x; n) \cong \tau(1; n)$.

We define an isomorphism

$$\psi_x : \tau(1; n) \to \tau(x; n),$$

graded by the depths of the trees, as follows: Given $\omega \in \tau(1; n)$ at depth $d$, we let $\psi_x(\omega) = \omega x^{2^{-d}}$, where $x^{2^{-d}}$ is obtained by moving $d$ steps backwards along $x$'s cycle. Now,

$$\left(\omega x^{2^{-d}}\right)^{2^d} = \omega^{2^d} x = x.$$  

Suppose now that at some intermediate stage, $\omega x^{2^{-d}}$ is in $x$'s cycle. Then

$$\omega^{2^t} x^{2^{-d}} = x^{2^t}.$$
for some $t$ and therefore $\omega^{2t}$ is contained in $x$’s cycle. But, for $s < d$, $\omega^{2t}$ is contained in $\tau(1; n) \setminus \{1\}$, a contradiction. Therefore, $\psi_x(\omega)$ is contained in $\tau(x; n)$ and has depth $d$. Suppose now that $\omega$ and $\eta$ are in $\tau(1; n)$ and

$$
\psi_x(\omega) = \psi_x(\eta).
$$

It follows that there respective depths are equal, say to $d$. Then

$$
\omega x^{2-d} = \eta x^{2-d},
$$

therefore $\omega = \eta$. This shows

$$
\tau(1; n) \hookrightarrow \tau(x; n).
$$

Now, for $x \in U(n)$, $x$ is in a cycle if and only if $x \in T_2(n)$, and at each such $x$ there is attached a tree $\tau(x; n)$ which contains an isomorphic copy of $\tau(1; n)$. We have

$$
|T_2(n)||S_2(n)| = |U(n)| = \sum_{x \in T_2(n)} |\tau(x; n)| \geq t_2(n)|\tau(1; n)|,
$$

with equality if and only if $|\tau(x; n)| = |\tau(1; n)|$ for all $x \in T_2(n)$. Thus, it is sufficient to show $|S_2(n)| = \tau(1; n)$, But, for $y \in U(n)$, $y \in S_2(n)$ if and only if the order of $y$ is a power of $2$, if and only if $y \in \tau(1; n)$. QED

The last line of the above proof in fact gives something stronger. With $S_2(n)$ being a 2-group, there exist integers $m_1 \geq m_2 \geq \cdots \geq m_h$ so that

$$
S_2(n) \cong \bigoplus_{j=1}^{h} \mathbb{Z}/2^{m_j}\mathbb{Z}.
$$

Let $\iota$ be the isomorphism mapping $S_2(n)$ to this product of cyclic groups. The depth of the tree $\tau(1; n)$ coincides with $m_1$, and more generally, the entire structure of $\tau(1; n)$ is that of this direct sum of cyclic 2-groups.

Suppose $x \in V(\Gamma_n)$. We write $d_\iota^-(v)$ to denote the in-degree of $v$ restricted to the tree containing $v$. Thus, if $v$ is not in a cycle, $d_\iota^-(v) = d_\iota^-(v)$. If $v$ is contained in a cycle, then $d_\iota^-(v) = d_\iota^-(v) - 1$.

**Corollary 7.** For $p$ an odd prime, $\tau(1; p^s)$ is a dyadic tree of depth $s_2(p) = s_2(p^s)$. Let $V_0 \cup V_1 \cup \cdots \cup V_s$ be a grading of the vertices of $\tau(1; p)$ into depths. Then

$$
\left\{
\begin{array}{ll}
1, & v \in V_0; \\
2, & v \in V_1 \cup V_2 \cup \cdots \cup V_{s-1}; \\
0, & v \in V_s.
\end{array}
\right.
$$

**Proof:** $(\mathbb{Z}/p^n\mathbb{Z})^*$ is a cyclic group of order $(p-1)p^{n-1}$. Let $g$ be a generator and $h = g^{2(p^n)}$. Given any $1 \leq i \leq 2^s$, where $s = s_2(p)$, we have

$$
h^i \mapsto (h^i)^2 \mapsto (h^i)^4 \mapsto \cdots \mapsto (h^i)^{2^s} = 1,
$$
possibly the path reaches 1 earlier. This gives \(|S_2(p^a)|\) distinct elements in \(\tau(1, p^a)\), which therefore exhausts the tree. Now let \(v \in \tau(1, p^a)\), and write \(v = h^i\), where \(0 \leq i \leq 2^s - 1\). If \(i = 0\), then both \(h^0\) and \(h^{2^s-1}\) square to give \(h^0\). But we only include the latter in the tree. So \(d^\tau(h^0) = 1\). For \(i = 2j, 1 \leq j \leq 2^{s-1} - 1\), both \(h^j\) and \(h^{j+2^{s-1}}\) square to \(h^i\), so \(d^\tau(v) \geq 2\) if \(v \in V_1 \cup V_2 \cup \cdots \cup V_{d-1}\). Now, the number of vertices in \(\tau(1; p^a)\) is \(2^s\). \(|V_0| = 1, |V_s| = 2^{s-1}, |V_1 \cup V_2 \cup \cdots \cup V_{s-1}| = 2^{s-1} - 1\). Therefore,

\[
2^s = \sum_{v \in \tau(1; p^a)} d^\tau(v) = \sum_{v \in \tau(1; p^a)} d^\tau(v) \geq 2 \cdot 2^{s-1},
\]

with equality if and only if \(d^\tau(h^i) = 2\) for all even \(i \in \{1, 2, \ldots, 2^s - 1\}\) and \(d^\tau(h^i) = 0\) for all odd \(i\). QED

The fact that \(U(p^a)\) is cyclic for \(p \neq 2\) is essential to this proof. In particular, the conclusion of the corollary is false for \(p = 2\). We should be able to give an explicit description of \(\tau(1; 2^a)\), using the fact that

\[
U(2^a) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a-2}\mathbb{Z}
\]

for \(a \geq 2\).

