169.

EISENSTEIN'S GEOMETRICAL PROOF OF THE FUNDAMENTAL THEOREM FOR QUADRATIC RESIDUES. (*Translated from the Original Memoir*, Crelle, t. XXVIII. (1844), *with an Addition, by* A. CAYLEY.)

[From the *Quarterly Mathematical Journal*, vol. I. (1857), pp. 186—191.]

LET p be a positive odd prime, a the aggregate of all the even numbers $< p$ and > 0, viz. $a = 2,\ 4,\ 6, \ldots p-1$; and let q be any integer not divisible by the modulus p; then if r denote the general term of the residues of the multiples qa in respect to the modulus p, it is clear that the numbers of the series the general term of which is $(-)^r r$ will coincide to multiples of p près with the numbers of the series a; so that we shall have the two congruences

$$q^{\frac{1}{2}(p-1)} \Pi a \equiv \Pi r \pmod{p}, \text{ and } \Pi a \equiv (-)^{\Sigma r} \Pi r \pmod{p},$$

from which it follows that

$$q^{\frac{1}{2}(p-1)} \equiv (-)^{\Sigma r} 1 \pmod{p}, \text{ and therefore } \left(\frac{p}{q}\right) = (-)^{\Sigma r} 1.$$

Let $E\left(\frac{qa}{p}\right)$ denote the greatest whole number contained in the fraction $\frac{qa}{p}$, then it is clear that $\Sigma qa = p\Sigma E\left(\frac{qa}{p}\right) + \Sigma r$; and since all the a's are even, and $p \equiv 1 \pmod{2}$ it follows that $\Sigma r \equiv \Sigma E\left(\frac{qa}{p}\right) \pmod{2}$; and we have, therefore,

$$\left(\frac{q}{p}\right) = (-)^{\Sigma E\left(\frac{qa}{p}\right)}.$$

When $q = 2$, the formula gives at once the value of $\left(\frac{2}{p}\right)$; when, on the other hand, q is odd, and therefore $q-1$ even, we find, by a simple transformation,

$$\Sigma E\left(\frac{qa}{p}\right) \equiv -E\left(\frac{q}{p}\right) + E\left(\frac{2q}{p}\right) - E\left(\frac{3q}{p}\right) \ldots \pm E\left(\frac{\frac{1}{2}(p-1)\,q}{p}\right)$$

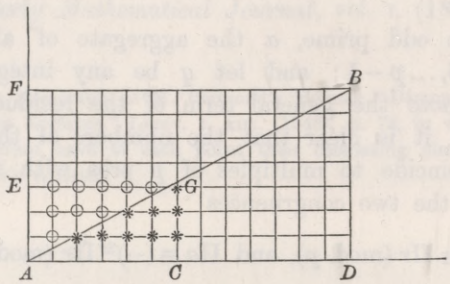
$$\equiv E\left(\frac{q}{p}\right) + E\left(\frac{2q}{p}\right) + E\left(\frac{3q}{p}\right) \ldots + E\left(\frac{\frac{1}{2}(p-1)\,q}{p}\right), \text{ (mod. 2)};$$

and if the last sum be represented by μ, then also

$$\left(\frac{q}{p}\right) = (-)^{\mu} 1.$$

Imagine now in a plane, a rectangular system of coordinates (x, y) and the whole plane divided by lines parallel to the axes at distances $= 1$ from each other into squares of the dimension $= 1$. And let the angles which do not lie on the axes of coordinates be called "lattice points."

Take, now, upon any vertical parallel a point corresponding to the ordinate y, then $E(y)$ will denote the number of lattice points which lie between this point and the horizontal axis; and, in like manner, taking upon any horizontal parallel a point



corresponding to the abscissa x, then $E(x)$ will denote the number of lattice points which lie between this point and the vertical axis. If, therefore, we draw in the plane a curve the equation of which is $y = \phi x$, then the sum

$$E\phi 1 + E\phi 2 + E\phi 3 + E\phi 4 + \&c.,$$

will denote the number of lattice points which lie between the curve and the axis of x, including any lattice points which lie upon the curve.

