G. Eisenstein, 2.

Applications of algebra to transcendental arithmetic.

Given two algebraic equations whatsoever, we can eliminate the unknown quantity x in two different ways, either by putting in place of the x in the second its value taken from the first, or putting in place of the x in the first its value taken from the second, without changing essentially the result of the elimination. We will see in what follows that the reciprocity laws for quadratic, cubic and biquadratic residues, (theorems as celebrated by the difficulty of their proof as by the assiduity with which the greatest mathematicians have occupied their time on them), are nothing other than the arithmetical interpretation of a simple algebraic fact about which we are going to speak. Thus for example, taking $\sin v = x$, if we designate two odd prime numbers by p and q (real), and by $x = \pm\alpha$ or respectively $x = \pm\beta$ the sets of roots of the two equations $\sin pv/\sin v = 0$, $\sin qv/\sin v = 0$, we will see that under the moduli q, p that the residues of $p^{\frac{1}{2}(q-1)}$ and $q^{\frac{1}{2}(p-1)}$ depend resp. on two expressions $\Pi(\beta^2 - \alpha^2)$ and $\Pi(\alpha^2 - \beta^2)$, where the multiplication is carried through all values of α and β; there exist analogous results for cubic and biquadratic residues. The method which leads us to these results is very simple, it treats the comparison of the two numbers in a perfectly symmetrical manner, and in these demonstations conserves the analogy which exists between theorems covering residues for different powers. As for the rest, we are able to consider the investigation of the first elements of a new doctrine where we transfer arithmetical questions to algebra and analysis, in such a manner that all difficulties are reduced to those offering us calculation. I start this material by beginning with quadratic residues.

§1.
Quadratic residues

Given an odd prime number (real and positive) p, we can always conceive of a system of residues for the modulus p, [1] distributed in two groups such that the terms composing the second group are opposite in sign to those of the first; we will represent general terms of these two groups by $\boldsymbol{r}$ and $-\boldsymbol{r}$; for example we can take for $\boldsymbol{r}$ the numbers 1, 2, 3, ... $\frac{1}{2}(p-1)$ and for $-\boldsymbol{r}$ the numbers -1, -2, -3, ... $-\frac{1}{2}(p-1)$. Granted that, if we multiply all the $\boldsymbol{r}$ by any whole number q not divisible by p, the residues of the product $q\boldsymbol{r}$ will find themselves in a part occupied by the $\boldsymbol{r}$ and a part occupied by the $-\boldsymbol{r}$. In consequence, according to these two cases we are distinguishing,

$$q\boldsymbol{r} \equiv \boldsymbol{r}', \qquad \text{or} \qquad q\boldsymbol{r} \equiv -\boldsymbol{r}' \pmod{p},$$

of the sort that $\boldsymbol{r}'$ is always to be found amongst the $\boldsymbol{r}$, we will have respectively

$$\sin q\boldsymbol{r}\omega/p = \sin \boldsymbol{r}'\omega/p, \quad \text{or} \qquad \sin q\boldsymbol{r}\omega/p = -\sin \boldsymbol{r}'\omega/p,$$

where we have made the abridgement $\omega = 2\pi$. We therefore have in every case

$$q\boldsymbol{r} \equiv \boldsymbol{r}'.(\sin q\boldsymbol{r}\omega/p)/(\sin \boldsymbol{r}'\omega/p) \pmod{p}.$$

Substituting in this expression for $\boldsymbol{r}$ all of its $\frac{1}{2}(p-1)$ values, and multiplying together all the expressions which that gives, we obtain, on observing again that all the $\boldsymbol{r}'$ coincide with all the $\boldsymbol{r}$:

$$q^{\frac{1}{2}(p-1)}\Pi\boldsymbol{r} \equiv \Pi\boldsymbol{r}'.\Pi(\sin q\boldsymbol{r}\omega/p)/\Pi(\sin \boldsymbol{r}'\omega/p) \equiv \Pi\boldsymbol{r}.\Pi\{(\sin q\boldsymbol{r}\omega/p)/(\sin \boldsymbol{r}\omega/p)\} \pmod{p},$$

