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

14th February 2013, revised 3rd December 2013, 11th November 2015
22nd April 2017 and 5th March 2018

Part I gave the total difference (disparity) between the quadratic residues for prime p = 4k – 1 by the formula

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

where $\lfloor\ \rfloor$ is the floor, or integer part, but which we need to prove is positive.

In Part III section 1 we will refer the reader to the forthcoming *Number, space and logic* [Ad18], where we examine the proof of the positive nature of the disparity, using the nonelementary methods of Hermann Weyl [We40], relating this result to the tenth discriminant theorem for discriminants of the form √(-p) for p = 4k – 1.

The methods involve the class number, H^-, in the disparity expression, implying we have obtained formulas for the class number in the case prime p = 4k – 1, and there are 7 negative such prime p discriminants for quadratic forms with $H^- = 1$.

Part III gives supplementary investigations, firstly from Part I.

In section 2, we give improved constraints on the disparity expression, a theorem on floor and ceiling functions, and discuss the relations between disparities for prime p = 4k – 1 and prime $p' = 4k' + p$.

In 3, we discuss some relations to results in Part I, but for prime q = 4k + 1.

In section 4 we continue from Part II the discussion of parabolas, both for p = 4k – 1 and $q = 4k'' + 1$. This includes further study of the trajectory region.

Section 5 looks at (2j)th power residues for p = 4k – 1.

In section 6 we compute the average value of a square in clock arithmetic (mod p), which gives the row that corresponds to this average value, and from this we obtain the average column position for the average square, thus proving positive total disparity.

In section 7 we discuss cases for investigation where the primes we have considered are replaced by composite numbers, in particular for 4k + 2 and 4k, comparing the situation for numbers 4k, which on counting the number of possibly multiply occurring residues has positive disparity, against the disparity for prime p = 4k – 1.

Keywords: elementary methods, quadratic residue, class number, tenth discriminant problem

1 The class number and the tenth discriminant problem.

1.1 A full account of the class field theory given in [We40] is now transferred to the chapter on class field theory in *Number, space and logic* [Ad18]. In that work we discuss the relation of the asymmetry theorem to the tenth discriminant problem. We relate the disparity expression to the class number H^- for quadratic forms.

This shows for p, but not q, we must consider negative discriminants. Since the value of the total disparity is H^- for $p \equiv 7 \pmod 8$ and $3H^-$ for $p \equiv 3 \pmod 8$, the class number cannot be 1 for discriminant $D = \sqrt{-p}$, with $p > 163$. □

From Part I, the simplified disparity expression is odd, therefore the class number for prime $p = 4k - 1$ cannot be even.

2 Further disparity expressions from Part I.

2.1 Section 3.4 of Part I deduces that the disparity for the first row is positive and equal to or greater than $\lfloor[(\sqrt{2}) - 1]\sqrt{(p-1)}\rfloor - 1$. This can be proved by induction on a natural number from $p \to p + 4$ using a binomial expansion and the relation

$$2\lfloor B\rfloor - \lfloor C\rfloor \geq \lfloor 2B - C\rfloor - 1.$$

The disparity is at its maximum on the first row. Further, section 6.1 of the same work shows that the disparity is always $\geq$ zero provided for row r

$$p > 32(2r-1)^3,$$

a near-maximum improvement using these techniques being

$$p > 32(2r-1)^3 - 8(2r-1).$$

Then the maximum r here is $\lfloor p^{1/3}/6.35\rfloor$.

Using the row to trajectory bijection of theorem 7.1 of Part I or alternatively the formula of theorem 4.1 and the result of 6.1 there, the disparity for trajectories given by $M \geq m > 0$, rather than the r for rows, is $\geq$ zero when

$$p > 32(2m - 3/2)^3 - 8(2m - 3/2),$$

and indeed the disparity is $\geq$ zero for $m = 1$, when this trajectory exists. We proved in Part I the disparity is not negative for $m = 0$. □

2.2 Theorem 2.2.1. Let $W > X > Y$, where W, X , Y and Z are positive rational and non natural numbers and all terms within floor and ceiling functions below are of this form. Then

$$-\lceil W - X\rceil + \lfloor W + X\rfloor \geq -\lceil W - Z - Y\rceil + \lfloor W - Z + Y\rfloor.$$

Proof. This essentially follows since $X > Y$. Choose Y approaching 0, in which case X approaches 0 or W. In the latter case Y can approach $W - Z$. □

2.3 The disparity formula for prime $p' = 4k' + p$ in terms of $p = 4k - 1$ is

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

where

$$B = \sqrt{1 + (4k'/p)}.$$

It is clear if B = 1 and $2\lfloor\sqrt{rp-(p/2)}\rfloor - \lfloor\sqrt{rp}\rfloor - \lfloor\sqrt{(r-1)p}\rfloor$ is negative, then the expression of the above form for B with B > 1 is at minimum the same, -1, as we have already proved in Part I. □

