New Demonstrations and Extensions of the Fundamental Theorem in the Doctrine of Quadratic Residues

The fundamental theorem of quadratic residues, which is considered among the most beautiful truths of higher arithmetic, was indeed easily discovered by induction, but demonstrated with far more difficulty. It often happens in this subject, that the demonstrations of the simplest truths, which offer themselves spontaneously to the inquirer by induction, are hidden in the deepest depths, and only after many fruitless attempts, quite possibly by a different path than that by which they were sought, can they finally be brought to light. Then it happens not infrequently, when at first one path has been discovered, that several more appear from time to time leading to the same goal, others shorter and more directly, others as if springing indirectly and from very different principles, between which you would hardly have suspected any connection with the question proposed. A strange connection of this kind between more abstruse truths not only gives a certain charm to these contemplations, but also deserves to be diligently investigated and analyzed, because not infrequently new resources or advances in science itself derive from this.

Therefore, although the arithmetical theorem which is being discussed here has been absolutely witnessed by previous work, which supplied four totally different demonstrations[1] , I nonetheless return again to the same theme, and add two other demonstrations, which will certainly throw a new light on this matter. Indeed, the former is in a way related to the third, because it proceeds from the same lemma. Afterwards, however, a different course is followed, so that it may rightly be regarded as a new demonstration, which will be seen to be, if not superior, at least not inferior to the third. On the other hand, the sixth demonstration is based on a completely different and more precise principle, and it represents a new example of surprising connections between arithmetical truths which at first sight are very far removed from each other. To these two demonstrations is added a new, very simple algorithm to determine whether a given integer is a quadratic residue or non-residue of a given prime number.

There was yet another reason, which prompted me to announce the new demonstrations at this particular moment, although they had been promised nine years ago. From 1805, when I began to investigate the theory of cubic and biquadratic residues, which is a much more difficult subject, I experienced almost the same fate as I once had in the theory of quadratic residues. Indeed, those theorems which completely exhaust these questions, and in which a wonderful analogy with the theorems relating to quadratic residues stands out, were immediately discovered by induction, as soon as a suitable way had been sought. However, they remained unsettled for a long time, and all efforts to find a demonstration were in vain. This was the very incentive for me to add more and more demonstrations to those already known about quadratic residues, supported by the hope that one or another of the many different methods might do something to illuminate an analogous line of reasoning. The hope was by no means in vain, and indefatigable labor was finally followed by prosperous success. It will soon be possible to bring the fruits of this vigilance to public light; but before embarking on this arduous task, I decided to return once more to the theory of quadratic residues, to complete all that still remained of that agenda, and thus to bid farewell to this sublime part of arithmetic.

[1] Two are set forth in sections 4 and 5 of Disquisitiones Arithmeticae; the third is in a special commentary (Commentt. Soc. Gotting. Vol. XVI), the fourth is inserted in the commentary: *Summatio Quarundam Serierum Singularium* (Commentt. Recentiores, Vol. I)

Fifth Demonstration of the Fundamental Theorem in the Theory of Quadratic Residues

Art. 1

We have already declared in the introduction that the fifth and third demonstration proceed from the same lemma. As a matter of convenience, it seems appropriate to repeat it in this place, with notation adapted to the present discussion.

Lemma 1. *Let m be a prime number (positive odd), and let M be an integer not divisible by m. Let the minimal positive residues of the numbers*

$$M, 2M, 3M, 4M, \ldots, \tfrac{1}{2}(m-1)M$$

modulo m be taken. These will be partly smaller than $\frac{1}{2}m$ and partly greater; let the multitude of the latter $= n$. Then M will be a quadratic residue or non-residue modulo m, according as n is even or odd.

Proof. Let those residues which are less than $\frac{1}{2}m$ be denoted a, b, c, etc. and let the rest, which are greater than $\frac{1}{2}m$ be denoted a', b', c', etc. The complements to m of the latter, $m-a'$, $m-b'$, $m-c'$, $m-d'$ etc., will all be smaller than $\frac{1}{2}m$, and they will be distinct both among themselves and from the residues a, b, c, d, etc. Therefore, with some change of order, they will be identical with the numbers 1, 2, 3, 4, ..., $\frac{1}{2}(m-1)$. So, by setting the product

