

An elementary proof of a theorem on quadratic residues

Submitted 5th October 2009, revised 17th March 2010

© 2009, 2010 Jim Adams

Abstract. Let a prime $p = 4k - 1$. We prove by elementary methods that the number of quadratic residues in the interval $[1, 2k - 1]$ is greater than in $[2k, 4k - 2]$.

Introduction.

Richard Guy in [2], 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 an elementary proof?

We call n^2 a *square* or a *square value*. A *quadratic residue*, b , is then a square value 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*.

The above result will follow for $p = 4k - 1$ if, in the first $(p + 1)/4$ rows, for the left interval $[1, 2k - 1]$, the number of quadratic residues derived from rows up to $T =$ the integer part of $(p + 10)/16$, together with the number after this row, is greater in ways to be specified on the left than on the right, $[2k, 4k - 2]$ interval.

Our plan of attrition on this problem is as follows.

In the *preliminary remarks*, we use two methods to show there are $(p - 1)/2$ non-zero quadratic residues between square values 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 square values 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 if $m \neq n \leq (p - 1)/2$, then $m^2 \neq n^2 \pmod{p}$.

In the section on the *theorem* 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 square values 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 $[2k, 4k - 2]$.

We then divide the rows into the first row, where we prove the number of square values is greater on the left hand part of **region H** than on the right, and row T , which is a row after which the difference in the number of columns between one square value and the next exceeds $(p - 1)/2$. Between rows 2 and T inclusive we subdivide the problem and compute some differences between the number of square values in

the left hand and right hand part of **region H**, which is at worst -1. On row T itself, the number of left hand part and right hand part square values are both 1. We count the deviations from regular oscillations between left and right hand parts.

Looking at the bottom part of the $p = 83$ table shown later, we see that the square values rise up from the left hand part of **region H** to the right, almost corresponding to a type of curve, which we call a *trajectory*, which we shall stipulate always 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 value is located at column $(p + 1)/4$ in the left hand part of **region H**. Further, the column spacing between adjacent square values for a trajectory increases by two each time.

Then, counting these square values from the first, labelled $v = 1$, to the rightmost square value on the first trajectory, we can see the number of square values is greater on the left than on the right.

For every other trajectory we are able to compute that the difference in number of square values between the left hand part and the right is at worst -1, and to find the differences between left and right totals. 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 this difference.

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. *If $m \neq n \leq (p - 1)/2$ or $p > m \neq n > (p - 1)/2$, with p prime, then $m^2 \neq n^2 \pmod{p}$.*

Proof. 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 .

Say $m > n$ 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 . ■

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 $-1 \pmod{p}$.

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**.

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

■

An identity for *Fermat's little theorem* uses Bernoulli numbers B^n . For $1 < q \in \mathbf{N}$, let powers of B in quotation marks within a sum of terms be interpreted as B^n . Then

$$y^q - y = \sum_{f=0}^{y-1} [(f+1)^q - f^q - 1]$$

$$= q \sum_{g=1}^{q-1} \left\{ \frac{[(q-1)! / (g!(q-g)!)]}{["(y+B-1)^{q-g+1} - B^{q-g+1}"] / (q-g+1)} \right\} = qL,$$

by Faulhaber's formula [1]. This incidental identity with $q = (p-1)/2$ prime results in

$$2y^{(p-1)/2} \equiv 2y - L \pmod{p}. \blacksquare$$

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

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 $0^2, 1^2, \dots, (p-1)^2$.

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

region D	<u>0</u>
region E	<u>1</u> 2 3 <u>4</u> 5 6 7 8 <u>9</u>
region F	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 (mod p), all the squares that are possible (mod p^2).

Likewise, since

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

those squares which are non-zero (mod p^2), repeat in just two non-overlapping sets (mod p^2), regions **E** and **F**.

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 (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 (mod p^2), maps to precisely $(p-1)/2$ separate squares (mod p), because otherwise there would be less than $(p-1)/2$ of them. 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 $n \pmod{p}$. 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 (mod p), otherwise it is not. ■

Detailed proof of the theorem.

Example. $p = 83$, $(p - 1)/2 = 41$ (odd), number of rows = $(p + 1)/4 = 21$. Square values 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 – those ancillary to the theorem are asterisked.

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 square value 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 square values 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. For the *first row* with columns > 0 and $\leq (p - 1)/2$, the highest square value 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 square values 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

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

4. For a *subsequent* rth 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 rth row of the left hand part of **region H** has at most one less square value than the right hand part, the difference being, taking integer parts

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

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

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

Hence

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

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 square values, 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.

5*. *The number of square values for a complete row is*

$$\text{int}\{\sqrt{a + b}\} - \text{int}\{\sqrt{a}\} = \text{int}\{\sqrt{rp - 1}\} - \text{int}\{\sqrt{rp - p}\},$$

and since \sqrt{rp} is not a square

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

Consider the number of square values 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

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

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 $\text{bit}\{X\} > \text{bit}\{A\} > \frac{1}{2}$, 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 $\text{bit}\{A\} \leq \frac{1}{2}$, 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 square values for row $(r + 1)$ will always be less than or equal to row r when

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

and so this will always occur when

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

Hence if $r = 1$ this must happen when $p \geq 19$, for $r = 2$ when $p \geq 139$, and generally for a prime $(4k - 1)$ when $p > 16r^3$.