For k′ = 1, the terms we have been dealing with can also be expressed as

$$2\lfloor\sqrt{rp-(p/2)+4r-2}\rfloor - \lfloor\sqrt{rp+4r}\rfloor - \lfloor\sqrt{(r-1)p+4(r-1)}\rfloor,$$

and it is interesting that

$$2\lfloor\sqrt{4r-2}\rfloor - \lfloor\sqrt{4r}\rfloor - \lfloor\sqrt{4(r-1)}\rfloor = 0,$$

since $4r-2$ is not a square, so if s^2 is the highest square less than r this expression is

$$2(2s-1) - 2s - 2(s-1).$$ □

3 Relations with results for q = 4k′ + 1.

3.1 The section relates results for numbers q = 4k + 1 with those for primes p = 4k – 1. We sketch some of the results for q.

For prime q = 4k + 1, 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, consequently it is at position (3q + 1)/4 from the left.

The intervals for the disparity are [1, (q – 1)/2] and [(q + 1)/2, q – 1]. We know that when q is not prime but still 4k + 1 the occupancy theorem for residues given in Part I fails, so multiply occupied residues correspond to different squares. However, the expressions involving floor functions and square roots which we are using ignore this fact, but in the computations we could use this is benign. The disparity formula is retained by incorporating each duplicate residue separately in its count. We could compare this disparity containing duplicate residues against a formulation of the disparity for p.

If we count the number of quadratic residues for q, this is (q – 1)/2 = 2k, and since there is complete symmetry between the left and right hand parts of the rows under the transformation n → (q – n), the number in each side is k, where our objective might be to show there are more residues for prime p on the left hand side of the rows than the right, the number of residues is (p + 1)/2 = 2k, so the expression is greater than k.

3.2 The section continues results for primes q = 4k′ + 1 with those for p = 4k – 1, in particular we transform from the disparity expression for p to the shifted disparity expression for q.

The intervals for the disparity are [1, (q – 1)/2] and [(q + 1)/2, q – 1]. Thus the disparity for a row r is

$$[2\lfloor\sqrt{[rq-(q+1)/2]}\rfloor - \lfloor\sqrt{(rq-1)}\rfloor - \lfloor\sqrt{[(r-1)q]}\rfloor].$$

Again $\lfloor\sqrt{(rq-1)}\rfloor = \lfloor\sqrt{(rq)}\rfloor$, so the sum is

$$0 = 2\Sigma[r = 1 \text{ to } (q-1)/4][\lfloor\sqrt{[rq-(q+1)/2]}\rfloor - \lfloor\sqrt{(rq)}\rfloor] + \lfloor\sqrt{[q(q-1)/4]}\rfloor,$$

with the last term equating to (q – 1)/2. □

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

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

is even. This is the *shifted disparity for* q.

From examples we see lattice points for m = 0 in $[1, k']$ and $[3k' + 2, 4k']$ minus those in the interval $[k' + 1, 3k']$ are positive. A similar statement may be made for rows.

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

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

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

The shifted disparity expression for each row is

$$2\lfloor\sqrt{[(r - 1)q + ((q + 3)/4)]}\rfloor + [-\lfloor\sqrt{[(r - 1)q]}\rfloor + \lfloor\sqrt{[(r - 1)q + q]}\rfloor] - 2\lfloor\sqrt{[(r - 1)q + (3(q - 1)/4)]}\rfloor.$$

Consequently the total shifted disparity is

$$2\Sigma[r = 1 \text{ to } (q - 1)/4][\lfloor\sqrt{[rq - 3(q - 1)/4]}\rfloor - \lfloor\sqrt{[rq - (q + 3)/4]}\rfloor] + (q - 1)/2,$$

since for $r = (q - 1)/4$

$$(q - 1)/2 = \lfloor\sqrt{(rq)}\rfloor. \ \square$$

By corresponding reasoning to p on disparities, for $q = 4k' - 3$ we conjecture there are less quadratic residues in $[k' + 1, 3k']$ than non-zero such residues elsewhere.

3.4 Both in the q case, and in the p case which we will describe, the row formulas can be used in the trajectory region. The r = 1 to (p + 1)/4 region contains the same number of residues, in the same columns, as the r = (p + 5)/4 to p region, and the row formulas can be applied here too. The row formulas employed are more tractable than the direct cases using row region or trajectory region type equations, terms being of the form $\lfloor\sqrt{[(p^2 + bp + c)/2^d]}\rfloor$, but the situation is complicated, and probably still intractable. The regions determined by parabola methods, in particular for h = 3, may however be effective in determining such a solution.

