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

jim-adams@supanet.com

15th February 2012, revised 8th February 2013

Abstract. In Part I we obtained a formula for the number of quadratic residues for prime p = 4k – 1 in the interval [1, 2k – 1] minus those in [2k, 4k – 2], which we called the total disparity. Hermann Weyl in 1940, using transcendental methods, asked for an elementary proof of the positive nature of this expression.

In Part II we divide intervals into rows, the rth row being [(r – 1)p, rp – 1]. A feature between row 2 and, using the floor function, row T = $\lfloor (p + 9)/16 \rfloor$ is that we can trace quadratic residue curves, *parabolas* that first move left and then right. The trajectory region below row T to row (p + 1)/4 has similar aspects to the row region. We use these features to investigate the positive value of the disparity expression.

Part III will further estimate this asymmetry, when we will compare p = 4k – 1 methods with results for q = 4k + 1. It will also compare our techniques with other established methods and specify the relations of this problem to the class number for quadratic forms. An estimate and confirmation of the positive disparity combined with sophisticated transcendental results implies a proof of the absence of the tenth discriminant in the $\sqrt{-p}$ case.

Keywords: elementary methods, quadratic residue

1 Synopsis of Part I, introduction to Part II and a plan of Part III.

1.1 Richard Guy in [Gu04], unsolved problem **F5**, asks: If a prime p = 4k – 1, there are more quadratic residues in the interval [1, 2k – 1] than in [2k, 4k – 2], but all known proofs use Dirichlet's class-number formula. Is there a proof by elementary methods? The problem was obtained arising from consideration of work by Davenport [2Da99]. Continuing from Part I, we investigate this result.

1.2 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.

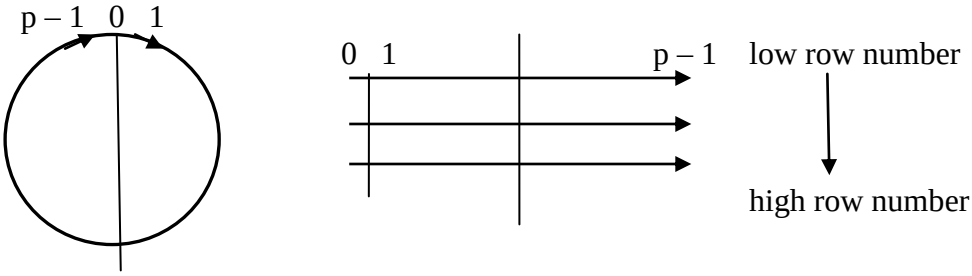


Figure 1.1

Each traversal of the clock above on the left with prime p = 4k – 1 hours is transformed into the rows on the right, and correspondingly for the quadratic residues belonging to them. The theorem to be proved states there are more quadratic residues on the right hand side of the clock, or equivalently more in total on the left hand side of the rows.

If p – 1 has a divisor s, this is part of a more general problem to rank the number of power residues within s intervals.

1.3 A synopsis of some results in Part I is that for each row there is at worst a *disparity* of minus 1, this being the number of quadratic residues in the interval [1, 2k – 1] minus those in [2k, 4k – 2]. The number of rows before a residue repeats is (p + 1)/4 and up to this row all residues are accommodated. A standard result is that the number of residues ≠ 0 is (p – 1)/2. Row $T = \lfloor (p + 9)/16 \rfloor$ is significant. The criterion we use is: up to what value for a perfect square n^2 in the left or right hand part of a row is the difference between the next square ≤ (p – 1)/2? The row corresponding to this is row T. As described in Part I, the phenomenon we observe after row T is that of *trajectories*, which begin at column (p + 1)/4 on row (p + 1)/4 and ascend as a parabola traversing successively lesser row numbers from the left to the right, switching back to the left on the same row as the final residue on the right for a new traversal of a trajectory.

1.4 The distribution of residues up to row T has a remarkable structure. We can trace quadratic residue curves, consisting of *parabolas* which first move left and then right. We can partition these parabolas so that residues are counted once only.

Below row T up to row (p + 1)/4, which is the last row up to which quadratic residues are distinct, the trajectory parabola diagram is in some ways the mirror image of that for rows, the reflection being about a horizontal axis.

The main objective of our work is to derive the positive total disparity for quadratic residues from a study of parabolas in the row and the trajectory region. A subsidiary objective is to relate these investigations to the class number, H.

1.5 Section 2 displays the phenomenon of quadratic residues in the row region from row 1 to T, which trace out parabolas. For prime $p = 4k - 1 = 1031$, an example diagram is drawn and a table of formulas for the parabolas is listed. We then derive the general parabola equation and the formulas for its parameters.

Although this diagram shows quadratic residues not fitting, as yet, any parabolas, the table provides such equations. These are fragments, described in section 3, where a definition of the partition of the diagram into bands is provided.

Section 4 sketches, for parabolas in the trajectory region – from row T to row $(p + 1)/4$, what section 2 performed for parabolas in the row region.

In section 5 the apparatus and formulas necessary to derive the positive nature of the total disparity in the row region are provided in the limited case of single fragments, defined as for 'low p'. Where floor and ceiling functions are present, their analysis is largely deferred until section 8.

Section 6 describes the structure of multiple fragments, synonymous with 'higher p'. An innovation in this section is to partition into bands not defined by natural number rows.

1.6 Part III extends to the trajectory region the tasks carried out in sections 5 and 6.

We will estimate there the entire disparity, which also ties in results from Part I on the first rows of the row region, and the beginning trajectories, $m = 0$ onwards, in the trajectory region.

Part III relates results for primes $q = 4k' + 1$ compared with those for $p = 4k - 1$ and derives some other results, in particular on transforming from the disparity expression for p to the shifted disparity expression for q.

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

1.7 The style we adopt in this paper is to ensure that the material is semantically understood by examples, and that results are explored through a natural development showing their history. This is in accordance with our philosophy that mathematics is a process of exploration and detection. When encountered in this work for the first time, the names of significant ideas are *italicised*. Equations are used as freely as words, and theorems, which may be unnamed, are treated either as the topic of a numbered paragraph, or its conclusion.

2 Parabolas for rows.

2.1 If we look at the distribution of quadratic residues for prime $p = 4k - 1 = 4 \times 258 - 1 = 1031$ up to row T = 65 shown in the graph and table below, we note a number of remarkable properties.

The distribution of quadratic residues, seemingly random at first sight, can be filled out with overlapping parabolas. For the three parabolas extending from rows 29 and 30, writing these as

$$G = a^2r^2 + br + c,$$

where r is a row number and G is the value of a quadratic residue, we observe that a = 3 for all three parabolas. A very slight upwards slope is evident in the distribution from left to right of the minimums of the parabolas. The minimum occurs for dG/dr = 0, so $r_{min} = \lfloor -b/2a^2 \rfloor$. Immediately above it, there are four parabolas and a = 4, likewise for the five parabolas above it, a = 5, for the six we find a = 6, and for seven a = 7. Below the set of three parabolas there are five parabolas with double row spacing, all with a = 2½, and below that towards row T, this time with single spacing, there are two parabolas with a = 2. These latter parabolas overlap a region discussed in Part I leading up to row T where there is non-negative disparity.

