# The average connectivity of a family of expander graphs

Patrick Bahls
Department of Mathematics
University of North Carolina, Asheville, NC 28804
pbahls@unca.edu

**Abstract**

We compute the limiting average connectivity $\bar{\kappa}$ of the family of 3-regular expander graphs whose members are formed from the finite fields $\mathbb{Z}_p$ by connecting every $x \in \mathbb{Z}_p$ with $x \pm 1$ and $x^{-1}$, all computations performed modulo $p$. Namely, we show

$$\lim_{p \to \infty} \bar{\kappa}(\mathbb{Z}_p) = 3$$

for primes $p$. We compare this behavior with an upper bound on the expected value of $\bar{\kappa}(\mathbb{Z}_n)$ for a more general class $\{\mathbb{Z}_n\}_{n \in \mathbb{N}}$ of related graphs.

## 1 Introduction

In [2], Beineke, Oellermann, and Pippert defined the *average connectivity* of a finite graph in order to generalize connectivity by giving a more robust measure of a graph's integrity.

Let $G = (V, E)$ be a finite undirected graph. We denote by $uv$ the edge from $u$ to $v$, or by $\langle u, v\rangle$ only when simply juxtaposition might cause confusion. Given $u \neq v \in V$, an alternating sequence $p = (u = u_0, e_1, u_1, ..., e_n, u_n = v)$ of consecutively incident vertices and edges is called a $(u, v)$-*path of length* $n$ if $i \neq j \Rightarrow u_i \neq u_j$. Any collection $P(u, v)$ of such paths will be called *disjoint* if $p \neq q \in P(u, v) \Rightarrow p \cap q = \{u, v\}$. We then define

$$\kappa_G(u, v) = \max\{|P| \mid P = P(u, v) \text{ is disjoint}\}.$$

From this, the *connectivity* of $G$ is defined by

$$\kappa(G) = \min\{\kappa_G(u, v) \mid u \neq v \in V\},$$

giving the smallest number of edges whose removal will result in separation of two or more remaining vertices.

A more "global" measure of connectivity is given by the average connectivity,

$$\bar{\kappa}(G) = \frac{1}{\binom{|V|}{2}} \sum_{u \neq v \in V} \kappa_G(u, v),$$

giving the expected number of edges one would have to remove to disconnect distinct vertices selected uniformly randomly. For instance, while $\kappa(K_n) = \bar{\kappa}(K_n) = n - 1$ for a complete graph $K_n$ on $n$ vertices, if $K_n^*$ is formed from $K_n$ by adding a single edge incident to one of the original vertices, $\kappa(K_n^*) = 1$ while $\bar{\kappa}(K_n^*) = \frac{n^2-2n+3}{n+1} \approx n-2$ gives a better amortized picture of the graph's structure.

In this paper we investigate the behavior of $\bar{\kappa}$ as applied to a family of *expander graphs*, $\{\mathbb{Z}_p\}_{p \text{ prime}}$, defined by $\mathbb{Z}_p = (V, E)$,

$$V = \{0, 1, ..., p-1\}, E = \left\{x(x \pm 1), xx^{-1} \mid x \in V\right\},$$

where all computations are modulo $p$ and we define $0^{-1} = 0$. The resulting graph, though not simple, is 3-regular, if one defines the *degree* of a vertex to be the number $d(v)$ of undirected edges incident to it.

**Note.** This notion of degree contrasts from the usual one in that here a self-loop contributes only a single edge, rather than 2, to the degree of the vertex incident to it.

Like other expander graph families, this collection of graphs enjoys properties that make it useful in coding theory, random number generation, network design, statistical modeling, and myriad other mathematical settings. For more information on expander graphs, the reader should consult the excellent survey article [5] by Hoory, Linial, and Wigderson; for our purposes it is enough to know that expanders are highly, yet efficiently, well-connected. Just how well-connected we hope to measure using $\bar{\kappa}$.

It is obvious that in computing $\bar{\kappa}$ no pair of vertices can contribute a quantity greater than the minimum of the pair's vertex degrees. Thus, since each $\mathbb{Z}_p$ is 3-regular, we hope that $\bar{\kappa}(\mathbb{Z}_p) \approx 3$. In fact, we will prove

**Theorem 1.1.** *Let $\mathbb{Z}_p$ be the graph defined as above. Then* $\lim_{p \to \infty} \bar{\kappa}(\mathbb{Z}_p) = 3$.