$$1.2.3.4.\ldots.\tfrac{1}{2}(m-1) = P$$

we will have

$$P = abcd\cdots \times (m-a')(m-b')(m-c')(m-d')\ldots$$

and thus

$$(-1)^n P = abcd\cdots \times (a'-m)(b'-m)(c'-m)(d'-m)\ldots$$

Furthermore, according to the modulus m,

$$PM^{\frac{1}{2}(m-1)} \equiv abcd\cdots \times a'b'c'd'\cdots \equiv abcd\ldots(a'-m)(b'-m)(c'-m)(d'-m)\ldots$$

and thus

$$PM^{\frac{1}{2}(m-1)} \equiv P(-1)^n$$

Hence $M^{\frac{1}{2}(m-1)} = \pm 1$, where the sign is positive if n is even and negative if n is odd, and with the help of the theorem of *Disquisitiones Arithmeticae* Art. 106, the truth of the lemma follows automatically. □

Theorem. *Let m, M be positive odd relatively prime integers, and let n be the multitude of minimal positive residues of the numbers*

$$M, 2M, 3M, \ldots, \tfrac{1}{2}(m-1)M$$

modulo m, which are greater than $\frac{1}{2}m$; and likewise let N be the multitude of minimal positive residues of the numbers

$$m, 2m, 3m, \ldots, \tfrac{1}{2}(M-1)m$$

modulo m which are greater than $\frac{1}{2}M$. Then the three numbers n, N, $\frac{1}{4}(m-1)(M-1)$ will either be all even, or one will be even and two will be odd.

Proof. Denote

by f the complex of numbers $1, 2, 3, \ldots, \frac{1}{2}(m-1)$,

by f' the complex of numbers $m-1, m-2, m-3, \ldots, \frac{1}{2}(m+1)$,

by F the complex of numbers $1, 2, 3, \ldots, \frac{1}{2}(M-1)$,

by F' the complex of numbers $M-1, M-2, M-3, \ldots, \frac{1}{2}(M+1)$,

Then n will indicate how many numbers Mf have their minimal positive residues modulo m in the complex f', and likewise N will indicate how many numbers mF have their least positive residues modulo M in the complex F'. Finally, denote

by ϕ the complex of numbers $1, 2, 3, \ldots, \frac{1}{2}(mM-1)$

by ϕ' the complex of numbers $mM-1$, $mM-2$, $mM-3$, $\ldots$, $\frac{1}{2}(mM+1)$

Every integer not divisible by m must be congruent, modulo m, to either a residue from f or a residue from f', and likewise any integer not divisible by M must be congruent, modulo M, to either a residue from F or a residue from F'. It follows that all the numbers ϕ, among which obviously no one occurs that is simultaneously divisible by m and M, can be divided into eight classes in the following way.

I. In the first class there will be those numbers congruent to any number from f modulo m, and congruent to any number from F modulo M. We will denote the multitude of these numbers by α.

II. Numbers congruent to residues from f, F' modulo m, M resp., the multitude of which is β.

III. Numbers congruent to residues from f', F modulo m, M resp., the multitude of which is γ.

IV. Numbers congruent to residues from f', F' modulo m, M resp., the multitude of which is β.

V. Numbers divisible by m, and congurent to one of the residues from F modulo M.

VI. Numbers divisible by m, and congurent to one of the residues from F' modulo M.

VII. Numbers divisible by M, and congurent to one of the residues from f modulo m.

VIII. Numbers divisible by M, and congurent to one of the residues from f' modulo m.

Obviously, classes V and VI taken together will include all of the numbers mF. The multitude of numbers contained in VI will be $= N$, and thus the population of numbers contained in V will be $\frac{1}{2}(M-1) - N$. Likewise, classes VII and $VIII$ taken together will contain all the nubmers Mf, in class $VIII$ there will be found n numbers, and in class VII there will be $\frac{1}{2}(m-1) - n$.