3.5 The case for p is that both the first two rows together and the m = 0 trajectory have positive disparity. Since the first two rows together for q have positive disparity, the m = 0 trajectory has negative disparity and the total disparity for q is zero, the question may be posed as to whether the positive disparity for p may be obtained as a 'squeeze' theorem between a lower and a higher q. This could be obtained if the regions containing parabolas in the p and q cases could be compared as to their disparity, but this prospect appears remote using floor functions. Parabola methods applied to obtain a squeeze theorem may be effective.

3.6 Results relating to a squeeze theorem may be obtained as follows. For primes q of the form 4k' + 1, we introduce the row value T_q. As for T and p in Part I, section 3.2 and 3.3, the criterion we use is: up to what row value for a perfect square n^2 is the difference between the next square $\leq (q - 1)/2$? So we obtain

$$n \le (q - 5)/4,$$

which must occur on either row $T_q = \lfloor (q + 3)/16 \rfloor$ or $T_q - 1$.

The column for $[(q - 5)/4]^2$ is situated at

$$[(q - 5)/4]^2 - q(T_q - 1) = \lfloor (3q + 25)/16 \rfloor,$$

that is, always on the left at row T_q. This is in contradistinction to the case for p, where if $p = 4k - 1$, $k = 4\alpha + \beta$ and $\beta = 0, 1, 2$ or 3, for $\beta = 0$ or 1 the $(p - 3)/4$ perfect square is on the right, and is only on the left for $\beta = 2$ or 3. However, row T_q has only two residues, as is the case for T.

We choose a new condition defining a new region up to row S_p for prime p by

$$(n + 1)^2 - n^2 \le (p + 1)/4,$$

or

$$n \le \lfloor (p - 3)/8 \rfloor.$$

The row for n must lie between $\lfloor (p - 3)/8 \rfloor^2/p$ and $\lfloor [(p - 3)/8]^2 + (p - 2) \rfloor/p$, that is, it must be at row S_p or $S_p - 1$, where

$$S_p = \lfloor (p + 57)/64 \rfloor.$$

If k is odd, $\lfloor [(p - 3)/8] \rfloor^2$ is in row S_p, since it is situated in column

$$\lfloor [(p - 3)/8] \rfloor^2 - p(S_p - 1) = \lfloor (9p + 9)/64 \rfloor = \lfloor 36k/64 \rfloor,$$

otherwise it is situated in row $S_p - 1$, column $\lfloor (57p + 49)/64 \rfloor$.

Then inside the $1 \to S_p$ region there are at least always three residues, and outside of this region never more than four residues.

For S_q, being the corresponding row for prime q, if we choose

$$(n + 1)^2 - n^2 \le (q - 1)/4,$$

or

$$n \le (q - 5)/8,$$

the row S_q is given by

$$S_q = \lfloor (q + 53)/64 \rfloor,$$

and putting

$$q = p + 2,$$

if k is odd $\lfloor [(q - 5)/8] \rfloor^2$ is at row S_q in column

$$\lfloor [(q - 5)/8] \rfloor^2 - q(S_q - 1) = \lfloor (9q + 25)/64 \rfloor = \lfloor (9p + 43)/64 \rfloor = \lfloor (36k + 34)/64 \rfloor,$$

otherwise it is situated in row $S_q - 1$ and column

$$\lfloor (57q + 81)/64 \rfloor = \lfloor (57p + 195)/64 \rfloor.$$

For k even the value of the maximum residue for S_p and S_q differs by two columns, otherwise they are identical. But if the maximum residue in the $1 \to S_p$ region differs from that of the $1 \to S_q$ region residue by at most two columns, so do the residues for lesser square values.

We may mimic this situation in the S_p region by shifting, as a worst case, the mid column one to the left. But under this rearrangement, since a residue to the left of the true mid column is accompanied for p by no residue to the right, and vice-versa, the difference between these two cases involves at most in total one residue.

Thus the disparity in the $1 \to S_p$ region differs from the disparity in the $1 \to S_q$ region by at most two. □

3.7 In the trajectory region we introduce row U satisfying between quadratic residues (n + 1) and n

$$(n + 1)^2 - n^2 \geq p - (p + 1)/4,$$

that is

$$n \geq \lfloor (3p - 5)/8 \rfloor.$$

The row for U must lie between $\lfloor (3p - 5)/8 \rfloor^2/p$ and $\lfloor [(3p - 5)/8]^2 + (p - 2) \rfloor/p$, which implies for $p > 3$

$$U = \lfloor (9p - 30)/64 \rfloor \text{ or } \lfloor (9p + 34)/64 \rfloor.$$

Inside the $U \rightarrow V = (p + 1)/4$ region there are at least always three residues, and outside of this region never more than four residues.

For U_q, being the corresponding row for prime q,

$$(n + 1)^2 - n^2 \geq q - (q - 1)/4,$$

or

$$n \geq 3(q - 1)/8,$$

so that

$$U_q = \lfloor (9q - 18)/64 \rfloor \text{ or } \lfloor (9q + 46)/64 \rfloor. \square$$

3.8 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 $\pi/2$.

