

The Connection Among the Amount of Classes in Which Binary  
Forms of the Second Degree are Distributed and Their  
Determinants

First Commentary (II)

Presented to the Royal Society 1837 . . . .

from *Werke* Vol. III, pp. 276-

by C. F. Gauss

translated by Sky Shields

September 26, 2007

1.

Thirty six years have now elapsed since the marvellous connection treated in this commentary is dedicated was first disclosed, [and] which was then announced at the end of the *Disquisitiones Arithmeticae*. But other occupations have for a long time detracted from this investigation [scrutatione], until in recent times [I have] returned to them and will enlarge upon them with new attention. And yet since the extent of this new part of Higher Arithmetic exceeds the limits of one commentary, this first will be dedicated to forms with negative determinant: however forms with a positive determinant, which require wholly special treatment, are reserved for another commentary.

2.

For our purpose, the work will be/concern a theorem indeed essentially arithmetic, whose nature can be presented more conveniently and clearly in a geometric form.

Let there be, in an infinite plane, a figure bounded by any lines whatever. It's area can be approximately assigned if the plane is divided into a number of squares, and first those which are entirely within the figure, and then those cut the boundary of the figure are counted, and it is evident that the area indeed [justo] turns out to be greater or lesser depending on whether the latter squares are omitted or included with the former: indeed, if [it pleases] the squares located on the boundary are partly excluded and partly included according to any principle of regularity whatever, the error can sometimes be positive, sometimes negative, it will necessarily be less than the sum of all of the squares on the border. When fewer squares are taken, the area will be more exactly determined in this way, and if such an approximation is taken to infinity, or the squares are taken as small a possible [licebit], the error will turn out smaller than any given quantity. On this account therefore it can clearly be seen in and of itself, it is not despised to build a rigorous proof. [??]

Two squares have can have either one, two, or no angle points in common; in the first and second case they are said to be contiguous, in the third, disjoint [seperate]. Evidently, squares which are all contiguous with one another number four at the most [ ], and among five different squares at least two must be disjoint [seperate]. Now, since the distance between two points in disjoint squares cannot be made less than the side of a square, which we will designate by  $a$ , it is clear, from whatever place of some square do indeed pass sequentially through a second, third, and fourth square, reaching at last a fifth, the length of the path certainly cannot be less than  $a$ . And since similar reasoning if the line continually passes through other squares, the portion [pars] between the fifth and ninth, but not between the ninth

and thirteenth, etc., cannot be less than  $a$ , we conclude easily that any closed curve which touches each of  $n$  different squares can certainly not be less than  $\frac{(n-4)a}{4}$ . Therefore conversely a closed curve whose length is  $= l$  certainly cannot touch more than  $4 + \frac{4l}{a}$  different squares, [ ] whose area  $= 4aa + 4al$  can become less than any given quantity when  $a$  decreases to infinity, the same applies even more [a potiori] to the error of the quadrature which was spoken of above.

3.

The principle for the admission or exclusion of squares on the border of the proposed figure [figurae positorum] can be established in numerous ways: the most simple of these can be seen by simply [tantummodo] considering the location of the centers and of their squares such that the squares are admitted whose centers are within the figure, and those are excluded whose centers are outside the figure, and finally the decision is left whether to include those whose center happens to be on the periphery itself among the interior or exterior [squares]. In place of the center we can also choose any other points whatever which are similarly situated with respect to the individual squares.

This done, the matter is reduced to conceiving points as distributed [disseminata] equidistantly in a plane and in a line: which done, we can prove [affirmare] by the theorem in the preceding article, the number of points contained in the figure multiplied by the square of the distance of two neighboring points gives the nearly or exactly the area of the figure if the measure of that distance is taken as sufficiently small, or, in the common manner of speaking, the product produces that area if the distance is infinitely small.

4.

The curve which is expressed by the equation

$$app + 2bpq + cq = 1$$

between the orthogonal coordinates  $p$ ,  $q$ , is a conic section, and moreover [quidem] an ellipse, if  $a$ ,  $c$ , and  $ac - bb$  are positive quantities: this area circumscribed by an ellipse turns out to be  $= \frac{\pi}{\sqrt{(ac-bb)}}$ . The value of the quantity  $app + 2bpq + cq$  outside the ellipse is everywhere greater than 1, and within the ellipse less than 1, nowhere negative.

A system of points is conceived in the plane in which the ellipse is situated, distributed such that they form squares whose sides  $= \lambda$  are parallel to the axis of coordinates, where it does not matter [nihil refert] whether the origin of coordinates or the center of the ellipse coincides with one these points or not. Let the number of points within the ellipse, including those which are in the periphery itself, be  $= m$ , and therefore by the theorem of the preceding article  $\frac{\pi}{\sqrt{(ac-bb)}}$  will be the limit of the quantity  $m\lambda\lambda$ , which can approach it as closely as can be desired if  $\lambda$  decreases infinitely.