In exactly the same way all the numbers ϕ' will be distributed into eight classes $IX - XVI$. If we keep the same order in so doing, then it is easy to see that the numbers in classes

IX, X, XI, XII, XIII, XIV, XV, XVI

are the complements to mM of the numbers in classes

IV, III, II, I, VI, V, VIII, VII

respectively, so that in class IX there will be δ numbers, in class X, there will be γ, and so on. Now, it is clear that if all the numbers of the first class are joined with all the numbers of the ninth class, one will have all the numbers below mM which are congruent to any number from f modulo m and any number from F modulo M. It is easily seen that the multitude of these is equal to the multitude of all the combinations of one individual from f and one individual from F. Thus we have

$$\alpha + \delta = \tfrac{1}{4}(m-1)(M-1)$$

and similarly

$$\beta + \gamma = \tfrac{1}{4}(m-1)(M-1)$$

If we join together all of the numbers in the classes II, IV, VI, we shall obviously have all the numbers below mM, which are congruent to any residue from F' modulo M. At the same time, these numbers can also be presented in this way:

$$F', M + F', 2M + F', 3M + F', \ldots, \tfrac{1}{2}(m-3)M + F'$$

from which the multitude of all of them will be $= \frac{1}{4}(m-1)(M-1)$, or in other words we will have

$$\beta + \delta + N = \tfrac{1}{4}(m-1)(M-1)$$

Similarly, from the union of all classes III, IV, VII we may deduce

$$\gamma + \delta + n = \tfrac{1}{4}(m-1)(M-1)$$

From these four equations arises the following:

$$2\alpha = \tfrac{1}{4}(m-1)(M-1) + n + N$$

$$2\beta = \tfrac{1}{4}(m-1)(M-1) + n - N$$

$$2\gamma = \tfrac{1}{4}(m-1)(M-1) - n + N$$

$$2\delta = \tfrac{1}{4}(m-1)(M-1) - n - N,$$

each of which shows the truth of the theorem. □

Art. 3

If we assume that m and M are prime numbers, the fundamental theorem will follow directly from the combination of the preceding theorem with the lemma of Art. 1. For it is clear that

I. Whenever one or both of m, M is of the form $4k+1$, the number $\frac{1}{4}(m-1)(M-1)$ will be even, and therefore either both m and M are quadratic residues of each other, or both are quadratic non-residues of each other.

II. Whenever m, M are both of the form $4k+3$, the number $\frac{1}{4}(m-1)(M-1)$ will be odd, hence one of the numbers n, N must be even and the other odd, and therefore one of the numbers m, M is a quadratic residue of the other, and the other is a quadratic non-residue of the one.

Sixth Demonstration of the Fundamental Theorem in the Theory of Quadratic Residues

Art. 1

Theorem. *Let p be a prime number (odd positive), n a positive integer not divisible by p, x an indeterminate quantity. Then the function*

$$1 + x^n + x^{2n} + x^{3n} + etc. + x^{np-n}$$

will be divisible by

$$1 + x + xx + x^3 + etc. + x^{p-1}$$

Proof. Let g be a positive integer such that $gn \equiv 1 \pmod{p}$, and set $gn = 1 + hp$. Then one has

$$\begin{aligned}\frac{1 + x^n + x^{2n} + x^{3n} + \text{etc.} + x^{np-n}}{1 + x + xx + x^3 + \text{etc.} + x^{p-1}} &= \frac{(1 - x^{np})(1 - x)}{(1 - x^n)(1 - x^p)} \\ &= \frac{(1 - x^{np})(1 - x^{gn} - x + x^{hp+1})}{(1 - x^n)(1 - x^p)} \\ &= \frac{1 - x^{np}}{1 - x^p} \cdot \frac{1 - x^{gn}}{1 - x^n} - \frac{x(1 - x^{np})}{1 - x^n} \cdot \frac{1 - x^{hp}}{1 - x^p}\end{aligned}$$

therefore the function is manifestly integral. □

So any integral function of x which is divisible by $\frac{1-x^{np}}{1-x^n}$, will also be divisible by $\frac{1-x^p}{1-x}$.

Art. 2

Let α denote a positive primitive root modulo p, i.e. let α be a positive integer such that the minimal positive residues of its powers $1, \alpha, \alpha\alpha, \alpha^3, \ldots, \alpha^{p-1}$ modulo p are identical, without respect to order, with the numbers $1, 2, 3, \ldots, p-1$. Further denote by fx the function

$$x + x^{\alpha} + x^{\alpha\alpha} + x^{\alpha^3} + \text{etc.} + x^{\alpha^{p-2}} + 1$$

It is clear that $fx - 1 - x - xx - x^3 - \text{etc.} - x^{p-1}$ will be divisible by $1 - x^p$, and therefore more importantly $\frac{1-x^p}{1-x} = 1 + x + xx + x^3 + \text{etc.} + x^{p-1}$, by which the function fx itself will also be divisible. From this it follows, since x is an indeterminate quantity, that $f(x^n)$ is divisible by $\frac{1-x^{np}}{1-x^n}$, and therefore (by the previous article) also by $\frac{1-x^p}{1-x}$, whenever n is an integer not divisible by p. On the other hand, whenever n is an integer divisible by p, each part of the function $f(x^n)$, diminished by 1, will be divisible by $1 - x^p$. Therefore in this case $f(x^n) - p$ will also be divisible by $1 - x^p$ and therefore also by $\frac{1-x^p}{1-x}$.