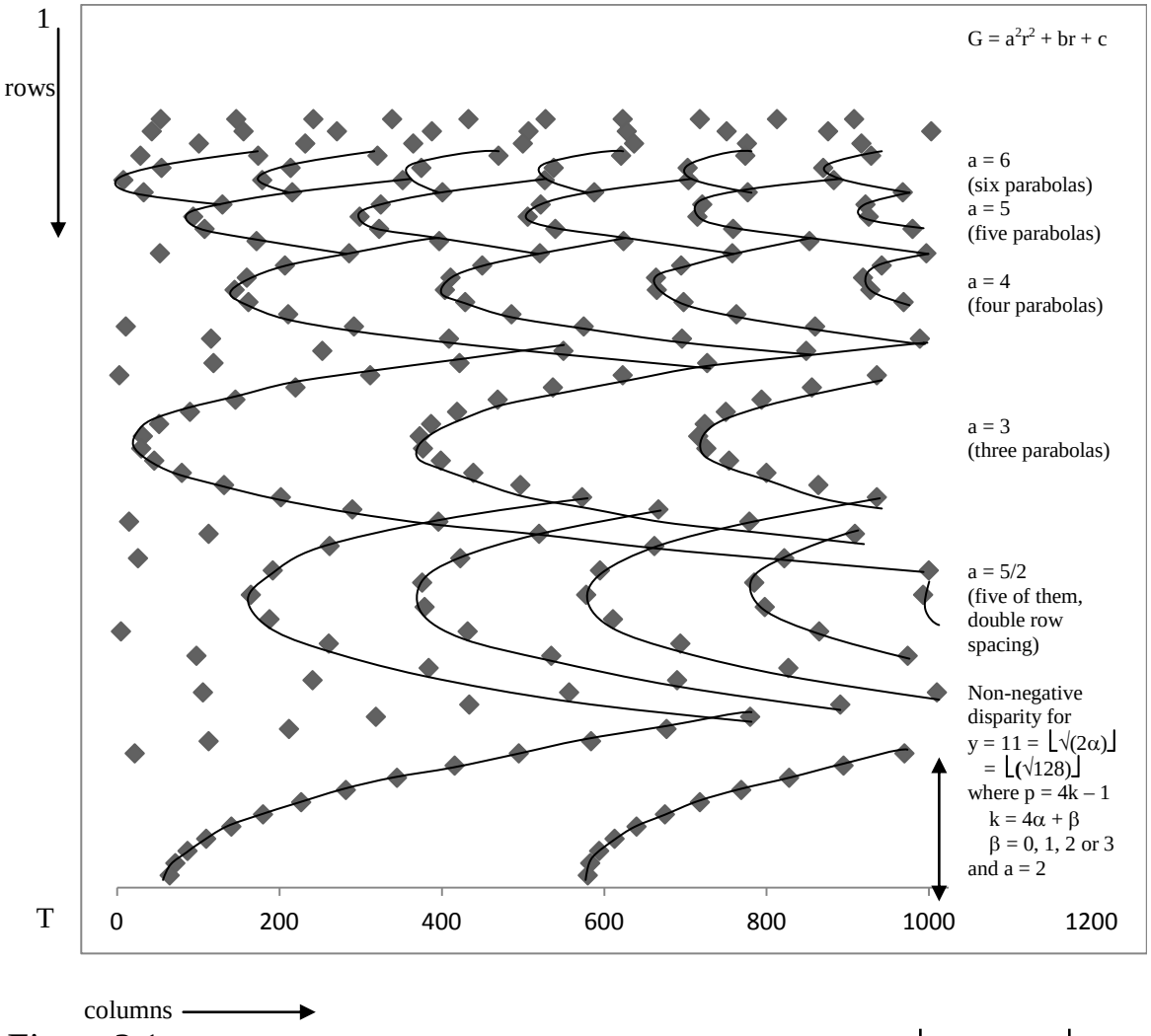


Figure 2.1 *Parabolas of perfect squares for* p = 1031, *where* T = 65 = ⌊(p + 9)/16⌋.

In more detail, the parabolas given by $G = a^2r^2 + br + c$ in left to right sequence may be represented by the equations and relationships

Set of	Equation for G	b difference	c increment	h	j
7	$49r^2 – 611r + 1931$	14		7	30
	$49r^2 – 597r + 1992$		61	7	31
	$49r^2 – 583r + 2055$		63	7	32
	$49r^2 – 569r + 2120$		65	7	33
	$49r^2 – 555r + 2187$		67	7	34
	$49r^2 – 541r + 2256$		69	7	35
	$49r^2 – 527r + 2327$		71	7	36
6	$36r^2 – 587r + 2400$	12		6	37
	$36r^2 – 575r + 2475$		75	6	38
	$36r^2 – 563r + 2552$		77	6	39
	$36r^2 – 551r + 2631$		79	6	40
	$36r^2 – 539r + 2712$		81	6	41
	$36r^2 – 527r + 2795$		83	6	42
5	$25r^2 – 561r + 3240$	10		5	47
	$25r^2 – 551r + 3335$		95	5	48
	$25r^2 – 541r + 3432$		97	5	49
	$25r^2 – 531r + 3531$		99	5	50
	$25r^2 – 521r + 3632$		101	5	51
fragment	$16r^2 – 551r + 4631$			4	60
4	$16r^2 – 543r + 4752$	8		4	61
	$16r^2 – 535r + 4875$		123	4	62
	$16r^2 – 527r + 5000$		125	4	63
	$16r^2 – 519r + 5127$		127	4	64
fragment	$9r^2 – 539r + 7755$			3	82
3	$9r^2 – 533r + 7920$	6		3	83
	$9r^2 – 527r + 8087$		167	3	84
	$9r^2 – 521r + 8256$		169	3	85
fragments	$6¼r^2 – 531r + 11031$			2½	100
	$6¼r^2 – 528½ r + 11131¼$			2½	100½
5	$6¼r^2 – 526r + 11232$	2½		2½	101
	$6¼r^2 – 523½r + 11333¼$		101¼	2½	101½
	$6¼r^2 – 521r + 11435$		101¾	2½	102
	$6¼r^2 – 518½r + 11537¼$		102¼	2½	102½
	$6¼r^2 – 516r + 11640$		102¾	2½	103
fragment	$4r^2 – 527r + 16907$			2	126
2	$4r^2 – 523r + 17160$	4		2	127
	$4r^2 – 519r + 17415$		255	2	128

It can be observed that all such parabolas follow the equation

$$G = (hr + j)^2 – p(r – 1)$$

where h and j are given in the table columns above.

We wish to establish parabolas as a function of the row, r. By the Euclidean algorithm each positive number, n, can be represented as

$$n = hr + j,$$

with the expression unique if $0 \leq j < r$, and not unique if j is free. We choose the latter alternative. Thus each perfect square can be represented in multiple ways by

$$n^2 = (hr + j)^2.$$

We now map these perfect squares onto rows by subtracting, for each row, the length of previous rows, so for the rth row we subtract $p(r - 1)$, there being zero subtraction for r = 1. Then since the sum of a straight line and an algebraic parabola is a parabola,

$$G = n^2 - p(r - 1)$$
$$= (hr + j)^2 - p(r - 1)$$

is a parabola.

We note in the special case h = 2½, that in order for n to be a whole number, j is a natural number plus ½ when r is odd. More generally, when h is rational in lowest terms, then (hr + j) is a whole number. We describe parabolas with such rational h as *stratified*, otherwise as *unstratified*. For parameter h = 2½ the parabola sets split into two alternating strata, or called stratums, depending on whether rows are even or odd.

2.2 At row related r_{min} the gradient of the parabola with respect to r is zero

$$dG/dr = 2h^2r + 2hj - p = 0,$$

so

$$r_{min} = (p - 2hj)/2h^2,$$

which gives the minimum value of the parabola G as

$$G_{min} = -(p^2/4h^2) + p[(j/h) + 1].$$

2.3 We will determine the maximum number of perfect squares, M_{max}, between the row floors $\lfloor r_{min} \rfloor$ or the row ceilings $\lceil r_{min} \rceil$ for a sequence of parabolas determined by the r_{min} for constant h.

The perfect squares at whole number rows above and below r_{min} are usually to the right of G_{min}. An exception on the right is when $G_{min} \leq$ column $(p - 1)$ and both the row floor $\lfloor r_{min} \rfloor$ and the row ceiling $\lceil r_{min} \rceil$ contain quadratic residues 'beyond' this column. In this exceptional case row $\lfloor r_{min} \rfloor$ promotes an extra residue to row $\lceil r_{min} \rceil$ otherwise one of $\lfloor r_{min} \rfloor$ or $\lceil r_{min} \rceil$ contain residues on or between G_{min} and column $(p - 1)$. Thus effectively either $\lfloor r_{min} \rfloor$ or $\lceil r_{min} \rceil$ contain at least M_{max} parabolas derived from counting the instances of G_{min} along r_{min} at constant h.

For G_{min} the difference between values corresponding to j and $(j + \delta)$ is

$$p\delta/h < p,$$

reducing to

$$\delta < h.$$

Since a sequence of δ intervals contains $(\delta + 1)$ end points for the intervals, the maximum number of perfect squares for the parabolas for each h is

$$M_{max} = h.$$

If $\lfloor r_{min} \rfloor$ or $\lceil r_{min} \rceil$ promotes a residue to the next row, we describe this as an example of fragments, to be described later, in which δ starts from -1 and M_{max} is nominally h.

2.4 The increment of r_{min} at j to r_{min} at $j + M_{max} - 1$ is

$$(-M_{max} + 1)/h = (1/h) - 1.$$

This is the slope we referred to previously.

2.5 If we wish to determine the value of j from r_{min}, then because the increments of r_{min} are small over a range of j increasing for fixed h, this depends very sensitively on r_{min}.

