Werk

Titel: Messenger of mathematics

Verlag: Macmillan

Jahr: 1876

Kollektion: mathematica

Signatur: 8 MATH I, 1022:5

Werk Id: PPN599484047_0005

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN599484047_0005|LOG_0040

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

ON THE LAW OF RECIPROCITY OF QUADRATIC RESIDUES.

By Professor *Paul Mansion*.

THE simplest demonstration that has been given of the law of reciprocity is due to Zeller (*Berliner Monatsbericht*, 1872, pp. 846–847), and depends, as also Gauss's third and fifth and Schaar's third demonstrations (*Bulletins de Bruxelles*, 1ère série, t. XIV., No. 2), on a lemma of Gauss, and a theorem of Euler which gives a criterion for distinguishing residues from non-residues. This theorem of Euler is usually demonstrated by means of the theory of primitive roots and indices (Gauss, *Disquisitiones*, No. 106), which renders the investigation of the law of reciprocity somewhat difficult.

I recently remarked that this theorem of Euler's was an immediate consequence of Fermat's theorem, which is itself an evident corollary from Gauss's lemma; so that we thus obtain a complete and entirely elementary demonstration of the law of reciprocity in the following manner:

I. *Gauss's Lemma.* If q is prime to the uneven prime p, the smallest remainders in absolute value, positive or negative, of the products

$$q, 2q, 3q \ldots, \tfrac{1}{2}(p-1)\,q \ldots\ldots\ldots\ldots\ldots\ldots(1),$$

divided by p, will be the numbers

$$\pm 1, \pm 2, \pm 3 \ldots, \pm \tfrac{1}{2}(p-1)\ldots\ldots\ldots\ldots\ldots(2),$$

and we shall have

$$q^{\frac{1}{2}(p-1)} \equiv (-1)^i \pmod{p},$$

i being the number of negative remainders in the series (2).

Let, in fact, for the modulus p,

$$q \equiv \pm r_1,\ 2q \equiv \pm r_2 \ldots,\ \tfrac{1}{2}(p-1)\,q \equiv \pm r_{\frac{1}{2}(p-1)} \ldots\ldots(3),$$

These remainders are all different, for if at the same time

$$aq \equiv \pm r,\ bq \equiv \pm r,$$

there would result

$$(a \pm b)\, q \equiv 0 \pmod{p},$$

which is impossible, since q is prime to p, and $a \pm b < p$, if ap and bq are chosen in the series (1).

Multiplying together all the congruencies (3),* and putting

$$P = 1.2.3 \ldots \tfrac{1}{2}(p-1) = r_1 r_2 r_3 \ldots r_{\frac{1}{2}(p-1)},$$

we have evidently $Pq^{\frac{1}{2}(p-1)} \equiv (-)^i P$,

viz. $q^{\frac{1}{2}(p-1)} \equiv (-1)^i$.

Cor. *Fermat's Theorem.* Squaring this congruence, we shall have

$$q^{p-1} \equiv (\text{mod. } p),$$

which is Fermat's theorem, since q is any number prime to p.

II. *Euler's Criterion.* The remainders resulting from the division of $1^2, 2^2, 3^2 \ldots \{\frac{1}{2}(p-1)\}^2$ by p, give $\frac{1}{2}(p-1)$ quadratic residues of p, all different. For if $s^2 \equiv s'^2 \pmod{p}$, and $s < s' < \frac{1}{2}p$, then we should have $(s'-s)(s'+s)$ divisible by p, which is impossible, since $s'-s$, $s'+s$ are each both less than p. There are no residues of p less than p, except those which have been mentioned, for $(p-x)^2$, $(mp+x)^2$, divided by p give the same residues as x^2. Consequently, of the numbers $1, 2, 3 \ldots (p-1)$, there are $\frac{1}{2}(p-1)$ which are residues, and $\frac{1}{2}(p-1)$ which are non-residues. All the other residues or non-residues are obtained by adding to them a multiple of p.