Art. 3

Theorem. *Let*

$$x - x^{\alpha} + x^{\alpha\alpha} - x^{\alpha^3} + x^{\alpha^4} - etc. - x^{\alpha^{p-2}} = \xi.$$

Then $\xi\xi \mp p$ will be divisible by $\frac{1-x^p}{1-x}$, where the sign is positive if p is of the form $4k+1$ and negative if p is of the form $4k+3$.

Proof. It is easy to see that of the $p-1$ functions

$$\begin{aligned}
&+x\xi - xx + x^{\alpha+1} - x^{\alpha\alpha} + \text{etc.} + x^{\alpha^{p-2}+1}\\
&-x^{\alpha}\xi - x^{2\alpha} + x^{\alpha\alpha+\alpha} - x^{\alpha^3+\alpha} + \text{etc.} + x^{\alpha^{p-1}+\alpha}\\
&+x^{\alpha\alpha}\xi - x^{2\alpha\alpha} + x^{\alpha^3+\alpha\alpha} - x^{\alpha^4+\alpha\alpha} + \text{etc.} + x^{\alpha^p+\alpha\alpha}\\
&-x^{\alpha^3}\xi - x^{2\alpha^3} + x^{\alpha^4+\alpha^3} - x^{\alpha^5+\alpha^3} + \text{etc.} + x^{\alpha^{p+1}+\alpha^3}
\end{aligned}$$

etc. up to

$$-x^{\alpha^{p-2}}\xi - x^{2\alpha^{p-2}} + x^{\alpha^{p-1}+\alpha^{p-2}} - x^{\alpha^p+\alpha^{p-2}} + \text{etc.} + x^{\alpha^{2p-4}+\alpha^{p-2}}$$

the first will be $= 0$, and each of the others will be divisible by $1-x^p$. Therefore the sum of all of them will be divisible by $1-x^p$. This sum is

$$\begin{aligned}
&= \xi\xi - (f(xx)-1) + f(x^{\alpha+1})-1) - (f(x^{\alpha\alpha+1})-1) + (f(x^{\alpha^3+1})-1) - \text{etc.} + (f(x^{\alpha^{p-2}+1})-1)\\
&= \xi\xi - f(xx) + f(x^{\alpha+1}) + f(x^{\alpha+1}) - f(x^{\alpha\alpha+1}) + f(x^{\alpha^3+1}) - \text{etc.} + f(x^{\alpha^{p-2}+1}) = \Omega
\end{aligned}$$

Therefore this expression Ω will be divisible by $\frac{1-x^p}{1-x}$. Now among the exponents $2, \alpha+1, \alpha\alpha+1, \alpha^3+1, \ldots, \alpha^{p-2}+1$ the only one divisible by p will be $\alpha^{\frac{1}{2}(p-1)}+1$, and so by the preceding article, the individual parts of the expression Ω,

$$f(xx), f(x^{\alpha+1}), f(x^{\alpha\alpha+1}), f(x^{\alpha^3+1})\text{etc.}$$

except for the single term $f(x^{\alpha^{\frac{1}{2}(p-1)}+1})$, will be divisible by $\frac{1-x^p}{1-x}$. It is therefore permissible to delete these parts, so that the function

$$\xi\xi \mp f(x^{\alpha^{\frac{1}{2}(p-1)}+1})$$

remains divisible by $\frac{1-x^p}{1-x}$. Above the sign will be positive or negative according as p is of the form $4k+1$ or of the form $4k+3$. And since $f(x^{\alpha^{\frac{1}{2}(p-1)}+1}) - p$ is divisible by $\frac{1-x^p}{1-x}$, it follows that $\xi\xi \mp p$ must also be divisible by $\frac{1-x^p}{1-x}$. □

In order that the double sign may not introduce any ambiguity, we will denote by ϵ the number $+1$ or -1, depending on whether p is of the form $4k+1$ or $4k+3$. Therefore, $\frac{(1-x)(\xi\xi-\epsilon p)}{1-x^p}$ will be an integral function of x, and we will denote it by Z.