In order to obtain this fact, we need to find a way of navigating through the graphs $\mathbb{Z}_p$, and of enumerating the paths we find in our travels. This involves a few number theoretic facts in which both the distribution of inverses modulo $p$ and properties of quadratic residues play important roles.

We note that the connectivity $\kappa(\mathbb{Z}_p) = 2$ for all primes $p$, since we need only remove two edges, $\langle 0, 1\rangle$ and $\langle p-1, 0\rangle$, in order to obtain two connected components.

In the concluding section we will compare the behavior of $\mathbb{Z}_p$, $p$ prime, with that of a class of more general graphs $\mathbb{Z}_n$, for arbitrary $n \in \mathbb{N}$.

## 2 Paths in $\mathbb{Z}_p$

Let us first examine the coarse structural elements of $G = \mathbb{Z}_p = (V, E)$, particularly those of $E$.

We realize $\mathbb{Z}_p$ geometrically as a circle subdivided $p$ times, and for each edge $xx^{-1}$ we include a straight line segment interior to the circle between the appropriate vertices. These interior edges we will call *chords*, the remaining edges, *boundary* edges. When considered in sequence, chords may be take on a natural orientation, as we will see below. For the purpose of computing average connectivity, we have no need for self-loops or multiple edges. Therefore, we may discard the loops at the vertices $\{0, 1, p-1\}$, and should $x^{-1} = x \pm 1$, we may remove one of the edges incident these two vertices, leaving a single boundary edge between them. In our modified, now simple, graph, each vertex $v$ has degree $d(v) \in \{2, 3\}$, so every pair $\{u, v\}$ will contribute either 2 or 3 to $\bar{\kappa}(\mathbb{Z}_p)$, since traversing the boundary in either direction from $u$ to $v$ gives two paths.

For our first lemma and throughout, we remind the reader of the *Legendre symbol* $\left(\frac{a}{b}\right)$, which we will need only for positive integers. We let $\left(\frac{a}{b}\right) = 1, -1$ according as whether $a$ is a quadratic residue modulo $b$ or not. That is, $\left(\frac{a}{b}\right) = 1$ if and only if the equation $x^2 \equiv a \bmod b$ has a solution in the ring $\mathbb{Z}_b$. (For more number theoretic details, please consult [6].)

**Lemma 2.1.** *Let $p \geq 11$ be prime. Then if $p \equiv 2, 3 \bmod 5$, $\mathbb{Z}_p$ has 3 vertices of degree 2; if $p \equiv 1, 4 \bmod 5$, $\mathbb{Z}_p$ has 7 vertices of degree 2.*

*Proof.* Every $\mathbb{Z}_p$ has at least 3 vertices of degree 2, namely $\{0, 1, p-1\}$. The only other such vertices arise from pairs $\{x, x^{-1} = x + 1\}$, where without loss we assume $x < x^{-1}$.

Should such vertices appear, $x(x + 1) = x^2 + x \equiv 1 \bmod p$, so the quadratic equation $x^2 + x - 1 \equiv 0 \bmod p$ is solvable. Since $(4, p) = 1$, $4x^2 + 4x - 4 \equiv 0 \bmod p$ is also solvable. Completing the square we obtain the equation $(2x + 1)^2 \equiv 5 \bmod p$, which is solvable if and only if $\left(\frac{5}{p}\right) = 1$. However, quadratic reciprocity implies that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. Yet $\left(\frac{p}{5}\right) = 1$ if and only if $p \equiv 1, 4 \bmod 5$, so we obtain new vertices of degree 2 only in these cases, and here the frequency of quadratic residues gives two new pairs of such vertices, giving us a total of 7 should $p \equiv 1, 4 \bmod 5$ hold. □

Of importance will be the way in which chords intersect. A *chord component* (or simply *component*) is a collection $C$ of chords, maximal with respect to the following property:

$$c \in C \Rightarrow \text{ there exists } c' \in C, c' \neq c, \text{ such that } c \cap c' \neq \emptyset.$$

We may abuse this notation by using "component" to refer also to the vertices incident to edges of $C$.