Suppose now, to return to the subject, that AB represents the straight line which has for its equation $y = \frac{q}{p}x$, where p and q are now assumed to be both of them positive

odd primes; and let $AD = FB$ be $= p$, $AF = DB = q$, $AC = EG = \frac{1}{2}(p-1)$, $AE = CG = \frac{1}{2}(q-1)$. Then if μ denote the number of the lattice points between AB and AD as far as the ordinate CG inclusively (these lattice points are distinguished in the figure by the mark [*]), by what precedes $\left(\frac{q}{p}\right) = (-)^{\mu} 1$. But since the equation of the straight line AB may also be written $x = \frac{p}{q} y$, we have in the same way, if ν denote the number of the lattice points which lie between AB and AF as far as the abscissa EG inclusively (these are distinguished in the figure by the mark [◦]), $\left(\frac{p}{q}\right) = (-)^{\nu} 1$. But the lattice points marked with [*] and [◦] taken together, i.e. all the lattice points to the right, and all the lattice points to the left of AB, make up the entire system of lattice points of the rectangle $AEGC$, the number of which is $\frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$; consequently, $\mu + \nu = \frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1)$, and therefore

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-)^{\mu+\nu} 1 = (-)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(q-1)} 1$$

which is the theorem in question.

It may be noticed that the foregoing transformation $\Sigma E\left(\frac{qa}{p}\right) \equiv \mu \pmod 2$ may itself be proved by the simple geometrical consideration that $\Sigma E\left(\frac{qa}{p}\right)$ is nothing else than the number of lattice points which lie on the even ordinates (those corresponding to $x = 2, 4, 6, \ldots p-1$) between AB and AD as far as BD, and that each ordinate, between the axes AD and BF exclusively, contains $(q-1)$, i.e. an even number of lattice points; and besides, that the two triangles BAD and ABF are congruent, and that the latter of them stands in the same relation to BF and BD as the former does to AD and AF; the completion of which is left to the reader.

Remark. There are figures for which simple formulæ may be obtained for the number of the interior lattice points. Imagine, for example, a circle, the centre of which lies in the axis of coordinates, and the radius of which is $\sqrt{m}$, then the number S of the lattice points which lie within the circle, including those which lie on the axes, is given by the following formula,

$$S = 1 + 4\{E(m) - E(\tfrac{1}{3}m) + E(\tfrac{1}{5}m) - \&c.\}$$

continued until the series stops of itself. It is easy to see that the equation expresses a relation between the number of lattice points of the circle and the number of lattice points of a segment included between two rectangular hyperbolas. Writing in the formula

$$\frac{1}{m} S = \frac{1}{m} + 4\left\{\frac{1}{m} Em - \frac{1}{m} E(\tfrac{1}{3}m) + \frac{1}{m} E(\tfrac{1}{5}m) - \&c.\right\}$$

$m = \infty$, the left-hand side becomes equal to π, and the right-hand side becomes equal to $4(1 - \frac{1}{3} + \frac{1}{5} - \&c.)$, which gives the formula of Leibnitz. There are similar

formulæ for the number of lattice points of a system of sectors of ellipses or hyperbolas; and similar relations exist also in space, and in cases of more than three dimensions. We shall return to this important subject, which has the closest connection with the properties of the higher forms, upon another occasion.

(*Addition by the Translator.*) Eisenstein is now, alas! dead; too soon for the complete development of his various and profound researches in elliptic functions and the theory of numbers; and the promise at the conclusion of the foregoing memoir has not, I believe, been fulfilled. The formula in the Remark must, I think, have been established by geometrical considerations, and would have served to give the number of decompositions of a number into the sum of two squares; but, as I do not perceive how this is to be done, I shall follow a reverse course, and establish the theorem from considerations founded on the theory of numbers. I remark, first, that the number of lattice points in a quadrant of the circle, inclusive of those on the vertical axis, but exclusive of those on the horizontal axis and of the centre, is equal to $E\sqrt{m}+E\sqrt{(m-1)}+E\sqrt{(m-4)}+E\sqrt{(m-9)}+$&c.; and that this sum, multiplied by four and increased by unity, gives precisely the number of lattice points of the circle, including those on the horizontal and vertical axes. The formula to be established is therefore

$$E\sqrt{m}+E\sqrt{(m-1)}+E\sqrt{(m-4)}+E\sqrt{(m-9)}+\&c.=E(m)-E(\tfrac{1}{3}m)+E(\tfrac{1}{5}m)-E(\tfrac{1}{7}m)+\&c.$$

where, as already noticed, the left-hand side denotes the number of lattice points of a quadrant of the circle, inclusive of those on the vertical axis, but exclusive of those on the horizontal axis and of the centre.