If we suppose the origin of coordinates to coincide with some system of points, setting  $p = \lambda x$ ,  $q = \lambda y$ , evidently  $x$  and  $y$  will be integral numbers for individual points of the system, and conversely any combination of integral values of the quantities  $x$ ,  $y$ , will correspond to one of a system of points. Hence, the number  $m$  is nothing other than the amount of all combinations of integral values of the quantities  $x, y$ , for which  $F$  is not larger than  $M$ , if for the sake of brevity we denote the function, or second order form  $axx + 2bxy + cyy$  by  $F$ , and the quantity  $\frac{1}{\lambda\lambda}$  by  $M$ . The determinant of this form is  $bb - ac$ , for which we write  $-D$ . This done, our theorem can now be expressed thus:

**THEOREMA I.** *The number  $m$  of all combinations of integral values of the indeterminates  $x$ ,  $y$ , for which the value of the negative determinant  $-D$  of the form does not exceed the limit  $M$ , but approximates  $\frac{\pi M}{\sqrt{D}}$  infinitely as  $M$  grows infinitely [?? fit  $= \frac{\pi M}{\sqrt{D}}$ , proxime quidem, sed approximatione in infinitum crescente, dum  $M$  crescit in infinitum]. It scarcely needs to be advised that by this infinite approximation (and just as if in consequence) is not thus understanding, as if the difference between  $\frac{\pi M}{\sqrt{D}}$  and  $m$  were to decrease infinitely, but [rather] that the ratio between these two quantities will approach equality infinitely, or  $\frac{\pi M}{m\sqrt{D}} - 1$  decreases infinitely.*

5.

For [ad] actually producing the enumeration, it can turn out that for individual integral values of  $x$  between the limits  $-\sqrt{\frac{cM}{D}}$  and  $+\sqrt{\frac{cM}{D}}$  two values of  $y$  are calculated corresponding to the equation  $F = M$ , and hence a number of integers are automatically obtained lying between them. If this number is the same for opposite values of  $x$ , we are freed from exactly half of our work. Thus the thing can also be accomplished such that the values of  $x$  enumerated correspond to individual values of  $y$  between the limits  $-\sqrt{\frac{aM}{D}}$  and  $+\sqrt{\frac{aM}{D}}$ . By a suitable combination of both methods the labor can be significantly lightened, since thus established this is not carried out completely: it will suffice to attach some of the simplest cases.

Let the form be  $F = xx + yy$ , or the curve of a circle, and designate by  $r, r', r'', r''', \dots, r^{(r)}$  the next smaller integers than

$$\sqrt{M}, \sqrt{M-1}, \sqrt{M-4}, \sqrt{M-9}, \dots, \sqrt{M-rr}$$

or these themselves, if some among them happen to be integers. Then the amount sought will be

$$\begin{aligned} m &= 2r + 1 + 2(2r' + 1) + 2(2r'' + 1) + 2(2r''' + 1) + \text{etc.} + 2(2r^{(r)} + 1) \\ &= 1 + 4r + 4r' + 4r'' + 4r''' + \text{etc.} + 4r^{(r)} \end{aligned}$$

However it is more expedient to obtain the same, denoting by  $q$  the next smaller integer than  $\sqrt{\frac{1}{2}M}$  (or this quantity itself, if it is an integer), by aid of the formula

$$m = 4qq + 1 + 4r + 8(r^{(q+1)} + r^{(q+2)} + r^{(q+3)} + \text{etc.} + r^{(r)})$$

In this way the following appear:

$M$	$m$	$M$	$m$	$M$	$m$
100	317	1000	3149	10000	31417
200	633	2000	6293	20000	62845
300	949	3000	9425	30000	94237
400	1257	4000	12581	40000	125629
500	1581	5000	15705	50000	157093
600	1885	6000	18853	60000	188453
700	2209	7000	21993	70000	219901
800	2521	8000	25137	80000	251305
900	2821	9000	28269	90000	282697
1000	3149	10000	31417	100000	314197

6.

