# An elementary investigation of the prime p = 4k – 1 asymmetry theorem for quadratic residues I

Jim H. Adams

jim-adams@supanet.com

27th December 2010, revised 27th December 2011

**Abstract.** Let a prime p = 4k – 1. We prove by elementary methods a formula for the number of quadratic residues in the interval [1, 2k – 1] minus those in [2k, 4k – 2]. This number is equal to the disparity expression

$$\sum_{r=1}^{k}[2\lfloor\sqrt{rp-(p/2)}\rfloor-\lfloor\sqrt{rp}\rfloor-\lfloor\sqrt{(r-1)p}\rfloor]$$

where $\lfloor\ \rfloor$ is the floor, or integer part. We partition this summation between rows, r, up to $T = \lfloor(p + 9)/16\rfloor$, and define *trajectories* after this row, providing a formula also for the trajectories. Hermann Weyl in 1940, using transcendental methods, asked for an elementary proof of the positive nature of the total disparity expression, which is investigated in Part II using *parabolas* which occupy the row and trajectory regions. In Part I we obtain row and trajectory information using local and global arguments.

Keywords: elementary methods, quadratic residue, disparity, trajectory

## 1 Introduction.

Richard Guy in [Gu04], unsolved problem **F5**, asks: If a prime $p = 4k - 1$, there are more quadratic residues in the interval $[1, 2k - 1]$ than in $[2k, 4k - 2]$, but all known proofs use Dirichlet's class-number formula. Is there a proof by elementary methods? This problem was obtained arising from consideration of work by Davenport [Da80]. However, Hermann Weyl in 1940 [We40] asked a more detailed question.

We call $n^2$ a *square* or a *perfect square*. A *quadratic residue*, b, is then a square reduced (mod p), so $n^2 = ap + b$, where $b < p$. Natural numbers here are in lower case.

A *row* is then the corresponding interval not reduced (mod p), so that the first row is $[0, p - 1]$ and the second row is $[p, 2p - 1]$, etc. We specify that [0] is at *column* 0.

Our plan of investigation into revealing a *formula* for the difference between the total number of left hand interval $[1, 2k - 1]$, and the right, $[2k, 4k - 2]$ interval perfect squares, for $p = 4k - 1$ in the first $(p + 1)/4$ rows, is as follows.

In the *preliminary remarks*, we use two different methods to show there are $(p - 1)/2$ non-zero quadratic residues between perfect squares $0^2$ and $(p - 1)^2$. The first method uses Fermat's little theorem, which states for p prime

$$y^p - y \equiv 0 \pmod{p},$$

and the second uses perfect squares rather than reduction (mod p). To prove this we use a special case of the binomial theorem, which indicates symmetries in the quadratic residues for each row, so the same non-zero quadratic residues occur for both $n^2$ and $(p - n)^2$. Essential to this understanding is the *occupancy theorem*, which states that $m \neq n \pmod{p}$ and $m \neq p - n \pmod{p}$ if and only if $m^2 \neq n^2 \pmod{p}$.

In the section leading to the formula we first provide an example of $p = 4k - 1 = 83$. The rows are displayed up to row $(p + 1)/4$, which is the maximum row up to which perfect squares do not occupy the same column.

We divide each interval $[0, 4k - 2]$ corresponding to its reduction (mod p) into three sectors. **Region G** corresponds to the interval [0], the *left hand part* of **region H** is the interval $[1, 2k - 1]$ and the *right hand part* of **region H** is $[2k, 4k - 2]$.

For each row the difference between the number of perfect squares in the left hand minus the right hand part of **region H** is at worst -1. For the first row, we prove the number of perfect squares is greater on the left hand part of **region H** than on the right, and descend to row T, a row after which the difference in the number of columns between one perfect square and the next exceeds $(p - 1)/2$.

Looking at the bottom part of the $p = 83$ table shown later, the perfect squares rise up from the left hand part of **region H** to the right, fitting a curve we call a *trajectory*, which we stipulate ascends from left to right, so a new trajectory starts when the curve switches from the right to the left hand part of **region H**. We will prove that the first such bottom square is located at column $(p + 1)/4$ in the left hand part of **region H**.

Then, counting these perfect squares from the first, labelled $v = 1$, to the rightmost square on the first trajectory, we can see the number of perfect squares is greater or equal on the left compared with the right.

For every other trajectory we are able to compute that this disparity is at worst -1. The trajectories ascend, finally overlapping row T. Knowing the number of trajectories after the first is M = the floor of either (p + 1)/16 or (p – 15)/16, we give an explicit formula for the combined row and trajectory disparities.

We derive simplified formulas for the total disparity, bounds on the positive value of the total disparity by purely algebraic means and find a condition for the number of perfect squares in a row to decrease as the rows increment. We show that, ignoring rows with an even number of squares, clusters of rows with the same odd number of squares, to which disparities only belong, do not overlap on incrementing rows.

We discuss and compute constraints on -1 disparities for small row values, explicitly up to row 5. We then deduce the absence of disparities for row T and for rows nearing row T, although p = 67 is an exception, there being y rows before T in this case, where $y^2 < 2\alpha$, in which $k = 4\alpha + \beta$, $\beta = 0, 1, 2$ or 3.

For *trajectories*, we establish a bijective mapping between rows and trajectories. Then, describing trajectories by a parabola, and also rows, we treat square values as *lattice points*, and use global counting methods for internal partitions. We show that the number of -1 disparities do not necessarily *evaporate* as we approach row T.

Subsequent work will discuss a new feature, *parabolas*, and relate the above discussion to the tenth discriminant problem.

## 2 Preliminary remarks.

For p an odd prime, *quadratic reciprocity* theorems follow partly from Fermat's little theorem by considering $y(y^{(p-1)/2} – 1)(y^{(p-1)/2} + 1) \equiv y((y^2)^{(p-1)/2} – 1) \equiv 0 \pmod p$, so all squares $\neq 0 \pmod p$ belong to the $(y^{(p-1)/2} – 1)$ equivalence class [Ad14]. □

We will prove $y^{(p-1)/2} \equiv 1 \pmod p$ has (p – 1)/2 root positions. For quadratic residues, the *occupancy theorem* asserts that these are all occupied by specific numbers.

**Theorem 2.1 (the occupancy theorem)**. Assign all numbers (mod p), p prime. Then $m^2 \neq n^2$ *if and only if* $m \neq n$ *and* $m \neq (p – n)$.

*Proof.* A two way implication holds. We will prove that $m^2 – n^2 \equiv 0 \pmod p$ leads to a contradiction, which would mean $(m – n)(m + n) = \nu p$ for some $\nu$.

Put m > n and $m, n \leq (p – 1)/2$, so $(m + n) < p – 1$ and also $(m – n) < (p – 1)/2$. But p, being prime, must be a factor of (m – n), (m + n) or both, and this is impossible.

If $p > m \neq n > (p – 1)/2$, then $2p – 1 > (m + n) > p$ and $(p – 3)/2 \geq (m – n) \geq 1$, so neither (m + n) nor (m – n) is divisible by p

If say $n < (p – 1)/2$ and $p > m \geq (p – 1)/2$ then the only possibility is (m + n) = p, since
(m – n)(m + n) = [a number < p][a number $\geq$ (p – 1)/2]. □

**Theorem 2.2.1 (v 1)**. *Let* $0 < y < p$, *with* p *odd* (*for example* p *prime*) *and* $m \in \mathbf{N}$, *then*
$y^{(p-1)/2} \equiv (-1)^{(p-1)/2}(mp – y)^{(p-1)/2} \pmod p$.

*Proof.* Consider (p – 1)/2 *even*. A binomial expansion, leaving out terms in mp to a power, which are ≡ 0 (mod p), indicates that $y^{(p-1)/2} \equiv (-y)^{(p-1)/2}$ (mod p). If (p – 1)/2 is *odd*, so p = 4k – 1, then the binomial expansion gives $y^{(p-1)/2} \equiv -(-y)^{(p-1)/2}$ (mod p). □

Our theorem has the following consequences.

Taking the typical example for the p = 11 table below, $y^5$ repeats mod 11 in three regions, **A**, **B** and **C**, the above equation representing symmetries in regions **B** and **C**.

*Table:* p = 11, (p – 1)/2 = 5.

| **y ≡ (mod p)** | **$y^5$** | **$y^5$ (mod 11)** | **region** |
|---|---|---|---|
| 0 | 0 | 0 | **A** |
| 1 | 1 | 1 | **B** |
| 2 | 32 | -1 | |
| 3 | 243 | 1 | 0 < n ≤ (p – 1)/2 |
| 4 | 1024 | 1 | |
| 5 | 3125 | 1 | |
| 6 | 7776 | -1 | **C** |
| 7 | 16807 | -1 | |
| 8 | 32768 | -1 | (p – 1)/2 < n < p |
| 9 | 59049 | 1 | |
| 10 | 100000 | -1 | |
| 11 ≡ 0 (mod 11) | | | **repeats** |

For (p – 1)/2 *odd*, if 0 < n ≤ (p – 1)/2, i.e. region **B**, then there are δ terms ≡ 1 (mod p) and (p –1)/2 – δ terms ≡ -1 (mod p), so there must be in the (p – 1)/2 < n < p region **C**, δ terms ≡ -1 (mod p) and (p – 1)/2 – δ terms ≡ +1 (mod p), giving the complete set of (p – 1)/2 occupied root positions for both 1 (mod p) and -1 (mod p).