Let Xn be the number of ways in which the integer number n can be expressed as the sum of two squares. {If $n=\alpha^2+\beta^2$, then if α and β are unequal, and neither of them is zero, this counts as two decompositions, viz. $x=\alpha$, $y=\beta$ or $x=\beta$, $y=\alpha$; but if $\alpha=\beta$, this counts only as a single decomposition; or if either of the numbers α, β, e.g. α, is zero, then, since $y=0$ is excluded, this counts as a single decomposition, $x=0$, $y=\beta$.} Xn will denote the number of lattice points *on* the quadrant of the circle radius $\sqrt{n}$. Suppose also that $E'\left(\frac{1}{k}n\right)$ stands for unity or zero, according as $\frac{1}{k}n$ is or is not an integer. Then as m passes through the integer number n, i.e. from a value between $n-1$ and n to a value between n and $n+1$, the left-hand side of the equation is increased by Xn, and the right-hand side of the equation is increased by $E'(n)-E'(\frac{1}{3}n)+E'(\frac{1}{5}n)-$&c. We ought therefore to have

$$Xn=E'(n)-E'(\tfrac{1}{3}n)+E'(\tfrac{1}{5}n)-E'(\tfrac{1}{7}n)+\&c.,$$

and conversely from this equation, the original equation will at once follow. The right-hand side denotes, it should be observed, the number of factors of n of the form $\equiv 1 \pmod 4$, less the number of factors of the form $\equiv 3 \pmod 4$. Let $n=2^k f^\alpha f'^{\alpha'}\dots g^\beta g'^{\beta'}\dots$ where f, $f'\dots$ are odd primes $\equiv 1 \pmod 4$ and g, $g'\dots$ are odd primes $\equiv 3 \pmod 4$. Consider first the factors g, $g'\dots$, and forming the product

$$(1+g\dots+g^\beta)(1+g+\dots g'^{\beta'})\dots,$$

it is easy to see that if all or any one or more of the indices β, β'... are odd, then the number of terms of the product which are $\equiv 1 \pmod 4$ is equal to the number of terms of the product which are $\equiv 3 \pmod 4$; but if all the indices β, β'... are even, then the number of terms of the first form is greater by unity than the number of terms of the second form. Now the terms of the product $(1+f+\dots f^{\alpha})(1+f'+\dots f'^{\alpha'})\dots$ are all $\equiv 1 \pmod 4$, and the number of terms is $(1+\alpha)(1+\alpha')\dots$. Hence if all or any one or more of the indices β, β'... are odd, then the number of factors of n of the first form *less* the number of factors of the second form is zero; but if the indices β, β'... are all even, the number of factors of the first form *less* the number of factors of the second form is $(1+\alpha)(1+\alpha')\dots$, i.e. we have

$$E'(n) - E'(\tfrac{1}{3}n) + E'(\tfrac{1}{5}n) - \&c. = 0, \text{ or } = (1+\alpha)(1+\alpha')\dots,$$

according as β, β'... are all or any one or more of them odd, or according as they are all of them even. Now it is well known that the number $n = 2^k f^{\alpha} f'^{\alpha'} \dots g^{\beta} g'^{\beta'} \dots$ does not, in the case of all or any one or more of the indices β, β'... being odd, admit of decomposition into two squares, i.e. in this case $Xn = 0$; but if the indices β, β'... are all even, then the number n will admit of precisely as many decompositions into two squares as the number $n' = 2^k f^{\alpha} f'^{\alpha'} \dots$ (in fact, the only decompositions of n are those obtained from the decompositions of n' by multiplying the roots into the common factor $g^{\frac{1}{2}\beta} g'^{\frac{1}{2}\beta'} \dots$), and the number of decompositions of n' is moreover equal to the number of decompositions of $n'' = f^{\alpha} f'^{\alpha'} \dots$, which last number is in fact the product of the numbers of decompositions of f^{α}, $f'^{\alpha'} \dots$; the number of decompositions of n into two squares (estimated according to the foregoing convention) is thus shown to be, in the case of β, β'..., all of them even, equal to $(1+\alpha)(1+\alpha')\dots$. And we have therefore in every case

$$Xn = E'(n) - E'(\tfrac{1}{3}n) + E'(\tfrac{1}{5}n) - \&c.,$$

and the principal theorem is thus shown to be true.