Relating p results to q, for possibly non-prime (p – 2) and (p + 2) we note the parabola

$$n^2 - p(r - 1) = \tfrac{1}{2}\{[n^2 - (p - 2)(r - 1)] + [n^2 - (p + 2)(r - 1)]\},$$

and on setting $q = p - 4g + 2$, that the difference in d(v) between the q and p perfect squares is always $(p + 3)/2 - 3g$. $\square$

4 Fragment and parabola computations for the trajectory region.

4.1 Concerning fragments, there are two major differences for trajectory fragments compared with row fragments. Firstly, on wrap-round, the continuation 'beyond' column (p – 1) becomes a fragment displaced positionally downwards, and since under the mapping $a = e \rightarrow s$, the trajectory region is a type of mirror image of the row region reflected about row T, this introduces an asymmetry between the row and trajectory regions. Secondly, the trajectory parabolas ascend directionally upwards on stepping from left to right, the full range of the row numbers being (e – d) in a traversal. These aspects induce modifications.

4.2 The instances for different j for a given h of trajectory parabolas with associated fragments trace a trajectory, and Part I has shown that an even number of residues in a trajectory has a non-negative disparity whilst an odd number gives a positive disparity or a lowest disparity of -1.

For trajectory parabolas, it is convenient to consider bands not delimited by rows, but by trajectories. In order to paste trajectory bands together as in section 4.1, we define bands as closed at the top trajectory, and open at the delimiting bottom trajectory, where residues are excluded from the range. We specify that when there is a gap at the

bottom of the rightmost ambit, the trajectory corresponding to the bottom residue in the ambit is closed, otherwise only the top trajectory extremity is closed.

4.3 We review the contents of 5.2 of Part II, but for trajectory parabolas and their fragments, in the context of these bands.

Trajectory parabola fragments are absent except when derived from a sequence of trajectory parabolas cutting the right hand edge.

Concerning the wrap-round constituting this fragment formation, we derive that, as the top rightmost ambit residue at v_{top} ascends beyond column $(p - 1)$ to $v_{top} + (n - 1)e$, row r_{vtop} decrements to $r_{vtop} - (n - 1)(e - d) + 1$. The continuation of the bottom rightmost ambit at v_{bottom} transforms to a fragment at row $r_{vbottom} + (n - 1)(e - d) + 1$. This is in accordance with the fact that the fragment given by $\delta = -1$ satisfies at row r

$$G_{frag} = (hr + j_{edge} - h)^2 - p(r - 1)$$
$$= G_{edge\ at\ (r-1)} - p.$$

Where the rightmost trajectory parabola ambits are joined, there are no fragments, without qualification, and the number of residues for each set of trajectory parabolas within the ambit is h. The absence of bogus fragments corresponding to greater or lesser values of h is an instance of the asymmetry between the row and trajectory regions partitioned by row T, or equivalently the ascending left to right nature of the trajectories defining the band limits.

4.4 Of interest to the results on the class number in *Number, space and logic* is the prime $p = 163$, where $\sqrt{(-163)}$ is the highest discriminant with $H^- = 1$. The total disparity here is $3H^-$, as is also confirmed by the formula of theorem 4.3 of Part I.

Set of	Equation for G	h	j
4	$16r^2 - 107r + 212$	4	7
	$16r^2 - 99r + 227$	4	8
	$16r^2 - 91r + 244$	4	9
	$16r^2 - 83r + 263$	4	10
fragment	$9r^2 - 103r + 263$	3	10
3	$9r^2 - 97r + 284$	3	11
	$9r^2 - 91r + 307$	3	12
	$9r^2 - 85r + 332$	3	13
fragments	$25r^2/4 - 98r + 332$	2½	13
	$25r^2/4 - 95½r + 345¼$	2½	13½
5	$25r^2/4 - 93r + 359$	2½	14
	$25r^2/4 - 90½r + 373¼$	2½	14½
	$25r^2/4 - 88r + 388$	2½	15
	$25r^2/4 - 85½r + 403¼$	2½	15½
	$25r^2/4 - 83r + 419$	2½	16
2	$4r^2 - 87r + 524$	2	19
	$4r^2 - 83r + 563$	2	20

The diagram and equation table for p = 163 is given above, where $h_{max} = \lfloor 83^{1/3} \rfloor = 4$. We have for this explicit example the central parabola for h = 3/2 is to the right of the mid column.

4.5 In section 2.6 of Part II, we have considered parabolas up to a maximum value of h, h_{max}, where

$$h_{max} = \lfloor [(p + 3)/2]^{1/3} \rfloor,$$

the minimum value of r for this h being

$$r = \lfloor (p/2h^2) - (1/h)\lfloor p/4h \rfloor + 1 - 1/h \rfloor,$$

which is equal to $\lfloor p/4h^2 \rfloor$ or $\lceil p/4h^2 \rceil$.