Given $\mathbb{Z}_p$, the number of chord components in $E$ will be very small, as we will see in the next section. For now, let us prove the following

**Proposition 2.2.** *If $u, v \in V$ lie in the same chord component, then $\kappa_G(u, v) = 3$.*

*Proof.* Given $u, v \in C$, we must describe how to obtain 3 vertex-disjoint paths from $u$ to $v$.

Begin by selecting from $C$ a shortest sequence of chords $P = (c_1, c_2, ..., c_k)$ such that $c_i = \langle \iota_i, \tau_i \rangle$ $(i = 1, ..., k)$, $\iota_1 = u$, $\tau_k = v$, and $c_i$ crosses $c_{i+1}$ $(i = 1, ..., k-1)$. (That is, $c_i$ and $c_{i+1}$ intersect as straight segments in the plane.) Note that endpoints of consecutive chords are not necessarily adjacent as vertices in $G$. Note also that chords carry a natural orientation: for $i \geq 2$ the boundary of the entire graph is divided into two components by removing the vertices $\iota_{i-1}$ and $\tau_{i-1}$. Then $\iota_i$ lies in the component of the graph's boundary that does not contain the endpoints of $c_{i+1}$. In this manner the chords in the path $P$ are "directed" from $u$ to $v$.

All three paths we construct will make use only of chords from this *chord path*, as well as certain boundary edges.

Consider the chord path $P$ lying in $\mathbb{Z}_{31}$ shown in Figure 1 (all other chords are omitted for clarity); we describe the manner in which its chords intersect. The transition $c_i \to c_{i+1}$ constitutes a *left turn* if one of the following conditions is met:

1. $\iota_i < \iota_{i+1} < \tau_i$ (in which case either $\tau_{i+1} < \iota_i$ or $\tau_{i+1} > \tau_i$) or

2. $\tau_i < \tau_{i+1} < \iota_i$ (in which case either $\iota_{i+1} < \tau_i$ or $\iota_{i+1} > \iota_i$).

In any other case, the transition $c_i \to c_{i+1}$ is a *right turn*.

In our example, the transition from $c_1 = \langle 8, 4 \rangle$ to $c_2 = \langle 6, 26 \rangle$ is a right turn, because $\tau_1 < \iota_1$ but $\tau_2$ is not between these two values. Similarly, we have a right turn from $c_2$ to $c_3 = \langle 29, 15 \rangle$ since $\iota_2 < \tau_2$ while $\iota_3$ is not between these values. The transition from $c_3$ to $c_4 = \langle 11, 17 \rangle$ is a left turn, however, since $15 < 17 < 29$.

Any maximal subsequence of consecutive chords $S = (c_m, ..., c_n) \subseteq P$ in which every intervening turn is of the same type is called a *segment* in the path $P$. In our example, $P$ has two segments, $(c_1, c_2, c_3)$ and $(c_4)$.

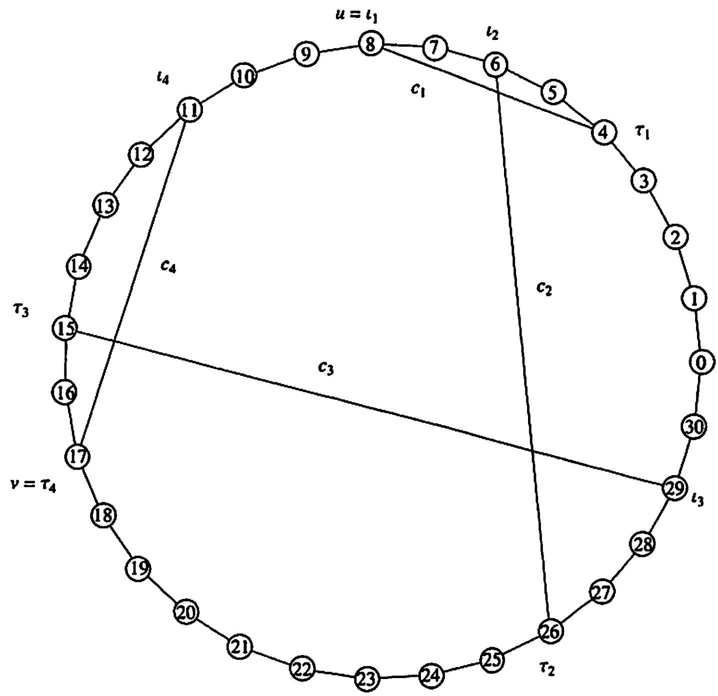


Figure 1: A chord path

To each segment $S$ of $P$ there corresponds a subset $\partial S$ of the graph's boundary edges. With $S$ as above,