Note that for $p = 151$, the number of square values for the left hand part of **region H** can increase as the row number increases. For row 4 there is one square value, $22^2 = 484$ on the left, and for row 5 two such square values, $25^2 = 625$ and $26^2 = 674$.

For $p = 127$, the same type of situation occurs on the right of **region H**. For row 4 there is one such square value, 484, and for row 5 two square values, $24^2 = 576$ and 625.

6*. If we determine *the column of a square value for a particular row*, for row 2 the first square value is situated in the left hand part at column $[\text{int}\{\sqrt{p-1} + 1\}]^2 - p$, and since $\sqrt{4k-2} = \sqrt{2(2k-1)}$ is not an integer, this is at

$$2\text{int}\{\sqrt{p-1}\} - 1 + \text{int}\{\text{bit}\{\sqrt{p-1}\}[2 + \text{bit}\{\sqrt{p-1}\}]\}.$$

On row r , the x th square value starting from $x = 1$ in row 2 is situated at column

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

To determine $\text{int}\{\sqrt{p-1}\}$, a binomial expansion gives the value $\text{int}\{2\sqrt{k}\} - 1$, so that if in this expression we set

$$k = \sigma^2 + \rho,$$

with $0 \leq \rho < \sigma^2$, so that

$$\lambda\sigma \leq \rho < (\lambda + 1)\sigma$$

then

$$2\sqrt{k} = 2\sigma[1 + (\rho/\sigma^2)]^{1/2} \\ = 2\sigma + \lambda + (\rho - \lambda\sigma)/\sigma - \dots$$

so

$$\text{int}\{2\sqrt{k}\} = 2\sigma + \lambda.$$

7*. 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 $a = (4k - 1)\text{int}\{(4k - 7)/16\}$ and $b = (4k - 2)$ that the 'minus 1' alluded to previously disappears, namely

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

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

For $\beta = 0, 1$

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

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

$$2(4\alpha + 2) = (4\alpha + 3) + (4\alpha + 1).$$

8*. 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 $a = (4k - 1)\text{int}\{(4k - 7 - 16y)/16\}$, with b as before.

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

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

For $\beta = 0$ this difference is

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

for $\beta = 1$

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

$\beta = 2$ gives

$$\begin{aligned} & 2\text{int}\{\sqrt{[16\alpha^2 - 16\alpha y + 24\alpha - 7y + 3]}\} - \text{int}\{\sqrt{[16\alpha^2 - 16\alpha y + 32\alpha - 7y + 6]}\} \\ & - \text{int}\{\sqrt{[16\alpha^2 - 16\alpha y + 16\alpha - 7y]}\} \end{aligned}$$

and for $\beta = 3$

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

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 $\beta = 1$ and with $4 \leq \alpha \leq 7$ (p prime implies $\alpha \neq 2$ or 3) 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 surplus

$2[4\alpha] - [4\alpha] - [4\alpha - 1]$,
 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 $\alpha \geq 6$ (α 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' anomaly for $y = 1$.

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

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

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

For $\beta = 2$ we have a difference

$$\begin{aligned}
 & 2\text{int}\{[4\alpha - 2y + 3 + (-4y^2 + 5y - 6)/8\alpha - \dots]\} \\
 & - \text{int}\{[4\alpha - 2y + 4 + (-4y^2 + 9y - 4)/8\alpha - \dots]\} \\
 & - \text{int}\{[4\alpha - 2y + 2 + (-4y^2 + y - 4)/8\alpha - \dots]\} \\
 & = [8\alpha - 4y + 4] - [4\alpha - 2y + 3] - [4\alpha - 2y + 1],
 \end{aligned}$$

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 again 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 $\beta = 2$, with successively $y = 2, 3$ and > 3 , a zero difference holds.

For $\beta = 3$ we are dealing with

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

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' anomaly.

9*. For further differences 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 square values 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

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

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 verify this always holds.

10. We now prove the theorem for rows up to T . The following square values, taken from the table example for $p = 83$ already given, can be associated with one another. Here $L \equiv$ the left and $R \equiv$ the right hand part of this previous table, so each square value ends in the same number.

A	B	C	D
	R 400	R 400	L 1600
L 1	L 361	L 441	L 1521
L 4	R 324	R 484	L 1444
L 9	L 289	L 529	L 1369
L 16	L 256	R 576	R 1296
L 25	R 225	R 625	R 1225
L 36	L 196	L 676	R 1156
R 49	L 169	R 729	L 1089
R 64	R 144	L 784	L 1024
R 81	L 121	L 841	R 961
L 100	L 100	R 900	R 900

Since column A contains θ^2 , this entails column B contains $400 - 40\theta + \theta^2$, column C contains $400 + 40\theta + \theta^2$ and column D $1600 - 80\theta + \theta^2$, so because half of $p = 83$ is close to $40 = (p - 3)/2$, columns B and C tend to *oscillate* between left and right hand parts for low θ . The 400 used here is the square value $(p - 3)^2/16$ in row T.