There is a region between $r = \lfloor p^{1/3}/6.35 \rfloor$ and the row for h_{max}, $\lfloor p^{1/3}/1.26 \rfloor$, of length up to $\lceil 0.63617p^{1/3} \rceil$ rows, which if each row had disparity -1 would have less negative disparity than the amount by which the first two rows have positive disparity. □

4.6 For odd h we apportion the central ambit between two scenarios: where A_{mid} does not intersect column (p – 1)/2, and the case where it does.

For the first scenario the condition on A_{mid} is

$$(p/h)[p/(4h) - \lfloor p/(4h) \rfloor] = \zeta < p/(2h) + ½, \quad (1)$$

or from 6.4 equation (5) for p = 4k – 1, k = ωh + ξ, 0 < ξ < h, where ξ = 0 does not satisfy the condition on A_{mid},

$$\xi < ¼ + (h/2) + [h^2/(2p)].$$

We make the observation that when h = 3, the number (4k – 1)/(4h) = k/3 – 1/12, so that if k = 1 (mod 3), except in the case k = 1, the number 4k – 1 is divisible by 3 and is not prime. This means that for h = 3 the minimum value of $p/(4h) - \lfloor p/(4h) \rfloor$ is 2/3 – 1/12 = 7/12, and since p > 7, A_{mid} intersects column (p – 1)/2. □

4.7 Independently, the band is given by

$$\Delta_{y,0} = 2^{-y}p/\{[h^2 - 1/2^{2y-2}]h\}, \quad (2)$$

where from 6.4 (8)

$$y = \lceil ½\log_2\{[8h^2 + p^2/(4[\zeta + (p/h) - 1]) - \sqrt{\{48 + 4p^2h^2/[\zeta + (p/h) - 1] + p^4/(64[\zeta + (p/h) - 1]^2)\}}]/2h^4\} \rceil. \quad (3)$$

□

4.8 It is of significance for the direction in which we are travelling that the sum of the bands $\Sigma\Delta_{y,z}$ given by 6.4 (5) of Part II for high p bounded by h and (h + 2) which approaches

$$p(2h + 1)/[4h^2(h + 1)^2]$$

is 5p/144 for $\Sigma\Delta_{y,z}$ with h = 2. Since the row region occupies approximately (p + 9)/16 rows, the sum of these bands, which describes the h = 3 region, is about 5/9 of the total row region, asymptotically. □

4.9 The value of A_{mid} for the parabola one to the left of the central ambit parabola, A_{mid-1}, which in the example of 5.12 we denoted by I, does not satisfy the equivalent of equation (1), that is in both scenarios A_{mid-1} exists and is positive, where we now have

$$A_{mid-1} = 2\{(p/h)[p/(4h) - \lfloor p/(4h) \rfloor + (h + 1)/2] - (p + 1)/2\}^{½}/h > 0,$$

since

$$p/(4h) - \lfloor p/(4h) \rfloor \geq 3/(4h)$$

and

$$h_{max} = \lfloor [(p + 3)/2]^{1/3} \rfloor . \square$$

4.10 *Definition*. The ambits K_i, i = 1, ... h are those intersections with the rightmost edge at column (p – 1) for parabolas with $\delta = i - 1$, and the ambits J_i, i = 1, ... (h – 1)/2 or (h + 1)/2 for $\delta = i - 1$ are those intersections with the mid column (p – 1)/2.

Theorem 4.10.1. For i in the range 1 to (h – 1)/2

$$J_i > K_{(h+1)/2 + i}.$$

Proof. From section 4.11

$$J_i = 2\{(p/h)[p/(4h) - \lfloor p/(4h) \rfloor + h - i] - (p + 1)/2\}^{1/2}/h,$$

and by a determination of 5.10

$$K_i = 2\{(p/h)[p/(4h) - \lfloor p/(4h) \rfloor + h - i] - (p + 2)/2 - p/(2h)\}^{1/2}/h. \square$$

Using theorem 4.10.1, let W be the variable $(p - 2hj)/2h^2$ and Z = (h + 1)/(2h). Then the start row for J_i is

$$W - J_i/2$$

and the end row is

$$W + J_i/2.$$

Likewise, in this instance using the same W, the start row for $K_{(h+1)/2 + i}$ is

$$W - Z - K_{(h+1)/2 + i}/2$$

and the end row is

$$W - Z + K_{(h+1)/2 + i}/2.$$

Definition. For variable W

$$|J_i| = -\lceil W - J_i/2 \rceil + \lfloor W + J_i/2 \rfloor$$
$$|K_i| = -\lceil W - K_i/2 \rceil + \lfloor W + K_i/2 \rfloor.$$