Since for parabolas with minimums G_{min} there are normally h perfect squares around row r_{min}, if they were equidistributed – they are not, a denser distribution is to the left because spacing between residues increases, the maximum start value of G_{min} is approximately, but less than

$$G_{min} \approx p/h$$

giving the first value of j for this h as less than

$$j_{start} \approx 1 + (p/4h) - h.$$

The following table gives the true values of j_{start} for p = 1031 and those as computed by the above approximate formula.

h	j_{start} computed	j_{start} actual
7	30.8	30
6	37.9	37
5	47.5	47
4	61.4	61
3	83.9	83
2½	101.6	101
2	127.8	127

As is readily observed, for a natural number h

$$j_{start} \approx \lfloor p/4h \rfloor + 1 - h \qquad (1)$$

fits these values. This induces the modified formula

$$G_{min} \approx (p/h)[1 - (p/4h) + \lfloor p/4h \rfloor]. \qquad (2)$$

On the other end of the range, if the minimum value of G_{min} is near zero – but the minimum quadratic residue not in the first row is in a column > 1, then

$$j_{start} > (p/4h) - h,$$

giving of course

$$G_{min} > p \equiv 0 \pmod{p}.$$

It is the case that 4h does not divide p, and we now confirm

$$j_{start} = \lfloor p/4h \rfloor - h + 1,$$

and thus we have corroborated equation (2). For δ varying between 0 and (h – 1), the general value of G_{min} along row related r_{min} is now

$$G_{min} = (p/h)[1 - (p/4h) + \lfloor p/4h \rfloor + \delta].$$

2.6 We will consider a maximum suitable value of (h + 1), h_{max}, to occur when the difference as a function of h between $r_{min}(h)$ and $r_{min}(h + 1) \approx 1$. Since

$$r_{min}(h) \approx (p/4h^2) - (1/h) + 1,$$

where we have used $j \approx 1 + (p/4h) - h$, if

$$r_{min}(h) - r_{min}(h + 1) \approx 1$$

then

$$4h^4 + 8h^3 + 8h^2 + (4 - 2p)h - p \approx 0,$$

which is satisfied approximately by

$$(1 + 2h)^3 \approx 4p.$$

Putting $h_{max} = h + 1$ gives as a *definition* from the approximate value $\approx \lfloor (p/2)^{1/3} + ½ \rfloor$,

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

3 Unstratified single fragments for rows.

3.1 Unstratified parabolas may be partitioned into horizontal *bands* so there is no overlap. We note a result of Part I; if there is an even number of quadratic residues in any row, the disparity is not negative. Thus when h is even the parabolas between rows where the rightmost parabola is situated must have non-negative disparity if there are no additional residues further on the left hand side of the row belonging to a *fragment* of a parabola, or belonging to a parabola with an upper h above them.

The *ambit* of the rightmost parabola is the range of rows for which there exist residues for the parabola, as shown in figure 3.1. Ambits will be classified as to whether h is even or odd. Where it exists a *gap* is the range of rows between ambits.

As a consequence, whenever the ambits of the rightmost parabolas for adjoining values of h have a gap, the topmost residue for a parabola with value h may be considered as continuing 'beyond' column (p – 1), wrapping round so it is in the leftmost row of the topmost residue, in a fragment. The row regions between fragment intersections if they exist for contiguous h are the *bands*, otherwise these bands are situated in the early rows between where the rightmost parabolas are *joined* for parabolas given by (h + 1) and h. In later rows there is a gap between such ambits.

In order that contiguous bands fit together, the bands are *closed* at the top row, that is, contain the topmost residues, and are *open* at the bottom, where residues are excluded from the range. We specify that when there is a gap at the bottom, ambits are all closed, otherwise only the top extremity of the ambit is closed.

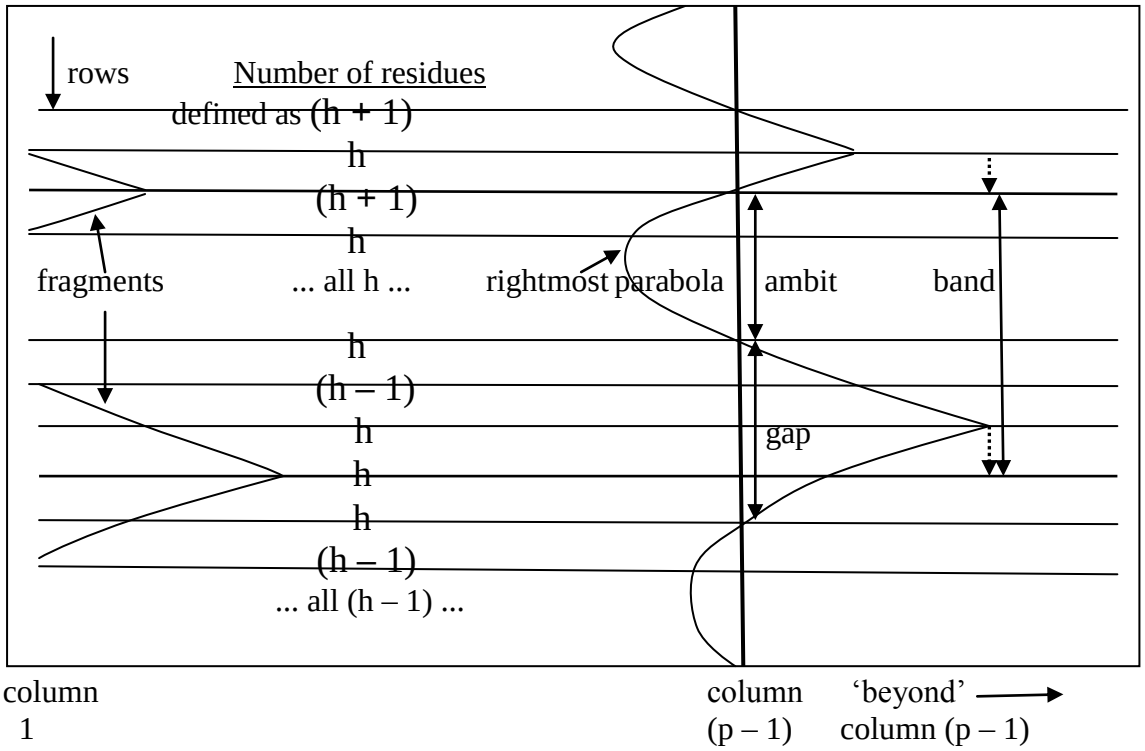


Figure 3.1 *Parabolas, ambits, gaps, bands and fragments*

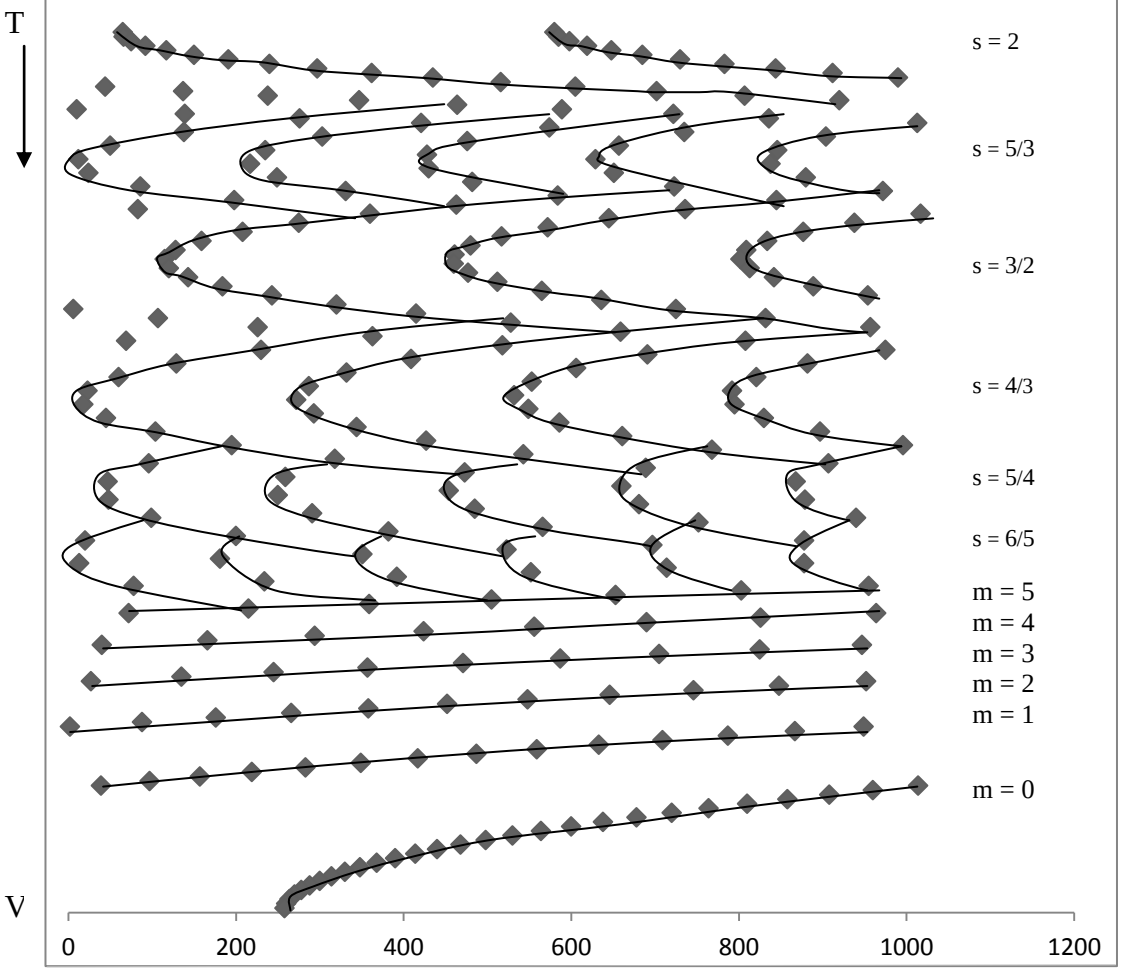
4 Trajectories and trajectory parabolas.

4.1 For trajectories, Part I has proved that the vth perfect square counting backwards from the last distinct quadratic residue at v = 1 is at column

$$D(v) = v(v - 1) + (p + 1)/4 \pmod p, \qquad (1)$$

where we are taking residues (mod p). The trajectory is a parabola (mod p). Six trajectories are traced from m = 0 to m = 5 in the bottom part of Figure 4.1.