For every residue a, we have by definition

$$x^2 \equiv a \pmod{p},$$

and, raising this congruence to the power $\frac{1}{2}(p-1)$,

$$x^{p-1} \equiv a^{\frac{1}{2}(p-1)}.$$

But, by Fermat's theorem, $x^{\frac{1}{2}(p-1)} \equiv 1$. Whence

$$a^{\frac{1}{2}(p-1)} - 1 \equiv 0.$$

Fermat's theorem expresses that the congruence

$$x^{p-1} - 1 = (x^{\frac{1}{2}(p-1)} - 1)(x^{\frac{1}{2}(p-1)} + 1) \equiv 0,$$

is satisfied by the $p-1$ values $1, 2, 3, \ldots p-1$. Among these $p-1$ solutions, *the* $\frac{1}{2}(p-1)$ *residues of* p *satisfy the relation*

$$x^{\frac{1}{2}(p-1)} - 1 \equiv 0 \pmod{p},$$

* Poinsot has probably deduced his *new* demonstration (*Réflexions sur les principes fondamentaux de la théorie des nombres*, Ch. II., No. 1) of Fermat's theorem from this process of Gauss's, in order to demonstrate the subsidiary lemma.

as we have seen. Therefore *the* $\frac{1}{2}(p-1)$ *non-residues are the solutions of*

$$x^{\frac{1}{2}(p-1)}+1\equiv 0 \text{ (mod. } p).$$

The residues and the non-residues not comprised between 0 and p satisfy these same relations, because

$$x^{\frac{1}{2}(p-1)}\equiv(x+mp)^{\frac{1}{2}(p-1)} \text{ (mod. } p).$$

III. *Law of Reciprocity* (Zeller's demonstration).

1. We have seen above that

$$q^{\frac{1}{2}(p-1)}\equiv(-1)^i \text{ (mod. } p),$$

i being the number of the smallest remainders in absolute value, and negative, of

$$q, 2q, 3q\ldots, \tfrac{1}{2}(p-1)q \ldots\ldots\ldots\ldots\ldots\ldots(1),$$

when divided by p. We shall also have, if q is prime,

$$p^{\frac{1}{2}(q-1)}\equiv(-1)^j \text{ (mod. } q),$$

j being the number of the smallest remainders in absolute value, and negative, of

$$p, 2p, 3p\ldots, \tfrac{1}{2}(q-1)p \ldots\ldots\ldots\ldots\ldots\ldots(4),$$

when divided by q. By Euler's criterion, *if* $i+j$ *is even, p and q will be simultaneously residues or non-residues the one of the other; if* $i+j$ *is uneven, p will be a residue of q, and q a non-residue of p, or, inversely, according as i is even or uneven.*

2. The number $i+j$ will only be uneven if p and q are both of the form $4n+3$. Suppose $p<q$. (1°) Every number r smaller than $\frac{1}{2}p$ presents itself as a remainder in the series (1) with the sign $\pm$, in the series (2) with the sign $\mp$. In fact, if $hq-kp=r$, also $kp-hq=-r$, and necessarily we have $k>\frac{1}{2}q$, $h<\frac{1}{2}q$ simultaneously. It follows that there are in one or the other series of remainders $\frac{1}{2}(p-1)$ remainders less than $\frac{1}{2}p$, and negative viz. $-1, -2, -3\ldots-\frac{1}{2}(p-1)$.

(2°) The negative remainders comprised in absolute value between $\frac{1}{2}p$ and $\frac{1}{2}q$, and given consequently by the series (4), are always associated together in pairs, unless $(p+1)$, $(q-1)$, are divisible by 4. The product $\frac{1}{2}(q-1)p$ gives a positive remainder, viz. $\frac{1}{2}(q-p)$. Let

$$kp-hq=-r,\ \tfrac{1}{2}p<r<\tfrac{1}{2}q,\ k<\tfrac{1}{2}(q-1),$$

then

$$k'p-h'q=-r',\ \tfrac{1}{2}p<r'<\tfrac{1}{2}q,$$

if $k+k'=\frac{1}{2}(q-1)$, $h+h'=\frac{1}{2}(p+1)$, $r+r'=\frac{1}{2}(p+q)$,

whence there are always two remainders $-r$, $-r'$ associated and comprised in absolute value between $\frac{1}{2}p$, $\frac{1}{2}q$, unless $r=r'$, which requires $h=h'=\frac{1}{4}(p+1)$, $k=k'=\frac{1}{4}(q-1)$. Thus the number m of the negative remainders comprised between $\frac{1}{2}p$, $\frac{1}{2}q$ is only uneven if $p+1$ or $p-3$ and $q-1$ are divisible by 4.

