

An elementary proof of a formula on quadratic residues

27th December 2010

© 2009, 2010 Jim Adams

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

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

where int is the integer part of a real number. We prove this positive.

We partition this summation between the rows, r , up to $T = \operatorname{int}\{(p+9)/16\}$, and define 'trajectories' after this row, providing a formula also for the trajectories.

Introduction.

Richard Guy in [1], 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 [3]. Is there an elementary proof? However, Yuri Manin and Alexei Panchishkin [2] state: for every choice of axioms there will always be statements which can be formulated in an elementary way, and which are decidable, but cannot be deduced using only elementary methods.

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 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 $m \equiv n \pmod{p}$ and $m \not\equiv p - n \pmod{p}$ if and only if $m^2 \equiv n^2 \pmod{p}$.

In the section on 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 integer part of either $(p + 1)/16$ or $(p - 15)/16$, we give an explicit formula for the combined row and trajectory disparities.

We next investigate constraints on -1 disparities. We then formulate our problem as a Diophantine one. Using lattice point counting arguments for $p = 4k - 1$ shows the total disparity is greater than zero, but symmetry constraints for prime $q = 4k' - 3$ imply a zero disparity expression for q . We relate results for q to those for p . Other methods involve the class number in the disparity expression, where we close.

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. ■

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.

We now prove the occupancy theorem, also applicable on adding γp to all ranges.
Assigning all numbers \pmod{p} , p prime, $m^2 \neq n^2$ 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 ν .

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 $(m - n)(m + n) = [a \text{ number } < p][a \text{ number } \geq (p - 1)/2]$. ■

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 $\equiv 0 \pmod{p}$, indicates that $y^{(p-1)/2} \equiv (-y)^{(p-1)/2} \pmod{p}$. If $(p - 1)/2$ is odd, so $p = 4k - 1$, then the binomial expansion gives $y^{(p-1)/2} \equiv -(-y)^{(p-1)/2} \pmod{p}$. ■

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: $p = 11$, $(p - 1)/2 = 5$.

$y \equiv (\text{mod } p)$	y^5	$y^5 \pmod{11}$	region
0	0	0	A
1	1	1	B $0 < n \leq (p - 1)/2$
2	32	-1	
3	243	1	
4	1024	1	
5	3125	1	
6	7776	-1	C $(p - 1)/2 < n < p$
7	16807	-1	
8	32768	-1	
9	59049	1	
10	100000	-1	
$11 \equiv 0 \pmod{11}$			repeats

For $(p - 1)/2$ odd, if $0 < n \leq (p - 1)/2$, i.e. region **B**, then there are δ terms $\equiv 1 \pmod{p}$ and $(p - 1)/2 - \delta$ terms $\equiv -1 \pmod{p}$, so there must be in the $(p - 1)/2 < n < p$ region **C**, δ terms $\equiv -1 \pmod{p}$ and $(p - 1)/2 - \delta$ terms $\equiv +1 \pmod{p}$, giving the complete set of $(p - 1)/2$ occupied root positions for both $1 \pmod{p}$ and $-1 \pmod{p}$.

Table: $p = 17$, $(p - 1)/2 = 8$.

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

If $(p - 1)/2$ is *even*, with the δ terms $\equiv 1 \pmod{p}$ for region **B** below, there are δ terms $\equiv 1 \pmod{p}$ in region **C**, opposite in sign to the odd case. Thus there are 2δ 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 δ slots in this region, likewise in region **C**. ■