Figure 4.1 *Graphs of trajectories are given by* D *and trajectory parabolas by* $L = s^2r^2 + ur + w$, *for prime* p = 1031, *here below row* $r = T = \lfloor (p + 9)/16 \rfloor = 65$ *to row* $V = (p + 1)/4 = 258$, *with row numbers increasing the lower the row in the diagram, and with columns containing quadratic residues*.



Simultaneously, this equation also fits trajectory parabola curves, shown above these trajectories in the example diagram for p = 1031. As v increments to (v + e), where e is the number of trajectory parabolas along a row, the residue along the trajectory parabola goes back one residue. More generally, if the quadratic residue for a chosen trajectory is the vth, then the nth residue along a particular trajectory parabola corresponds to v + (n – 1)e.

For p = 1031, the trajectory parabolas given by $L = s^2r^2 + ur + w$ listed in increasing column sequence may be represented by the equations and relationships

e	Equation for L	u difference	w increment	h = s	j
2	$4r^2 - 523r + 17160$			2	127
	$4r^2 - 519r + 17415$	4	255	2	128
fragment	$[25r^2 - 4699r + 219043]/9$			5/3	458/3
5	$[25r^2 - 4689r + 219960]/9$			5/3	459/3
	$[25r^2 - 4679r + 220879]/9$	10/9	919/9	5/3	460/3
	$[25r^2 - 4669r + 221800]/9$	10/9	921/9	5/3	461/3
	$[25r^2 - 4659r + 222723]/9$	10/9	923/9	5/3	462/3
	$[25r^2 - 4649r + 223648]/9$	10/9	925/9	5/3	463/3
fragment	$9r^2/4 - 521r + 29930½$			3/2	340/2
3	$9r^2/4 - 519½r + 30101¼$			3/2	341/2
	$9r^2/4 - 518r + 30272$	1½	170¾	3/2	342/2
	$9r^2/4 - 516½r + 30443¼$	1½	171¼	3/2	343/2
fragment	$[16r^2 - 4679r + 339904]/9$			4/3	575/3
4	$[16r^2 - 4671r + 341055]/9$			4/3	576/3
	$[16r^2 - 4663r + 342208]/9$	8/9	1153/9	4/3	577/3
	$[16r^2 - 4655r + 343363]/9$	8/9	1155/9	4/3	578/3
	$[16r^2 - 4647r + 344520]/9$	8/9	1157/9	4/3	579/3
5	$[25r^2 - 8296r + 688896]/16$			5/4	820/4
	$[25r^2 - 8286r + 690537]/16$	10/16	1641/16	5/4	821/4
	$[25r^2 - 8276r + 692180]/16$	10/16	1643/16	5/4	822/4
	$[25r^2 - 8266r + 693825]/16$	10/16	1645/16	5/4	823/4
	$[25r^2 - 8256r + 695472]/16$	10/16	1647/16	5/4	824/4
6	$[36r^2 - 12959r + 1166399]/25$			6/5	1068/5
	$[36r^2 - 12947r + 1168536]/25$	12/25	2137/25	6/5	1069/5
	$[36r^2 - 12935r + 1170675]/25$	12/25	2139/25	6/5	1070/5
	$[36r^2 - 12923r + 1172816]/25$	12/25	2141/25	6/5	1071/5
	$[36r^2 - 12911r + 1174959]/25$	12/25	2143/25	6/5	1072/5
	$[36r^2 - 12899r + 1177104]/25$	12/25	2145/25	6/5	1073/5

Note that the equations for L for the set of two trajectory parabolas are identical to the corresponding set already encountered for the G row parabolas. This is no accident. The equations for L are identical to G with h and j given in the table above, as is expected since quadratic residues below row T correspond by the same representation criterions to those above row T.

For row r we will represent v by

$$v = (-sr + f), \qquad (2)$$

and denote the number of times rows for which there are pairs of residues in the same row running across trajectory parabolas by d.

The rows with $s \leq 2$ contain in each row either a single residue, left or right of column $(p - 1)/2$, with respectively a positive or negative disparity, or alternatively a pair of residues, for which there is always no net disparity. Observationally, these rows cluster into irregular and regular sets. The regular sets contain a repeating pattern in row order of g rows with a single residue and d rows with a pair of residues. Then the number of trajectory parabolas satisfies

$$e = 2d + g.$$

We have seen that trajectory parabolas trace a leftward then rightward movement, which means that each parabola within a regular set alternates from single residues with negative disparity to those with positive disparity, and back to those with negative disparity, or an incomplete and relative portion of this.

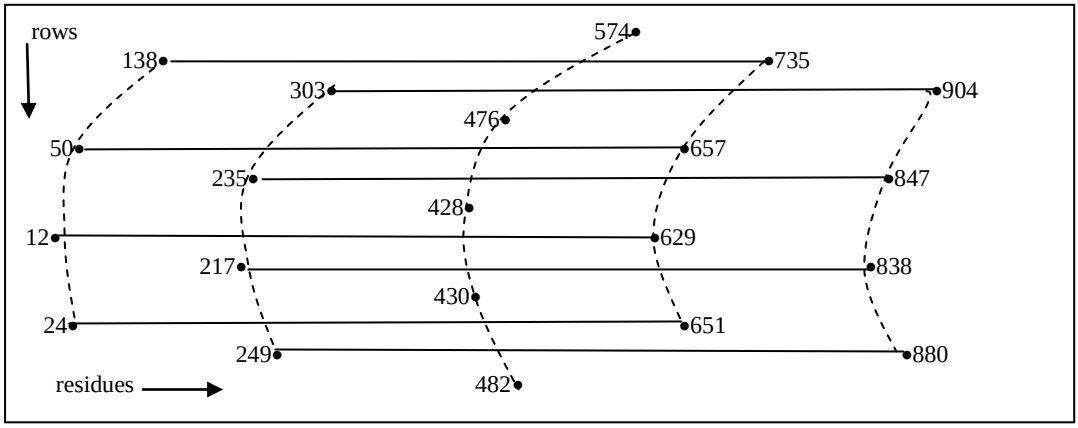


Figure 4.2 *Trajectory parabolas for* h = 5/3, p = 1031. *Residues in pairs for a row are connected with a horizontal line.*

Corresponding to the increment $v \rightarrow v + (n - 1)e$, the row of the trajectory parabola for that quadratic residue decrements by (d + g) = (e – d) rows under the mapping

$$v \rightarrow \{-s[r - (n - 1)(e - d)] + f\} = \{v + s(n - 1)(e - d)\},$$

so we identify (n – 1)e and s(n – 1)(e – d):

$$s = e/(e - d). \qquad (3)$$

Thus as previously defined, the trajectory parabolas correspond to stratified parabolas for the row equations.

On incrementing within the trajectory parabola to v + (n – 1)e we obtain from (1) the relationship

$$L[v + (n - 1)e] = L(v) + (n - 1)e[2v + (n - 1)e - 1] \pmod p . \qquad (4)$$

On removing the (mod p) condition from equation (1), we observe that the last perfect square on row (p + 1)/4, where v = 1, has the value

$$n^2 = v(v - 1) + (p + 1)/4 + p\{[(p + 1)/4] - 1\}$$

and that the perfect square corresponding to v in the same m = 0 trajectory is at

$$n_v^2 = v(v - 1) + (p + 1)^2/4 - vp, \qquad (5)$$

where the perfect square is independent of the m value here, so (5) generally holds.

As the trajectory parabola ascends, v transforms to v + (n – 1)e and simultaneously row r_v decrements to $r_v - (n - 1)(e - d)$, thus

$$L[v] = n_v^2 - (r_v - 1)p, \qquad (6)$$

$$L[v + (n - 1)e] = L[v] + (n - 1)\{e[2v + (n - 1)e - 1] - dp\}. \qquad (7)$$

To consider an example of equation (7), the 351st perfect square for p = 1031 is at row r = 120 and is the quadratic residue $L[v] = (351)^2 - (120 - 1)1031 = 512$ at this column. Now the value of v here is (p – 1)/2 – 351 + 1 = 165. On the same trajectory parabola, which is in a set of e = 3, d = 1, the 348th perfect square is at row r = 118 and is the quadratic residue L[v + 3] = 477, where [v + 3] is 168. The difference L[v + 3] – L[v] is -35, which in accordance with (7), is the value e[2v + e – 1] – dp.

5 Parabola and single fragment computations for the row region.

5.1 In Part I we established, except for p = 67, the non-negative disparity up to row y above row T, where $y^2 < 2\alpha$, with $k = 4\alpha + \beta$ and $\beta = 0, 1, 2$ or 3. We are able to extend these procedures to the properties of parabolas as we ascend from row T.

5.2 Fragments are absent except when derived from a sequence of parabolas on the right, and are formed from a wrap-round located on the left of parabola continuations 'beyond' column (p – 1) on the right.

A row with an even number of residues has a non-negative disparity, and with an odd number has a positive disparity or a lowest disparity of -1.