3°. From the equality $i+j=\frac{1}{2}(p-1)+m$, we can deduce the following consequences: If $p-1$ is divisible by 4, m is even and also $i+j$. If $p-3$, $q-1$ are divisible by 4, m and $\frac{1}{2}(p-1)$ are uneven, $i+j$ is even. Finally, if $p-3$, $q-3$ are divisible by 4, $\frac{1}{2}(p-1)$ is uneven, m is even, and $i+j$ is uneven.

Combining these different results, we have the law of reciprocity. *If p and q are two prime numbers, uneven and positive, q is the residue or non-residue of p, according as p is the residue or non-residue of q, unless $p-3$, $q-3$ are divisible by* 4. *In this case, if p is the residue of q, q is a non-residue of p, and if p is a non-residue of q, q is a residue of p.*

TRANSACTIONS OF SOCIETIES.

London Mathematical Society.

Thursday, December 9th.—Prof. H. J. S. Smith, F.R.S., President, in the Chair. Major J. R. Campbell and Prof. G. M. Minchin were elected Members.

Prof. Clifford read a paper "On the Transformation of Elliptic Functions," in which he attempted to apply Jacobi's geometrical representation of the addition-theorem in elliptic functions to the theory of their transformation. Prof. Cayley spoke on "A system of Algebraical Equations connected with Malfatti's Problem." The communication was an extension of a paper by the same gentleman in the *Cambridge and Dublin Mathematical Journal*, tom. IV., 1849, pp. 270–275. The Chairman next communicated three short notes.

(i) *On a Problem of Eisenstein's.* If p is an uneven prime, the function $4\frac{x^p-1}{x-1}=Z$ can always be expressed in the form $Y^2-(-)^{\frac{1}{2}(p-1)}pX^2$, where X and Y are rational and integral functions of x having integral coefficients. This is a theorem of Gauss. Eisenstein's problem (Crelle's *Journal*, vol. XXVII., p. 83) is "To determine the cases in which the equation $Z=Y^2-(-)^{\frac{1}{2}(p-1)}pX^2$ admits of a multiplicity of solutions, and to ascertain the law connecting the various solutions, when there is more than one." The solution of this problem is as follows; If $[T, U]$ is *any* solution whatever in integral numbers of the equation $T^2-(-)^{\frac{1}{2}(p-1)}pU^2=4$, and $[X, Y]$ is any one given solution of Gauss' equation, then all the solutions of Gauss' equation are comprised in the formula

$$[\tfrac{1}{2}\{TX+(-)^{\frac{1}{2}(p-1)}pUV\},\ \tfrac{1}{2}(UX+TY)].$$

Thus, if $p=4n+3$, the equation admits of but one solution (the four solutions $[\pm X, \pm Y]$ being regarded as but one) except in the case $p=3$, when it admits of three; if $p=4n+1$, the equation admits of an infinite number of solutions. That the functions $[\frac{1}{2}(TX+pUY), \frac{1}{2}(UX+TY)]$ are all of them solutions of Gauss's equation, is evident; the proof that this formula comprises all the solutions of the equation is less elementary, because it depends on the irreducibility of the function Z. There exists a general theory of the representation of rational and integral functions of x by quadratic forms; such representation being, of course, only possible when the given function of x is capable of resolution into two factors by the adjunction of a quadratic surd.