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

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

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

region D	<u>0</u>																																										
region E	<table style="border: none; width: 100%; text-align: center;"> <tr> <td><u>1</u></td><td>2</td><td>3</td><td><u>4</u></td><td>5</td><td>6</td> </tr> <tr> <td>7</td><td>8</td><td><u>9</u></td><td></td><td></td><td></td> </tr> </table>	<u>1</u>	2	3	<u>4</u>	5	6	7	8	<u>9</u>																																	
<u>1</u>	2	3	<u>4</u>	5	6																																						
7	8	<u>9</u>																																									
region F	<table style="border: none; width: 100%; text-align: center;"> <tr> <td></td><td></td><td></td><td>10</td><td>11</td><td>12</td><td>13</td> </tr> <tr> <td>14</td><td>15</td><td><u>16</u></td><td>17</td><td>18</td><td>19</td><td>20</td> </tr> <tr> <td>21</td><td>22</td><td>23</td><td>24</td><td><u>25</u></td><td>26</td><td>27</td> </tr> <tr> <td>28</td><td>29</td><td>30</td><td>31</td><td>32</td><td>33</td><td>34</td> </tr> <tr> <td>35</td><td><u>36</u></td><td>37</td><td>38</td><td>39</td><td>40</td><td>41</td> </tr> <tr> <td>42</td><td>43</td><td>44</td><td>45</td><td>46</td><td>47</td><td>48</td> </tr> </table>				10	11	12	13	14	15	<u>16</u>	17	18	19	20	21	22	23	24	<u>25</u>	26	27	28	29	30	31	32	33	34	35	<u>36</u>	37	38	39	40	41	42	43	44	45	46	47	48
			10	11	12	13																																					
14	15	<u>16</u>	17	18	19	20																																					
21	22	23	24	<u>25</u>	26	27																																					
28	29	30	31	32	33	34																																					
35	<u>36</u>	37	38	39	40	41																																					
42	43	44	45	46	47	48																																					
next p^2	<u>49</u>																																										

Since, by the binomial theorem for squares,

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

these p squares fill, in p iterations $(\text{mod } p)$, 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

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

Although the non-constructive ‘pigeon hole principle’ can act as a barrier to understanding, we now apply this principle here.

Since there are p squares $(\text{mod } p^2)$, there are $(p - 1)/2$ non-zero squares $(\text{mod } p)$. 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 $(\text{mod } p)$, 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 $(\text{mod } p)$. 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 $n \pmod{p}$. 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 $(\text{mod } p)$, otherwise it is not. ■

Detailed proof of 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	<u>1</u>	3	<u>4</u>	7	<u>9</u>	10	11	12	<u>16</u>	17	21	23	<u>25</u>	26	27	28	29	30	31	33	<u>36</u>	37	38	40	41
83	<u>100</u>										<u>121</u>														
166	<u>169</u>															<u>196</u>									
249	<u>256</u>																				<u>289</u>				
332											<u>361</u>														
415											<u>441</u>														
498											<u>529</u>														
581	blank																								
664	<u>676</u>																								
747																					<u>784</u>				
830	<u>841</u>																								
913	blank																								
996											<u>1024</u>														
1079	<u>1089</u>																								
1162	blank																								
1245	blank																								
1328																					<u>1369</u>				
1411																					<u>1444</u>				
1494											<u>1521</u>														
1577											<u>1600</u>														
1660											<u>1681</u>														

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	<u>49</u>	51	59	61	63	<u>64</u>	65	68	69	70	75	77	78	<u>81</u>									
83	<u>144</u>																								
166	<u>225</u>																								
249											<u>324</u>														
332											<u>400</u>														
415											<u>484</u>														
498																					<u>576</u>				
581	<u>625</u>																								
664											<u>729</u>														
747	blank																								
830											<u>900</u>														
913	<u>961</u>																								
996	blank																								
1079																					<u>1156</u>				
1162											<u>1225</u>														
1245	<u>1296</u>																								
1328	blank																								
1411	blank																								
1494	blank																								
1577	blank																								
1660	blank																								

We make the following observations.

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.

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

$$T = \text{the integer part of } [p+10]/16.$$

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 9α , 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 $(5p+9)/16$.

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

$$\text{int}\{\sqrt{[(p-1)/2]}\} - \{\text{int}\{\sqrt{(p-1)}\} - \text{int}\{\sqrt{[(p-1)/2]}\}\},$$

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

$$\geq \text{int}\{[(\sqrt{2}) - 1]\sqrt{(p-1)}\} - 1.$$

5. For a *subsequent* r th row with non-blank columns on the left hand part of **region H**

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

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

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

The r th row of the left hand part of **region H** has at most one less perfect square than the right hand part, the difference being, taking integer parts

$$\begin{aligned} & \{ \text{int}\{\sqrt{[(2rp-p-1)/2]}\} - \text{int}\{\sqrt{[(r-1)p]}\} \} - \\ & \{ \text{int}\{\sqrt{[rp-1]}\} - \text{int}\{\sqrt{[(2rp-p-1)/2]}\} \} \\ & = 2\text{int}\{\sqrt{[(2rp-p-1)/2]}\} - \text{int}\{\sqrt{[rp-1]}\} - \text{int}\{\sqrt{[(r-1)p]}\}. \end{aligned}$$