Where the ambits are joined, there are no fragments. In this case h corresponds with the number of residues, except for the particular case of the row corresponding to the join itself, where the lower rightmost parabola given by h may be considered continuing upwards to give a fragment wrapped round on the same row, which is the same as part of a left upper parabola given by (h + 1). Thus if the parabola below it has parameter h, the disparity at the join is for (h + 1) residues.

By the same type of argument, the topmost residue for an ambit has (h + 1) residues for its row when there is a fragment present.

For the interior of the ambit with parameter h, there are h parabolas and no fragments.

For the bottom part of an ambit followed by a gap, the bottom row of the ambit has h residues. When the gap between ambits is greater than one row, so there is more than one residue in the fragment, then the residues for the fragment derived from the parabola of the ambit appear two rows below the bottom residue for this ambit, on considering the parabola to continue 'beyond' column (p – 1) for the bottom residue of the parabola.

Thus, since there will be (h – 1) parabolas for this row, and one fragment, the number of residues in the row is h. It is also the case that the number of parabolas in the row immediately below the ambit is (h – 1), and there is no fragment residue, so this can be identified with the number of residues for this row.

5.3 When single fragments are present both for the band given by h and the band given by (h + 1), then for the fragments at the top of both bands, the topmost residues for the ambit have respectively (h + 1) and (h + 2) instances, and thus the rows with an even number of residues in the topmost row of the ambit may be accounted with a row in the other band in the interior of its ambit with an even h. Likewise the row with an odd number of topmost residues may be accounted with an interior row for odd h in the other band.

For fragments at the bottom of the band, the corresponding situation is that for an ambit given by h, there are first (h – 1) then h residues at the bottom rows, and for ambit (h + 1) there are h and then (h + 1) residues. Once again, overall the number of even or odd residues in a row may be accounted as remaining constant.

5.4 Row fragments are positioned to the left of row parabolas, and are described by the same type of equation for that h. So if the leftmost parabola is given by parameter j, the corresponding fragment is given by (j – 1), and (j – 2), etc. if there is more than one.

If the top and bottom segment of the same fragment correspond to parameter values h_{h+1} and h_h and j_{h+1} and j_h respectively, then these segments meet in the fragment when

$$(h_{h+1}r + j_{h+1})^2 - p(r - 1) = (h_h r + j_h)^2 - p(r - 1)$$

or

$$(h_{h+1} - h_h)r = j_h - j_{h+1},$$

where, if $h_{h+1} > h_h$,

$$h_{h+1} - h_h \leq 1.$$

Further, for multiple fragments given by $j_h - |\delta|$ and $j_{h+1} - |\delta|$, the value of $j_h - j_{h+1}$ is unaltered, and thus if present all multiple fragments intersect at the same row.

These fragment intersections when they exist define the extremities of the bands, say for between (h + 1) and h, at

$$r_{\text{band end}}(h + 1, h) = \lfloor p/4h \rfloor - \lfloor p/4(h + 1) \rfloor + 1.$$

As a function of h – the greater the h, the lesser the row – there will be a gap between ambits, so fragments will exist for unstratified parabolas, when on adjusting for wrap-round

$$r_{\text{band end}}(h + 1, h) - 1 - r_{\text{edge most}}(h + 1) > 0.$$

A more symmetrical designation is

$$r_{\text{edge least}}(h) - r_{\text{edge most}}(h + 1) > 0.$$

Avoiding here these direct calculations, we make some simple observations.

The existence of a join between parabolas defined by parameters h and (h + 1), means that there exist respective rightmost parameters j'_h and j'_{h+1}, where

$$j'_h = j'_{h+1} + \kappa$$

such that

$$[hr + j'_h]^2 - p(r - 1) = G,$$

and

$$[(h + 1)r + j'_{h+1}]^2 - p(r - 1) = G,$$

which implies that

$$r_{\text{join}} = \kappa.$$

Where there is a fragment, we have defined this as at $r_{\text{join}} + 1$.

For positive B and C, if $B - \lfloor B \rfloor \geq C - \lfloor C \rfloor$, then

$$\lfloor B \rfloor - \lfloor B - C \rfloor = \lfloor C \rfloor$$

and if $B - \lfloor B \rfloor < C - \lfloor C \rfloor$, then

$$\lfloor B \rfloor - \lfloor B - C \rfloor = \lceil C \rceil.$$

Now $j'_h = \lfloor p/4h \rfloor$ and $j'_{h+1} = \lfloor p/4(h + 1) \rfloor$, so that

$$\lfloor p/4h \rfloor - \lfloor p/4(h + 1) \rfloor = r_{\text{join}}, \qquad (1)$$

where we set

$$B = p/4h$$

$$C = p/[4h(h + 1)],$$

so that either $\lfloor C \rfloor = r_{join}$ or $\lceil C \rceil = r_{join}$.

Let $p = 16\alpha + 4\beta - 1$, where $\beta = 0, 1, 2$ or 3. Then

$$p/4h = 4(\alpha/h) + (\beta/h) - (1/4h).$$

Take the example $\beta = 0$. If h divides 4α then $B - \lfloor B \rfloor$ is large, Likewise $C - \lfloor C \rfloor$ is large if $h(h + 1)$ divides 4α. But if $h(h + 1)$ divides 4α, so does h, so that under the latter divisibility constraint or for instance $h = 3$

$$B - \lfloor B \rfloor < C - \lfloor C \rfloor$$

giving

$$\lceil p/4h(h + 1) \rceil = r_{join}. \qquad (2)$$

The conditions are not all listed here. The alternative rightmost join satisfies

$$\lfloor p/4h(h + 1) \rfloor = r_{join}. \qquad (3)$$

Moreover, when $G > p$, or

$$[h r_{join} + j'_h]^2 - p r_{join} > 0,$$

we infer that a fragment exists derived from the band. By definition the upper fragment equation contains residues within the band, provided this fragment equation does not specify a bogus fragment residing in an upper parabola. But in this situation a fragment will be present derived from the bottom part of the parabola, even if this is not directly in the band, and since h decrements with increasing r, this is not a bogus fragment.

5.5 Parabolas for the band encompassing the band edges for $(h + 1)$ and h obey

$$r = j_h - j_{h+1}$$
$$= \lfloor p/4h \rfloor - \lfloor p/4(h + 1) \rfloor + 1, \qquad (4)$$

and we obtain for the fragment join

$$r = \lceil p/4h(h + 1) \rceil + 1 \qquad (5)$$

or

$$r = \lfloor p/4h(h + 1) \rfloor + 1, \qquad (6)$$

which may be compared with equations (2) and (3).

5.6 The insertion within a new band of stratified row parabolas with

$$h_s = [h_{h+1} + h_h]/2 = [(h + 1) + h]/2$$

annihilates at least the fragment elements occupying the previous join given by (5) or (6), where even the rightmost ambit, obtained from equation (12), engulfs

$$(p - 2h_s j_s)/2h_s^2 \approx p/(4h_s^2).$$

5.7 Equation (1) of section 2.5 for unstratified parabolas does not always hold for stratified parabolas, with the consequence that (5) and (6) are not always valid. The equation for a stratified parabola in the row region is

$$(h_s r + j_s)^2 - p(r - 1),$$

in which h_s may be a multiple of ½ and

$$j_s = \lfloor p/4h_s \rfloor - h_s + 1 + \delta - \tfrac{1}{2}\nu_s,$$

where here the *stratification number* $\nu_s = 0$ or 1. For $h_s = h - \tfrac{1}{2}$, the fragment join of parabolas given by h_s and h then satisfies at $\nu_s = 1$

$$r = 2[\lfloor p/4h_s \rfloor - \lfloor p/4h \rfloor],$$

being one more at $\nu_s = 0$.

5.8 If for natural numbers h and j

$$G = (hr + j)^2 - p(r - 1) \quad (7)$$

and for possibly different h and j, h is an arbitrary rational μ_h/σ_h in lowest terms, and j is μ_j/σ_j in lowest terms, then if

$$G = [(\mu_h/\sigma_h)r + \mu_j/\sigma_j]^2 - p(r - 1)$$

is the same G and r is the same, then

$$(\mu_h/\sigma_h)r + \mu_j/\sigma_j = hr + j. \quad (8)$$

For arbitrary r, if r is a multiple of σ_h, this implies $\sigma_j = 1$. If

$$r_{\sigma h} = r \pmod{\sigma_h}, \quad (9)$$

but $r_{\sigma h} \neq r$, then μ_j/σ_j is not a natural number, and

$$\mu_j = -\mu_h r\sigma_j \pmod{\sigma_h}. \quad (10)$$

We deduce there exist new parameters for h and j which represent the same residue. If there is a sequence of equations (7) for a given value of r in this equation, then there exist σ_h strata in r given by the left hand side of (8) satisfying (9) and (10), and this covers all quadratic residues covered by (7). An example would be h = 7/3 or 8/3, each of which corresponds to parabolas in the row region.