$$\partial S = [\tau', \iota_{m+1}] \cup [\tau_m, \iota_{m+2}] \cup [\tau_{m+1}, \iota_{m+3}] \cup \cdots \cup [\tau_{n-2}, \iota_n],$$

where $[u, v]$ denotes the collection of boundary edges between $u$ and $v$, with the obvious orientation. Also, $\tau'$ is the final vertex of the preceding segment in $P$; if $S$ is the first segment, $\tau' = \iota_1$. (If $m = n$, $\partial S = \emptyset$.) We call the collection of edges contained in a segment $S$ together with its boundary $\partial S$, the *leg* corresponding to $S$.

**Lemma 2.3.** *Let $P$ be a chord path with $N$ segments, $S_1, S_2, ..., S_N$, and let $\tau_j'$ denote the final vertex in the $j$th segment. Denote by $\overline{\partial S}$ the traversal of $\partial S$ in the orientation opposite that given above.*

1. *If $N$ is odd and $P$ begins with a right turn, the following vertices appear on the boundary of $G$ in the order given, reading clockwise from the initial vertex of $S_1$:*

$$\partial S_1, \partial S_3, ..., \partial S_N, \overline{\partial S}_{N-1}, \overline{\partial S}_{N-3}, ...\overline{\partial S}_2.$$

*If $N$ is even, the ordering reads instead*

$$\partial S_1, \partial S_3, ..., \partial S_{N-1}, \overline{\partial S}_N, \overline{\partial S}_{N-2}, ..., \overline{\partial S}_2.$$

*If $P$ begins with a left turn, the above give a counterclockwise listing of the same vertices.*

2. *Let $\iota_j$ denote the initial vertex of $S_j$, and let $\tau_j''$ denote the endpoint of the penultimate chord in $S_j$, should $S_j$ have more than one chord. Then if $P$ begins with a right turn, the vertices $\iota_j$ and $\tau_j''$ appear within the order given above as follows:*

$$...\partial S_j, \tau_j'', \iota_{j+2}, \partial S_{j+2}, ..., \overline{\partial S}_k, \iota_k, \tau_{k-2}'', \overline{\partial S}_{k+2}, ....$$

*As before, if $P$ begins with a left turn, this listing gives a counterclockwise ordering.*

*Proof.* This lemma is easily proven by induction on $N$, simply by applying the definitions both of $P$ and $S_j$, and of right and left turns. ☐

We may describe an edge path $p$ in the graph by the manner in which it traverses each leg of $P$, tacitly applying Lemma 2.3 where needed.

Let $S_j = (c_1, ..., c_n)$ be the $j$th segment in $P$. Our path $p$ begins at $\iota_1$. We may first follow $c_1$ to $\tau_1$, and from here travel along the boundary edges $[\tau_1, \iota_3]$ to $\iota_3$. From here, we follow $c_3$ to $\tau_3$, and then proceed along the boundary to $\iota_5$, and so forth. If $S$ has even length $n$, the $S$-portion of the path $p$ will proceed in this fashion until we conclude by crossing $c_{n-1}$ to $\tau_{n-1}$, from which we may follow the boundary from to the initial vertex of the segment $S_{j+2}$, omitting $S_{j+1}$. A similar traversal of $S_{j+2}$ may proceed from there. If $n$ is odd, we conclude by crossing $c_n$ to $\tau_n$, putting us in a place to begin a traversal of $S_{j+1}$ as described in the next paragraph. We refer to the above method of traversing a segment as a *chord-first traversal*, or simply a *C-traversal.*

