IGL Project Report*

The Quadratic Residue Random Walk: The Geometry of Gauss Sums

A.J. Hildebrand (Faculty Mentor)†

M. Tip Phaovibul (Project Leader)
Yiwang Chen, Yusheng Feng, Mateusz Wala (Undergraduate Members)

December 12, 2012

Abstract

The sequence of quadratic residues modulo a prime p is a sequence of $p-1$ symbols 1 or -1 that encodes the solubility of quadratic congruences modulo p and that behaves in many respects like a random binary sequence of length $p-1$. In this project we studied a certain "random walk" in the plane formed with this sequence, the "Quadratic Residue Random Walk" (QRRW). The QRRW modulo p is a finite walk in the plane consisting of $p-1$ steps of unit length and starting at the origin.

A famous result of Gauss predicts the *end point* of a QRRW, but what happens along the way is rather mysterious and has not been unexplored in the literature. A cursory examination of QRRW graphs shows random-like features such as sudden turns, sharp cusps, and ragged edges, but also some unexpected symmetries, though no obvious patterns.

The goal of this project was to unravel some of these mysteries. We identified six distinct shapes for a QRRW, and we correlated these shapes with congruence classes of p modulo small primes. We developed efficient algorithms and C code to facilitate large scale computations of QRRWs, and we used the campus computing cluster to carry out these computations. We computed a variety of quantities associated with a QRRW, such as the maximal distance to the origin and the amount of time spent in each quadrant. We also created animations showing the evolution of a QRRW.

*This is a preliminary report that summarizes the results of a research project carried out in Fall 2012 at the Illinois Geometry Lab (IGL), `www.math.illinois.edu/igl`.

†Department of Mathematics, University of Illinois, Urbanam, IL, 61801; email `ajh@illinois.edu`

1 Gauss Sums: Definition

> *Hardly a week may have gone by in the last four years without one or more unsuccessful attempts to unravel this knot. [...] But all the brooding, the searching, was to no avail, and I had sadly to lay down my pen again. A few days ago, I finally succeeded—not by my efforts, but by the grace of God, I should say.* –*Carl Friedrich Gauss, Sept. 3, 1805*

The problem that so fascinated (and frustrated) Gauss over a four year period is the evaluation of so-called "Gauss sums", which are defined below. *Throughout this section p denotes an odd prime number.*

Definition.

- ***Quadratic residues and nonresidues.*** *An integer n not divisible by p is called a quadratic residue modulo p if the congruence $n \equiv x^2 \bmod p$ has a solution, and a quadratic non-residue modulo p otherwise.*
- ***Legendre symbol.*** *The Legendre symbol modulo p, $\left(\frac{n}{p}\right)$, is defined as 1 if n is a quadratic residue modulo p, and -1 if n is a quadratic non-residue modulo p.*

Example. *For $p = 7$, the quadratic residues among $\{1, 2, \ldots, 6\}$ are $1, 2, 4$, and the quadratic non-residues are $3, 5, 6$. The values of $\left(\frac{n}{7}\right)$ for $n = 1, 2, \ldots, 6$ are $1, 1, -1, 1, -1, -1$.*

Definition. *The **Gauss Sum modulo** p, $G(p)$, is defined by either of the following formulas:*

$$G(p) = \sum_{n=1}^{p} e^{2\pi i n^2/p} \quad \textit{(Exponential Sum Version)} \tag{1}$$

$$G(p) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e^{2\pi i n/p} \quad \textit{(Quadratic Residue Version)} \tag{2}$$

The right hand sides of (1) and (2) have a completely different shape, and it is not at all obvious that the two formulas define the same quantity. Amazingly, this is indeed the case:

Proposition. *The two definitions (1) and (2) for the Gauss sum $G(p)$ are equivalent; that is, we have*

$$\sum_{n=1}^{p} e^{2\pi i n^2/p} = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e^{2\pi i n/p}.$$

The equivalence of the two definitions of $G(p)$ is not hard to prove, and can be found in most texts on analytic number theory. It is also not too hard to prove that $|G(p)| = \sqrt{p}$, and that $G(p)$ must be either purely real, or purely imaginary, thus leaving four possible values for $G(p)$: $\pm\sqrt{p}$ and $\pm i\sqrt{p}$.