5.9 Let ε be a positive real number less than one. By a formula of Wallis the square root may be expressed as an extended binomial series. To eighth order this is

$$\varepsilon^{1/2} = 1 - \tfrac{1}{2}(1 - \varepsilon) - (1/8)(1 - \varepsilon)^2 - (1/16)(1 - \varepsilon)^3 - (5/128)(1 - \varepsilon)^4 - (7/256)(1 - \varepsilon)^5 - (21/1024)(1 - \varepsilon)^6 - (33/2048)(1 - \varepsilon)^7 - (429/32768)(1 - \varepsilon)^8.$$

When $\theta = (1 - \varepsilon)$, the nth root of ε may be obtained as

$$\varepsilon^{1/n} = \sum_{r=0}^{\infty} \rho_{n,r}\theta^r. \quad (11)$$

The designation, for r > 2,

$$\rho_{n,r} = -(n - 1)[\prod_{s=2}^{r-1}(sn - 1)]/r!n^r,$$

corresponds with a Taylor series expansion

$$(1 - \theta)^{1/n} = f(-\theta) = f(0) - f'(0)\theta + f''(0)\theta^2/2 - ...$$

When ε is close to 0, equation (11) has bad convergence. If we set

$$\psi - 1 \leq 1/\varepsilon^{1/2} \leq \psi,$$

so that $1/(\psi^2\varepsilon)^{1/2}$ is near 1, on choosing this rather than $\varepsilon^{1/2}$ in (11), an expansion for $\varepsilon^{1/2}$ may be obtained with good convergence as $\varepsilon^{1/2} \to 0$.

5.10 To determine the ambit, a general parabola intersects the G = (p – 1) right hand edge at

$$G_{edge} = (hr + j)^2 - p(r - 1) = (p - 1)$$

which corresponds to a quadratic equation in the row r

$$h^2r^2 + (2hj - p)r + j^2 + 1 = 0,$$

with solution

$$r_{edge} = (p - 2hj)/2h^2 \pm [(p - 2hj)/2h^2]\{1 - 4h^2(j^2 + 1)/(p - 2hj)^2\}^{1/2}, \quad (12)$$

where if the square root is expressed in the form (11) it satisfies

$$1 - \varepsilon = 4h^2(j^2 + 1)/(p - 2hj)^2. \quad (13)$$

Substitution (13) may be acceptable provided

$$p > 4hj.$$

The value of j for this h is

$$j_{start} + \delta = \lfloor p/4h \rfloor + 1 - h + \delta,$$

where $\delta < h$, and since $p = 4k - 1$

$$p - 4hj \geq 3,$$

so the series is convergent, but as may be seen with the example $p = 1031$, $h = 3$, $j = 85$, convergence may be slow. This indicates we may resort to ψ techniques for (12).

With r increasing from the top of the diagram to the bottom, the least value of r here is $r_{edge\ least}$ and the highest value $r_{edge\ most}$. Neither $r_{edge\ least}$ nor $r_{edge\ most}$ are a whole number. For the moment, ignoring floor and ceiling functions for rows, the ambit is

$$A_{edge} = r_{edge\ most} - r_{edge\ least}$$
$$= [(p - 2hj)^2 - 4h^2(j^2 + 1)]^{1/2}/h^2,$$

where for the parabola

$$j = \lfloor p/4h \rfloor + 1 - h + \delta = \lfloor (p - 3)/4h \rfloor + 1 - h + \delta,$$

so this is simply

$$A_{edge} = 2\{(p/h)[(p/4h) - \lfloor p/4h \rfloor - 1 + h - \delta] - 1\}^{1/2}/h.$$

5.11 Where there are an odd number of residues in the ambit for the rightmost parabola, so this excludes the top row for an ambit with h odd, the residues on the left parabolas for this ambit may be cancelled against those on the right, leaving the determination of the total disparity for this ambit to the mid parabola, which often straddles column $(p - 1)/2$.

This parabola intersects the mid-range $(p - 1)/2$ when

$$G_{mid} = (hr + j)^2 - p(r - 1) = (p - 1)/2,$$

that is

$$h^2r^2 + (2hj - p)r + j^2 + (p + 1)/2 = 0,$$

with solutions

$$r_{mid} = (p - 2hj)/2h^2 \pm [(p - 2hj)/2h^2]\{1 - 4h^2[j^2 + (p + 1)/2]/(p - 2hj)^2\}^{1/2}.$$

Ignoring again floor and ceiling functions gives the mid-range ambit as

$$A_{mid} = \{(p - 2hj)^2 - 4h^2[j^2 + (p + 1)/2]\}^{1/2}/h^2.$$

For the mid-range parabola, since h is odd

$$j_{mid} = j_{start} + \lfloor h/2 \rfloor,$$
$$= \lfloor p/4h \rfloor - \lfloor h/2 \rfloor = \lfloor (p - 3)/4h \rfloor - \lfloor h/2 \rfloor,$$

so this ambit is

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

and $A_{mid} < A_{edge}$.

For $\delta = \lceil h/2 \rceil - 1$, if $G_{min} < (p - 1)/2$ this means A_{mid} is real and since $h \leq h_{max}$ is odd, there is a constraint always present if h divides k in $p = 4k - 1$:

$$(p/h)[(p/4h) - \lfloor p/4h \rfloor] > (p/h)[(h/2) - \lfloor h/2 \rfloor] + ½$$
$$= (p/2h) + ½. \qquad (14)$$

For the mid parabola, the related disparity is obtainable from the ambits and is

$$A_{mid} - (A_{edge} - A_{mid}) = 2A_{mid} - A_{edge}$$
$$= 4\{(p/h)[(p/4h) - \lfloor p/4h \rfloor + \lfloor h/2 \rfloor] - (p + 1)/2\}^{1/2}/h$$
$$- 2\{(p/h)[(p/4h) - \lfloor p/4h \rfloor] - 1\}^{1/2}/h.$$

For A_{mid} real, if we put

$$\zeta = (p/h)[(p/4h) - \lfloor p/4h \rfloor]$$

and

$$\eta = (p/2h) + ½,$$

where we have seen $\zeta > \eta$, then this disparity expression is

$$4\zeta^{½}[1 - \eta/\zeta]^{½}/h - 2\zeta^{½}[1 - 1/\zeta]^{½}/h$$
$$= 2\zeta^{½}\{1 - \eta/\zeta + 1/2\zeta + \Sigma(i = 2 \text{ to } \infty)(\rho_{2,i}/\zeta^{i})[-2\eta^{i} + 1]\}/h.$$

More generally, the intersection within the band of any parabola on the left with the mid column at $(p - 1)/2$ is of interest in determining the disparity. This middle ambit is

$$A_{mid} = r_{mid\ most} - r_{mid\ least}$$
$$= 2\{(p/h)[(p/4h) - j] - (p + 1)/2\}^{½}/h,$$

where now

$$j = j_{start} + \delta$$
$$= \lfloor p/4h \rfloor + 1 - h + \delta,$$

and $\delta = 0$ begins at j_{start} and is at most $\lceil h/2 \rceil - 1$.

5.12 The range of rows is not given by the ambit, but by the band. We derive an expression for the disparity from the diagram below for low p with single fragments on the left. The example gives three parabolas, so h = 3. Parabola ambits, which intersect rows at quadratic residues, are given by I and J truncated by the mid column $(p - 1)/2$, by fragment ambit F, and by ambit K = F sliced at the rightmost column at $(p - 1)$. Fragment ambit F has its counterpart in K, which because of the relative displacement is identical in magnitude to F but is not in the same position.

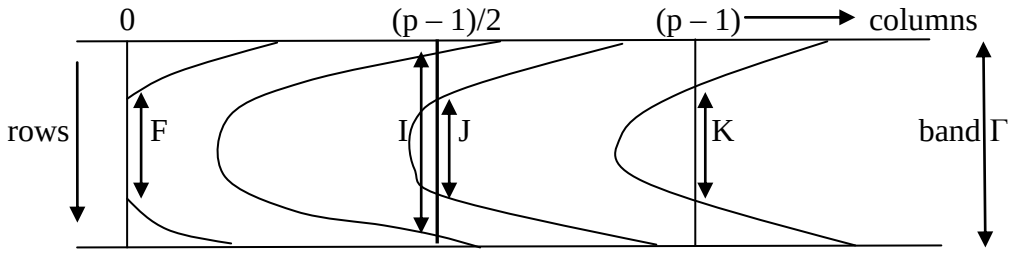


Figure 5.1 *Intersection of parabola segments with mid and end columns at low* p

Let the number of rows in the band be Γ. The disparity for the band is consequently

$$(\Gamma - F) + I + J - (\Gamma - I) - (\Gamma - J) - K = 2I + 2J - 2K - \Gamma. \qquad (15)$$

5.13 On observing the configuration of parabolas, we make an assessment at low p.

Within the band, for h odd, the central parabola has low disparity, possibly negative. If there is a gap on the right, cancelling the rightmost ambit for rows against the parabola that is one to the left of the central parabola, the number of remaining residues has low disparity. On adding the residues obtained from the fragments on the left when there is a gap, the row disparity for odd h is non negative.

When h is even and there are no fragments, there is zero disparity, and if there is a gap on the right, the disparity is zero spanned by the rightmost ambit not on its first row. Since there is a displacement by one in the row for the fragment on the left 'obtained' from the right gap, except for twice corresponding to the gaps above and below, there is then an even number of residues including fragments for the gap region of the band, and so the row disparity is zero when this happens.