Let $\text{int}\{A\}$ be the integer part of the positive real number A and $\text{bit}\{A\}$ be $A - \text{int}\{A\}$. The maximum value of $\text{int}\{2A\} - 2\text{int}\{A\}$ is 1 (the minimum is zero) and the maximum value of $\text{int}\{C+D\} - \text{int}\{C\} - \text{int}\{D\}$ 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

$$\begin{aligned} & \text{int}\{2\sqrt{[a+(b/2)]}\} + \text{bit}\{2\sqrt{[a+(b/2)]}\} \\ & > \text{int}\{\sqrt{(a+b)} + \sqrt{(a)}\} + \text{bit}\{\sqrt{(a+b)} + \sqrt{(a)}\}. \end{aligned}$$

Hence

$$\begin{aligned} & \text{int}\{2\sqrt{[a+(b/2)]}\} \geq \text{int}\{\sqrt{(a+b)} + \sqrt{(a)}\} \\ & \geq \text{int}\{\sqrt{(a+b)}\} + \text{int}\{\sqrt{(a)}\}. \end{aligned}$$

The maximum disparity is when $\text{int}\{2\sqrt{[a+(b/2)]}\} - 2\text{int}\{\sqrt{[a+(b/2)]}\} = 1$ and when $\text{int}\{\sqrt{(a+b)} + \sqrt{(a)}\} - \text{int}\{\sqrt{(a+b)}\} - \text{int}\{\sqrt{(a)}\} = 0$. In this case

$$2\text{int}\{\sqrt{[a+(b/2)]}\} \geq \text{int}\{\sqrt{(a+b)}\} + \text{int}\{\sqrt{(a)}\} - 1.$$

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

$$2\text{int}\{\sqrt{[a+(b/2)]}\} = \text{int}\{\sqrt{(a+b)}\} + \text{int}\{\sqrt{(a)}\} - 1.$$

The result above follows putting $a = (r-1)p$ and $b = (p-1)$.

Note that $\text{int}\{2\sqrt{[a+(b/2)]}\} - 2\text{int}\{\sqrt{[a+(b/2)]}\} = 1$ implies $\text{int}\{2\sqrt{[a+(b/2)]}\}$ 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.

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 $> (p-1)/2$ on the left, so that position n on the right is occupied, then the next position on the right hand part would be at least $[(p-1)/2] + 2n + 2$ on the right, which goes past its boundary.

Conversely, if the right is blank, then the left if occupied in position n , is at an interval $(p - 1)/2 + [(p - 1)/2 - n]$ from the right hand edge of the right hand part, and the next interval is at least $2[(p - 1) - n] - 2$ to the left of this edge, with $n < (p - 1)/2$, which once again goes past its boundary.

Similar 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 $i = 1, \dots, x$ 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

$$(u - 1)p + (p + 1)/2 = n^2 - w_1,$$

$$(u - 2)p + (p + 1)/2 = (n - 1)^2 - w_2,$$

...

$$(u - x)p + (p + 1)/2 = (n - x + 1)^2 - w_x,$$

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.

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 v th 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

$$(sp - 1)^{(p - 1)/2} - 1 \not\equiv 0 \pmod{p}.$$

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 $X \geq 6$, from

$$2\text{int}\{X/\sqrt{3}\} - \text{int}\{X\} \geq 0.$$

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 0 in the above expression) and 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

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

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

$$j_{\max} = \text{int}\{\sqrt{[p \text{int}\{(p + 10)/16\}]} - 1\} = (p - 7)/4$$

for $k \equiv 0$ or $1 \pmod{4}$, and $p > 3$, but for $k \equiv 2$ or $3 \pmod{4}$

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

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

$$J = \text{int}\{[\sqrt{(M + 3/4)p - 2}] + 1/2\},$$

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

$$[\sqrt{(M + 13/16)p}] + 1 > J > [\sqrt{(M + 11/16)p}] - 1,$$

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

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

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

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

giving $M = \text{int}\{(p - 15)/16\}$, or zero for $p \leq 11$.