Then applying theorem 4.10.1 with $X = J_i/2$ and $Y = K_{(h+1)/2 + i}/2$,

$$|J_i| > |K_{(h+1)/2 + i}|. \square$$

The central term, which if on the right of (p – 1)/2 has integer disparity $-E_{y,z}$, where we assume this case means $|J_{(h+1)/2}| = 0$, has general integer disparity

$$2|J_{(h+1)/2}| - E_{y,z},$$

whereas the negative integer disparity due to the other parabolas to the right of column (p – 1)/2 is

$$-|K_h| - \Sigma(i = (h + 3)/2 \text{ to } h - 1)E_{y,z}. \qquad (4)$$

We will assume the maximum value of $|J_i|$ is truncated at $E_{y,z}$. Theorem 5.10.1 and (4) imply $|J_i| = E_{y,z}$ for i = 1 to (h – 3)/2.

Only K_h contributes a fragment. The positive disparity due to this fragment and parabolas up to i = (h – 1)/2 is

$$E_{y,z} - |K_h| + \Sigma(i = 1 \text{ to } (h - 3)/2)E_{y,z} + |J_{(h-1)/2}| - (E_{y,z} - |J_{(h-1)/2}|).$$

The total disparity in the interior of the $\Delta_{y,z}$ band is then

$$2|J_{(h-1)/2}| + 2|J_{(h+1)/2}| - 2|K_h| - E_{y,z}, \qquad (5)$$

essentially the same result as equation 5.12 (15) of Part II. $\square$

4.11 We indicate some rule-of-thumb calculations which indicate this approach might be successful.

The row region is of depth ≈ p/16 rows.

For even h, except for one row each time a fragment appears for the first time, the disparity is zero. These odd h fragment disparities, which can be ±1, may be approximately cancelled against linked odd (h – 1) disparities, which have an even number of residues whenever a new fragment appears, but otherwise have ±1 disparity.

Each h band is of depth ≈ p/h^3.

For odd h there are ≈ 1/h of its residues in the central parabola. Thus the total number of central odd h parabola residues in the row region is

$$X \approx \Sigma[i = 1 \text{ to } \lfloor \tfrac{1}{2} h_{max} \rfloor = \lfloor \tfrac{1}{2}(p/2)^{1/3} \rfloor] p/(2i + 1)^4.$$

The top row has positive disparity of

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

so we have to prove

$$Y > \text{disparity for } X.$$

If all central odd h parabolas had negative disparity, then the first term (h – 3) is p/81, so this clearly fails for high enough p.

However, we have proved that h = 3 is an exceptional case, in that it straddles the mid column and we will be able to prove that for low p (or high p including fragments), if ¾ of the (p/81) disparities are positive, we have, where the second term for X is (p/625),

$$(p/162) – (p/625) – (p/2401) – \text{ ... etc.} > 0.$$

We note that for interspersion, say between h = 3 and h = 4, we have

$$h_{interspersed} = (3 + 4)/2 = 7/2,$$

but this is properly divided in separate rows into parabolas related to h = 3, with some inverted h = 3 characteristics (a right of mid column central parabola, not straddling the mid column), and h = 4 (with an even number of residues, and zero disparity, except for appearances of new fragments).

The intrusion of a new fragment in an interspersed band shifts the stratums to the left, so that, if divided into two stratums, they interchange. In this circumstance, using the interspersed h example 7/2, the h = 3 portion becomes the h = 4 portion, and the h = 4 portion becomes the h = 3 portion, and the latter is now promoted to straddle the mid column.

The rightmost ambit for the h = 3 parabola is large in comparison with its interspersed colleagues.

So there is also some hope for a proof by these methods! What is more, the techniques of section 7 can be extended to the parabola case discussed here. □

5 Even power residues for prime p = 4k - 1.

5.1 We have seen that for a prime p that the number of quadratic residues not equal to zero is (p – 1)/2. Further, if p = 4k – 1, we deduced that if x is a quadratic residue, then –x is not, and vice versa, that if –x is a quadratic residue, then x is not. Thus for prime p = 4k – 1 the number of non-residues is also (p – 1)/2. By the occupancy theorem, these residues are all distinct.

If a non-residue is squared, it becomes a quadratic residue and since for p = 4k – 1

a (non-residue)^2 = (minus the non-residue)^2 = (the quadratic residue)^2,

we will find it is possible to define a bijection of

(quadratic residues) to (quadratic residues)^j.

By the binomial expansion (mod p) we have seen that

$(x – y)^p = xp – px^{p-1}y + [p(p – 1)/2]x^{p-2}y^2 –... – y^p \pmod p = x^p – y^p \pmod p$,

so $x^p = y^p$ if and only if x = y.

For some j let

$x^p – x^j = 0 \pmod p$.

Then this is impossible if $j \neq p$ provided $x \neq 0$ and $x \neq \pm 1$, since p is a prime 4k – 1 and must permute cyclically $x \rightarrow x^j$, provided $j \neq p$ and $x \neq \pm 1$.