5.14 For natural numbers h – 1, h and h + 1 defining parabolas, from equation (4) the value of the width of the band, Γ_h, for h is

$$\lfloor p/4(h-1)\rfloor + \lfloor p/4(h+1)\rfloor - 2\lfloor p/4h\rfloor, \qquad (16)$$

where we have defined that the bottom positioned row of the band is omitted, and for which if selected rows are cut out from the encompassing range of (p + 1)/4 rows occupying the row and trajectory regions, the sum of the bands is

$$\Sigma\Gamma_h = (p+1)/4 - \text{row excisions}.$$

Stripping off the floor functions in (16) and then reimposing them on the result, we obtain

$$\lfloor p/[2(h-1)h(h+1)]\rfloor + 2 \geq \Gamma_h \geq \lfloor p/[2(h-1)h(h+1)]\rfloor - 1.$$

5.15 We have shown that

$$j = j_{start} + \delta = \lfloor p/4h\rfloor - h + 1 + \delta.$$

For h odd the value of the displacement δ for J is (h – 1)/2, for I it is one to the left at (h – 3)/2, and for K it is (h – 1).

This implies the ambits I, J and K without the floor functions applied have the values

$$I = [p^2 - 4h\lfloor p/4h\rfloor p + 2hp - 2h^2]^{½}/h^2,$$
$$J = [p^2 - 4h\lfloor p/4h\rfloor p - 2hp - 2h^2]^{½}/h^2,$$
$$K = [p^2 - 4h\lfloor p/4h\rfloor p - 4h^2]^{½}/h^2 = F.$$

Expressing I and J in terms of K

$$I = K[1 + (2p + 2h)/(h^3K^2)]^{½},$$
$$J = K[1 - (2p - 2h)/(h^3K^2)]^{½}.$$

A straightforward binomial expansion of I and J has bad convergence. Nevertheless we can establish on squaring that

$$3K > I + J > 2K.$$

A sufficient pair of conditions is that J exists and secondly

$$I \leq \Gamma_h, \qquad (17)$$

otherwise the I parabola is not included in this way in the disparity count.

It follows from (15) that when conditions (17) hold the disparity is greater than I + J – Γ_h and less than I + J + K – Γ_h, but we find if we wish to prove I + J > Γ_h, the contrary result holds for high enough p. Indeed, 3K < Γ_h in such circumstances, viz:

$$9K^2 = 9[p^2 - 4h\lfloor p/4h\rfloor p - 4h^2]/h^4,$$

and we have seen that

$$\Gamma_h^2 \approx p^2/[2(h-1)h(h+1)]^2.$$

However, for any h

$$1 > (p/4h) - \lfloor p/4h\rfloor > 0,$$

and thus for the same values of h, $9K^2$ is ‘linear’ in p, whereas Γ_h^2 contains its square, so that the ratio of Γ_h to K increases with p and therefore without limit.

This indication is less disturbing than it may seem at first, arising from the fact that as p increases, although the size of Γ_h increments in greater proportion than the increment of h_{max}, simultaneously the presence of multiple fragments becomes dominant at higher p, so (15) for single fragments needs adapting. We deal with this in the next section.

6 Multiple fragments in the row region.

6.1 Figure 2.1 displays two fragments between h = 5/2 and h = 2. However, these are stratified fragments, with joins on different rows.

A multiple fragment on row r = $(j_h - j_{h+1})$ with multiplicity $|\delta|$ satisfies

$$G = [h(j_h - j_{h+1}) + j_h - |\delta|]^2 - p[(j_h - j_{h+1}) - 1].$$

On putting $C = \lfloor p/4h(h + 1) \rfloor$ or $\lceil p/4h(h + 1) \rceil$, if $G < 1$ and $|\delta| > 1$, say $|\delta| = 2$,

$$G = h^2C^2 + [2h(\lfloor p/4h \rfloor - 1) - p]C + [\lfloor p/4h \rfloor - 1]^2 < 1,$$

if there are no multiple fragments. Whenever this relation continues to be the case more stringently on putting $C = p/4h(h + 1) + 1$ and substituting $p/4h$ for $\lfloor p/4h \rfloor$, then

$$(hC + p/4h)^2 < (2h + p)C + 2p/4h,$$

which gives

$$p^2/[8(h + 1)^2] + (2h + 1)p^2/[16(h + 1)^2h^2] + 1 < p^2/[8h(h + 1)] + p,$$

so that multiple fragments ($\delta < -1$) do not exist for $16(h + 1)^2h^2 > p$.

6.2 We now demonstrate the behaviour, the example immediately following being for p = 100,003, of quadratic residues in the Γ region between h = 3 and h = 4 for a fragment join above, and a fragment join below defined by the conjunction of h = 3 and $h_s = 5/2$ fragments. We could choose stratification number ν = 0 for the latter.

Using the formulas already deduced, the join above is at row 2084, and the join below at row 3335, the value of Γ being thus 1251 rows. The rightmost ambit spans 92 rows. The first fragment derived from the rightmost parabola then tracks the entirety of the range of columns derived from the rows, cutting the rightmost edge at row 2664 on the top and 2894 at the bottom, the span between these fragment segments being 231 rows inclusive.

This behaviour is replicated in further traversals of complete sets of p columns. Since there are h parabolas, the fragments are stratified in h trajectory sets, the original fragment stratum returning to itself cyclically at the (h + 1)th trajectory set.

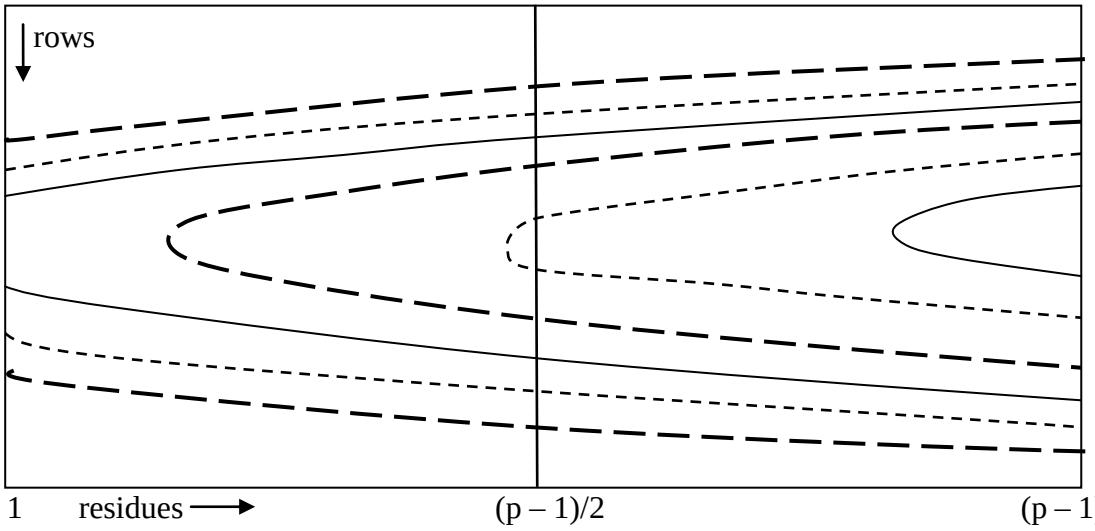


Figure 6.1 Multiple fragments traversing all columns for high p, h = 3

For each complete traversal in the row region of a stratum of a fragment trajectory, when this intersects the rightmost edge at real value r the corresponding continuation image on the left is displaced downwards to r + 1.

These fragment trajectories then define, in turn, further sets of parabolas, and this allocates at high enough p a nesting process of fragments defining parabolas, which define fragments defining parabolas, etc.

The fragment trajectories and parabolas cover the entire set of residues in the Γ band. This includes fragment trajectories in the upper and lower regions of Γ which terminate before the (p – 1) edge.

Since p is finite, an objective is to specify a method of descent in counting residues that allows for this nesting process.

6.3 An alternative approach which we will select is to intersperse between contiguous parabola parameters h_s and h_t, which may or may not be stratified, the parabolas generated by $\frac{1}{2}(h_s + h_t)$. This defines a nesting process for these parameters. A question we must then answer is whether this approach is equivalent to the one given in 6.2.

The ascending fragment trajectories of 6.2 derived from parabolas with parameter h_s are dually described by fragment trajectories with parameter $h_t > h_s$ descending from the h_t parameter parabolas.

These fragment trajectories completely cover the region they encompass, as do their derived parabolas, which may in turn have their own associated fragments. The cover provided by this *interspersion* process is as complete as that provided in the multiple fragment approach.