Alternatively, we may begin along the boundary $\partial S$, at the terminal vertex $\tau'$ of the previous segment, $S_{j-1}$. We proceed along the boundary edges $[\iota_1, \iota_2]$, from there crossing $c_2$ to $\tau_2$, then once more returning to the boundary, and so forth. If $n$ is odd, we follow the boundary to the initial vertex of $S_{j+2}$, omitting $S_{j+1}$, ready to begin a C-traversal of $S_{j+2}$. If $n$ is even, we end at $\tau_j'$ and are in position to begin a traversal of $S_{j+1}$ as just described. This sort of traversal will be called *boundary-first*, or a *B-traversal.*

As above, if a path $p$ traverses neither a segment's chords nor its boundary, we say the path is an *omission* that segment. Note that the first segment $S_1$ can be omitted by proceeding from its initial vertex $\iota_1$ to the initial vertex of $S_2$.

We are almost ready to describe our disjoint paths. Suppose $P$ has $N$ segments, and let $s : \{1, 2, ..., N\} \to \{E, O\}$ be defined by $s(j) = E$ if $S_j$ has even length, and $s(j) = O$ otherwise. We now define three edge paths in the following fashion:

1. $p$ is given by a sequence $\{p(j)\}_{j=1}^{N}$ in $\{B, C, -\}$, these symbols indicating, respectively, a B-traversal, a C-traversal, or an omission, of the corresponding segment.
2. If $p(j) = B$ and $s(j) = E$, then $p(j + 1) = B$.
3. If $p(j) = B$ and $s(j) = O$, then $p(j + 1) = -$.
4. If $p(j) = C$ and $s(j) = E$, then $p(j + 1) = -$.
5. If $p(j) = C$ and $s(j) = O$, then $p(j + 1) = B$.
6. If $p(j) = -$, then $p(j + 1) = C$.

**Lemma 2.4.** *The rules given above define edge paths in $G$.*

*Proof.* The above rules are defined precisely in order to ensure we obtain a path. For instance, after a B-traversal of an even-length segment $S_j$, we end at $\tau_j'$, poised to B-traverse $S_{j+1}$. The other transitions are just as easily checked. □

**Lemma 2.5.** *Any path $p$ satisfying (1)-(6) above is completely determined by its first coordinate. Moreover, if $p(1) \neq q(1)$, then $p$ and $q$ overlap only at their initial and terminal points, $u$ and $v$.*

*Proof.* A glance at the rules shows that they are completely deterministic, so $p(j + 1)$ depends entirely on $p(j)$, and thus inductively $p$ depends only on $p(1)$. Because of the way B- and C-traversals and omissions are defined, $p$ and $q$ will be disjoint if we can show that $p(j) \neq q(j)$ for all $j$, should $p(1) \neq q(1)$ hold.

Inductively, assume that $p(j) \neq q(j)$ for some $j$. If $s(j + 1) = E$, Rules (2), (4), and (6) ensure that $p(j+1) \neq q(j+1)$. If $s(j+1) = O$, Rules (3), (5), and (6) play the same role, so in either case $p(j + 1) \neq q(j + 1)$. □

Lemmas 2.4 and 2.5 together imply the existence of three mutually disjoint edge paths from $u$ to $v$: each is determined by a sequence in $\{B, C, -\}$ beginning with a different symbol.

This concludes the proof of Proposition 2.2. □

# 3 Component structure

Our goal is to show that nearly every vertex of degree 3 lies in the same chord component of $G = \mathbb{Z}_p$.

Our first easy fact is the following lemma, whose proof uses the symmetry of the graph $G$ across an imaginary line drawn from 0 to the midpoint of $[\frac{p-1}{2}, \frac{p+1}{2}]$. If we place 0 at the rightmost extremum of the graph and number in a counterclockwise fashion, our symmetry axis is horizontal. We call the portion of $G$ above this axis the *top half*, $G_t$, of the graph, the *bottom half* $G_b$ defined similarly. Note $G_t \cap V = \{1, 2, ..., \frac{p-1}{2}\}$ and $G_b \cap V = \{\frac{p+1}{2}, ..., p-2, p-1\}$.