*Table:* p = 17, (p – 1)/2 = 8.

| **y ≡ (mod p)** | **$y^8$** | **$y^8$ (mod 17)** | **region** |
|---|---|---|---|
| 0 | 0 | 0 | **A** |
| 1 | 1 | 1 | **B** |
| 2 | 256 | 1 | |
| 3 | 6561 | -1 | 0 < n ≤ (p – 1)/2 |
| 4 | 65536 | 1 | |
| 5 | 390625 | -1 | |
| 6 | 1679616 | -1 | |
| 7 | 5764801 | -1 | |
| 8 | 16777216 | 1 | |
| 9 | 43046721 | 1 | **C** |
| 10 | 100000000 | -1 | |
| 11 | 214358881 | -1 | (p – 1)/2 < n < p |
| 12 | 429981696 | -1 | |
| 13 | 815730721 | 1 | |
| 14 | 1475789056 | -1 | |
| 15 | 2562890625 | 1 | |
| 16 | 4294967296 | 1 | |
| 17 ≡ 0 (mod 17) | | | **repeats** |

If $(p - 1)/2$ is *even*, with the $\delta$ terms $\equiv 1 \pmod p$ for region **B** above, there are $\delta$ terms $\equiv 1 \pmod p$ in region **C**, opposite in sign to the odd case. Thus there are $2\delta$ slots for $2\delta = (p - 1)/2$ quadratic residues of $1^2$ to $4\delta^2$ in the combined **B** and **C** region, and these slots in **B** (and **C**) are completely occupied. So $\delta = (p - 1)/4$ in the **B** region, and similarly the residues $\equiv -1 \pmod p$ occupy $\delta$ slots in this region, likewise in region **C**. □

We now address the above considerations from a slightly different point of view.

**Theorem 2.2.2 (v 2)**. If we look at the table for squares, say in the (mod 7) example that follows, there are p squares from 0 to $p^2 - 1 \pmod{p^2}$, being $0^2, 1^2, \ldots (p - 1)^2$.

*Table:* p = 7, squares (underlined) to $p^2 = 49$. Region **E** columns = region **F** columns.

| | |
|---|---|
| **region D** | 0 |
| **region E** | 1 2 3 4 5 6<br>7 8 9 |
| **region F** | 10 11 12 13<br>14 15 16 17 18 19 20<br>21 22 23 24 25 26 27<br>28 29 30 31 32 33 34<br>35 36 37 38 39 40 41<br>42 43 44 45 46 47 48 |
| **next $p^2$** | 49 |

Since, by the binomial theorem for squares,

$$(p + n)^2 \equiv n^2 \pmod p,$$

these p squares fill, in p iterations (mod p), all the squares that are possible $(\text{mod } p^2)$.

Likewise, since

$$(p - n)^2 \equiv n^2 \pmod p,$$

those squares which are non-zero $(\text{mod } p^2)$, repeat in just two non-overlapping sets $(\text{mod } p^2)$, in regions **E** and **F**, since there are no other inequivalent natural number relations satisfying

$$(\theta p - \lambda n)^2 \equiv n^2 \pmod p.$$

Ignoring local behaviour, we now apply global reasoning, using the non-constructive pigeon hole principle.

Since there are p squares $(\text{mod } p^2)$, *there are* $(p - 1)/2$ *non-zero squares* (mod p). The first overlapping set $\neq 0$, in region **E**, being the first $(p - 1)/2$ squares $(\text{mod } p^2)$, maps to precisely $(p - 1)/2$ separate squares (mod p), otherwise there would be less of them than $(p - 1)/2$. We are using here full occupancy of the square slots. □

A 'crossing out' method can be used, analogous to the 'sieve of Eratosthenes' for primes, for determining whether a number is or is not a square (mod p). Set up a grid of width p and depth $> (p - 1)^2/4p$ and $< [(p - 1)^2/4p] + 1$ with the first column labelled 0. Determine the column for a number n given by n (mod p). Put an X in column 0, an X in column 1 with no space between columns 0 and 1, an X in column 4 with two spaces between columns 1 and 4, and so on, increasing the number of spaces by two each time and continuing into other rows if necessary. If the column corresponding to n is reached, it is a square (mod p), otherwise it is not. □

## 3 Detailed proofs leading to the disparity formula.

*Example.* p = 83, (p – 1)/2 = 41 (odd), number of rows = (p + 1)/4 = 21. Perfect squares are underlined. Columns unoccupied by a quadratic residue are suppressed.

| **region G** | **region H, left hand part** |
|---|---|
| 0 | 1 3 4 7 9 10 11 12 16 17 21 23 25 26 27 28 29 30 31 33 36 37 38 40 41 |
| 83 | 100 121 |
| 166 | 169 196 |
| 249 | 256 289 |
| 332 | 361 |
| 415 | 441 |
| 498 | 529 |
| 581 | blank |
| 664 | 676 |
| 747 | 784 |
| 830 | 841 |
| 913 | blank |
| 996 | 1024 |
| 1079 | 1089 |
| 1162 | blank |
| 1245 | blank |
| 1328 | 1369 |
| 1411 | 1444 |
| 1494 | 1521 |
| 1577 | 1600 |
| 1660 | 1681 |

*Example* (*continued*). Table for the right hand part of **region H**, with **region G** inserted for reference. p = 83, (p – 1)/2 = 41 (odd), number of rows = (p + 1)/4 = 21. Squares are underlined. Columns unoccupied by a quadratic residue are suppressed.

| **region G** | **region H, right hand part** |
|---|---|
| 0 | 44 48 49 51 59 61 63 64 65 68 69 70 75 77 78 81 |
| 83 | 144 |
| 166 | 225 |
| 249 | 324 |
| 332 | 400 |
| 415 | 484 |
| 498 | 576 |
| 581 | 625 |
| 664 | 729 |
| 747 | blank |
| 830 | 900 |
| 913 | 961 |
| 996 | blank |
| 1079 | 1156 |
| 1162 | 1225 |
| 1245 | 1296 |
| 1328 | blank |
| 1411 | blank |
| 1494 | blank |
| 1577 | blank |
| 1660 | blank |

We make the following observations.

**3.1** *To calculate the depth, or number of rows, of the above table*, for (p – 1)/2 odd = 2k – 1, we have seen previously that the depth in **region G** and **H** generally satisfies

$(p-1)^2/4p = (p-2)/4 + 1/(4p)$

$< \text{depth} < (p+2)/4 + 1/(4p) = [(p-1)^2/4p] + 1,$

so the depth must be the whole number $k = (p+1)/4$. There are thus only $(p+1)/4$ rows we need to consider before the columns containing a quadratic residue repeat.

**3.2** We now introduce the *row parameter* T. The criterion we use is: up to what value for a perfect square $n^2$ in the left or right hand part of **region H** is the difference between the next square $\leq (p-1)/2$? In this case, since the interval between each pair of perfect squares decrements by 2 going backwards from this row, all rows prior to this are also occupied on the left and right.

So our criterion is

$$(n+1)^2 - n^2 \leq (p-1)/2$$

or

$$n \leq (p-3)/4.$$

Thus the rightmost value of $n^2$ corresponds to row related value $r_{min}$, extending to

$$r_{min}p = (p-3)^2/16$$

$$r_{min} = [p - 6 + (9/p)]/16$$

and the leftmost value of $n^2$ corresponds to row related value $r_{max}$, with

$$r_{max}p = (p-3)^2/16 + (p-2)$$

$$r_{max} = [p + 10 - (23/p)]/16.$$

The actual row lies between $r_{min}$ and $r_{max}$, and is either row T or row $(T-1)$, where

T = the integer part of $[p+10]/16$.

**3.3** *We will find the column for* $[(p-3)/4]^2$. It follows from the computation of row T, with $p = 4k - 1$, that if $k = 4\alpha + \beta$ with $\beta = 0, 1, 2$ or 3, then if $\beta = 0$ or 1, $T = \alpha$, and if $\beta = 2$ or 3 then $T = \alpha + 1$.

We see $[(p-3)/4]^2$ *is in row* T, since it is situated at column $[(p-3)/4]^2 - p(T-1)$.

For $\beta = 0$ this square is then at $9\alpha$, for $\beta = 1$ it is at $13\alpha + 3$, $\beta = 2$ is at $\alpha + 1$ and $\beta = 3$ gives $5\alpha + 4$. Consequently for $\beta = 0$ this perfect square is on the right at the column $9(p+1)/16$, for $\beta = 1$ on the right at $(13p + 9)/16$, for $\beta = 2$ on the left at $(p + 9)/16$ and for $\beta = 3$ also on the left at $(5p + 9)/16$.

**3.4** For the *first row* with columns $> 0$ and $\leq (p-1)/2$, the highest perfect square has

$$j^2 \leq (p-1)/2$$

and there are j of them. Thus

$$j \leq \sqrt{(p-1)/2}.$$

For the first row with columns $> (p-1)/2$ and $\leq (p-1)$, the perfect squares satisfy

$$\sqrt{(p-1)/2} < j \leq \sqrt{p-1},$$

thus we note that the first row of the left hand part of **region H** has a larger set of values than the right hand part, the difference being, taking integer parts

$$\lfloor\sqrt{(p-1)/2}\rfloor - [\lfloor\sqrt{p-1}\rfloor - \lfloor\sqrt{(p-1)/2}\rfloor],$$

which is non-negative for $p \leq 23$, and positive for $p > 23$, for the above expression satisfying with respect to the following number the relation

$$\geq \lfloor(\sqrt{2} - 1)\sqrt{p-1}\rfloor - 1.$$

**3.5** For *a subsequent* rth *row* with non-blank columns on the left hand part of **region H**

$$\sqrt{(r-1)p} < j \le \sqrt{(2rp-p-1)/2},$$

and for the non-blank right hand part of **region H**

$$\sqrt{(2rp-p-1)/2} < j \le \sqrt{rp-1}.$$

**Theorem 3.5 (disparities)**. *The* rth *row of the left hand part of* **region H** *has at most one less perfect square than the right hand part. The difference is, taking integer parts*

$$[\lfloor\sqrt{(2rp-p-1)/2}\rfloor - \lfloor\sqrt{(r-1)p}\rfloor] - [\lfloor\sqrt{rp-1}\rfloor - \lfloor\sqrt{(2rp-p-1)/2}\rfloor] = 2\lfloor\sqrt{(2rp-p-1)/2}\rfloor - \lfloor\sqrt{rp-1}\rfloor - \lfloor\sqrt{(r-1)p}\rfloor.$$

*Proof*. Let $\lfloor A\rfloor$ be the floor of the positive real number A and bit{A} be $A - \lfloor A\rfloor$. The maximum value of $\lfloor 2A\rfloor - 2\lfloor A\rfloor$ is 1, where the minimum is zero, and the maximum value of $\lfloor C + D\rfloor - \lfloor C\rfloor - \lfloor D\rfloor$ is 1, with minimum zero.