Thus non-residues are permutations which can be relabelled to the cyclic permutations (2, 3, ..., (p – 1)), that is, cyclic permutations on (p – 3)/2 objects. This implies the same happens for jth powers of quadratic residues.

It follows that theorems such as the prime = 4k – 1 quadratic residue asymmetry theorem also hold for (2j)th powers. □

6 Positive total disparity from the arithmetic average of squares.

To get the average of the squares in clock arithmetic (mod p) where p is prime, we use a result of [CG06] p 47, that

$1^2 + 2^2 + ... + [(p – 1)/2]^2 = [(p – 1)/2]p[(p + 1)/2]/6$.

Thus this sum of squares = 0 (mod p).

There are (p – 1)/2 such squares, so that their arithmetic average is

p(p + 1)/12.

Since a row is of length p columns, in (p + 1)/12 rows the columns of length the size of an average square will appear once. There are (p + 1)/4 rows, thus the columns of this length will span 3 of these instances.

Another way of stating this is that the average square, which is biased towards higher squares, will occupy on average a column at one third along a row. This means that the total number of quadratic residues before column (p + 1)/3 exceeds the total number after it. This proves the positive nature of the total disparity expression. □

Is (p + 1)/3 a whole number?

Since p = 4k – 1, this number is k/3. But k = 1 (mod 3) is impossible when p ≠ 3 and p is prime, because then

$$p = 4(3m + 1) – 1 = 12m – 3,$$

which is composite for p ≠ 3. However, k = 0 (mod 3) is possible, for example

$$p = 12m – 1 = 11 \text{ or } 23,$$

and k = 2 (mod 3) gives primes, as in

$$p = 12m + 7 = 7, 19, 31, \text{ etc.}$$

Then (p + 1)/3 is a whole number for k = 0 (mod 3), but not for k = 2 (mod 3).

For k = 0 (mod 3), (p + 1)/12 is a quadratic residue, since by quadratic reciprocity, for primes 3 and 4k – 1,

$$(3^{p-1)/2} \pmod p)(p^{(3-1)/2} \pmod 3) = -1,$$

and in this case p (mod 3) = (12m – 1) (mod 3) = -1 (mod 3), thus $3^{(p-1)/2} \pmod p = 1$, and 3 is a quadratic residue (mod p), which implies 1/3 is a quadratic residue, because $(3 \times 1/3) = 1$ and 1 is a quadratic residue. But we have seen that $(p + 1)/4$ is always a quadratic residue, thus in this case (p + 1)/12 is a quadratic residue. □

7 Composite numbers.

7.1 In order to investigate the problem further, we could look at quadratic residues for composite numbers, in the hope that going outside the problem might yield additional information. Irrespective of this hope, the programme is of intrinsic interest. We could subdivide our investigations, for primes p, $p' = 4k – 1$ and q, $q' = 4k + 1$ for congruence arithmetic mod 2p, 2q, pq, pp' and qq', also inspecting mod p^2 and q^2.

7.2 We will first look at the cases q = 4k + 2 and q = 4k.

Conjecture 7.2.1. *Let m be a residue* mod (4k + 2) *and* n_m *be the number of residues occupying* m. *Then* m + k *is a residue and* $n_m = n_{m+k}$.

From this would follow
Corollary 7.2.2. *The total disparity for* q = 4k + 2 *is zero*.

The reader is invited to see if this result can be obtained from the product 2(2k + 1).

Lemma 7.2.3. *For* q = 4k *the number of residues on the interval* [1, 2k] *on the first row is not less than twice that for the corresponding interval* [2k + 1, 4k].

Proof. The number of residues on the left hand side of the first row is $\lfloor\sqrt{2k}\rfloor$ and the number on the right is $\lfloor\sqrt{4k}\rfloor – \lfloor\sqrt{2k}\rfloor$. Thus their ratio is $\lfloor\sqrt{2k}\rfloor/[\lfloor\sqrt{4k}\rfloor – \lfloor\sqrt{2k}\rfloor]$, so that on multiplying the numerator and denominator by $\lfloor\sqrt{4k}\rfloor + \lfloor\sqrt{2k}\rfloor$ this is just

$$[\lfloor\sqrt{2k}\rfloor\lfloor\sqrt{4k}\rfloor/2k] + 1,$$

which is not less than than 2 when k = 2n, and also when k = 2n + 1. □

Theorem 7.2.4. *For rows 1 to k the total disparity for* q = 4k (*the number of residues occupying columns* 1 *to* 2k *in the first row minus those on columns* 2k + 1 *to* 4k – 1) *is positive.*

To formulate hypotheses it is instructive to look at the cases k = 5, 6 and 8.