**Lemma 3.1.** *Let $C$ be a component and let $u \in C$ satisfy $u \in G_t \Leftrightarrow u^{-1} \in G_b$. Then $v \in C \Leftrightarrow p - v \in C$ for all vertices $v \in C$.*

*Proof.* This follows from the fact that the chords $\langle u, u^{-1}\rangle$ and $\langle p-u, p-u^{-1}\rangle$ intersect. □

The same symmetry shows that for every component contained entirely in $G_t$ (resp. $G_b$), there is another contained entirely in $G_b$ (resp. $G_t$). Our next step is to constrain the size and number of these components; by symmetry we will work only with components lying entirely in $G_t$.

**Proposition 3.2.** *Let $C \subsetneq G_t$ be a component. Then $|C| = O(\sqrt{p})$.*

To prove this result we will need some probabilistic results indicated by Gonek, Krishnaswami, and Sondhi in [4]. As in that paper, given a prime $p$, an integer $H < p$, and integers $M, N$ such that $[M, M+N) \subseteq (0, p)$, we let

$$f(m, H) = |\{n \in [m, m+H) \mid n^{-1} \bmod p \in [M, M+N)\}|,$$

for $0 \le m \le p-1$.

**Note.** The value $f(m, H)$ gives the number of elements in the interval $[m, m+H)$ of length $H$ that are inverses (modulo $p$) of elements in the fixed interval $[M, M+N)$. For instance, if $f(m, H)$ is large, the interval $[m, m+H)$ contains a large number of inverses modulo $p$. We desire that $f$ not be too large in order to ensure that inverses are distributed quite evenly throughout $\mathbb{Z}_p$.

Simple computation yields a mean of $\frac{NH}{p}$ for $f(m, H)$ over all $m$, and the function

$$\mathcal{M}_k(H, p) = \sum_{m=0}^{p-1} \left(f(m, H) - \frac{NH}{p}\right)^k$$

gives the $k$th moment about this mean.

We will need the following fact, a special case of the main theorem from [4], credited to Cobeli, [3]:

**Theorem 3.3.** *For any prime $p$ and $N, H < p$, $\mathcal{M}_2(H,p) = HN - \frac{HN^2}{p} + O(H^2\sqrt{p}\log^2 p)$, where the constant involved in the big-oh term is independent of the choice of $p$.*

The exact portion of the righthand side of Theorem 3.3 represents the second moment, $\mu_2(H, \frac{N}{p})$, of a binomial random variable with parameters $H$ and $\frac{N}{p}$.

*Proof of Proposition 3.2.* Let $C$ be the largest component contained completely within $G_t$. We note that $C$ is convex, in that $x, y \in C \Rightarrow [x, y] \subseteq C$. Thus we may suppose $C = \{x, x+1, ..., x+N-1\}$, so $|C| = N$. Let $H = N$. We obtain $f(x \pm i, N) = N - i$ for $0 \le i < N$, and $f(m, N) = 0$ whenever $|m - x| \ge N$, modulo $p$. Thus we may easily compute $\mathcal{M}_2(N,p)$:

$$\mathcal{M}_2(N,p) = (N-\frac{N^2}{p})^2+2\sum_{i=1}^{N-1}(i-\frac{N^2}{p})^2+(p-2N+1)\frac{N^4}{p^2} = \frac{1}{3}N+\frac{2}{3}N^3-\frac{1}{p}N^4.$$

Meanwhile $\mu_2(N, \frac{N}{p}) = N^2 - \frac{1}{p}N^3$, and the equality in Theorem 3.3 obtains if and only if

$$\frac{1}{3}N - N^2 + \left(\frac{2}{3} + \frac{1}{p}\right)N^3 - \frac{1}{p}N^4 \le cN^2\sqrt{p}\log^2 p$$

for some constant $c$ independent of $p$. Clearing denominators we see

$$pN - 3N^2p + 2N^3p + 3N^3 - 3N^4 \le c'N^2p^{3/2}\log^2 p$$

must hold for a fixed $c'$.