Determine the $\pm$ sign in these formulas, however, proved to be much harder. Gauss' key achievement in this connection, and the object of of his four year quest, is the determination of these signs with the following theorem:

Theorem (Gauss (1805))**.** *The Gauss sums $G(p)$ are given by the following formulas:*

$$G(p) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \bmod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

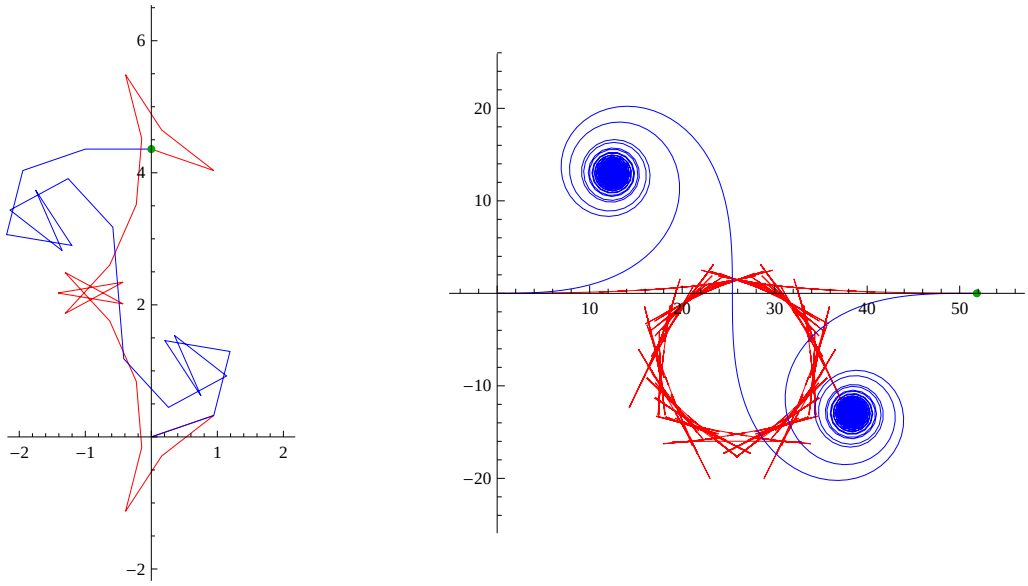

Figure 1: The exponential sum and quadratic residue versions of the Gauss Walk for $p = 19$ (left figure) and $p = 2689$ (right figure). The exponential sum versions have a relatively smooth path and spiral features. The quadratic residue versions have a more ragged path, with sudden turns and sharp edges and behave more like a true random walk.

2 Gauss Sums: Geometric Interpretation

The Gauss sums have a natural geometric interpretation by interpreting the terms as steps in a walk in the complex plane, starting at the origin. We will call such a walk a **Gauss Walk**. The two versions (1) and (2) of the Gauss sums yield two types of Gauss Walks:

- **Exponential Sum Gauss Walk:** A walk with p steps, starting at the origin, with the n-th step given by $e^{2\pi i n^2/p}$.
- **Quadratic Residue Gauss Walk:** A walk with $p-1$ steps, starting at the origin, with the n-th step given by $\left(\frac{n}{p}\right) e^{2\pi i n/p}$.

By the above proposition and Gauss' Theorem, both versions of the Gauss Walk terminate at the same point, given by $(\sqrt{p}, 0)$ if $p \equiv 1 \bmod 4$, and $(0, \sqrt{p})$ if $p \equiv 3 \bmod 4$.

Figure 1 shows the two versions of the Gauss Walk for $p = 19$ and $p = 2689$. As predicted by Gauss' Theorem, both versions end in the same point, namely $(0, \sqrt{19})$ for $p = 19$, and $(\sqrt{2689}, 0)$ for $p = 2689$. (Note that $19 \equiv 3 \bmod 4$ and $2689 \equiv 1 \bmod 4$.)

The exponential sum version has a rather regular smooth shape, with interesting spiral-type features. It has been thoroughly analyzed by D.H. Lehmer (1972) and is fairly well understood.

By contrast, the quadratic residue version resembles more a true random walk; hence we will call it the **Quadratic Residue Random Walk (QRRW)**. The QRRW does not seem to have been studied in the literature, and its behavior is rather mysterious, with many ragged edges, sudden turns, but also some interesting symmetries. The main goal of this project is to develop a better understanding of the QRRW and get to the bottom of some of its mysteries.

3 Classification of Shapes of a QRRW

We have identified six distinctive shapes of a QRRW, shown in Figure 2 below.