We procure the theorem of article 4 with greater generality in the following way. THEOREMA II. *If not all combinations of integral values of the quantities  $x, y$ , for which  $F$  does not surpass the value  $M$  are collected, but only by jumps, for example those where [...eae, ubi...]  $x$  is congruent to a given number  $G$  with respect to a given modulus  $g$ , and  $y$  is congruent to a given number  $H$  with respect to a given modulus  $h$ , the number of these combinations,  $m'$  will be approximately expressed by  $\frac{\pi M}{gh\sqrt{D}}$ , where the approximation becomes infinitely more exact as  $M$  grows infinitely.*

In truth [revera] setting  $x = gx' + G, y = hy' + H$ , it becomes clear that  $m'$  is the number of all combinations of integral values of the quantities  $x', y'$  for which

$$agg(x' + \frac{G}{g})^2 + 2bgh(x' + \frac{G}{g})(y' + \frac{H}{h}) + chh(y' + \frac{H}{h})^2$$

does not exceed the value  $M$ . Therefore it is evident that if a system of points is supposed distributed in a plane as in article 4, but yet such that it is not the origin of coordinates but rather a point whose coordinates are  $p = \frac{G\lambda}{g}, q = \frac{H\lambda}{h}$  with which some system of points coincides,  $m'$  expresses the number of points within the ellipse whose equation is

$$aggpp + 2bghpq + chhq = 1$$

always counting those which lie on the periphery [? *iacentum semper adnumeratis si quae sunt in peripheria ipsa*]. The limit of the area of this ellipse will be  $= \frac{\pi}{gh\sqrt{(ac-bb)}} = \frac{\pi}{gh\sqrt{D}}$ , to which the product  $m'\lambda\lambda = \frac{m'}{M}$  approaches infinitely if  $\lambda$  decreases or  $M$  increases infinitely.

It is clear further, that our theorem includes those cases where one of the two indeterminates  $x, y$ , only progresses by jumps while the other value is not subject to any conditions. Moreover, it is clear that this is the same as if either  $h$  or  $g$  were set = 1.

7.

That which has so far been discussed, is independent of the coefficients of the form  $axx + 2bxy + cyy$ : indeed [*vero*] hereafter we suppose these coefficients to be integers. Hence, any combination of values of the integral quantities  $x, y$ , will produce an integral value of the form, or corresponds to the representation of some integral number by that form. Hence it is clear that the complex of all combinations of values of the integral quantities  $x, y$ , for which the form  $F = axx + 2bxy + cyy$  does not assume values greater than the limit  $M$ , will be the same as the complex of all representations of integral numbers which do not exceed the limit  $M$ , or up to and including this limit if it is an integral number. And now [*quodsi*] we denote, on account of brevity, the number of different representations of the determinate integer  $n$  by the form  $F$  by  $F(n)$  or, whenever there is no fear of ambiguity, simply by  $F_n$ , the number expressed above by  $m$  will be  $= F_0 + F_1 + F_2 + F_3 + \text{etc.} + F_M$ , and our first theorem assumes the following form.

THEOREMA III. *The approximate expression of the aggregate  $F_0 + F_1 + F_2 + \text{etc.} + F_M$  becomes infinitely accurate as  $M$  grows to infinity.*

8.

The third theorem concerning *all* numbers agrees with another, [which] only concerns odd numbers. Clearly, odd numbers cannot be represented by the form  $F$ , if  $a$  and  $c$  are simultaneously even: wherefore the investigation will be restricted to three remaining cases.

I. Whenever  $a$  is odd,  $c$  even, an odd number will be represented by giving  $x$  an odd value and maintaining an arbitrary value for  $y$ . Therefore theorem II, setting  $g = 2, G = 1, h = 1$ , shows that the number of all combinations of such values of  $x, y$ , which bring about odd values of the form [ $F$ ] less than the limit  $M$ , are infinitely nearly expressed by  $\frac{\pi M}{2\sqrt{D}}$  if  $M$  grows infinitely.

II. Whenever  $a$  is even,  $c$  odd, for the representation of odd numbers it is required that  $y$  be odd, hence setting  $g = 1, h = 2, H = 1$ , it is reduced to the same conclusion [ ].

III. Whenever either  $a$  or  $c$  is odd, either an odd value of  $x$  is combined with an even value of  $y$ , or an even value of  $x$  with an odd value of  $y$ , in order to produce an odd value of the formula. The amount of all combinations of either the first type or second type, for which the value of the form does not exceed the limit  $M$ , is infinitely nearly expressed by  $\frac{\pi M}{4\sqrt{D}}$ , consequently the number of all combinations which produce odd values of the form not exceeding the limit  $M$  is also expressed in infinite approximation by  $\frac{\pi M}{4\sqrt{D}}$ .

Now, since the complex of all such combinations is none other than the complex of all representations of all numbers 1, 3, 5, 7 . . .  $M$  whenever  $M$  is an odd integer, or 1, 3, 5, 7 . . .  $M - 1$  whenever  $M$  is even, we have

THEOREMA IV *The aggregate*

$$F_1 + F_3 + F_5 + F_7 \dots + F_M \quad \text{or} \quad F_1 + F_3 + F_5 + F_7 \dots + F(M - 1)$$

(depending on whether  $M$  is odd or even) is expressed in infinite approximation by  $\frac{\pi M}{2\sqrt{D}}$ , consequently  $F$  is a form in which one or both of the coefficients  $a, c$  is odd.