For positive real numbers a and b, on squaring twice we confirm

$$2\sqrt{a + (b/2)} > \sqrt{a+b} + \sqrt{a}.$$

Thus

$$\lfloor 2\sqrt{a + (b/2)}\rfloor + \text{bit}[2\sqrt{a + (b/2)}] > \lfloor\sqrt{a+b} + \sqrt{a}\rfloor + \text{bit}[\sqrt{a+b} + \sqrt{a}].$$

Hence

$$\lfloor 2\sqrt{a + (b/2)}\rfloor \ge \lfloor\sqrt{a+b} + \sqrt{a}\rfloor$$
$$\ge \qquad\qquad \ge$$
$$2\lfloor\sqrt{a + (b/2)}\rfloor \quad \lfloor\sqrt{a+b}\rfloor + \lfloor\sqrt{a}\rfloor.$$

The maximum disparity occurs when $\lfloor 2\sqrt{a + (b/2)}\rfloor - 2\lfloor\sqrt{a + (b/2)}\rfloor = 1$ and when $\lfloor\sqrt{a+b} + \sqrt{a}\rfloor - \lfloor\sqrt{(a+b)}\rfloor - \lfloor\sqrt{(a)}\rfloor = 0$. In this case

$$2\lfloor\sqrt{a + (b/2)}\rfloor \rfloor \ge \lfloor\sqrt{a+b}\rfloor + \lfloor\sqrt{a}\rfloor - 1.$$

However, the only case where the '*minus* 1' above is operative is when

$$2\lfloor\sqrt{a + (b/2)}\rfloor \rfloor = \lfloor\sqrt{a+b}\rfloor + \lfloor\sqrt{a}\rfloor - 1.$$

The result above follows putting a = (r – 1)p and b = (p – 1). □

Note that $\lfloor 2\sqrt{a + (b/2)}\rfloor - 2\lfloor\sqrt{a + (b/2)}\rfloor = 1$ implies $\lfloor 2\sqrt{a + (b/2)}\rfloor$ is odd.

We infer that when a row has an even number of perfect squares, because the difference between the left hand part and right hand part is at most -1, there must be an equal number in the left and right hand parts, or an excess of left over right.

**3.6** Next consider **region H** *after row* T, that is, where the difference between adjacent perfect squares > (p – 1)/2.

On *blanks*, no row can be entirely blank – this is self-evident.

No row can contain a blank on the left, or respectively the right, part and two or more entries on the right, or respectively left, part, since if the separation between perfect squares is > (p – 1)/2, with a blank left, so that position n on the right is occupied, the next position on the right hand part would be at least [(p – 1)/2] + n + 2 further on the right, which goes past its boundary.

Similarly, if the right is blank, then if the left interval is occupied at greatest position n, the preceding square value is a distance at least (p – 1) – n – 2 to the left of this n, with n ≤ (p – 1)/2, which is not in the left interval.

These arguments show that, starting from the last row, if the left hand or right hand parts contain a blank, then preceding rows of both sides can contain no more than one perfect square in the left hand part and one in the right.

Under certain conditions, if the right hand part of **region H** contains entries sufficiently near its left hand edge, then the corresponding left hand part of **region H** is blank.

In this situation, counting from the last row, if i = 1, … x successive perfect squares are situated on the right hand part of **region H** in position $w_x$ from the left edge of that part, and square $n^2$ is in row u, then

$$(u – 1)p + (p + 1)/2 = n^2 – w_1,$$
$$(u – 2)p + (p + 1)/2 = (n – 1)^2 – w_2,$$
$$\dots$$
$$(u – x)p + (p + 1)/2 = (n – x + 1)^2 – w_x,$$

with each $w_i$ positive and $w_{x+1} < p$, i.e.

$$p = (n – x + 1)^2 – (n – x)^2 – w_x + w_{x+1},$$

so

$$2n – 2x + 1 > w_x.$$

Conversely, for the first x in sequence satisfying the relation $w_{x+2} > p$, all rows identified by 1 to x are blank on the left hand part of **region H**.

Also, for this particular x, $w_{x+1}$ in the right hand part is matched by a perfect square in the left hand part, which is the start of a new trajectory.

**3.7** *We now work back from the last perfect square* in **region H**. This concerns the number $[(p – 1)/2]^2$, so this is on place $[p(p + 1) – (p – 1)^2]/4$ from the *rightmost* column of this row, i.e. this last perfect square is at (p + 1)/4 from the *left hand side* of **region H**.

Further, the column spacing between adjacent squares for a trajectory increases by two each time, so the vth perfect square counting backwards from the last perfect square at v = 1 is at

$$[(p + 1)/4] + 2[1 + 2 + \dots (v – 1)] = (p + 1)/4 + v(v – 1)$$

from the left hand side of **region H**. So provided

$$(p + 1)/4 + v(v – 1) \leq (p – 1)/2$$

the last v quadratic residues are on the left hand part of **region H**, with

$$v \leq (\sqrt{p – 2} + 1)/2.$$

We have argued that if it is not in the first r non-blank rows, the row corresponding to this v + 1 is blank on the left hand part. In the previous table for p = 83 we see the two adjacent blank lines for the left hand part of **region H** are on the right hand part a continuation of the *trajectory* of rows, the last such with also one square on the left.

For p = 4k – 1, so (p – 1)/2 is odd, sp – 1 is not a quadratic residue, since

$$(sp - 1)^{(p-1)/2} - 1 \neq 0 \pmod{p}.$$

Thus for the right hand part

$$(p + 1)/4 + v(v - 1) \leq p - 2,$$

and so

$$(\sqrt{p - 2} + 1)/2 < v \leq (\sqrt{3p - 8} + 1)/2,$$

which means for the first pass through of this trajectory the number of perfect squares on the left is not less than those on the right. This can be deduced, for X > 12, from

$$2\lfloor X/\sqrt{3}\rfloor - \lfloor X\rfloor > 0.$$

**3.8** We will work in the region *beginning from the bottom row trajectory up to the trajectory starting just before row* T. At most one perfect square exists in both the left hand and right hand parts of these trajectories.

Since trajectories are ascending and terminate on the right, there is an *overlap* of the last perfect square of a trajectory with the right hand part of row T – then subtract a residue from the right hand side of row T – this will improve our result by 1.

We calculate that, on the left hand part, for the (m + 1)th pass through on a trajectory

$$mp < (p + 1)/4 + v(v - 1) \leq mp + (p - 1)/2$$

so

$$[\sqrt{(4m - 1)p} + 1]/2 < v \leq [\sqrt{(4m - 1)p - 2} + 1]/2.$$

For m = 0, however, the left hand side is zero in the above expression. On the right hand part of **region H** we have

$$mp + (p - 1)/2 < (p + 1)/4 + v(v - 1) \leq (m + 1)p - 2$$

so

$$[\sqrt{(4m + 1)p - 2} + 1]/2 < v \leq [\sqrt{(4m + 3)p - 8} + 1]/2.$$

**3.9** *To calculate the number of trajectories up to the one intersecting with row* T, note that the perfect squares from 1 to the last square in row T always satisfy

$$j^2 < pT.$$

The number of perfect squares from 1 up to and including row T, but without the overlap perfect square, is then

$$j_{max} = \left\lfloor \sqrt{p\left\lfloor \frac{p+10}{16} \right\rfloor} \right\rfloor - 1 = (p - 7)/4$$

for k ≡ 0 or 1 (mod 4), and p > 3, but for k ≡ 2 or 3 (mod 4)

$$j_{max} = (p - 3)/4.$$

The total number of residues is (p – 1)/2.

If the number of trajectories from the end to the trajectory overlapping with row T is (M + 1), where the number of trajectory perfect squares is

$$J = \left\lfloor \sqrt{\left(M + \frac{3}{4}\right)p - 2} + \frac{1}{2} \right\rfloor,$$

then we have just deduced

$$(p - 1)/2 = j_{max} + J.$$

We verify from a binomial theorem expansion, that even in the least favourable cases

$$\sqrt{\left(M + \tfrac{13}{16}\right)p} + 1 > J > \sqrt{\left(M + \tfrac{11}{16}\right)p} - 1,$$

so when $j_{max} = (p - 7)/4$, then

$$[p - 11 + (1/p)]/16 < M < [p + 7 + (81/p)]/16,$$

which implies $M = \lfloor (p + 1)/16 \rfloor$, and when $j_{max} = (p - 3)/4$, we find

$$[p - 19 + (9/p)]/16 < M < [p - 1 + (25/p)]/16,$$

giving $M = \lfloor (p - 15)/16 \rfloor$, or zero for $p \leq 11$.