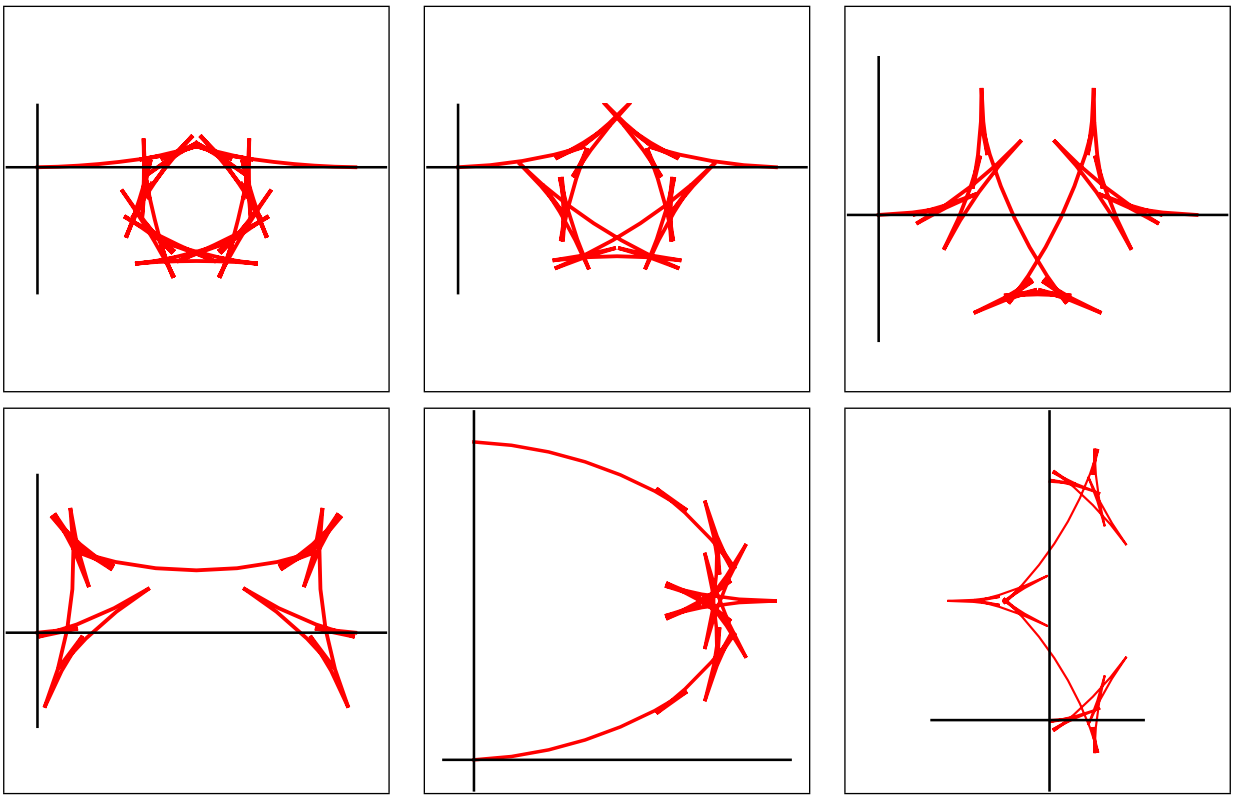

Figure 2: The six shapes of a QRRW, corresponding to primes of type $(1,1,1,1)$, $(1,1,1,-1)$, $(1,1,-1,*)$, $(1,-1,*,*)$, $(-1,1,*,*)$, $(-1,-1,*,*)$, respectively.

We have found that the six shapes are completely determined by values of the four Legendre symbols $\left(\frac{k}{p}\right)$ for $k=-1,2,3,5$. More specifically, the six shapes identified in Figure 2 correspond to values $(1,1,1,1)$, $(1,1,1,-1)$, $(1,1,-1,*)$, $(1,-1,*,*)$, $(-1,1,*,*)$, $(-1,-1,*,*)$, respectively, for 4-tuple

$$\left(\left(\frac{-1}{p}\right),\left(\frac{2}{p}\right),\left(\frac{3}{p}\right),\left(\frac{5}{p}\right)\right). \tag{3}$$

We call the tuple (3) the **type** of p.

Figure 3 below shows graphs of the QRRW for a sequence of 18 consecutive primes p starting with 530. The distinctive shapes are recognizable among these graphs, though they seem to occur in random order.