---

[1] on exclusion from this of terms of such a system which is a multiple of the modulus, which we always tacitly suppose.

thus, if we divide the two members of this congruence by $\Pi \boldsymbol{r}$, which is permissible since $\Pi \boldsymbol{r}$ is not divisible by the modulus p, we will have

(1) $\quad q^{\frac{1}{2}(p-1)} \equiv \Pi\{(\sin q\boldsymbol{r}\omega/p)/(\sin \boldsymbol{r}\omega/p)\} \pmod{p}$.

This formula expresses the quadratic character of q with respect to p. Suppose now that q is also an odd prime number, then the quadratic character of p with respect to q will be expressed in similar manner by the formula

(2) $\quad p^{\frac{1}{2}(q-1)} \equiv \Pi\{(\sin p\boldsymbol{\rho}\omega/q)/(\sin \boldsymbol{\rho}\omega/q)\} \pmod{q}$,

(the multiplication relates to $\boldsymbol{\rho}$) which is the general expression of a set of numbers which together with $-q$ consists of a system of residues for the modulus q.

We are concerned therefore to make a comparison between the quadratic characters on the right of formulas (1) and (2). If we make $\sin v = x$, the quantities

$\sin pv/\sin v = \boldsymbol{P}, \qquad \sin qv/\sin v = \boldsymbol{Q}$

are whole number functions in x of degrees respectively $p - 1$ and $q - 1$; moreover, putting $\sin \boldsymbol{r}\omega/p = \alpha$, $\sin \boldsymbol{\rho}\omega/q = \beta$, the roots of the equation $\boldsymbol{P} = 0$ are designated by $\pm\alpha$ and those of the equation $\boldsymbol{Q} = 0$ by $\pm\beta$. That being so, the second member of formula (1) will be equivalent to the product of the values which take the expression $\boldsymbol{Q}$, putting there for x all the values of α, and likewise we obtain the second member of formula (2) putting in $\boldsymbol{P}$ for x all the β values, making the product of the expressions which result. We then have

$\boldsymbol{P} = (-1)^{\frac{1}{2}(p-1)}\Pi(x^2 - \alpha^2)2^{p-1}, \qquad \boldsymbol{Q} = (-1)^{\frac{1}{2}(q-1)}\Pi(x^2 - \beta^2)2^{q-1}$,

thus these become

(3) $\quad q^{\frac{1}{2}(p-1)} \equiv \boldsymbol{C}\Pi(\alpha^2 - \beta^2) \pmod{p}$,

(4) $\quad p^{\frac{1}{2}(q-1)} \equiv \boldsymbol{C}\Pi(\beta^2 - \alpha^2) \pmod{p}$,

where each value of α has to be combined with each value of β. $\boldsymbol{C}$ is a constant found to be

$\boldsymbol{C} = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}2^{\frac{1}{2}(p-1)(q-1)}$.

Now the number of the α is $\frac{1}{2}(p - 1)$, and the number of the β is $\frac{1}{2}(q - 1)$, consequently the number of combinations of α and β will be $\frac{1}{2}(p - 1)\frac{1}{2}(q - 1)$, where finally we take

$\Pi(\alpha^2 - \beta^2) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}\Pi(\beta^2 - \alpha^2)$.

This last equation compared with (3) and (4) gives immediately the law of quadratic residues. If we wish to evaluate the constant $\boldsymbol{C}$, we need to use tangents instead of sines.

§2.
Biquadratic residues

Biquadratic residues can be treated in an absolutely similar manner. Elliptic functions, or rather that particular space of elliptic functions which is derived from the leminiscate, play here the role of sines; we must first say a few words about these functions.