## 4 Disparity formulas and a condition for positive total disparity.

**4.1** *Putting this all together*, and using the values shown later

$$\lfloor \sqrt{rp - \tfrac{p+1}{2}} \rfloor = \lfloor \sqrt{rp - \tfrac{p}{2}} \rfloor,$$

$$\lfloor \sqrt{rp - 1} \rfloor = \lfloor \sqrt{rp} \rfloor,$$

and that subsequent investigation shows the difference for row T is zero, the difference between the residues in the left hand part minus the right hand part therefore sums in total to equal to

(difference in 1st row) + (difference in rows 2 to (T – 1)) + (overlap row T)
+ (difference for trajectories 1 to M) + (difference for trajectory m = 0).

Using previous results, we obtain as **Theorem 4.1 (the total difference expression)**

$$2\lfloor \sqrt{p/2} \rfloor - \lfloor \sqrt{p} \rfloor + \sum_{r=2}^{T-1} [2\lfloor \sqrt{rp - (p/2)} \rfloor - \lfloor \sqrt{rp} \rfloor - \lfloor \sqrt{(r-1)p} \rfloor] + 1$$
$$+ \sum_{m=1}^{M} [2\lfloor \sqrt{\left(m + \tfrac{1}{4}\right)p - \tfrac{1}{2}} + \tfrac{1}{2} \rfloor$$
$$- \lfloor \sqrt{\left(m + \tfrac{3}{4}\right)p - 1} + \tfrac{1}{2} \rfloor - \lfloor \sqrt{\left(m - \tfrac{1}{4}\right)p} + \tfrac{1}{2} \rfloor$$
$$+ 2\lfloor \sqrt{\tfrac{p}{4} - \tfrac{1}{2}} + \tfrac{1}{2} \rfloor - \lfloor \sqrt{\tfrac{3}{4}p - 1} + \tfrac{1}{2} \rfloor. \square$$

**4.2 Theorem 4.2 (central interval quadratic residues)**. *Let prime* $p = 4k - 1$. *There are* $(p + 1)/4$ *quadratic residues in the interval* $[(p + 1)/4, (3p - 1)/4]$.

*Proof.* The interval is the last k slots in the left hand part of **region H** and the first k slots in the right hand part of **region H**. These slots are antisymmetric in the sense that if x is at a quadratic residue then p – x is not, and if x is not at a quadratic residue then p – x is. Thus the sum of the number of quadratic residues in this interval is k. □

It follows by identical reasoning that there are (k – 1) quadratic residues in the combined intervals $[1, k - 1] \cup [3k, 4k - 2]$, and consequently the number of quadratic residues in $\{[1, k - 1] \cup [3k, 4k - 2]\}$ minus $[k, 3k - 1]$ is -1. We call this the *shifted disparity* for $p = 4k - 1$.

**4.3 Theorem 4.3 (simplified total disparity and simplified total shifted disparity)**. The total disparity is

$$\sum_{r=1}^{\frac{p+1}{4}}[2\lfloor\sqrt{rp-(p/2)}\rfloor-\lfloor\sqrt{rp}\rfloor-\lfloor\sqrt{(r-1)p}\rfloor] \quad (1)$$

or equivalently this can be simplified to

$$2\sum_{r=1}^{\frac{p+1}{4}}[\lfloor\sqrt{rp-(p/2)}\rfloor-\lfloor\sqrt{rp}\rfloor]+(p-1)/2.\ \square \quad (2)$$

For the total shifted disparity, the intervals are $\{[1, (p-3)/4] \cup [3(p+1)/4, p-1]\} - [(p+1)/4, (3p-1)/4]$, so for a row the shifted disparity is

$$\{\lfloor\sqrt{(r-1)p+\tfrac{p-3}{4}}\rfloor-\lfloor\sqrt{(r-1)p}\rfloor + \lfloor\sqrt{(r-1)p+p-1}\rfloor-\lfloor\sqrt{(r-1)p+\tfrac{3p-1}{4}}\rfloor\} - \{\lfloor\sqrt{(r-1)p+\tfrac{3p-1}{4}}\rfloor-\lfloor\sqrt{(r-1)p+\tfrac{p-3}{4}}\rfloor\}.$$

Now $\lfloor\sqrt{rp-1}\rfloor = \lfloor\sqrt{rp}\rfloor$, because $r < p$ and $rp$ is not a square. Thus this sum from 1 to $(p+1)/4$ is

$$2\sum_{r=1}^{\frac{p+1}{4}}[\lfloor\sqrt{rp-\tfrac{3(p+1)}{4}}\rfloor-\lfloor\sqrt{rp-\tfrac{p+1}{4}}\rfloor]+\lfloor\sqrt{\tfrac{p+1}{4}}\rfloor$$

and the value of the total shifted disparity is -1, so that zero is

$$0 = 2\sum_{r=1}^{\frac{p+1}{4}}[\lfloor\sqrt{rp-\tfrac{3(p+1)}{4}}\rfloor-\lfloor\sqrt{rp-\tfrac{p+1}{4}}\rfloor]+(p+1)/2.\ \square \quad (3)$$

Without the floor functions operating, (1) is positive, as under the same circumstances are (2) + (3) and (2) – (3). For instance, (2) + (3) sums to terms $[p(p-1)/(32X^{3/2})] + \Delta$, where $X = rp - (5p+3)/8$ and $\Delta$ is a negative valued sum of higher order terms.

**4.4** We now obtain, using the simplified expression for the total disparity, a necessary and sufficient condition for its positive nature.

**Theorem 4.4 (condition for a positive total disparity)**. *The total disparity is positive if and only if there exists a* $\nu_N$ *satisfying* (10), *defined in* (7) *and* (8), *so that relation* (12) *holds*.

*Proof*. Expanded out, the total disparity expression can be written as

$$2[\lfloor\sqrt{p/2}\rfloor-\lfloor\sqrt{p}\rfloor+\lfloor\sqrt{3p/2}\rfloor-\lfloor\sqrt{2p}\rfloor + \lfloor\sqrt{5p/2}\rfloor-\lfloor\sqrt{3p}\rfloor+\ldots+\lfloor\sqrt{\left(r-\tfrac{1}{2}\right)p}\rfloor-\lfloor\sqrt{rp}\rfloor+\ldots + (p-3)/2-(p-1)/2] + (p-1)/2. \quad (4)$$

Consider the series

$$U = \sum_{r=1}^{\frac{p+1}{2}}[(-1)^{r+1}[a+\sum_{s=1}^{r-1}[\varepsilon_s]]], \quad (5)$$

then this sum is

$$U = -\sum_{s=1}^{\frac{p+1}{4}}[\varepsilon_{2s-1}].$$

If we say (4) is of the form

$$2U + (p - 1)/2, \qquad (6)$$

then the first term is

$$a = \lfloor \sqrt{p/2} \rfloor,$$

and the last term equates to

$$(p - 1)/2 = \lfloor \sqrt{p/2} \rfloor - U + \sum_{s=1}^{\frac{p-3}{4}} [\varepsilon_{2s}].$$

As incidental motivation, we note that

$$\lfloor \sqrt{(r-2)p} \rfloor < \lfloor \sqrt{rp} \rfloor,$$

since by a binomial expansion of the left hand side

$$\lfloor \sqrt{rp} - \sqrt{p/r} - \Delta \rfloor < \lfloor \sqrt{rp} \rfloor,$$

where the representation of higher order terms, $-\Delta$, is negative, and the lowest value of $\lfloor \sqrt{p/r} \rfloor$ is $\lfloor \sqrt{4p/(p+1)} \rfloor$, the value of which is 1. All other values of $\lfloor \sqrt{p/r} \rfloor$ are equal or greater than 2.

We see that $\varepsilon_{(p-1)/2} = 0$. If we evaluate $\varepsilon_{(p-3)/2}$, this is just

$$\lfloor \sqrt{(r - \tfrac{1}{2})p} \rfloor - \lfloor \sqrt{(r-1)p} \rfloor,$$

where $r = (p + 1)/4$, so this is

$$\lfloor (p-1)/2 \rfloor - \lfloor (p-2)/2 \rfloor = 1.$$

This is part of a more general phenomenon for $\varepsilon_{2s+1}$ and $\varepsilon_{2s}$, within limits.

For the $\varepsilon$ terms in the series (5) for sufficiently small always even or always odd r, there exists a t with

$$\Sigma(\text{t successive values})\varepsilon_r \geq \Sigma(\text{t successive values})\varepsilon_{r+2},$$

this condition being

$$\varepsilon_r \geq \varepsilon_{r+2t}.$$

Similar considerations lead us to ask whether, starting from s = 1

$$\Sigma(\text{t successive values})\varepsilon_{2s} \geq \Sigma(\text{t successive values})\varepsilon_{2s+1},$$

where we will be choosing $t = (p - 3)/4$.

Consider for positive $B_s$ and $C_s$

$$\sum_{s=1}^{N} B_s > \sum_{s=1}^{N} C_s,$$

then

$$\sum_{s=1}^{N} [\lfloor B_s \rfloor] \geq \sum_{s=1}^{N} [\lfloor C_s \rfloor] - (N - 1),$$

so that there will be values $-N \leq \nu_N \leq N$ satisfying

$$\sum_{s=1}^{N} [\lfloor B_s \rfloor] \geq \sum_{s=1}^{N} [\lfloor C_s \rfloor] - (\nu_N - 1).$$

We stipulate that the floor function satisfies

$$-\lfloor B \rfloor = \lfloor -B \rfloor.$$

Now

$$\varepsilon_{2s} = \lfloor \sqrt{(s + \tfrac{1}{2})p} \rfloor - \lfloor \sqrt{sp} \rfloor,$$

$$\varepsilon_{2s+1} = \lfloor \sqrt{(s+1)p} \rfloor - \lfloor \sqrt{(s + \tfrac{1}{2})p} \rfloor.$$

Let

$$E_{2s} = \sqrt{\left(s + \tfrac{1}{2}\right)p} - \sqrt{sp},$$

$$E_{2s+1} = \sqrt{(s+1)p} - \sqrt{\left(s + \tfrac{1}{2}\right)p}.$$

We will also write

$$bit_{2s} = E_{2s} - \varepsilon_{2s}, \tag{7}$$

$$bit_{2s+1} = E_{2s+1} - \varepsilon_{2s+1}. \tag{8}$$

Then

$$E_{2s} > E_{2s+1},$$

since in terms of $\sqrt{\left(s + \tfrac{1}{2}\right)p}$

$$E_{2s} = \sqrt{\left(s + \tfrac{1}{2}\right)p}[1 - [1 - [1/(2s+1)]]^{1/2}],$$

$$E_{2s+1} = \sqrt{\left(s + \tfrac{1}{2}\right)p}[[1 + [1/(2s+1)]]^{1/2} - 1],$$

and the result follows to second order on a binomial expansion.