Art. 4

Let q be an odd positive number, so that $\frac{1}{2}(q-1)$ is an integer. Then $(\xi\xi)^{\frac{1}{2}(q-1)} - (\epsilon p)^{\frac{1}{2}(q-1)}$ will be divisible by $\xi\xi - \epsilon p$, and therefore by $\frac{1-x^p}{1-x}$. If we set $\epsilon^{\frac{1}{2}(q-1)} = \delta$ and

$$\xi^{q-1} - \delta p^{\frac{1}{2}(q-1)} = \frac{1-x^p}{1-x} Y,$$

then Y will be an integral function of x, and $\delta = +1$, whenever one of the numbers p, q is of the form $4k+1$, and on the contrary $\delta = -1$, whenever both p and q are of the form $4k+3$.

Art. 5

Now let us assume that q is also a prime number (different from p). Then it is clear from the theorem proven in Disquisitiones Arithmeticae, Art. 51, that

$$\xi^q - (x^q - x^{q\alpha} + x^{q\alpha\alpha} - x^{q\alpha^3} + \text{etc.} - x^{q\alpha^{p-2}})$$

is divisible by q, or of the form qX, where X is an integral function of x even with respect to the numerical coefficients (which also applies to the rest of the integral functions Z, Y, W occurring here). Let us denote by μ the index of the number q with respect to the primitive root α modulo p, i.e. let $q = \alpha^\mu \pmod{p}$. Then the numbers $q, q\alpha, q\alpha\alpha, q\alpha^3, \ldots, q\alpha^{p-2}$ will be congruent to $\alpha^\mu, \alpha^{\mu+1}, \alpha^{\mu+2}, \ldots, \alpha^{p-2}, 1, \alpha, \alpha\alpha, \ldots, \alpha^{\mu-1}$ modulo p, and therefore

$$\begin{array}{l}
x^q - x^{\alpha^\mu} \\
x^{q\alpha} - x^{\alpha^{\mu+1}} \\
x^{q\alpha\alpha} - x^{\alpha^{\mu+2}} \\
x^{q\alpha^3} - x^{\alpha^{\mu+3}} \\
\quad \vdots \\
x^{q\alpha^{p-\mu-2}} - x^{\alpha^{p-2}} \\
x^{q\alpha^{p-\mu-1}} - x \\
x^{q\alpha^{p-\mu}} - x^\alpha \\
x^{q\alpha^{p-\mu+1}} - x^{\alpha\alpha} \\
\quad \vdots \\
x^{q\alpha^{p-2}} - x^{\alpha^{\mu-1}}
\end{array}$$

will all be divisible by $1 - x^p$. Taking these quantities alternately positively and negatively, and summing up, it becomes clear that the function

$$x^q - x^{q\alpha} + x^{q\alpha\alpha} - x^{q\alpha^3} + \text{ etc.} - x^{q\alpha^{p-2}} \mp \xi$$

will be divisible by $1 - x^p$, provided that the sign is taken to be positive or negative according as μ is even or odd, i.e. as q is a quadratic residue or non-residue modulo p. So, let us set

$$x^q - x^{q\alpha} + x^{q\alpha\alpha} - x^{q\alpha^3} + \text{ etc.} - x^{q\alpha^{p-2}} - \gamma\xi = (1 - x^p)W$$

where $\gamma = +1$ or $\gamma = -1$ according as q is a quadratic residue or non-residue modulo p. Then clearly W will be an integral function.