Should $N \sim p^{1/2+\epsilon}$ for $\epsilon > 0$, the lefthand side of this equation has order $p^{5/2+3\epsilon}$, while the righthand side has order $p^{5/2+2\epsilon}\log^2 p$, a contradiction for large enough $p$. Thus $N = O(\sqrt{p})$, as claimed. □

Finally, we can limit the number of vertices involved in components $C \subseteq G_t$:

**Proposition 3.4.** *The total number of vertices lying in components contained completely in $G_t$ is $O(\sqrt{p})$.*

This result is obtained almost immediately from the following:

**Lemma 3.5.** *Given any number $n < p$, there are either 0 or 2 values $x \in \{2, 3, ..., p-2\}$ such that $x < x^{-1}$ and $x^{-1} - x = n$. In either case, no more than one such $x$ lies in $G_t$.*

Indeed, assume Lemma 3.5. Note that by Proposition 3.2 any $x \in C \subsetneq G_t$ satisfies $x^{-1} - x \leq |C| - 1 = O(\sqrt{p})$, yet Lemma 3.5 implies that this difference occurs at most once among all pairs $\{x, x^{-1}\}$ in $G_t$. There can thus be no more than $O(\sqrt{p})$ such inverse pairs in $G_t$, establishing Proposition 3.4.

*Proof of Lemma 3.5.* Suppose $x < x^{-1}$ and $x^{-1} - x = n < p$. Then $x^2 + nx - 1 \equiv 0 \bmod p$, and since $(4,p) = 0$, the equation $4x^2 + 4nx - 4 \equiv 0 \bmod p$ has the same solutions modulo $p$. Completing the square, we find $x$ must satisfy $(2x+n)^2 \equiv n^2 + 4 \bmod p$; this equation is solvable if and only if $\left(\frac{n^2+4}{p}\right) = 1$, in which case there are two solutions modulo $p$, only one of which (our purported $x$) lies in $2, \ldots, \frac{p-1}{2}$. $\square$

# 4 Computing $\bar{\kappa}(\mathbb{Z}_p)$

We can now prove the stated limit for $\bar{\kappa}(G)$, $G = \mathbb{Z}_p$.

*Proof of Theorem 1.1.* Given $x \neq y \in V(G)$, Section 2 assures us that the pair $\{x, y\}$ contributes either 2 or 3 to $\bar{\kappa}(G)$, depending on whether or not $x$ and $y$ lie in different components. Let $C$ be the (unique) maximal component in $G$, comprising at least $p - k\sqrt{p}$ of $G$'s vertices, $k$ independent of $p$, by Proposition 3.2.

We obtain a lower bound for $\bar{\kappa}(G)$ by treating every pair of vertices chosen from $V \setminus C$ as though they lie in different components. That is,

$$\bar{\kappa}(G) \geq \frac{1}{\binom{|V|}{2}}\left(2\binom{|V \setminus C|}{2} + 2|V \setminus C| \cdot |C| + 3\binom{|C|}{2}\right) > \frac{3\binom{|C|}{2}}{\binom{|V|}{2}}.$$

Thus

$$\lim_{p \to \infty} \bar{\kappa}(G) \geq \lim_{p \to \infty} 3\frac{(p - k\sqrt{p})(p - k\sqrt{p} - 1)}{p(p-1)} = 3.$$

Meanwhile, of course, the upper bound $\bar{\kappa}(G) \leq 3$ is trivial. $\square$

**Remark.** While a direct proof is not attempted here, it is possible that all vertices of degree 3 are contained in the maximal component $C$, for *any* $p$; the author has verified this fact for the first 100000 primes.

# 5 A comparison

We may naturally generalize the class of graphs $\{\mathbb{Z}_p\}_{p \text{ prime}}$ in the following manner: let $n \in \mathbb{N}$ be given, and as before begin with the cycle graph $C_n$

with $n$ edges. For each $m \in \{0, 1, ..., n-1\}$ such that $(m, n) = 1$ and $m \neq m^{-1}$, append an edge $mm^{-1}$. (We may think of appending self-loops at all $m$ satisfying either $(m, n) > 1$ or $m = m^{-1}$, but these loops will not effect connectivity.) Denote the resulting graph by $\mathbb{Z}_n$. For completeness we may allow $\mathbb{Z}_1$ and $\mathbb{Z}_2$ to be the complete graphs on 1 and 2 vertices, respectively.

**Proposition 5.1.**

$$\limsup_{n \to \infty} \frac{1}{n} \sum_{m=1}^{n} \bar{\kappa}(\mathbb{Z}_m) \leq \frac{21}{8} < 3.$$

In this sense, among many others, the graphs $\mathbb{Z}_p$ for $p$ prime are exceptional.