We will designate by $x = \sin \operatorname{am} v$ the function of v which satisfies the equation

$\mathrm{d}x = \mathrm{d}v.\sqrt{(1 - x^2)}$,

and which at the same time vanishes with v. This function is periodic in two ways, indeed putting $\omega = 4\int_0^1 \mathrm{d}x/\sqrt{(1 - x^2)}$, we have $\sin \operatorname{am}(v + k\omega) = \sin \operatorname{am} v$; k is a complex integer of the form $a + bi$, where a and b are real whole numbers. Another property of this function is expressed by

$\sin \operatorname{am} iv = i \sin \operatorname{am} v$;

a very important property for our investigations is derived immediately from the differential equation, on observing that this does not vary under the simultaneous transformation of x to

ix and *v* to *iv*. We know elsewhere from research by Abel and Jacobi [2] that sin am $(u + v)$ can be expressed algebraically by sin am *u* and sin am *v*, and above all, when taking for *m* an *odd* complex integer, we can reduce sin am *mv* to a *rational* function of sin am *v*.

Let $m = a + bi$ be an odd prime complex number; let the norm be $\boldsymbol{N}(m)$, that is to say the real and positive integer $a^2 + b^2$, $= p = \boldsymbol{N}(m)$; we can always partition a system of residues for the modulus m, which contains p – 1 terms, after excluding that which is divisible by the modulus, in four groups, such that the terms of the 2nd, 3rd and 4th groups are inferred from those of the first on multiplying it by *i*, -1 and by *i* respectively. Then multiplying all the $\boldsymbol{r}$ by any complex integer *n* not divisible by *m*, the residues of the products $n\boldsymbol{r}$ will be found distributed between the $\boldsymbol{r}$, the $i\boldsymbol{r}$, $-\boldsymbol{r}$ or $-i\boldsymbol{r}$. According to these four cases we have described, let

$$n\boldsymbol{r} \equiv \boldsymbol{r}', \quad i\boldsymbol{r}', \quad -\boldsymbol{r}' \text{ or } \quad -i\boldsymbol{r}' \pmod{m},$$

where $\boldsymbol{r}'$ is situated amongst the $\boldsymbol{r}$. Having defined that, we will have according to the four cases

$$\{(\sin\text{am } n\boldsymbol{r}\omega/m)/(\sin\text{am } \boldsymbol{r}'\omega/m)\} = 1, i, -1 \text{ or } -i;$$

we will have *in every case*

$$n\boldsymbol{r} \equiv \boldsymbol{r}'\{(\sin\text{am } n\boldsymbol{r}\omega/m)/(\sin\text{am } \boldsymbol{r}'\omega/m)\} \pmod{m},$$

where, on observing that all the $\boldsymbol{r}'$ coincide with all the $\boldsymbol{r}$, and that $\Pi\boldsymbol{r}$ is not divisible by *m*, we obtain

$$(1) \qquad n^{\frac{1}{4}(p-1)} \equiv \Pi\{(\sin\text{am } n\boldsymbol{r}\omega/m)/(\sin\text{am } \boldsymbol{r}'\omega/m)\} \pmod{m},$$

the sign Π accompanying every $\boldsymbol{r}$. Supposing that *n*, also *m*, is an odd prime complex number and that the system of residues for the modulus *n* is also distributed between for groups such that their general terms are represented by $\boldsymbol{\rho}$, $i\boldsymbol{\rho}$, $-\boldsymbol{\rho}$, $-i\boldsymbol{\rho}$, we will have in an analogous way

$$(2) \qquad m^{\frac{1}{4}(p-1)} \equiv \Pi\{(\sin\text{am } m\boldsymbol{\rho}\omega/n)/(\sin\text{am } \boldsymbol{\rho}'\omega/n)\} \pmod{n},$$

where *q* is the norm of *n* and the multiplication traverses all values of $\boldsymbol{\rho}$.