Hence

$$\sum_{s=1}^{N} E_{2s} > \sum_{s=1}^{N} E_{2s+1},$$

so

$$\sum_{s=1}^{N} \varepsilon_{2s} \geq \sum_{s=1}^{N} \varepsilon_{2s+1} - (\nu_N - 1), \tag{9}$$

where also

$$\sum_{s=1}^{N} \varepsilon_{2s} \geq \sum_{s=1}^{N} \varepsilon_{2s+1} + \left\lfloor \sum_{s=1}^{N} [bit_{2s+1} - bit_{2s}] \right\rfloor + 1,$$

in which we may allocate

$$\nu_N = \left\lfloor \sum_{s=1}^{N} [-bit_{2s+1} + bit_{2s}] \right\rfloor. \tag{10}$$

The relationship between $\varepsilon_{2s}$ and $\varepsilon_{2s+1}$ may be encapsulated as

$$\sum_{s=1}^{N} [\varepsilon_{2s}] = -\lfloor \sqrt{p} \rfloor - \sum_{s=1}^{N} [\varepsilon_{2s+1}] + \lfloor \sqrt{Np} \rfloor.$$

Thus by (7)

$$2\sum_{s=1}^{N} [\varepsilon_{2s+1}] \leq \lfloor \sqrt{Np} \rfloor - \lfloor \sqrt{p} \rfloor + (\nu_N - 1),$$

and simultaneously

$$2\sum_{s=1}^{N} [\varepsilon_{2s}] \geq \lfloor \sqrt{Np} \rfloor - \lfloor \sqrt{p} \rfloor - (\nu_N - 1).$$

We can also prove

$$\sum_{s=1}^{N} [E_{2s}] < \sum_{s=1}^{N} [E_{2s-1}],$$

this following from the case for individual elements, implying for $-N \leq \nu'_N \leq N$

$$\sum_{s=1}^{N} [\varepsilon_{2s}] \leq \sum_{s=1}^{N} [\varepsilon_{2s-1}] + (\nu'_N - 1),$$

where now

$$\begin{aligned} \nu'_N &= \left\lfloor \sum_{s=1}^{N} [bit_{2s-1} - bit_{2s}] \right\rfloor \\ &= \left\lfloor \sum_{s=1}^{N} [bit_1 + bit_{2s+1} - bit_{2N+1} - bit_{2s}] \right\rfloor \\ &= -\nu_N + 0 \text{ or } \pm 1, \end{aligned}$$

so that by parallel reasoning using

$$\begin{aligned} \sum_{s=1}^{N} [\varepsilon_{2s}] = {} & \lfloor \sqrt{p/2} \rfloor - 2\lfloor \sqrt{p} \rfloor - \sum_{s=1}^{N} [\varepsilon_{2s-1}] \\ & + \left\lfloor \sqrt{(N-1)p} \right\rfloor - \left\lfloor \sqrt{\left(N - \tfrac{1}{2}\right)p} \right\rfloor + \lfloor \sqrt{Np} \rfloor, \end{aligned}$$

we derive

$$2\sum_{s=1}^{N}[\varepsilon_{2s-1}] \geq \lfloor\sqrt{p/2}\rfloor - 2\lfloor\sqrt{p}\rfloor - (\nu'_N - 1) + \lfloor\sqrt{(N-1)p}\rfloor - \lfloor\sqrt{\left(N-\tfrac{1}{2}\right)p}\rfloor + \lfloor\sqrt{Np}\rfloor,$$

from which we deduce

$$2\sum_{s=1}^{N}[\varepsilon_{2s+1}] \geq 3\lfloor\sqrt{p/2}\rfloor - 4\lfloor\sqrt{p}\rfloor + 2\lfloor\sqrt{(N+1)p}\rfloor - 2\lfloor\sqrt{\left(N+\tfrac{1}{2}\right)p}\rfloor - (\nu'_N - 1) + \lfloor\sqrt{(N-1)p}\rfloor - \lfloor\sqrt{\left(N-\tfrac{1}{2}\right)p}]\rfloor + \lfloor\sqrt{Np}\rfloor,$$

and under the same conditions

$$2\sum_{s=1}^{N}[\varepsilon_{2s}] \leq \lfloor\sqrt{p/2}\rfloor - 2\lfloor\sqrt{p}\rfloor + \lfloor\sqrt{(N-1)p}\rfloor - \lfloor\sqrt{\left(N-\tfrac{1}{2}\right)p}\rfloor + \lfloor\sqrt{Np}\rfloor + (\nu'_N - 1).$$

We now specialise for $\varepsilon_{2s}$ and $N = (p-3)/4$, giving

$$\tfrac{1}{2}\{\lfloor\sqrt{p/2}\rfloor - 2\lfloor\sqrt{p}\rfloor + [(p-5)/2] - \nu_N - 1 + (0 \text{ or } \pm 1)\} \geq -\sum_{s=1}^{\frac{p-3}{4}}[\varepsilon_{2s}] \geq \tfrac{1}{2}\{-\lfloor\sqrt{p}\rfloor + [(p-3)/2] - \nu_N + 1\},$$

whereas for $\varepsilon_{2s+1}$

$$\tfrac{1}{2}\{-\lfloor\sqrt{p}\rfloor + [(p-3)/2] + \nu_N - 1\} \geq \sum_{s=1}^{\frac{p-3}{4}}[\varepsilon_{2s+1}] \geq \tfrac{1}{2}\{3\lfloor\sqrt{p/2}\rfloor - 4\lfloor\sqrt{p}\rfloor + [(p-5)/2] + \nu_N + 1 - (0 \text{ or } \pm 1)\}. \qquad (11)$$

For equation (6) to be positive

$$(p-1)/2 > 2\varepsilon_1 + 2\sum_{s=1}^{\frac{p-3}{4}}[\varepsilon_{2s+1}].$$

Using the maximum value of $2\sum_{s=1}^{\frac{p-3}{4}}[\varepsilon_{2s+1}]$ in (11) gives

$$\nu_N \leq 2\lfloor\sqrt{p/2}\rfloor - \lfloor\sqrt{p}\rfloor - 1. \ \square \qquad (12)$$

In order to prove a positive total disparity, this result shows that general algebraic manipulations of the sort that are equivalent to the ignoring of the distribution of non-integer parts are ineffective, and so it is necessary to utilise the structure of the patterns of residues within the row and trajectory regions. Unresolved is whether a judicious choice of variables may be effective in cancelling or deriving these non-integer parts.

## 5 Ancillary remarks.

**5.1** *The number of perfect squares* for a complete row, r, is

$$\lfloor\sqrt{rp-1}\rfloor - \lfloor\sqrt{rp-p}\rfloor,$$

and since $\sqrt{rp}$ is not a square

$$\lfloor\sqrt{rp-1}\rfloor = \lfloor\sqrt{rp}\rfloor.$$

Consider the number of perfect squares for row r minus those for row (r + 1). This is

$$2\lfloor\sqrt{rp}\rfloor - \lfloor\sqrt{rp - p}\rfloor - \lfloor\sqrt{rp + p}]\rfloor.$$

**Theorem 5.1 (sum of floor functions involving plus and minus a constant)**

$$2\lfloor X\rfloor \geq \lfloor X + A - ½\rfloor + \lfloor X - A - ½\rfloor.$$

*Proof.* Floor values on the right are maximised as the value of bit{X} approaches 1, and the integer part on the left is unchanged by this. Then if bit{X} $\geq$ bit{A} > ½, the first integer part on the right is either $\lfloor X\rfloor + \lfloor A\rfloor$ or $\lfloor X\rfloor + \lfloor A\rfloor + 1$ and the second is $\lfloor X\rfloor - \lfloor A\rfloor - 1$, and if bit{X} > bit{A} and bit{A} $\leq$ ½, the first integer part on the right is $\lfloor X\rfloor + \lfloor A\rfloor$ and the second is either $\lfloor X\rfloor - \lfloor A\rfloor$ or $\lfloor X\rfloor - \lfloor A\rfloor - 1$. □

Thus the number of perfect squares for row (r + 1) will always be less than or equal to row r when

$$2\lfloor\sqrt{rp}\rfloor \geq \lfloor\sqrt{rp}[1 - (1/2r) - (1/8r^2) - \dots\ ]\rfloor + \lfloor\sqrt{rp}[1 + (1/2r) - (1/8r^2) + \dots - \dots\ ]\rfloor,$$

and so this will always occur when

$$\sqrt{rp}(1/8r^2) \geq ½.$$

Hence if r = 1 this must happen when p $\geq$ 19, for r = 2 when p $\geq$ 139 (although both these occur for all relevant p) and generally for a prime (4k – 1) when $p > 16r^3$.

Note that for p = 151, the number of perfect squares for the interval [1, 2k – 1], in the left hand part of **region H**, can increase as the row number increases. For row 4 there is one perfect square, $22^2 = 484$ on the left, and for row 5 two such squares, $25^2 = 625$ and $26^2 = 674$.