**Proposition 8. The structure of \(\tau(1; 2^a)\)**

**Proof:** First, \(\Gamma^*_a\) is connected. To see this, write \(U(2^a) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a-2}\mathbb{Z}\), provided \(a \geq 2\). Then squaring in \(U(2^a)\) can be actualized by multiplying by 2 in \(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a-2}\mathbb{Z}\). \(2^{a-2}\) annihilates each element of this group, thus, there is but one connected component. The source vertices in \(\tau(1; 2^a)\) correspond to the vertices of the form \((1, x)\). (A source vertex is one with \(d^\tau(v) = 0\).) Suppose \(a > 2\). \(V_{a-2}\) then contains \(2^{a-2}\) vertices, each vertex being a source vertex. For each \(1 < d < a - 2\), \(V_d\) has \(2^d\) vertices, exactly half of which are source vertices. \(V_1\) has three vertices, two of which are sources, and \(V_0\) has a single vertex.

This only leaves \(\Gamma^*_{2^a}\) and \(\Gamma^*_4\). \(\Gamma^*_{2^a}\) consists of a single loop with no edges. \(\Gamma^*_4\) consists of a single edge attached to a loop. QED

The above describes the tree structure of \(\Gamma^*_p\). We’ve already pointed out that \(\Gamma^Z_p\) is connected, with root at \(x = 0\). We now describe \(\tau(0; p^a)\).

**Proposition 9. The depth of \(\tau(0; p^a)\) is \([\log_2(a)]\).**

Any vertex in \(\tau(0; p^a)\) is a multiple of \(p\). It follows that the path with source at \(p\) has maximal length in \(\tau(0; p^a)\). This path is given by

\[
p \mapsto p^2 \mapsto p^{2^2} \mapsto \cdots p^{2^{[\log_2(a)]}} = 0.
\]

QED
Given a directed, rooted tree \( \tau \), we write \( V_j(\tau) \) for the vertices whose distance to the root is equal to \( j \).

**Proposition 10.** Suppose that \( n = a_1a_2 \), where \((a_1, a_2) = 1 \), and suppose \( x_1 \in \Gamma_{a_1}\) and \( x_2 \in \Gamma_{a_2} \) are each contained in cycles. Then

\[
V_k(\tau((x_1, x_2); a_1a_2)) = \bigcup_{j_1, j_2 \geq 0, j_1+j_2 \leq k} (V_{k-j_1}(\tau(x_1^{2^{-j_1}}))) \times (V_{k-j_2}(\tau(x_2^{2^{-j_2}}))).
\]

**Proof:** For \( 0 \leq j_1 \leq k \), let \( z_1 = x_1^{2^{-j_1}} \), so that \( z_1^{2^{j_1}} = x_1 \). Now let \( w_1 \in V_{k-j_1}(\tau(z_1; a_1)) \), so that \( w_1^{2^{k-j_1}} = z_1 \). Then

\[
w_1^{2^k} = (w_1^{2^{k-j_1}})^{2^{j_1}} = z_1^{2^{j_1}} = x_1.
\]

Similarly, define \( j_2, z_2 \) and \( w_2 \). Then \((w_1, w_2)^{2^k} = (x_1, x_2) \). Now let \( C \) denote the cycle generated by \((x_1, x_2)\). Not all such \((w_1, w_2)\)'s obtained as above lie in \( \tau((x_1, x_2); a_1a_2) \). In order for \((w_1, w_2) \in \tau((x_1, x_2); a_1a_2) \), we require that \((w_1, w_2)^{2^m} \not\in C \) for \( m < k \). Suppose now that neither \( j_1 \) nor \( j_2 \) is zero. Without loss of generality, suppose \( 0 < j_1 < j_2 \). Then \((w_1, w_2)^{2^{k-j_1}} \in C \). Therefore, if \((w_1, w_2) \in \tau((x_1, x_2), a_1a_2) \), then at least one of \( j_1 \) or \( j_2 \) must be zero, and if at least one of \( j_1 \) or \( j_2 \) is zero, then \((w_1, w_2) \in \tau((x_1, x_2), a_1a_2) \). QED

**Corollary 8.** The maximal tree depth in \( \Gamma_{a_1a_2} \) is the maximum of the maximal tree depths in \( \Gamma_{a_1} \) and \( \Gamma_{a_2} \).

**Proposition 11.** Suppose \( x \) and \( y \) are in \( \Gamma_n \), both \( x \) and \( y \) are vertices on the same cycle. Then \( \tau(x; n) \cong \tau(y; n) \).

**Proof:** Suppose first that \( n = p^a \). Then either \( x \) and \( y \) are both zero, in which case the result is vacuous, or else \( x \) and \( y \) are both in \((\mathbb{Z}/p^a\mathbb{Z})^*, \) in which case an above corollary applies, provided \( p \neq 2 \). \( \Gamma_{2^a} \) contains exactly two cycles, each of length 1, so again the result is vacuous in this case.

Suppose now that \( n = a_1a_2 \), where \((a_1, a_2) = 1 \), and suppose the conclusion of the proposition is true for both \( \Gamma_{a_1} \) and \( \Gamma_{a_2} \). The above proposition describes the structure of \( \tau((x_1, x_2); a_1a_2) \) in terms of the structures of trees attached to single cycles in \( \Gamma_{a_1} \) and \( \Gamma_{a_2} \), respectively. The result follows. QED