Figure 4 illustrates the connection between the shape of a QRRW graph and the type of the associated prime p. The figure shows, for each of the six types identified above, the graphs of the QRRW for the first three primes p greater than 540 that have this particular type. For example, the first row shows the graphs of the first three primes p greater than 540 of type $(1,1,1,1)$.

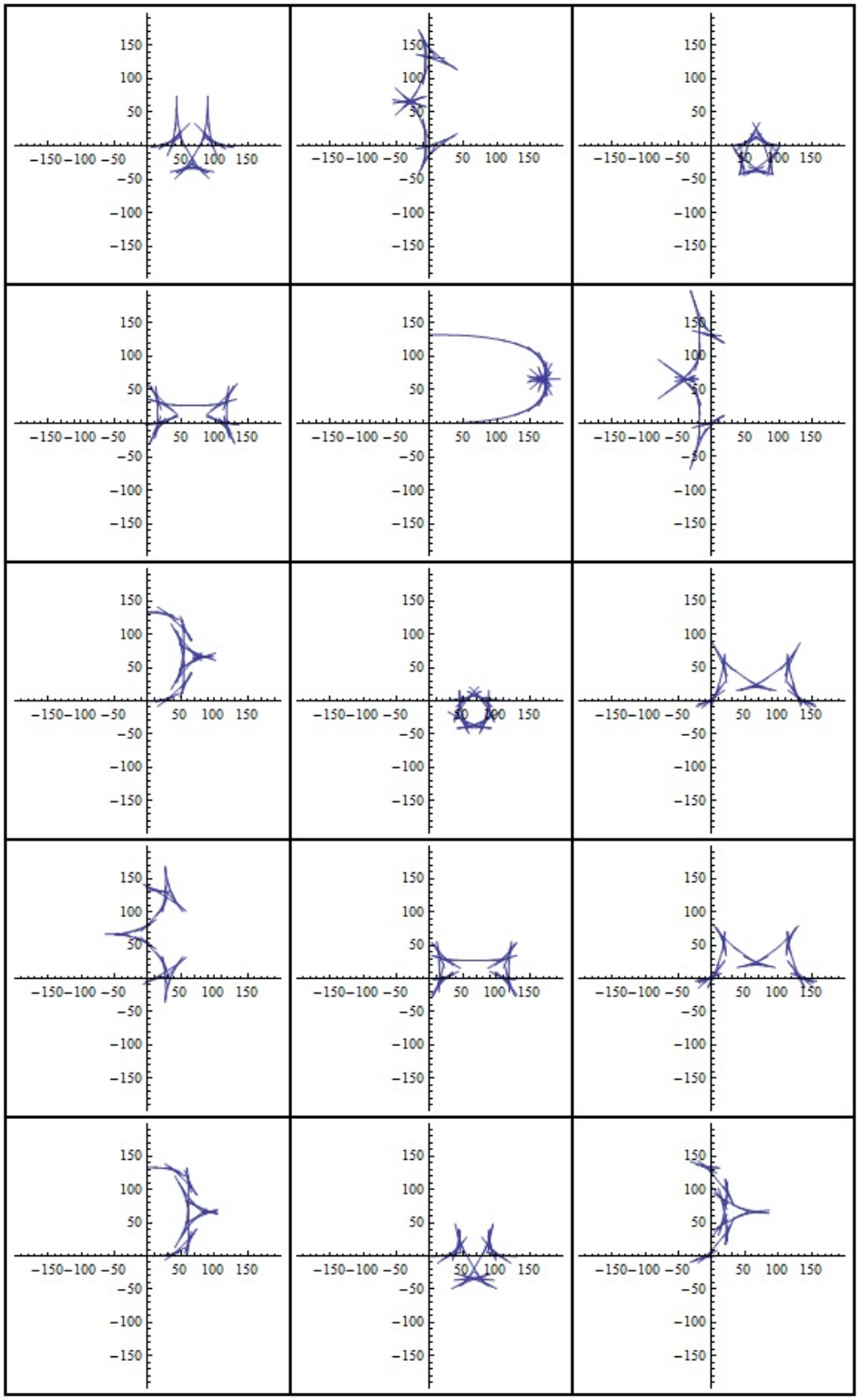

Figure 3: QRRW graphs for the first 18 primes greater than 540.