Art. 6

Having made these preparations, we deduce from a combination of the previous equations that

$$q\xi X = \epsilon p \left(\delta p^{\frac{1}{2}(q-1)} - \gamma\right) + \frac{1 - x^p}{1 - x}\left(Z\left(\delta p^{\frac{1}{2}(q-1)} - \gamma\right) + Y\xi\xi - W\xi(1 - x)\right)$$

Suppose that upon dividing the function ξX by

$$x^{p-1} + x^{p-2} + x^{p-3} + \text{etc.} + x + 1$$

we obtain a quotient U and remainder T, or in other words we have

$$\xi X = \frac{1 - x^p}{1 - x}U + T$$

where U and T are integral functions, even with respect to their numerical coefficients, and the degree of T is lower than that of the divisor. Then we will have

$$qT - \epsilon p \left(\delta p^{\frac{1}{2}(q-1)} - \gamma\right) = \frac{1 - x^p}{1 - x}\left(Z\left(\delta p^{\frac{1}{2}(q-1)} - \gamma\right) + Y\xi\xi - W\xi(1 - x) - qU\right)$$

which is obviously false unless both sides of the equation vanish individually. Therefore $\epsilon p\left(\delta p^{\frac{1}{2}(q-1)}-\gamma\right)$ will be divisible by q, and no less $\delta p^{\frac{1}{2}(q-1)}-\gamma$, and therefore because $\delta\delta=1$, the number $p^{\frac{1}{2}(q-1)}-\gamma\delta$ will be divisible by q.

Now if β denotes a positive or negative unit, according as p is a quadratic residue or non-residue of the number q, then $p^{\frac{1}{2}(q-1)}-\beta$ will be divisible by q, and therefore so will be $\beta-\gamma\delta$, but this is impossible unless $\beta=\gamma\delta$. Hence the fundamental theorem follows automatically. Namely,

I. Whenever both p, q, or both is of the form $4k+1$, and therefore $\delta=+1$, we will have $\beta=\gamma$, and therefore simultaneously q is a quadratic residue modulo p and p is a quadratic residue modulo q; or simultaneously q is a quadratic non-residue modulo p, and p is a quadratic non-residue modulo q.

II. When both p and q are of the form $4k+3$, and therefore $\delta=-1$, we will have $\beta=-\gamma$, and therefore simultaneously q is a quadratic residue modulo p and p is a quadratic non-residue modulo q; or simultaneously q is a quadratic non-residue modulo p, and p is a quadratic residue modulo q.

Q.E.D.

A new algorithm for deciding whether a given positive integer is a quadratic residue or a non-residue of a given positive prime number.

Art. 1

Before we explain the solution to this problem, we will briefly repeat here the solution given in the Disquisitiones Arithmeticae, which is indeed quite easily accomplished with the help of the fundamental theorem and the following theorems:

I. The relation of a number a to a number b (in so far as it is a quadratic residue or non-residue) is the same as that of a number c to b, if $a\equiv c$ (mod. b).

II. If a is a product of factors $\alpha,\beta,\gamma,\delta$ etc. and b is a prime number, then the relation of a to b will depend on the relations of the factors to b, so that a is a quadratic residue or non-residue modulo b according as between those factors are found to be an even or odd multitude of factors which are non-residues modulo b. Therefore, whenever any factor is squared, it will not be considered at all in this examination; and if any factor is a power of an integer with an odd exponent, it can be replaced with that integer instead.

III. The number 2 is a quadratic residue of any prime number of the form $8m+1$ or $8m+7$, and is a non-residue of any prime number of the form $8m+3$ or $8m+5$.

Having therefore proposed the number a, whose relation to the given prime number b is asked: if a is greater than b, then first of all substitute its minimal positive residue modulo b, by which remainder having been resolved into its prime factors, the question is reduced by theorem II to the discovery of the relations of each of these factors to b. The relation of the factor 2 (if its present either once, or three times, or five times, etc.) is known by theorem III. The relations of the rest to b, by the fundamental theorem, depends on the relations of b to each of the rest. In this way, therefore, instead of one relation of a given number to the prime number b, some relations of the number b to other odd primes smaller than b must be investigated, which problems will be reduced in the same way to smaller moduli, and obviously these successive decrements will finally be exhausted.

Art. 2

To illustrate this solution with an example, let us seek the relation of the number 103 to 379. Since 103 is already less than 379, and is itself a prime number, the fundamental theorem must be immediately applied,

which tells us that the relation sought is the opposite of the relation of the number 379 to 103. This again is equal to the relation of the number 70 to 103, which itself depends on the relations of the numbers $2, 5, 7$ to 103. The first of these is known by theorem III. The second, by the fundamental theorem, depends on the relation of 103 to 5, which by theorem I is equal to the relation of the number 3 to 5. This again, by the fundamental theorem, depends on the relation of 5 to 3, which by theorem 1 is equal to the relation of 2 to 3, which is known by theorem III. Likewise, the relation of the number 7 to 103 depends on the relation of the number 103 to 7, which by theorem I is equal to the relation of the number 5 to 7; this again, by the fundamental theorem, depends on the relation of the number 7 to 5, which is equal to the relation of the number 2 to 5. If it pleases us to turn this analysis into a synthesis, the decision of the question will be referred to fourteen points, which we set out here in full, so that the greater harmony of the new solution may shine out all the more clearly.