We have already remarked that we can evaluate the expression sin am *v* and consequently also sin am *mv*/sin am *v* by a rational function sin am *mv*. There exists between the numerator and the denominator of this rational function, which are of degree $p – 1$, a remarkable relation which depends on the residue of *m* with respect to the modulus $2 + 2i$. This relation reduces to its most simple form if we suppose *m* prime, that is to say $\equiv 1 \pmod{2 + 2i}$; in this case the value of (sin am *mv*)/(sin am *v*) takes the form $\varphi(x)/x^{p-1}\varphi(1/x)$, *x* is sin am *v* and $\varphi(x)$ an entire function of *x* of degree p – 1. In effect, suppose the fraction $\varphi(x)/\psi(x)$ is reduced to its simplest expression and the coefficient of the highest power in the numerator is equal to unity, which is permissible, if we manufacture from

$$(\sin\text{am } mv)/(\sin\text{am } v) = \varphi(x)/\psi(x),$$

the expression $y = x\,\varphi(x)/\psi(x)$ which vanishes with x, it will satisfy the differential equation $dy/\sqrt{(1 - y^4)} = m dx/\sqrt{(1 - x^4)}$, from which we see all the exponents of different powers in $\varphi(x)$ and in $\psi(x)$ are multiples of *four*; letting $y = 1/\eta$, $x = 1/i^{\mu}\xi$, where μ designates an indeterminate integer, the differential equation which we are going to write will change under this substitution as $i^{\mu} d\eta/\sqrt{(\eta^4 - 1)} = m d\xi/\sqrt{(\xi^4 - 1)}$ and we are able to dispose of μ in a way so that $d\eta/\sqrt{(1 - \eta^4)} = m d\xi/\sqrt{(1 - \xi^4)}$. This last equation will thus be satisfied by the integral $\eta = i^{\mu}\xi\psi(1/\xi)/\varphi(1/\xi)$, and as it is easy to see this, reduced to the form $i^{\mu}\xi^{p-1}\psi(1/\xi)/\xi^{p-1}\varphi(1/\xi)$, must coincide with the integral *y* which satisfies the same differential equation, so we will be

[2] See for example the 2nd, 3rd and 4th volume of this journal. It appears that Mr *Gauss* has already at the end of the last century been in possession of the principal theorems on these functions; in effect in the *Disquisitiones Arithmeticae* he had promised a work dealing with these functions, but it appears that the circumstances of other work had prevented him from executing his project.

able, using a complex unit, to equalise separately the numerators and denominators for the two integrals concerned. This gives $\psi(x) = i^{\nu}x^{p-1}/\varphi(1/x)$; ν is a real integer. To determine the value of it, we find $x = \sin\text{am}\,¼\omega = 1$ and $\sin\text{am}\,¼(m\omega) = \varphi(1)/i^{\nu}\varphi(1) = i^{-\nu}$, or for a prime value of m we have $\sin\text{am}\,¼(m\omega) = +1$ (Volume II, page 111 of this journal) and it follows $i^{\nu} = 1$, thus we have definitively $(\sin\text{am}\,m\nu)/(\sin\text{am}\,\nu) = \varphi(x)/x^{p-1}/\varphi(1/x)$, for a *prime* value of m; this is what we needed to prove.

If therefore we suppose that both m and n are $\equiv 1 \pmod{2 + 2i}$, and that we make

$$(\sin\text{am}\,m\nu)/(\sin\text{am}\,\nu) = \varphi(x)/x^{p-1}/\varphi(1/x),\quad (\sin\text{am}\,n\nu)/(\sin\text{am}\,\nu) = f(x)/x^{q-1}/f(1/x),$$
$$\sin\text{am}\,r\omega/m = \alpha,\qquad \sin\text{am}\,\rho\omega/n = \beta,$$

the roots of the equation $\varphi(x) = 0$ will be given by $\pm\alpha$, $\pm i\alpha$, and those of the equation $f(x) = 0$ by $\pm\beta$, $\pm i\beta$, such that we can write

$$(\sin\text{am}\,m\nu)/(\sin\text{am}\,\nu) = \Pi(x^4 - \alpha^4)/\Pi(1 - \alpha^4x^4),$$
$$(\sin\text{am}\,n\nu)/(\sin\text{am}\,\nu) = \Pi(x^4 - \beta^4)/\Pi(1 - \beta^4x^4).$$