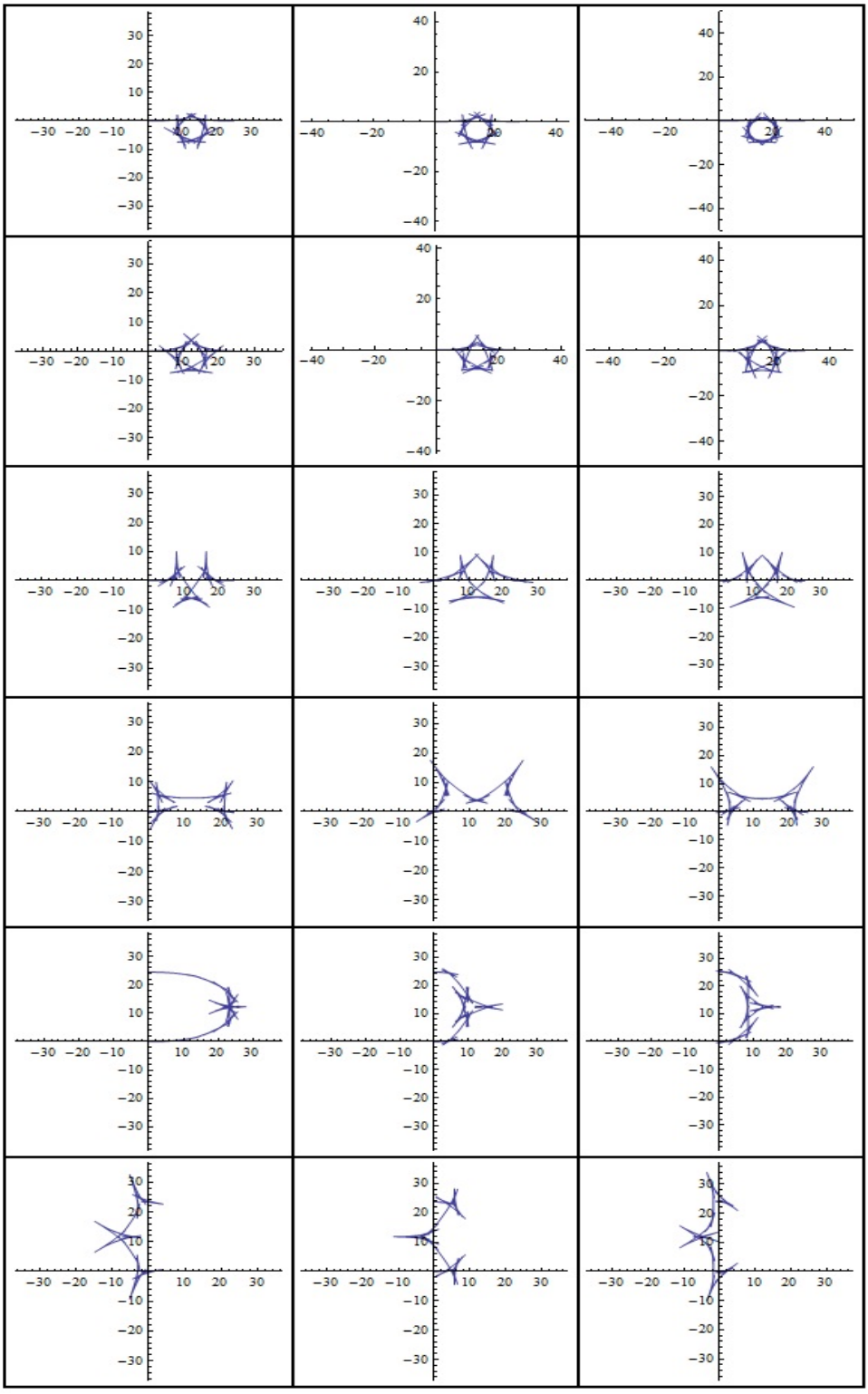

Figure 4: QRRW graphs grouped by type of prime. Each row represents primes of fixed type; the graphs shown are those for the first 3 primes greater than 540 of this type.

4 Maximal Distance to Origin of a QRRW

We developed efficient algorithms and C code to facilitate large scale computations of QRRWs. We carried out these computations on the campus computing cluster and so far have assembled complete data for QRRWs for all p up to $2 \cdot 10^6$.