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

$$\text{int}\{\sqrt{[rp - (p + 1)/2]}\} = \text{int}\{\sqrt{[rp - (p/2)]}\},$$

$$\text{int}\{\sqrt{[rp - 1]}\} = \text{int}\{\sqrt{[rp]}\},$$

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

$$\begin{aligned} & (\text{difference in 1}^{\text{st}} \text{ row}) + (\text{difference in rows 2 to } (T - 1)) + (\text{overlap row } T) \\ & + (\text{difference for trajectories 1 to } M) + (\text{difference for trajectory } m = 0). \end{aligned}$$

Using previous results, we obtain this total difference is equal to

$$\begin{aligned} & 2\text{int}\{\sqrt{(p/2)}\} - \text{int}\{\sqrt{p}\} \\ & + \sum_{[r = 2 \text{ to } (T - 1)]} [2\text{int}\{\sqrt{[rp - (p/2)]}\} \\ & - \text{int}\{\sqrt{[rp]}\} - \text{int}\{\sqrt{[(r - 1)p]}\}] + 1 \\ & + \sum_{[m = 1 \text{ to } M]} [2\text{int}\{\sqrt{[(m + 1/4)p - 1/2] + 1/2}\} \\ & - \text{int}\{\sqrt{[(m + 3/4)p - 1] + 1/2}\} - \text{int}\{\sqrt{[(m - 1/4)p] + 1/2}\}] \\ & + 2\text{int}\{\sqrt{[(p/4) - 1/2] + 1/2}\} - \text{int}\{\sqrt{[(3/4)p - 1] + 1/2}\}. \blacksquare \end{aligned}$$

Ancillary remarks.

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

$$\text{int}\{\sqrt{[rp - 1]}\} - \text{int}\{\sqrt{[rp - p]}\},$$

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

$$\text{int}\{\sqrt{[rp - 1]}\} = \text{int}\{\sqrt{[rp]}\}.$$

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

$$2\text{int}\{\sqrt{[rp]}\} - \text{int}\{\sqrt{[(r - 1)p]}\} - \text{int}\{\sqrt{[(r + 1)p]}\}.$$

Now in general

$$2\text{int}\{X\} \geq \text{int}\{X + A - 1/2\} + \text{int}\{X - A - 1/2\},$$

because the ints on the right are maximised as the value of $\text{bit}\{X\}$ approaches 1, and the int on the left is unchanged by this. Then if $\text{bit}\{X\} \geq \text{bit}\{A\} > 1/2$, the first int on the right is $\text{int}\{X\} + \text{int}\{A\} + 1$ and the second is $\text{int}\{X\} - \text{int}\{A\} - 1$, and if $\text{bit}\{X\} > \text{bit}\{A\}$ and $\text{bit}\{A\} \leq 1/2$, the first int on the right is $\text{int}\{X\} + \text{int}\{A\}$ and the second is either $\text{int}\{X\} - \text{int}\{A\}$ or $\text{int}\{X\} - \text{int}\{A\} - 1$.

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

$$\begin{aligned} 2\text{int}\{\sqrt{[rp]}\} & \geq \text{int}\{\sqrt{[rp]}\} [1 - (1/2r) - (1/8r^2) - \dots] \\ & + \text{int}\{\sqrt{[rp]}\} [1 + (1/2r) - (1/8r^2) + \dots - \dots], \end{aligned}$$

and so this will always occur when

$$[\sqrt{[rp]}\}(1/8r^2) \geq 1/2.$$

Hence if r = 1 this must happen when p ≥ 19, for r = 2 when p ≥ 139 (although both these occur for all relevant p) and generally for a prime (4k - 1) when p > 16r³.

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, 22² = 484 on the left, and for row 5 two such squares, 25² = 625 and 26² = 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.

12. 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*

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

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 $t \rightarrow t + 1$, 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 $r \rightarrow r'$ 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.

Some constraints on -1 disparities up to row T .