For p = 127, the same type of situation occurs on the interval [2k, 4k – 2], the right of **region H**. For row 4 there is one such perfect square, 484, and for row 5 two perfect squares, $24^2 = 576$ and 625.

**5.2** We now prove that -1 *disparities, that is excess of right hand over left hand perfect squares, occur in non-overlapping clusters of rows,* each cluster of which is designated by a different number of perfect squares for the row. We will ignore rows with an even number of squares, and since -1 disparities occur in rows with an odd number of squares, say 2t + 1, we have for these

$$\begin{aligned} 2t + 1 &= \lfloor\sqrt{rp}\rfloor - \lfloor\sqrt{(r - 1)p}\rfloor \\ &= \lfloor\sqrt{rp}\rfloor - \lfloor[\lfloor\sqrt{rp}\rfloor + \text{bit}\{\sqrt{rp}\}][1 - (1/2r) - (1/8r^2) - \dots]\rfloor \\ &= \lfloor\sqrt{rp}[(1/2r) + (1/8r^2) + \dots]\rfloor, \end{aligned}$$

so the lowest bit value of $\sqrt{rp}[(1/2r) + (1/8r^2) + \dots]$ satisfies to first order

$$2r(2t + 1) < \sqrt{rp} < 2r(2t + 2).$$

We can be precise by replacing r by a function slightly less than r, but approximately

$$4r(2t + 1)^2 < p < 4r(2t + 2)^2,$$

and the highest bit value satisfies

$$2r(2t) < \sqrt{rp} < 2r(2t + 1)$$

or

$$4r(2t)^2 < p < 4r(2t + 1)^2.$$

On incrementing $t \to t + 1$, r changes to r′. If a lowest bit value transforms to a lowest bit value then r decrements, likewise for a highest bit value transforming to a highest bit value. If a lowest bit value transforms to a highest bit value then $r \to r'$ decreases and if a highest bit value transforms to a lowest bit value then

$$4r'(2t + 3)^2 < p < 4r(2t + 1)^2,$$

and r again decrements.

For constant t, ignoring rows with an even number of perfect squares, as the values of r increase in sequence, this forms a cluster of filled-out rows of perfect squares and if t increments, it must correspond to a value of r before this cluster. Similarly, if t decrements, r comes after the cluster.

## 6 Some constraints on -1 disparities up to row T.

### 6.1 *For -1 disparities we investigate small row values*, r.

Since $\lfloor\sqrt{rp - \frac{p+1}{2}}\rfloor = \lfloor\sqrt{rp - (p/2)}\rfloor$, because p/2 is not an integer, the expression for the difference between left and right perfect squares may be written as

$$2\lfloor\sqrt{rp - (p/2)}\rfloor - \lfloor\sqrt{rp}\rfloor - \lfloor\sqrt{(r-1)p}\rfloor,$$

and using the relation again

$$2\lfloor X\rfloor \geq \lfloor X + A - ½\rfloor + \lfloor X - A - ½\rfloor,$$

with $X = \sqrt{(rp - (p/2))}$, we consider

$$2\lfloor X\rfloor - \lfloor X[1 - (1/(2r-1)) - (1/8(2r-1)^2) - \ldots]\rfloor$$
$$- \lfloor X[1 + (1/(2r-1)) - (1/8(2r-1)^2) + \ldots - \ldots]\rfloor,$$

so the difference is always greater or equal to 0 provided

$$[\sqrt{p}(2r-1)^{½}]/[8\sqrt{2}(2r-1)^2] \geq ½,$$

i.e. $p > 32(2r-1)^3$.

Thus for r = 2, we only have to check primes $\leq$ 863 to determine whether this always holds. It does. For r = 3, non-trajectory -1 disparities exist for primes p = 67, 211, 227, 487, 547, 739, 883, 1123 and 1163, for values $\leq$ 3967, with none elsewhere. For r = 4, the corresponding entire set of primes is 103, 151, 163, 307, 311, 347, 367, 631, 683, 739, 743, 1063, 1091, 1123, 1163, 1607, 1783, 2311, 2411, 2467, 2971, 3083, 3203, 3271, 3907, 3911, 4111, 4903, 5051 and 6007, and for r = 5, 107, 127, 199, 211, 227, 443, 463, 467, 487, 823, 907, 967, 1283, 1447, 1451, 1483, 1487, 1523, 1567, 2003, 2083, 2087, 2131, 2311, 2887, 3083, 3251, 3307, 3923, 4099, 5059, 5407, 6271, 6343, 6491, 6563, 6571, 7687, 7927, 8011, 8191, 9419, 9511, 11047, 11239, 11243, 13007 and 15131.

### 6.2 If we consider *the difference for row* T, where for $\alpha, \beta \in \mathbf{N}$

$$k = 4\alpha + \beta$$

with $\beta$ = 0, 1, 2 or 3, and omitting p = 3, 7 and 11 corresponding to $\alpha$ = 0 for $\beta$ = 1, 2 or 3, which we can deal with separately, if row

$$r = \lfloor(4k + 9)/16\rfloor,$$

we observe on setting p = 4k – 1 and (r – 1)p = (4k – 1)$\lfloor$(4k – 7)/16$\rfloor$ that the ‘minus 1’ alluded to previously disappears, namely

$$2\lfloor\sqrt{[(4k-1)\lfloor(4k-7)/16\rfloor + 2k - 1]}\rfloor$$

$$= \lfloor \sqrt{[(4k-1)\lfloor (4k-7)/16 \rfloor + 4k - 2]} \rfloor$$
$$+ \lfloor \sqrt{[(4k-1)\lfloor (4k-7)/16 \rfloor]} \rfloor,$$

since derived from this equality, and reversibly, the following identities are valid.

For $\beta = 0, 1$

$$2\lfloor \sqrt{[16\alpha^2 - 9\alpha + 4\beta\alpha]} \rfloor$$
$$= \lfloor \sqrt{[16\alpha^2 - \alpha + 4\beta\alpha - 1]} \rfloor + \lfloor \sqrt{[16\alpha^2 - 17\alpha + 4\beta\alpha - 4\beta + 1]} \rfloor,$$

so for $\beta = 0$ this reduces to

$$2[4\alpha - 2] = [4\alpha - 1] + [4\alpha - 3]$$

and for $\beta = 1$

$$2[4\alpha - 1] = [4\alpha] + [4\alpha - 2].$$

For $\beta = 2$ or 3

$$2\lfloor \sqrt{[16\alpha^2 + 7\alpha + 4\beta\alpha + 2\beta - 1]} \rfloor$$
$$= \lfloor \sqrt{[16\alpha^2 + 15\alpha + 4\beta\alpha + 4\beta - 2]} \rfloor + \lfloor \sqrt{[16\alpha^2 - \alpha + 4\beta\alpha]} \rfloor,$$

so for $\beta = 2$ this becomes

$$2[4\alpha + 1] = [4\alpha + 2] + [4\alpha],$$

whereas for $\beta = 3$ this implies

$$2[4\alpha + 2] = [4\alpha + 3] + [4\alpha + 1].$$

**6.3** *For the disparity using a row*, r, *prior to row* T, we consider

$$r = \lfloor (4k + 9)/16 \rfloor - y$$

where the minimum value of y is 0, which we have discussed already as row T, so choose y = 1, and the maximum value is

$$\lfloor (4k + 9)/16 \rfloor - 2 = \lfloor (4k - 23)/16 \rfloor.$$

Then $p(r - 1) = (4k - 1)\lfloor (4k - 7 - 16y)/16 \rfloor$.

We will investigate whether the ‘minus 1’ case disappears again, this time for totals under generalised assumptions. For each row $r < T$ we establish the difference

$$2\lfloor \sqrt{[(4k-1)\lfloor (4k-7-16y)/16 \rfloor + 2k - 1]} \rfloor$$
$$- \lfloor \sqrt{[(4k-1)\lfloor (4k-7-16y)/16 \rfloor + 4k - 2]} \rfloor$$
$$- \lfloor \sqrt{[(4k-1)\lfloor (4k-7-16y)/16 \rfloor]} \rfloor.$$

For $\beta = 0$ this difference is

$$2\lfloor \sqrt{[16\alpha^2 - 16\alpha y - 9\alpha + y]} \rfloor - \lfloor \sqrt{[16\alpha^2 - 16\alpha y - \alpha + y - 1]} \rfloor$$
$$- \lfloor \sqrt{[16\alpha^2 - 16\alpha y - 17\alpha + y + 1]} \rfloor,$$

for $\beta = 1$

$$2\lfloor \sqrt{[16\alpha^2 - 16\alpha y - 5\alpha - 3y - 2]} \rfloor - \lfloor \sqrt{[16\alpha^2 - 16\alpha y + 3\alpha - 3y - 1]} \rfloor$$
$$- \lfloor \sqrt{[16\alpha^2 - 16\alpha y - 13\alpha - 3y - 3]} \rfloor,$$

$\beta = 2$ gives

$$2\lfloor \sqrt{[16\alpha^2 - 16\alpha y + 15\alpha - 7y + 3]} \rfloor - \lfloor \sqrt{[16\alpha^2 - 16\alpha y + 23\alpha - 7y + 6]} \rfloor$$
$$- \lfloor \sqrt{[16\alpha^2 - 16\alpha y + 7\alpha - 7y]} \rfloor$$

and for $\beta = 3$

$$2\lfloor \sqrt{[16\alpha^2 - 16\alpha y + 19\alpha - 11y + 5]} \rfloor - \lfloor \sqrt{[16\alpha^2 - 16\alpha y + 27\alpha - 11y + 10]} \rfloor$$
$$- \lfloor \sqrt{[16\alpha^2 - 16\alpha y + 11\alpha - 11y]} \rfloor.$$

If $\alpha = 1$ then row T is at maximum row 2, and T is also 2 for $\alpha = 2$ and $\beta = 0$.