Suppose $0 < \theta^2 \leq (p - 3)/4$. Then column B entries of the form

$$(p - 3)^2/16 - [(p - 3)/2]\theta + \theta^2$$

will oscillate between the right hand part and the left hand part, or vice-versa, as θ increments from 1 by 1. The above expansion may be written in the form

$$(p - 3)^2/16 - [(p - 1)/2]\theta + \theta^2 - \theta,$$

thus the number of *transgressions* from the oscillation is at maximum given by the number of times $\theta^2 - \theta$ allows the crossing of a boundary between left and right of **region H**. Its maximum value is in this case

$$1 + \text{int}\{(\theta_{\max}^2 - \theta_{\max})/(p/2)\} = 1,$$

and if $0 < \theta^2 \leq (p - 3)/2$ the corresponding value is again 1.

If instead $(p - 3)/2 < \theta^2 \leq (p - 1)$, so we are now usually in the right hand part of **region H**, the number of transgressions is now (including the one already mentioned) at most 2.

The square value corresponding to the first square value in row 2, on the left, might not be included in the above pairing, but in the example can be paired with 400.

Since in the first row there is always an excess of left hand part square values over the right hand part by at least two (for $p \geq 11$), this proves the theorem for rows up to T.

11. Next consider **region H** after row T, that is, where the difference between adjacent square values $> (p - 1)/2$.

We now work back from the last square value 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 square value is at $(p + 1)/4$ from the *left hand side* of **region H**.

The v th square value counting backwards from the last square value 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 can also argue that if it is not in the first r non-blank rows, the row corresponding to $v + 1$ is blank on the left hand part. In the table above we see the two adjacent blank lines in the previous diagram for the left hand part of **region H** for $p = 83$ are on the right hand part a continuation of the *trajectory* of rows with just one square value 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 square values on the left is greater than those on the right.

12*. 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, hand part and two or more entries on the right, or respectively left, hand part, since if the separation between square values 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 square value 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 square values are situated on the right hand part of **region H** in position w_x from the left edge of that part, and square value 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 square value in the left hand part, which is the start of a new trajectory.

13. We will work in the region *beginning from the bottom row trajectory up to the trajectory starting just before row T*. At most one square value 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 square value 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

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

14*. There is a *bijection between square value 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

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

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

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

15. To calculate the number of trajectories up to the one intersecting with row T, note that the square values from 1 to the last square value in row T always satisfy $j^2 < pT$.

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

$$j_{\max} = \text{int}\{\sqrt{p \text{int}\{(p + 10)/16\}}\} - 1.$$

$$= (p - 7)/4$$

for $k = 0$ or $1 \pmod{4}$, and $p > 3$, but for $k = 2$ 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 square values is

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

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

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

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 $p \leq 11$.

16*. 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 $A = \lceil\sqrt{(h - 2)p} + 1\rceil/2$, $B = \lceil\sqrt{(hp - 2)} + 1\rceil/2$, $C = \lceil\sqrt{(h + 2)p - 8} + 1\rceil/2$ 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

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

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 discrepancy of -1.

Further, for general A, B and C, not necessarily of the form mentioned, these two effects *add*. Thus for at most M values, reduced by one for each occurrence of $\text{bit}\{B\} \leq 1/2$, and reduced 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.

17. Putting this all together, the positive differences between the residues in the left hand part minus the right hand part therefore sum to equal or greater than

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

Using these results, we obtain this total positive difference is equal to or greater than

$$\begin{aligned} & 2\text{int}\{\sqrt{(p-1)/2}\} - \text{int}\{\sqrt{p-1}\} \\ & + \sum_{r=2}^{(T-1)} [2\text{int}\{\sqrt{rp - (p+1)/2}\} \\ & - \text{int}\{\sqrt{rp-1}\} - \text{int}\{\sqrt{(r-1)p}\}] + 1 \\ & + \sum_{m=1}^M [\text{int}\{\text{bit}\{\sqrt{(4m-1)p} + 1/2\} \\ & + \text{bit}\{\sqrt{(4m+3)p-8} + 1/2\} \\ & - \text{int}\{2\text{bit}\{\sqrt{((4m+1)p-2)} + 1/2 - \epsilon\}\}] \\ & + 2\text{int}\{\sqrt{(p-2)} + 1/2\} - \text{int}\{\sqrt{(3p-8)} + 1/2\}. \end{aligned}$$

Problem. Determine the minimum values of the r and m summations. ■

References

- 1 J.H. Conway and R.K. Guy, *The Book of Numbers*, Copernicus (2006).
2. R.K. Guy, *Unsolved Problems in Number Theory*, Springer (2004).