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

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

$$2\text{int}\{\sqrt{(rp - (p/2))}\} - \text{int}\{\sqrt{(rp)}\} - \text{int}\{\sqrt{[(r - 1)p]}\},$$

and using the relation again

$$2\text{int}\{X\} \geq \text{int}\{X + A - 1/2\} + \text{int}\{X - A - 1/2\},$$

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

$$\begin{aligned} 2\text{int}\{X\} - \text{int}\{X[1 - (1/(2r - 1)) - (1/8(2r - 1)^2) - \dots]\} \\ - \text{int}\{X[1 + (1/(2r - 1)) - (1/8(2r - 1)^2) + \dots - \dots]\}, \end{aligned}$$

so the difference is always greater or equal to 0 provided

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

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

Thus for $r = 2$, we only have to check primes ≤ 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 ≤ 8783 , 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 .

14. 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

$$r = \text{int}\{(4k + 9)/16\},$$

we observe on setting $p = 4k - 1$ and $(r - 1)p = (4k - 1)\text{int}\{(4k - 7)/16\}$ that the ‘minus 1’ alluded to previously disappears, namely

$$\begin{aligned} 2\text{int}\{\sqrt{[(4k - 1)\text{int}\{(4k - 7)/16\} + 2k - 1]}\} \\ = \text{int}\{\sqrt{[(4k - 1)\text{int}\{(4k - 7)/16\} + 4k - 2]}\} \\ + \text{int}\{\sqrt{[(4k - 1)\text{int}\{(4k - 7)/16\}]}\}, \end{aligned}$$

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

For $\beta = 0, 1$

$$\begin{aligned} 2\text{int}\{\sqrt{[16\alpha^2 - 9\alpha + 4\beta\alpha]}\} \\ = \text{int}\{\sqrt{[(16\alpha^2 - \alpha + 4\beta\alpha - 1)]}\} + \text{int}\{\sqrt{[(16\alpha^2 - 17\alpha + 4\beta\alpha - 4\beta + 1)]}\}, \end{aligned}$$

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

$$\begin{aligned} 2\text{int}\{\sqrt{[16\alpha^2 + 7\alpha + 4\beta\alpha + 2\beta - 1]}\} \\ = \text{int}\{\sqrt{[(16\alpha^2 + 15\alpha + 4\beta\alpha + 4\beta - 2)]}\} + \text{int}\{\sqrt{[(16\alpha^2 - \alpha + 4\beta\alpha)]}\}, \end{aligned}$$

so for $\beta = 2$ this becomes

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

whereas for $\beta = 3$ this implies

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

15. For the disparity using a row, r , prior to row T, we consider

$$r = \text{int}\{(4k + 9)/16\} - y$$

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

$$\text{int}\{(4k + 9)/16\} - 2 = \text{int}\{(4k - 23)/16\}.$$

Then $p(r - 1) = (4k - 1)\text{int}\{(4k - 7 - 16y)/16\}$.

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

$$\begin{aligned}
& 2\text{int}\{\sqrt{[(4k-1)\text{int}\{(4k-7-16y)/16\} + 2k-1]}\} \\
& \quad - \text{int}\{\sqrt{[(4k-1)\text{int}\{(4k-7-16y)/16\} + 4k-2]}\} \\
& \quad - \text{int}\{\sqrt{[(4k-1)\text{int}\{(4k-7-16y)/16\}]\}}.
\end{aligned}$$

For $\beta = 0$ this difference is

$$\begin{aligned}
& 2\text{int}\{\sqrt{[16\alpha^2 - 16\alpha y - 9\alpha + y]}\} - \text{int}\{\sqrt{[16\alpha^2 - 16\alpha y - \alpha + y - 1]}\} \\
& \quad - \text{int}\{\sqrt{[16\alpha^2 - 16\alpha y - 17\alpha + y + 1]}\},
\end{aligned}$$

for $\beta = 1$

$$\begin{aligned}
& 2\text{int}\{\sqrt{[16\alpha^2 - 16\alpha y - 5\alpha - 3y - 2]}\} - \text{int}\{\sqrt{[16\alpha^2 - 16\alpha y + 3\alpha - 3y - 1]}\} \\
& \quad - \text{int}\{\sqrt{[16\alpha^2 - 16\alpha y - 13\alpha - 3y - 3]}\},
\end{aligned}$$