(ii) *On the joint invariants of two conics or two quadrics.* Let P and Q be two conics, and let 123 be any triangle self-conjugate with regard to P. Let also P_1, P_2, P_3 be the rectangles of the points 1, 2, 3 with regard to the conic P, these rectangles being taken upon transversals measured in any fixed direction; and let Q_1, Q_2, Q_3 have similar meanings with regard to the conic Q, the direction of the transversals being also fixed. Then the expression $\frac{Q_1}{P_1}+\frac{Q_2}{P_2}+\frac{Q_3}{P_3}$ has the same value for all self-conjugate triangles of P, and is, in fact, that invariant of P. Q which is linear with regard to Q and quadratic with regard to P, and the evanescence of which expresses that Q harmonically circumscribes P. The corresponding theorem in the geometry of the straight line is "If Q_1Q_2, P_1P_2 are two pairs of fixed points on a line, and if A_1A_2 is any pair of harmonic conjugates of P_1P_2, the value of the expression $\frac{A_1Q_1 . A_1Q_2}{A_1P_1 . A_1P_2}+\frac{A_2Q_1 . A_2Q_2}{A_2P_1 . A_2P_2}$ is independent of the particular pair A_1A_2 considered." From this theorem the result given above for two conics follows immediately; from it the corresponding property for two quadrics may be inferred, viz. $\frac{Q_1}{P_1}+\frac{Q_2}{P_2}+\frac{Q_3}{P_3}+\frac{Q_4}{P_4}=\text{constant}$; and so on for quadratic functions containing any number of indeterminates.

(iii) *On the equation $P \times D = constant$, of the geodesic lines of an ellipsoid.* From this equation (in which P is the perpendicular from the centre upon the tangent plane at any point of the geodesic, and D is the semi-diameter parallel to the tangent line of the geodesic), it is convenient to be able to infer directly the principal properties of the geodesic line, without having first to transform the equation into M. Liouville's form $\mu^2 \cos^2 i + \nu^2 \sin^2 i = a^2$. In Dr. Salmon's *Geometry of Three Dimensions*, the theorem of the constancy of the sum or difference of the geodesic radii vectores, drawn from any point of a line of curvature to two umbilics, is thus demonstrated. And it is worth while to add (though it is very improbable that the point has not been noticed before), that a proof of the theorem, that two geodesic tangents of a line of curvature, which intersect at right angles, intersect on a sphero-conic, may similarly be obtained without transforming the equation. Let Q be the point where the two geodesic tangents intersect at right angles, O the centre of the ellipsoid; let $c = OQ$, and let a, b be the semi-axes of the central section parallel to the tangent plane at Q. The two geodesics make angles of 45° with the lines of curvature at Q; hence, for either of these geodesic lines, $D^2 = \frac{2a^2b^2}{a^2+b^2}$. Let Q' be a second point where two geodesic tangents to the same line of curvature intersect at right angles; then $\frac{2P^2a^2b^2}{a^2+b^2} = \frac{2P'^2a'^2b'^2}{a'^2+b'^2}$, because $P \times D$ has the same value for all geodesic lines touching the same line of curvature. But $P^2a^2b^2 = P'^2a'^2b'^2$ because parallelepipeds circumscribing an ellipsoid with their faces parallel to conjugate diametral planes are equal. Hence $a^2 + b^2 = a'^2 + b'^2$. But also

$$a^2 + b^2 + c^2 = a'^2 + b'^2 + c'^2;$$

therefore $c = c'$ and Q and Q' lie on the same sphero-conic.

Mr. Tucker (in the absence of the author) brought before the Society a paper by Mr. H. W. Lloyd Tanner, "On the Solution of Certain Partial Differential Equations of the Second Order, having more than two Independent Variables." The equations considered are included in the form

$$\sum_{i=1}^{i=n}\sum_{j=1}^{j=n} V_{ij}\frac{d^2z}{dx_i dx_j} + V_0 = 0 \quad \text{.....(i)},$$

where V_{ij}, V_0 are functions of $x_1 \ldots x_n$, z, $p_1\left(\equiv\frac{dz}{dx_1}\right)\ldots p_n\left(\equiv\frac{dz}{dx_n}\right)$; and it is proposed to investigate the conditions that (i) should be soluble in terms of arbitrary functions, the arguments of which are definite functions of $Z, x_1, \ldots x_n$; and when these conditions are satisfied, to determine the solution. Three cases arise for discussion: (1) $n-1$ of the arguments independent; (2) n of them independent; (3) $n+1$ of them independent. The paper concludes with a note on the application of a similar method to equations of an order higher than the second.

R. TUCKER, M.A., *Hon. Sec.*