For y = 1, successive values of $\beta$ give the difference, for $\beta = 0$ and $\alpha = 3$

$2[4\alpha - 4] - [4\alpha - 3] - [4\alpha - 6]$

and for $\beta = 0$ and $\alpha > 3$

$2[4\alpha - 4] - [4\alpha - 3] - [4\alpha - 5]$,

for $\beta = 1$ with $\alpha = 4$ (p prime implies $\alpha \neq 2$ or 3)

$2[4\alpha - 4] - [4\alpha - 2] - [4\alpha - 5]$,

so that in this instance there is a 'minus 1' disparity, whereas for $\beta = 1$ and $5 \leq \alpha \leq 7$ the difference is

$2[4\alpha - 3] - [4\alpha - 2] - [4\alpha - 5]$

and for $\beta = 1$ and $\alpha \geq 8$

$2[4\alpha - 3] - [4\alpha - 2] - [4\alpha - 4]$.

For $\beta = 2$ we have the zero disparity

$2[4\alpha - 1] - [4\alpha] - [4\alpha - 2]$,

and for $\beta = 3$ and $\alpha = 2$ or 3 the value

$2[4\alpha] - [4\alpha + 1] - [4\alpha - 2]$,

whereas for $\beta = 3$ and $\alpha \geq 6$ (p is not prime for $\alpha = 4$ and 5) this is

$2[4\alpha] - [4\alpha + 1] - [4\alpha - 1]$.

Thus there is no 'minus 1' disparity for $y = 1$, except for $\alpha = 4$ and $\beta = 1$, i.e. $p = 67$.

Let us look at these differences for $y > 1$ and $y^2 < \alpha$.

For $\beta = 0$ a binomial expansion to sufficient convergence at second order gives the difference

$$\begin{aligned} &2\lfloor[4\alpha - 2y - (9/8) + (y/8\alpha)] + [-(y^2/2\alpha) + (81/512\alpha^2) + (y^2/512\alpha^2) \\ &\quad + (y^2/512\alpha^3) + (9y/16\alpha) - (y^2/16\alpha^2) - (9y^2/256\alpha^2)]\rfloor \\ &\quad - \lfloor 4\alpha[1 + [-(y/\alpha) - (1/16\alpha) + (y/16\alpha^2)]]^{1/2}\rfloor \\ &\quad - \lfloor\sqrt{[16\alpha^2 - 16\alpha y - 17\alpha + y + 1]}\rfloor \\ &\quad = [8\alpha - 4y - 4] - [4\alpha - 2y - 1] - [4\alpha - 2y - 3], \end{aligned}$$

with algebraic manipulation obtaining the same final conclusion for $\beta = 1$.

For $\beta = 2$ we have a difference

$$\begin{aligned} &2\lfloor[4\alpha - 2y + 15/8 + (-4y^2 - 7y + 3)/8\alpha - \ldots\rfloor \\ &\quad - \lfloor[4\alpha - 2y + 23/8 + (-4y^2 - 7y + 6)/8\alpha - \ldots\rfloor \\ &\quad - \lfloor[4\alpha - 2y + 7/8 + (-4y^2 - 7y)/8\alpha - \ldots\rfloor \\ &\quad = [8\alpha - 4y + 2] - [4\alpha - 2y + 2] - [4\alpha - 2y], \end{aligned}$$

and for $\beta = 3$, if $2y^2 < \alpha$ then the difference is

$[8\alpha - 4y + 4] - [4\alpha - 2y + 3] - [4\alpha - 2y + 1]$,

and if $y^2 < \alpha \leq 2y^2$, then it is

$[8\alpha - 4y + 2] - [4\alpha - 2y + 2] - [4\alpha - 2y]$.

So for $y > 1$ and $y^2 < \alpha$, there is no 'minus 1' disparity.

If we look at the differences for $y > 1$ and $\alpha \leq y^2 < 2\alpha$, for $\beta = 0$ we have either

$[8\alpha - 4y - 4] - [4\alpha - 2y - 1] - [4\alpha - 2y - 3]$

or the difference

$[8\alpha - 4y - 4] - [4\alpha - 2y - 1] - [4\alpha - 2y - 4]$.

For $\beta = 1$ the possibilities are

$[8\alpha - 4y - 6] - [4\alpha - 2y - 2] - [4\alpha - 2y - 4]$

or as before

$[8\alpha - 4y - 4] - [4\alpha - 2y - 1] - [4\alpha - 2y - 3]$.

If we look at $\beta = 2$, a zero or +1 difference holds.

For $\beta = 3$ we are dealing with

$$2\lfloor[4\alpha - 2y + 2 + (3/8) - [(256y^2 + 96y + 41)/(512\alpha)] - \ldots\rfloor$$
$$-\lfloor[4\alpha - 2y + 3 + (3/8) - [(256y^2 - 160y + 89)/(512\alpha)] - \ldots\rfloor$$
$$-\lfloor[4\alpha - 2y + 1 + (3/8) - [(256y^2 + 352y + 121)/(512\alpha)] - \ldots\rfloor,$$

so we have the zero difference

$$[8\alpha - 4y + 2] - [4\alpha - 2y + 2] - [4\alpha - 2y],$$

since a difference of 1 cannot exist for $\alpha = 2$, because there is no value $y = 2$.

Once again, this time for $\alpha \leq y^2 < 2\alpha$, there is no 'minus 1' disparity.

We can also consider leading coefficients of 1, 4 and 9 for $\alpha^2$, say $y = 3(\alpha + \gamma)/4$ with 4 as a leading coefficient of $\alpha^2$, to determine the value of the disparity.

## 7 Trajectories.

**7.1 Theorem 7.1 (row-trajectory bijection)**. *There is a bijection between perfect square difference terms prior to row* T *and terms for trajectory differences*.

*Proof*. If we represent row differences prior to T by

$$2\lfloor\sqrt{p(\mu + \tfrac{1}{2}) - \tfrac{1}{2}}\rfloor - \lfloor\sqrt{p(\mu + 1) - 1}\rfloor - \lfloor\sqrt{p\mu}\rfloor$$

using $\mu = T - 1 - y$, then we see a bijection for the transformation $\mu \leftrightarrow m - ¼$ under the square root, with a further ½ in the floor, provided we recall the trajectory term

$$-\lfloor\sqrt{p(m + \tfrac{3}{4}) - 2} + ½\rfloor$$

was obtained previously by eliminating the final non-square. If we ignore this, the term is equivalently

$$-\lfloor\sqrt{p(m + \tfrac{3}{4}) - 1} + ½\rfloor.\square$$

**7.2** *To estimate the difference between the left hand and right hand parts for any trajectory*, suppose $A < B < C$, $z \in \mathbf{Z}$ and we can prove

$$(B - A) > (C - B) + z$$

then, since the maximum inequality between $2\lfloor B\rfloor$ and $\lfloor 2B\rfloor$ amounts to -1,

$$\lfloor B\rfloor - \lfloor A\rfloor \geq \lfloor C\rfloor - \lfloor B\rfloor + z - 1.$$

With $A = [\sqrt{[(h - 2)p]} + 1]/2$, $B = [\sqrt{[(hp - 2)]} + 1]/2$, $C = [\sqrt{[(h + 2)p - 8]} + 1]/2$ and $h = 4m + 1$, on squaring the trajectory relation ($2B > A + C$) twice, we get the result

$$p + 2h - 4 > 0,$$

which always holds.

This was for $z = 0$. For $z = 1$, on squaring twice (this is all that is necessary) we see the general relation is not satisfied for $h \geq 5$, although it must hold if $\text{bit}\{B\} \leq ½$, that is, for all occurrences of

$$1 = 1 - \lfloor 2\text{bit}\{B - \varepsilon\}\rfloor,$$

where $\varepsilon$ is a positive not well-ordered infinitesimal ($\forall n \in \mathbf{N}_{\neq 0}$, $\neg\exists m \in \mathbf{N}$: $\varepsilon m > n$).

On the other hand, if the condition

$$\text{bit}\{A\} + \text{bit}\{C\} \geq 1$$

holds, then because $(2B > A + C)$ is always true,

$$2\lfloor B \rfloor \geq \lfloor A \rfloor + \lfloor C \rfloor,$$

that is, there is no disparity of -1.

Further, for general A, B and C, not necessarily of this form, these two effects *add*. Thus for each trajectory, increased by one to a non-negative amount for each occurrence of $\text{bit}\{B\} \leq ½$, and increased similarly for every $\text{bit}\{A\} + \text{bit}\{C\} \geq 1$, the disparity between the left hand part and the right hand part of **region H** is $\geq$ -1.

**7.3** Disparities may be formulated as the following *Diophantine set.*

A trajectory for $p = 4k - 1$ may be represented by a parabola

$$d(v) = (p + 1)/4 + v(v - 1),$$

where for the lowest trajectory $d \equiv n^2 \pmod p$.

The minimum is at $v = ½$. The parabola can be extended from $v = 1$ to $v = p - 1$, to cover the whole range of values of the trajectory square label number, v.

The row that d is in may be equipartitioned as $[-1/4 + np, -1/4 + np + p/2]$ for the left hand part and $[-1/4 + np + p/2, -1/4 + (n + 1)p]$ for the right, giving the same result as previously for the disparities.