$\beta = 2$ gives

$$\begin{aligned}
& 2\text{int}\{\sqrt{[16\alpha^2 - 16\alpha y + 15\alpha - 7y + 3]}\} - \text{int}\{\sqrt{[16\alpha^2 - 16\alpha y + 23\alpha - 7y + 6]}\} \\
& \quad - \text{int}\{\sqrt{[16\alpha^2 - 16\alpha y + 7\alpha - 7y]}\}
\end{aligned}$$

and for $\beta = 3$

$$\begin{aligned}
& 2\text{int}\{\sqrt{[16\alpha^2 - 16\alpha y + 19\alpha - 11y + 5]}\} - \text{int}\{\sqrt{[16\alpha^2 - 16\alpha y + 27\alpha - 11y + 10]}\} \\
& \quad - \text{int}\{\sqrt{[16\alpha^2 - 16\alpha y + 11\alpha - 11y]}\}.
\end{aligned}$$

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 β 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

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

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

For $\beta = 2$ we have a difference

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

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 difference holds.

For $\beta = 3$ we are dealing with

$$\begin{aligned} & 2\text{int}\{[4\alpha - 2y + 2 + (3/8) - [(256y^2 + 96y + 41)/(512\alpha)] - \dots]\} \\ & \quad - \text{int}\{[4\alpha - 2y + 3 + (3/8) - [(256y^2 - 160y + 89)/(512\alpha)] - \dots]\} \\ & \quad - \text{int}\{[4\alpha - 2y + 1 + (3/8) - [(256y^2 + 352y + 121)/(512\alpha)] - \dots]\}, \end{aligned}$$

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 α^2 , say $y = 3(\alpha + \gamma)/4$ with 4 as a leading coefficient of α^2 , to determine the value of the disparity.

Trajectories.

16. There is a bijection between perfect square difference terms prior to row T and terms for trajectory differences.

If we represent row differences prior to T by

$$2\text{int}\{\sqrt{[p(\mu + 1/2) - 1/2]}\} - \text{int}\{\sqrt{[p(\mu + 1) - 1]}\} - \text{int}\{\sqrt{[p\mu]}\}$$

using $\mu = T - 1 - y$, then we see a bijection for the transformation $\mu \leftrightarrow m - 1/4$ under the square root, with an additional $1/2$ in the int, provided we recall the trajectory term

$$- \text{int}\{\sqrt{[(p(m + (3/4)) - 2)] + 1/2}\}$$

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

$$- \text{int}\{\sqrt{[(p(m + (3/4)) - 1)] + 1/2}\}.$$

17. 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 $2\text{int}\{B\}$ and $\text{int}\{2B\}$ amounts to -1 ,

$$\text{int}\{B\} - \text{int}\{A\} \geq \text{int}\{C\} - \text{int}\{B\} + z - 1.$$

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 $\text{bit}\{B\} \leq 1/2$, that is, for all occurrences of

$$1 = 1 - \text{int}\{2\text{bit}\{B - \epsilon\}\},$$

where ϵ is positive and tends suitably to zero.

On the other hand, if the condition

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

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

$$2 \text{int}\{B\} \geq \text{int}\{A\} + \text{int}\{C\},$$

i.e. 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 $\text{bit}\{B\} \leq 1/2$, 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 -1 .

The positive value of the disparity expression.

18. 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 $v = 1/2$. The parabola can be extended from $v = 1$ to $v = p - 1$, to cover the whole range of values of 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.

19. We prove the positive nature of the disparity formula using lattice point counting methods for an increasing $d(v)$ valuation of v , or $f(n)$ of n .

We associate perfect squares with lattice points of $d(v)$ or $f(n)$ and show how 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 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 placed on the left somewhere in $L/(2c)$ equally divided portions, and on the right in $R/(2c)$ portions.

When the R interval contains two lattice points not all of which are in portions 1 and 4, then holding the same number of portions fixed, the previous L interval must have at least as many points, so the disparity is not -1. So assume an R interval has two lattice points within edge portions 1 and 4. Then the preceding L interval contains one lattice point or two. Thus the worst disparity in this case is -1.

Now consider the next intervals for higher values of d . If the previous R interval with disparity -1 had a point in edge portion 4 so that the next left hand interval would be blank, this violates our assumptions.

So consider the scenario where this next L interval has a lattice point in edge portion 4. Then the next R interval is blank, against our assumptions, or is occupied with at most one lattice point, giving a minimum disparity of zero. If we assume the next L interval is not blank, then again the disparity is zero. The process continues recursively, but must terminate finitely.