1. The number 2 is a quadratic residue of the number 103 (theor. III)
2. The number 2 is a quadratic non-residue of the number 3 (theor. III)
3. The number 5 is a quadratic non-residue of the number 3 (by I and 2)
4. The number 3 is a quadratic non-residue of the number 5 (fund. theor. and 3)
5. The number 103 is a quadratic non-residue of the number 5 (I and 4)
6. The number 5 is a quadratic non-residue of the number 103 (fund. theor. and 5)
7. The number 2 is a quadratic non-residue of the number 5 (theor. III)
8. The number 7 is a quadratic non-residue of the number 5 (I and 7)
9. The number 5 is a quadratic non-residue of the number 7 (fund. theor. and 8)
10. The number 103 is a quadratic non-residue of the number 7 (I and 9)
11. The number 7 is a quadratic non-residue of the number 103 (fund. theor. and 10)
12. The number 70 is a quadratic non-residue of the number 103 (II,1,6,11)
13. The number 379 is a quadratic non-residue of the number 103 (I and 12)
14. The number 103 is a quadratic non-residue of the number 379 (fund. theor. and 13)

In the following, for the sake of brevity, we will use the notation introduced in *Comment. Gotting. Vol. XVI)*. Namely, by $[x]$ we denote x itself, whenever x is an integer, or the greatest integer smaller than x, if x is a fractional quantity, so that $x - [x]$ is always a non-negative quantity less than unity.

Art. 3

Problem 1. *Let a and b be positive relatively prime integers, and set $[\frac{1}{2}a] = a'$, evaluate the sum*

$$\left[\frac{b}{a}\right] + \left[\frac{2b}{a}\right] + \left[\frac{3b}{a}\right] + \left[\frac{4b}{a}\right] + \textit{etc.} + \left[\frac{a'b}{a}\right]$$

Solution. For the sake of brevity, let us denote this kind of sum by $\phi(a, b)$, so that

$$\phi(b, a) = \left[\frac{a}{b}\right] + \left[\frac{2a}{b}\right] + \left[\frac{3a}{b}\right] + \text{etc.} + \left[\frac{b'a}{b}\right]$$

In the third demonstration of the fundamental theorem it was shown that, for the case where a and b are odd, we have

$$\phi(a, b) + \phi(b, a) = a'b'$$

and by following the same method the truth of this statement can also be extended to the case where either of the numbers a and b are odd, as we have already discussed there. Following the method by which the greatest common divisor of two integers is investigated, divide a by b, and let β be the quotient and c the remainder. Then divide b by c and so on, so as to obtain equations

$$\begin{aligned} a &= \beta b + c \\ b &= \gamma c + d \\ c &= \delta d + e \\ d &= \epsilon e + f \text{ etc.} \end{aligned}$$

□

In this way, through a series of continually decreasing numbers b, c, d, e, f etc. we shall at last arrive at unity, since by hypothesis a and b are relatively prime. Then the final equation will be

$$k = \lambda \ell + 1$$

We obviously have

$$\begin{aligned} \left[\frac{a}{b}\right] &= \left[\beta + \frac{c}{b}\right] = \beta + \left[\frac{c}{b}\right] \\ \left[\frac{2a}{b}\right] &= \left[2\beta + \frac{c}{b}\right] = 2\beta + \left[\frac{c}{b}\right] \\ \left[\frac{3a}{b}\right] &= \left[3\beta + \frac{c}{b}\right] = 3\beta + \left[\frac{c}{b}\right] \end{aligned}$$

etc., so

$$\phi(a,b) = \phi(b,c) + \frac{1}{2}\beta(b'b' + b')$$

and thus

$$\phi(a,b) = a'b' - \frac{1}{2}\beta(b'b' + b') - \phi(b,c)$$

By similar reasoning, if we set $[\frac{1}{2}c] = c'$, $[\frac{1}{2}d] = d'$, $[\frac{1}{2}e] = e'$ etc., then