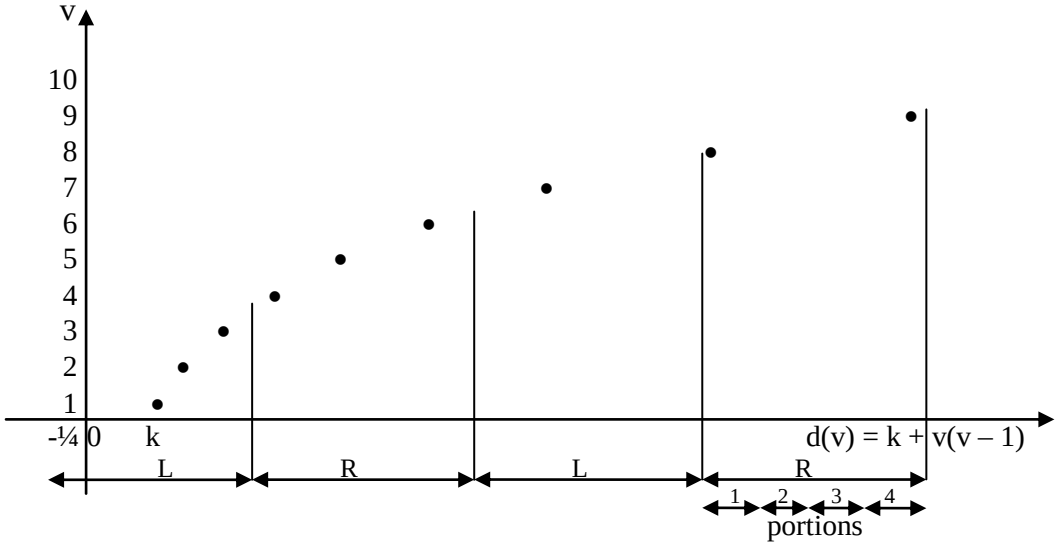
For rows up to T, the Diophantine set is simpler. We are dealing with

$$f(n) = n^2$$

under the same intervals as above. Zero is exceptionally included in the left hand equipartitioned interval.

**7.4** *We use lattice point counting methods for an increasing* d(v) *valuation of* v, *or* f(n) *of* n. These methods go beyond a purely local application of the floor function and the binomial theorem.

*Figure* 1. *Sketch of features of a trajectory parabola* (*on its side*) *for* $p = 4k - 1$.



We associate perfect squares with *lattice points* of d(v) or f(n) and investigate whether right hand interval lattice points giving -1 disparities *evaporate* as they converge to row T.

The trajectory parabola has a strictly monotonically increasing gradient, encapsulated in its integer lattice points of d(v), where the real number difference d(v + 1) – d(v) rises as v increases.

Assume we are on the part of the parabola in which both equipartitioned intervals, of length precisely p/2, are occupied for each row.

Let the interval on the left be denoted by L and that on the right by R. The maximum c lattice points of perfect squares in the L or R interval will be distributed between the left possessing L/(2c) equally divided portions, and on the right with R/(2c) portions. A lattice point (λ, ρ) L, R pair has λ lattice points in L and ρ in R.

R intervals with lattice points in portions 2 and 4 do not contribute directly to -1 disparities, except via previous R intervals with lattice points in portions 1 and 3. This is because when the R intervals contain two lattice points which are in portions 2 and 4, then holding the same number of portions fixed, the previous L interval must have at least two lattice points, in portions 2 and 4, or 1 and 3, and cannot therefore contribute to a minus 1 disparity.

The R interval which precedes this L, if it is not part of a (2, 2) lattice point L, R pair, has 3 or more lattice points, not discussed in this section, or one lattice point, which we have seen in section 4.2, must be part of a (2, 1) L, R pair with a +1 disparity and not a (1, 1) pair, since a sequence of (1, 1), (1, 2) (2, 2) L, R pairs is impossible; a (1, 1) pair cannot be followed by a (2, 2) pair.

If this (2, 2) pair not yet considered is in portions 2 and 4 for R, then iteratively we terminate finitely, or we end up with portions 1 and 3 in the L interval, leading at worst to portions 1 and 3 occupied again in a previous R interval. Alternatively, we are in an R interval with portions 1 and 3 filled directly.

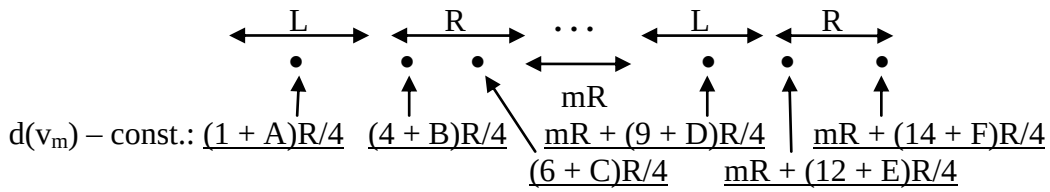
So a situation to consider is where lattice points for R in portions 1 and 3 are filled. Then the previous L interval to contribute a -1 disparity, must have one lattice point in portion 2 or 3. Portion 3 for L may generate portion 1 in L, which indicates no disparity, otherwise like portion 2, this implies that the R interval which preceded this L, if it exists, must have lattice points in 2 and 4, the only adverse case of which, as previously discussed, is to terminate with portions 1 and 3 in a preceding L.

There now appear to be two possibilities. We can have a disparity corresponding to lattice points for L in portions 1 and 3, and a further disparity in a subsequent R for lattice points again in 1 and 3. Alternatively, we might find a disparity corresponding to lattice points for R in portions 1 and 3 and a subsequent disparity for an R in portions 1 and 4.

**Theorem 7.4 (absence of disparity limitations for (1, 2) L, R lattice point pairs)**
Let $0 < B, C, E < 1$ and $0 < A, D, F < 2$. Consider a lattice point in L at d(v) = constant + (1 + A)R/4 and a point in R at d(v + 1) = const. + (4 + B)R/4, and that this R

contributes a portion 1 and 3 disparity. Lattice point 3 is at const. + (6 + C)R/4. Then consider a further L, R pair, separated from the first set by an interval of mR intervening pairs, with m even, contributing a disparity with the lattice points for R in portions 1 and 3 or 1 and 4, shown in the diagram below. The intervening pairs are assumed to have 2 lattice points in each of L and R, otherwise the disparity is +1. Let d(v + 2m + 5) = const. + mR + (14 + F)R/4 for this portion 3 or 4.

*Figure* 2. *Posited repeated -1 disparities for* (1, 2) L, R *pairs.*




Then

$$d(v + 2m + 5) - d(v + 2m + 4) = 2v + 2(2m + 4) = (2 + F - E)R/4,$$
$$d(v + 2m + 5) - d(v + 2m + 3) = 4v + 2(4m + 7) = (5 + F - D)R/4,$$
$$d(v + 2m + 5) - d(v + 2) = (4m + 6)v + (2m + 5)(2m + 4) - 2 = (8 + F - C)R/4 + mR,$$
$$d(v + 2m + 5) - d(v + 1) = (4m + 8)v + (2m + 5)(2m + 4) = (10 + F - B)R/4 + mR,$$
$$d(v + 2m + 5) - d(v) = (4m + 10)v + (2m + 5)(2m + 4) = (13 + F - A)R/4 + mR.$$

Eliminating F via the first equation, and then similarly E, gives

$$(4m + 2)v + (2m + 3)(2m + 2) - 2 = (3 - C + D)R/4 + mR,$$
$$(4m + 4)v + (2m + 3)(2m + 2) = (5 - B + D)R/4 + mR,$$
$$(4m + 6)v + (2m + 3)(2m + 2) = (8 - A + D)R/4 + mR,$$

and eliminating D and finally C gives

$$8v = (3 - A + B)R.$$

Alternatively, in order to eliminate v we obtain from the above

$$2v + 2 = (2 - B + C)p/8,$$
$$2v = (3 - A + B)p/8,$$

where we have made the substitution of p/2 for R. Then

$$16 = (-1 + A - 2B + C)p,$$

and all of this can occur for any p.

We now extend figure 2 on the left in a similar way, by making the substitutions $v \rightarrow v'$, $m \rightarrow m'$, $A \rightarrow X$, $B \rightarrow Y$, $C \rightarrow Z$, $D \rightarrow A$, $E \rightarrow B$ and $F \rightarrow C$. Then the first two equations we considered become

$$2v' + 2(2m' + 4) = (2 + C - B)R/4,$$
$$4v' + 2(4m' + 7) = (5 + C - A)R/4,$$

and hence

$$8v' + 16m' + 24 = (3 - A + B)R = 8v,$$

giving $v = v' + 3 + 2m'$, so there is no contradiction or restriction at this level.

Thus, and recursively, there is no inherent constraint obtained on chaining multiple -1 disparities using these methods, without further assumptions, under this fineness of resolution. □

So far, our geometrical techniques have not been effective in limiting the occurrence of the number of disparities within bounds that imply a positive value for the disparity expression. A calculation would reveal that the above methods do not sufficiently constrain disparities to be cancelled against surpluses in rows 1 and 2 and trajectory m = 0, nor in extensions to this idea using the techniques already employed.

This lesson impels us to seek detailed and precise information on quadratic residues in the regions not already covered. In Part II we achieve such a programme. It contains new insight into a feature – *parabolas*, by which the positive nature of the disparity formula can be investigated. We will also relate our work to the tenth discriminant problem.

## Acknowledgements

I would like to thank Richard Guy, without whom the work would not have been initiated, Ben Greenfield, who supplied the program to check the results of section 6.1 and extend them for r = 4 and 5, and Steven Miller, whose suggestions greatly improved the presentation.

## References

Ad14 J.H. Adams, *Some simple proofs on general reciprocity*, to appear in *Innovation in mathematics*, 2014.

Gu04 R.K. Guy, *Unsolved problems in number theory*, Springer, 2004.

Da80 H. Davenport, *Multiplicative number theory*, 2nd edition, Springer, 1980.

MP07 Yu.I. Manin and A.A. Panchishkin, *Introduction to modern number theory*, Springer, 2007.

We40 H. Weyl, *Algebraic theory of numbers*, Princeton University Press, 1940, p 193 – 201.