If instead the next L interval has a lattice point in portion 3, then the next R interval does not have a point in portion 1, so there is no -1 disparity – a point evaporates.

If the R interval contains $c - 2$ interior lattice points, then they do not occupy portions 1, $2c - 1$ and $2c$. Let us hold the number of portions at $2c$. The outer 1, $2c - 1$ and $2c$ points demonstrate the same behaviour as previously. The previous L interval gives at worst a -1 disparity with this R.

For higher values of d , if the previous disparity was -1 and L contains the same number of points as before, the next R interval has zero or more disparity, and if the process continues, it must terminate finitely.

If the disparity is now positive, an interior lattice point has evaporated from R, and this can happen anyway for zero disparity. If the previous L has contained fewer points, this reduction cannot revert to higher values.

Zero disparities can continue until they reach row T, when the process terminates. The trajectory intersecting with row T has one point in L and one point in R. Thus interior points must have already evaporated at most in this final trajectory.

So the -1 disparities evaporate, the maximum number being the greatest number of interior points plus one in any R interval with a -1 disparity, which are promoted to -1 disparities in subsequent iterations.

An analogous argument can be made for disparities which are ≥ 1 , just swap the words ‘left’ and ‘right’.

We have proved that the first row, $r = 1$, has positive disparity, and the first trajectory, $m = 0$, has disparity ≥ 0 , although for $q = 4k' - 3$ the trajectory begins on the right. For a row or trajectory to T, if the right hand number of lattice points is N_r for a row and N_t for a trajectory, then the maximum number of -1 disparities after this row or trajectory to T is $N_r - 1$ for rows and $N_t - 1$ for trajectories. We prove the disparity for row 2 $\geq N_r - 1$, or

$$3\text{int}\{\sqrt{(2p - p/2)}\} - 2\text{int}\{\sqrt{(2p)}\} - \text{int}\{\sqrt{p}\} + 1 \geq 0,$$

where a proof by induction shows that this holds.

For row $r = 3$ onwards compared with row 2, if we put in order boundary terms from the right hand part of **region H** without the ints, they satisfy

$$\sqrt{(rp)} > [\sqrt{(rp)}][1 - (1/2r)]^{1/2} > \sqrt{(2p)} > [\sqrt{(2p)}][1 - (1/4)]^{1/2}$$

and

$$\sqrt{(rp)} - \sqrt{(2p)} > [\sqrt{(rp)}][1 - (1/2r)]^{1/2} - [\sqrt{(2p)}][1 - (1/4)]^{1/2}.$$

Now if $A - B > C - D$ then

$$\text{int}\{A\} + \text{bit}\{A\} - \text{int}\{B\} - \text{bit}\{B\} > \text{int}\{C\} + \text{bit}\{C\} - \text{int}\{D\} - \text{bit}\{D\}$$

and since

$$\text{bit}\{A\} - \text{bit}\{B\} > -1$$

$$\text{bit}\{C\} - \text{bit}\{D\} < 1$$

we have

$$\text{int}\{A\} - \text{int}\{B\} \geq \text{int}\{C\} - \text{int}\{D\} - 1.$$

Thus from the right hand part the number of perfect squares is less than those for the right hand part of row 2 for all subsequent rows minus at most 1. We will cancel this minus one term against the trajectory overlap perfect square on row T, when the trajectory exists.

For trajectory $m = 1$ where this exists the trajectory disparity minus $(N_t - 1)$ is less than the disparity for row $r = 1$, the corresponding relation being, on binomial expansion, here to first order although this generally holds

$$2\text{int}\{\sqrt{(p/2)}\} - \text{int}\{\sqrt{p}\} + 2\text{int}\{[\sqrt{(7p)}/2 - 1/\sqrt{(7p)} + 1/2]\} \\ + \text{int}\{[\sqrt{(3p)}/2 + 1/2]\} - 3\text{int}\{[\sqrt{(5p)}/2 - 1/[2\sqrt{(5p)}] + 1/2]\} + 1 \geq 3,$$

which is valid by recursion.

Again, N_t for $m = 1$ is not less than $(N_t - 1)$'s for subsequent trajectories. Thus at the very least the disparity expression is greater than the disparity for trajectory $m = 0$, which is positive or zero. ■

Relations to other results.