Let values h_s, h_t be chosen which are whole numbers divided by a power of 2, 2^x, and let the numerator of h_s, h_t be μ_s, μ_t respectively, where μ_s is odd when μ_t is even, or vice-versa. Then the ascending fragments define parabolas stratified in μ_s trajectory sets and the descending fragments define parabolas stratified in μ_t trajectory sets. Since μ_s does not divide μ_t and μ_t does not divide μ_s, these parabolas return to themselves in stratums defined by $\mu_s + \mu_t$, and in order that the resulting parabolas traverse the same region of rows

$$h_\mu = (\mu_s + \mu_t)/2^{x+1}. \qquad (1)$$

The h_μ cover twice the number of rows spanning h_s or h_t, so that the parabolas covered by $(\mu_s + \mu_t)$ double the number of equivalence classes of row r pairs with parameter h_μ responsible for the return to the same parabola, where the parabolas

$$G_\mu = (h_\mu r + j_\mu)^2 - p(r - 1).$$

The introduction of h_μ partitions Γ, but we should note that since parabolas are stratified, so is Γ. The choice for h_μ is not the only one available. We have seen in section 5.8 that choices not divisible by a power of two can also be allocated, where this extends to the fragment trajectory region and applies also to the description in 6.2.

Nevertheless, the choice of (1) once made allows a regular and rapid cut in Γ, so that in its final stage the condition for high p, $\Gamma_h > 3K$ of 5.15, is violated.

6.4 We now provide more detailed interspersion calculations. Introducing interspersed parameters, a top level range of activity for h is the set {(h – 1), h, (h + 1)}, and a typical element of the yth stratified subdivision of h is

$$h_{y,z} = (2^{y-1}h + z)/(2^{y-1}), \text{ where } -2^{y-1} \leq z \leq 2^{y-1}.$$

The join between $h_{y,z}$ and $h_{y,z+1}$ is obtained by an extension of the reasoning of 5.7, being defined as the upper extremity of a band denoted by $\Gamma_{y,z}$ at

$$r_{\text{join } y,z+1} = 2^{y-1}[\lfloor p/(4h_{y,z})\rfloor - \lfloor p/(4h_{y,z+1})\rfloor] + 2^{y-1} - \nu, \tag{2}$$

where y and z are constant, and $0 \leq \nu \leq 2^{y-1}$ for the variable stratification number, ν.

On selecting the same ν for both band extremities, the value of the band $\Gamma_{y,z}$, which has become an equivalence class of bands over ν with the same band value, is consequently

$$\begin{aligned}\Gamma_{y,z} &= r_{\text{join } y,z} - r_{\text{join } y,z+1}\\ &= 2^{y-1}[\lfloor p/(4h_{y,z-1})\rfloor + \lfloor p/(4h_{y,z+1})\rfloor - 2\lfloor p/(4h_{y,z})\rfloor] &(3)\\ &= 2^{-y}\{p/[(h_{y,z-1})(h_{y,z+1})(h_{y,z})]\} + \lambda(y) &(4)\\ &> 2^{-y}\{p/[(h_{y,z-1})(h_{y,z+1})(h_{y,z})]\} - 2^{y-1}\\ &< 2^{-y}\{p/[(h_{y,z-1})(h_{y,z+1})(h_{y,z})]\} + 2^{y-1},\end{aligned}$$

where we have introduced a variable λ(y) defined by (3) and (4).

The total span of these $\Gamma_{y,z}$'s is

$$\begin{aligned}\sum_{z=0}^{\Omega=2^{y-1}} \Gamma_{y,z} &= r_{\text{join } y,0} - r_{\text{join } y,\Omega+1}\\ &= 2^{y-1}\{\lfloor p/4[h - (1/2^{y-1})]\rfloor - \lfloor p/4h\rfloor\\ &\qquad - \lfloor p/4(h+1)\rfloor + \lfloor p/4[(h+1) + (1/2^{y-1})]\rfloor\}\\ &\approx p(2h+1)(1 + (1/2^{y-1}))/[4(h^2 - (1/2^{2y-2}) + h - (1/2^{y-1}))h(h+1)],\end{aligned}$$

so that for y = 1, on ignoring floor functions

$$\Sigma_z\Gamma_{y,z} \approx p(2h+1)/[2(h^2 + h - 2)h(h+1)],$$

for y = 2

$$\Sigma_z\Gamma_{y,z} \approx 3p(2h+1)/[8(h^2 - ½)(h + 3/2)h(h+1)],$$

and for higher y the value approaches

$$\Sigma_z\Gamma_{y,z} \approx p(2h+1)/[4h^2(h+1)^2]. \tag{5}$$

To determine the range of the values of

$$\begin{aligned}\zeta/(p/h) &= p/(4h) - \lfloor p/(4h)\rfloor\\ &= (k/h) - (1/4h) - \lfloor (k/h) - (1/4h)\rfloor,\end{aligned}$$

put $k = \omega h + \xi$, $0 \leq \xi < h$. Then for these positive values if ξ = 0, ζ/(p/h) is

$$1 - (1/4h),$$

whereas for $\xi \neq 0$ it becomes

$$(\xi/h) - (1/4h), \tag{6}$$

so that the value of ζ/(p/h) is always not less than 3/(4h).

To maintain equation (15) for Figure 5.1 of section 5 in the circumstances of this section, the single fragment continuation with δ = -1 must intersect the mid (p – 1)/2 column at a row number $r_{\text{frag mid}}$ less than the interspersed fragment join given by (2). This determines y.

For computational reasons we might select interspersed bands $\Gamma_{y,z}$, for which we set z = 0, and choose the δ = -1 mid ambit. The condition is now to allocate a lowest $y \geq 1$ where

$$\Gamma_{y,0} < A_{\text{mid}(\delta=-1)},$$

so that

$$2^{-y}\{p/[(h_{y,-1})(h_{y,1})(h_{y,0})]\} + \lambda(y) < 2\{\zeta + (p-1)/2\}^{½}/h. \quad (7)$$

However, considerations on determining the sign of the total disparity in section 8 make it desirable to stipulate the more rigid constraint that within the band there is no second fragment in the stratum. We need to prove in this situation that the single fragment for the stratum intersects the $(p-1)/2$ column outside the band range.

A second fragment outside the band would then be a continuation of an edge ambit

$$A_{edge(\delta = h-2)} > \Gamma_{y,0}, \quad (8)$$

where

$$A_{edge(\delta = h-2)} = 2\{\zeta + (p/h) - 1\}^{½}/h,$$

but for the row region $h \geq 2$, giving

$$2\{\zeta + (p/h) - 1\} < 2\{\zeta + (p-1)/2\},$$

so this constitutes a more stringent condition on the single fragment and on y. □

On squaring both sides of (8)

$$2^{-2y-2}\{p^2/[h^2 - 1/2^{2y-2}]^2\} + 2^{-y-1}\{p/[h^2 - 1/2^{2y-2}]\}h\lambda(y) + \lambda^2(y)h^2/4 < \{\zeta + (p/h) - 1\}.$$

The lowest bound of $\lambda(y)$ is -2^{y-1}, when a quartic inequality in 2^{2y} holds

$$2^{-2y-2}\{p^2/[h^2 - 1/2^{2y-2}]^2\} - ¼\{p/[h^2 - 1/2^{2y-2}]\}h + 2^{2y-4}h^2 < \{\zeta + (p/h) - 1\},$$

also the highest bound of $\lambda(y)$ is 2^{y-1}, when

$$2^{-2y-2}\{p^2/[h^2 - 1/2^{2y-2}]^2\} + ¼\{p/[h^2 - 1/2^{2y-2}]\}h + 2^{2y-4}h^2 < \{\zeta + (p/h) - 1\}.$$

For example, if $\lambda(y) \approx 0$

$$p^2 < 4\{\zeta + (p/h) - 1\}[h^4 2^{2y} - 8h^2 + 2^{-2y+4}]. \quad (9)$$

6.5 The definition of $\lambda(y)$ has introduced undesirable complications in obtaining direct solutions. We therefore cut the Gordian knot and define

$$R_{join\ y,z+1} = 2^{y-1}[p/(4h_{y,z}) - p/(4h_{y,z+1})] + 2^{y-1} - \nu, \quad (10)$$

where $R_{join\ y,z+1}$ is not a natural number. The corresponding band is now not $\Gamma_{y,z}$ but $\Delta_{y,z}$ defined so that (4) holds identically with $\lambda(y) = 0$, that is

$$\Delta_{y,z} = 2^{-y}p/[(h_{y,z-1})(h_{y,z+1})(h_{y,z})]. \quad (11)$$

Moreover, relation (9) has become the defining equation for the natural number y.

The introduction of $\Delta_{y,z}$ in (11) implies that in order to satisfy the dual requirement of dealing simultaneously with rational $\Delta_{y,z}$ and whole number ambits, we can convert to natural number reasoning via the introduction of

$$E_{y,z} = \lfloor R_{join\ y,z} \rfloor - \lceil R_{join\ y,z+1} \rceil,$$

which is entirely within the $\Delta_{y,z}$ band.

Since p is prime, neither $R_{join\ y,z}$ nor $\Delta_{y,z}$ have natural number occurrences. This means for z varying from 0 to Ω

$$\sum_{z=0}^{\Omega} \Delta_{y,z} = R_{join\ y,0} - R_{join\ y,\Omega+1} = R_{join\ y,0} - \lfloor R_{join\ y,0} \rfloor + \sum_{z=0}^{\Omega} E_{y,z} + \Omega - R_{join\ y,\Omega+1} + \lceil R_{join\ y,\Omega+1} \rceil. \quad \square \quad (12)$$

References

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

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.