Proof. For quadratic residues (mod 4k), residues 0 to $\lfloor\sqrt{4k}\rfloor$ in the first row cover a set of rows that can be occupied by quadratic residues. This is because squares are of the form $4m^2$ or $4m^2 + 4m + 1$, thus the residues 0 to $\lfloor\sqrt{4k}\rfloor$, of which there are $\lfloor\sqrt{4k}\rfloor + 1$ satisfy

$$4(m + 4nk)^2 = 4m^2 \text{ (mod } 4k)$$

and

$$4(m + 4nk)^2 + 4(m + 4nk) + 1 = 4m^2 + 4m + 1 \text{ (mod } 4k).$$

The number of quadratic residues (mod 4k) for 1 to k^2 counting duplicates is k. Let us consider a highest value of m at $1 + [\lfloor\sqrt{4k}\rfloor/2]$. Then

$$(4k - m)^2 = m^2 \text{ (mod } 4k).$$

Thus selecting residues 0 to this value of m, and then $(4k - m)^2$ to 4k (mod 4k), we return to the residue 0, we cover all intermediate values, and

$$g + 4k = g \text{ (mod } 4k).$$

Thus quadratic residues occur in pairs except for the residue of k^2 when for highest m it is intermediate and distinct between $(4k - m)^2$ and m^2, in which case there is only one value. The row-trajectory bijection theorem 7.1 of part I also applies to residues here.

The residues for the first row have positive disparity, but the k residues in ascending sequence may not form a complete sequence to fill all available slot pairs in the first row completely, the residues for $(4k - m)^2$ and m^2 coinciding. After an occupied set of pairs the sequence of residues will repeat if continued, that is, starting again from a residue in [1, 2k], since the previous residue was in [2k + 1, 4k]. By lemma 7.2.3 if all the remaining residues filled up in [2k + 1, 4k], since there are half these slots occupied by pairs of residues compared with [1, 2k] and deeper layers are already filled with pairs of residues, the positive disparity is kept, even if one value of k^2 is in [2k + 1, 4k].

There remains the possibility that only a subset of a layer is filled. Let k′ be a prime divisor of k. Since there is only one cycle if k′ alone is filled (the argument says this cycle is not a product of permutations, so by a Frobenius automorphism type of argument, any generator will fill all the permutations for k′), it follows that $4k = 4k'j$ gives the same result as 4k′ multiplied by j, where by an induction procedure the theorem holds for 4k′. The same holds inductively for k′ a product of primes.

Thus, including the case of partial occupation by sets of surplus pairs of residues, the total disparity is positive. □

7.3 We now look at ways in which residues for 4k and 4k + 1 and 4k – 1 are related.

Example 7.3.1. Let k = 2, so 4k = 8. Define

$$r = \{17 - [17 \text{ (mod } 8)]\}/4k = 2,$$

then

$$17 \text{ (mod } 8) = 1,$$
$$17 + r \text{ (mod } 4k + 1) = 19 \text{ (mod } 9) = 1$$

and

$$17 - r \text{ (mod } 4k - 1) = 15 \text{ (mod } 7) = 1.$$

Theorem 7.3.2. *Let* x (mod 4k) = y *and define*

$$r = \{x - [x \pmod{4k}]\}/4k.$$

Then

$$[(x + r) \pmod{4k + 1}] = y$$

and

$$[(x - r) \pmod{4k - 1}] = y.$$

Proof. By definition and the Euclidean algorithm

$$x = 4kr + y,$$

so

$$x + r = (4k + 1)r + y,$$

which is the first result, and similarly

$$x - r = (4k - 1)r + y. \square$$

Corollary 7.3.3.

$$x \pmod{4k} = y = \tfrac{1}{2}[x \pmod{4k + 1} + r \pmod{4k + 1} + x \pmod{4k - 1} - r \pmod{4k - 1}]. \quad (1)$$

Example 7.3.4. Since for x = 17 we have $r = 2 < 4k + 1$ and $r < 4k - 1$, so that

$$x \pmod{4k + 1} + r \pmod{4k + 1} = y = 1$$

implies x (mod 4k + 1) is negative, then on cancelling r and –r in (1)

$$17 \pmod{4k} = \tfrac{1}{2}\{17 \pmod 9 \textit{ taken negatively} + 17 \pmod 7 \textit{) taken positively}\}$$

$$= \tfrac{1}{2}[-1 + 3] = 1. \square$$

References

Ad18 J.H. Adams, *Number, space and logic*, www.jimhadams.com, (2018).

Bu89 D.A. Buell, *Binary quadratic forms*, Springer (1989).

CG06 J.H. Conway and R.K. Guy, *The book of numbers*, Copernicus books, Springer imprint (2006).

1Da77 *The collected works of Harold Davenport*, vols I – IV, Academic Press (1977).

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

2Da99 H. Davenport, *The higher arithmetic*, 7th edition, Cambridge U.P. (1999).

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

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

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