20. Let prime $p = 4k - 1$. There are always $(p + 1)/4$ 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 . ■

21. For $q = 4k' - 3$, we recall there are $(q - 1)/4$ quadratic residues in each of the left and right hand parts. Thus *the disparity expression is zero in this case.*

Here the number of rows is $(q - 1)/4$, the last perfect square $[(q - 1)/2]^2$ being positioned at $(q - 1)/4$ from the rightmost column on the right hand part, at position $(3q + 1)/4$ from the left.

By symmetry the number of quadratic residues in $[2k' - 1, 3k' - 3]$ corresponds to an equal number in $[k', 2k' - 2]$ and of $[3k' - 2, 4k' - 4]$ to $[1, k' - 1]$ so the disparity for

$$\{[1, k' - 1] \cup [3k' - 2, 4k' - 4]\} - [k', 3k' - 3]$$

is even. We call this the *shifted disparity*.

These lattice points for $m = 0$ in $[1, k' - 1]$ and $[3k' - 2, 4k' - 4]$ minus those in the interval $[k', 3k' - 3]$ are greater in number than those in the middle interval for trajectory $m = 1$ where this exists. A corresponding statement may be made for rows.

Thus by similar evaporation of disparities, *for $q = 4k' - 3$ there are less quadratic residues in $[k', 3k' - 3]$ than non-zero such residues elsewhere.* ■

Relating p results to q , we note that setting $q = p - 4g + 2$, the difference in d between the q and p perfect squares is always $(p + 3)/2 - 3g$.

If we had represented the quadratic residues as a clock rather than a table of values, we then conclude that our results for $p = 4k - 1$ are similar to $q = 4k' - 3$, the latter rotated clockwise by $\pi/2$.

22. We relate the disparity expression to the class number H , taking our cue from [3]. This shows that for $p \equiv 7 \pmod{8}$ the disparity expression

$$\sum_{[r=1 \text{ to } (p+1)/4]} [2\text{int}\{\sqrt{[rp - (p/2)]}\} - \text{int}\{\sqrt{(rp)}\} - \text{int}\{\sqrt{[(r-1)p]}\}]$$

or equivalently

$$2\sum_{[r=1 \text{ to } (p+1)/4]} [\text{int}\{\sqrt{[rp - (p/2)]}\} - \text{int}\{\sqrt{(rp)}\}] + (p - 1)/2$$

is equal to H . For $p \equiv 3 \pmod{8}$ it equals $3H$.

We prove for $q \equiv 1 \pmod{8}$ the corresponding shifted disparity is a multiple of four, since considering the intervals

$$\{[1, k' - 1] \cup [3k' - 2, 4k' - 4]\} - [k', 3k' - 3],$$

the even disparity $[1, k' - 1] - [k', 2k' - 2]$ is duplicated.

The shifted disparity expression for each row is

$$\begin{aligned} & 2\text{int}\{\sqrt{[(r-1)q + ((q+3)/4)]}\} \\ & + [-\text{int}\{\sqrt{[(r-1)q]}\} + \text{int}\{\sqrt{[(r-1)q + q]}\}] \\ & - 2\text{int}\{\sqrt{[(r-1)q + (3(q-1)/4)]}\}. \end{aligned}$$

Consequently the total shifted disparity is

$$\begin{aligned} & 2\sum_{[r=1 \text{ to } (q-1)/4]} [\text{int}\{\sqrt{[rq - 3(q-1)/4]}\} - \text{int}\{\sqrt{[rq - (q+3)/4]}\}] \\ & + (q - 1)/2. \quad \blacksquare \end{aligned}$$

For the quadratic form with positive fundamental discriminant $q = 29 \equiv 5 \pmod{8}$ the shifted disparity is 8 and the class number is 1, so the shifted disparity here $\neq 2H$.

Acknowledgements

I would like to thank Ben Greenfield, who supplied the program to check the results of section 13 and extend them for $r = 4$ and 5.

References

1. R.K. Guy, *Unsolved Problems in Number Theory*, Springer (2004).
2. Yu.I. Manin and A.A. Panchishkin, *Introduction to Modern Number Theory*, Springer (2007).
3. H. Weyl, *Algebraic Theory of Numbers*, Princeton University Press (1940), p 193 – 201.