In particular, we studied the maximal distance to the origin attained in a QRRW. Let $D(p)$ denote the maximal distance to the origin of the QRRW modulo p, i.e., the maximal absolute value of the partial sums in (2). Since the endpoint of any Gauss Walk is at distance exactly $\sqrt{p}$ from the origin (by Gauss' Theorem), we have trivially $D(p) \geq \sqrt{p}$. Figure 5 shows the normalized quantities $D(p)/\sqrt{p}$ for primes up to $2 \cdot 10^6$. The data suggest that these quantities typically lie in a narrow range between 1 and 2, but that occasionally takes on larger values.

To examine this further, we kept track of "record" values of $D(p)/\sqrt{p}$. Table 1 below lists all record values of $D(p)/\sqrt{p}$ for $p \leq 2 \cdot 10^6$, and Figure 6 is a line plot of these record values. The values appear to grow like an iterated logarithm, which is what one would expect for a true random walk.

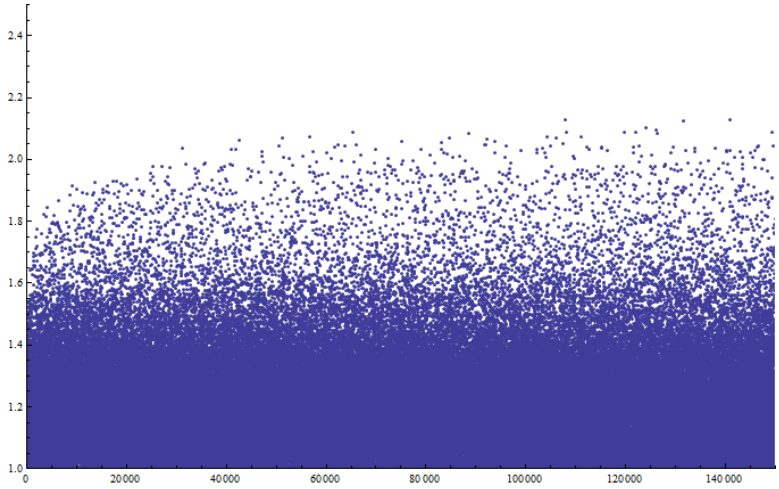

Figure 5: Normalized maximal distances $D(p)/\sqrt{p}$ for $p \leq 2 \cdot 10^6$.

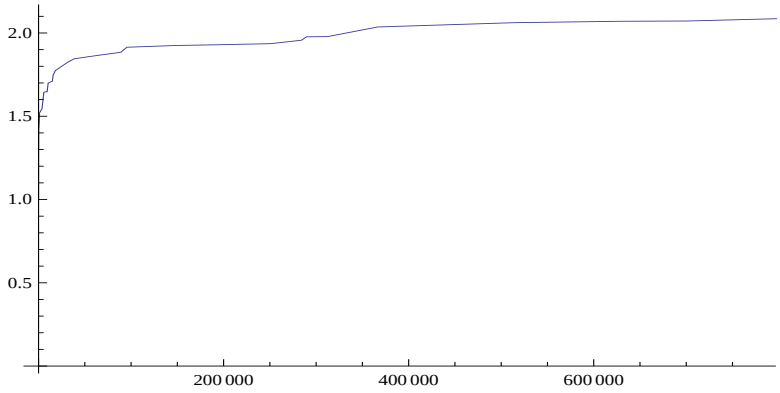

Figure 6: Record values of maximal distances $D(p)/\sqrt{p}$.

p	$D(p)/\sqrt{p}$
3	1
11	1.118647865
19	1.261658997
43	1.267673739
67	1.303477565
139	1.308877936
163	1.369982211
211	1.425040542
379	1.428758597
499	1.441700258
739	1.468334063
1051	1.5199258
2999	1.539339652
3671	1.542965245
5711	1.64317358
6551	1.646210656
9239	1.646749848
10391	1.69907878
14951	1.710600018

p	$D(p)/\sqrt{p}$
15791	1.747749721
18191	1.774100742
31391	1.823964635
38639	1.845341844
63839	1.865358759
88919	1.884026936
95471	1.914400678
147671	1.924730912
191231	1.929082853
250799	1.935837693
284231	1.956692746
289511	1.976972824
312311	1.978354065
366791	2.036249907
514751	2.061945738
628319	2.070277013
701399	2.071956753
819719	2.088943734
1412759	2.126872428

Table 1: List of all record values for the normalized distance $D(p)/\sqrt{p}$ for primes up to $2 \cdot 10^6$.