From this and the two formulas (1) and (2) we extract

$$(3)\qquad n^{¼(p-1)} \equiv \Pi(\alpha^4 - \beta^4)/\Pi(1 - \beta^4\alpha^4) \pmod{m},$$
$$(4)\qquad m^{¼(p-1)} \equiv \Pi(\beta^4 - \alpha^4)/\Pi(1 - \alpha^4\beta^4) \pmod{n},$$

where it is necessary to combine each value of α with each value of β. The number of these combinations being $¼(p-1)\,¼(q-1)$, only inspection of formulas (3) and (4) is sufficient to conclude immediately the fundamental theorem on biquadratic residues.

§3.
Remarks

To demonstrate the law of reciprocity relative to cubic residues, we do none other than replace the differential equation $dx = dv\sqrt{(1 - x^4)}$ by $dx = dv\sqrt{(1 - x^3)}$ or $dx = dv\sqrt{[x(1 - x^3)]}$; and instead of taking complex numbers of the form $a + bi$, it is only necessary to consider numbers composed of the roots of the equation $\zeta^2 + \zeta + 1 = 0$; for the rest the direction of the demonstration is perfectly analogous for that we have followed for biquadratic residues. For that reason, and since we believe we have indicated clearly the spirit of our method, we will leave to another occasion the more detailed examination of researches elsewhere which we have endeavoured to make on these applications of algebra and arithmetic. We will treat at that time especially residues of higher powers, of which the fundamental theorems depend on the elimination of many variables for three up to a large number of algebraic equations.

It is possible that one does not approve of the usage of trigonometric and elliptic functions in arithmetical reasoning; but we can make the observation that these functions do not enter except in a way of saying that is *symbolic*, and that it is possible to banish them completely without destroying the substance and basis of demonstrations. To see this relative to quadratic residues, take the congruence $q^{½(p-1)} \equiv \mathbf{C}\Pi(\alpha^2 - \beta^2) \pmod{p}$, where all the letters have the same signification as in § 1. For this formula giving the quadratic character of q with respect to p, everything depends essentially on the sign of the second member. If then we replace the α and β by other quantities α' and β', subject to the sole condition that $\alpha'^2 - \beta'^2$ always has the same sign as $\alpha^2 - \beta^2$, the product $C\Pi(\alpha'^2 - \beta'^2)$ always describes by its sign the character of q. We are therefore led to this remarkable theorem:

"If we construct any closed curve whatever, but symmetric with respect to two perpendicular axes, of a sort with four congruent parts, for which the values increase in the first quadrant: where we then divide the circumference of this curve in p and in q equal parts and where we designate by α and β respectively the positive values which correspond to

these two divisions, I say that q will or will not be a quadratic residue of p according to the product $(-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}\Pi(\alpha^2 - \beta^2) = \Pi(\beta^2 - \alpha^2)$ for which each value of α on combination with each value of β, will have the sign *plus* or the sign *minus*."

This theorem, of which the law of reciprocity is an immediate consequence, can be demonstrated in a purely arithmetical manner. There exists something analogous but more complicated for cubic and biquadratic residues, and we can say for the proof of the associated laws of reciprocity that we have no need of the formula for multiplication of elliptic functions. However it does not appear always preferable to avoid analytic functions in arithmetical research, especially when we see *a posteriori* that they do not enter essentially in the proofs and that they serve solely to fix ideas and abridge conclusions.

Berlin 13 February 1845.

This is a translation from the French [Ei1845] in Eisenstein's Mathematiche Abhandlungen. There is a commentary on this work by Kronecker, both in German [Kr1876] and French [Kr1880].

References.

Ei1845 G. Eisenstein, *2. Applications de l'Algèbra à l'Arithmétique transcendante*, 1845, Mathematische Abhandlungen, Georg Olms Hildesheim, 1967.

Kr1876 L. Kronecker, *II. Ueber das Reciprocitätsgesetz*, 1876, vol 2, Werke.

Kr1880 L. Kronecker, *III. Sur la loi de réciprocité*, 1880, vol 2, Werke.