*Proof.* Seeking an upper bound for $\frac{1}{n} \sum_{m=1}^{n} \bar{\kappa}(\mathbb{Z}_m)$, we lose nothing in assuming that for any given $m$, all of $\mathbb{Z}_m$'s vertices of degree 3 are in a single chord component. That is, for any $m \in \mathbb{N}$,

$$\bar{\kappa}(\mathbb{Z}_m) \leq \frac{2\left(\binom{m-\phi}{2} + (m-\phi)\phi\right) + 3\binom{\phi}{2}}{\binom{m}{2}},$$

where $\phi = \phi(m)$ is the Euler totient, giving the number of positive integers less than $m$ relatively prime to $m$.

Expanding the binomial coefficients and simplifying, we obtain

$$\bar{\kappa}(\mathbb{Z}_m) \leq 2 + \frac{\phi^2}{m(m-1)} - \frac{\phi}{m(m-1)}.$$

Thus

$$\frac{1}{n} \sum_{m=1}^{n} \bar{\kappa}(\mathbb{Z}_m) \leq \frac{1}{n} \left( 2n + \sum_{m=1}^{n} \frac{\phi^2}{m(m-1)} - \sum_{m=1}^{n} \frac{\phi}{m(m-1)} \right).$$

The second sum here has limit $\frac{1}{\zeta(2)} \log(n) = \frac{6}{\pi^2} \log(n)$ with very small error (see exercise 3.6 of [1]), and so contributes nothing to the limit after dividing by $n$. The first sum, on the other hand is easily evaluated more directly, after applying the estimate $\frac{\phi^2}{m(m-1)} \approx \frac{\phi^2}{m^2}$ for $m$ large. Using the divisor-sum formula for $\phi$, we have

$$\sum_{m=1}^{n} \frac{\phi^2}{m(m-1)} \approx \sum_{m=1}^{n} \frac{1}{m^2} \left( \sum_{d|m} \mu(d) \frac{m}{d} \right)^2 = \sum_{m=1}^{n} \left( \sum_{d|m} \frac{\mu(d)}{d} \right)^2,$$

where $\mu$ is the Möbius function. However, the inside sum can be replaced with the product $P_m = \prod_{p|m} \frac{p-1}{p}$ over all primes dividing $m$. When $m$ is even, $P_m \leq \frac{1}{2}$, so $P_m^2 \leq \frac{1}{4}$. In any case, and so in particular when $m$ is odd, $P_m^2 < 1$. Applying these facts to inequality given above, we have

$$\limsup_{n\to\infty} \frac{1}{n} \sum_{m=1}^{n} \bar{\kappa}(\mathbb{Z}_m) \leq 2 + \lim_{n\to\infty} \frac{n+1+\frac{n}{4}}{2n+1} = 2 + \lim_{n\to\infty} \frac{5n+4}{8n+4} = \frac{21}{8}.$$

□

**Remark.** Experimental evidence suggests

$$\lim_{n\to\infty} \frac{1}{n} \sum_{m=1}^{n} P_m^2 \approx 0.428,$$

significantly smaller than the $\frac{5}{8}$ used in the above proof, which can be improved to arbitrary precision in the obvious manner.

# References


[1] T.M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics (Springer-Verlag, New York-Heidelberg, 1976).

[2] L.W. Beineke, O.R. Oellermann, and R.E. Pippert, The average connectivity of a graph, *Discrete Math.* **252** (2002) 31–45.

[3] C.I. Cobeli, *Topics in the distribution of inverses (mod) q*, Ph.D. Dissertation, University of Rochester, 1997.

[4] S.M. Gonek, G.S. Krishnaswami, and V.L. Sondhi, The distribution of inverses modulo a prime in short intervals, *Acta Arith.* **102** (2002) no. 4, 315–322.

[5] S. Hoory, N. Linial, and A. Wigderson, Expander graphs and their applications, *Bull. Amer. Math. Soc. (N.S.)* **43** (2006) no. 4, 439–561.

[6] J.H. Silverman, *A friendly introduction to number theory*, 3rd ed. (Pearson Prentice Hall, Upper Saddle River, NJ, 2006).