$$\begin{aligned} \phi(b,c) &= b'c' - \tfrac{1}{2}\gamma(c'c' + c') - \phi(c,d) \\ \phi(c,d) &= c'd' - \tfrac{1}{2}\gamma(d'd' + d') - \phi(d,e) \\ \phi(d,e) &= d'e' - \tfrac{1}{2}\gamma(e'e' + e') - \phi(e,f) \end{aligned}$$

etc., up to

$$\phi(k,\ell) = k'\ell' - \tfrac{1}{2}(\ell'\ell' + \ell') - \phi(\ell,1)$$

Hence, since it is obvious that $\phi(\ell,1) = 0$, we derive the formula

$$\begin{aligned} \phi(a,b) = a'b' - b'c' + c'd' - d'e' + \text{etc.} \pm k'\ell' \\ - \tfrac{1}{2}\beta(b'b' + b') + \tfrac{1}{2}\gamma(c'c' + c') - \tfrac{1}{2}\delta(d'd' + d') + \text{etc.} \mp \tfrac{1}{2}\lambda(\ell'\ell' + \ell') \end{aligned}$$

Art. 4

It is easily concluded from what was set forth in the third demonstration, that the relation of the number b to a, whenever a is a prime number, is automatically known from the sum $\phi(a, 2b)$. Namely, b will be a quadratic residue of a or a quadratic non-residue according to whether this sum is an even or an odd number. For the same purpose the sum $\phi(a,b)$ itself may be used instead, with the same restriction, but the case where b is odd must be distinguished from that in which it is even. Specifically,

I. Whenever b is odd, b will be a quadratic residue or non-residue modulo a according as $\phi(a,b)$ is even or odd.

II. If b is even, the same rule will hold if, moreover a is of the form $8n+1$ or $8n+7$; if instead for an even value of b the modulus a is of the form $8n+3$ or $8n+5$, the opposite rule must be applied, namely that b is a quadratic residue modulo a if $\phi(a,b)$ is odd, and it is a non-residue if $\phi(a,b)$ is even.

All of this can be very easily derived from Art. 4 of the third demonstration.

Art. 5

Example. If we ask for the relation of the number 103 to the number 379, we must first compute the sum $\phi(379,103)$:

$a=379$	$a'=189$	
$b=103$	$b'=51$	$\beta=3$
$c=70$	$c'=35$	$\gamma=1$
$d=33$	$d'=16$	$\delta=2$
$e=4$	$e'=2$	$\epsilon=8$

hence

$$\phi(379,103)=9639-1785+560-32-3978+630-272+24=4786$$

and thus 103 is a quadratic residue modulo 379. If we wish to use the sum $\phi(379,206)$ for the same end, we have the following:

379	189	
206	103	1
173	86	1
33	16	5
8	4	4

and from this we deduce

$$\phi(379,206)=19467-8858+1376-64-5356+3741-680+40=9666$$

Therefore 103 is a quadratic residue modulo 379.

Art. 6

Since in order to determine the relation of the number b to a it is not necessary to calculate the individual parts of the aggregate (a,b), but rather it is sufficient to know how many of them are odd, our rule can also be presented as follows.

As above, let $a=\beta b+c$, $b=\gamma c+d$, $c=\delta d+e$ etc., until in the series of numbers a,b,c,d,e etc. unity has been reached. Set $[\frac{1}{2}a]=a'$, $[\frac{1}{2}b]=b'$, $[\frac{1}{2}c]=c'$ etc., let μ be the multitude of odd numbers in the series a', b', c' etc. which are immediately followed by an odd number, and let ν be the multitude of odd numbers in the series β,γ,δ etc. such that the corresponding number in the series b',c',d' is of the form $4n+1$ or $4n+2$. With this being done, b will be a quadratic residue or non-residue modulo a according as $\mu+\nu$ is even or odd, except in the single case where b is even and simultaneously a is of the form $8n+3$ or $8n+5$, in which case the opposite rule applies.

In our example, the series a',b',c',d',e' has two consecutive pairs of odd numbers, so $\mu=2$, and in the series $\beta,\gamma',\delta',\epsilon'$ there are two odd ones, but the corresponding numbers in the series b', c', d', e' are of the form $4n+3$, so $\nu=0$. Therefore, $\mu+\nu$ is even, and therefore 103 is a quadratic residue modulo 379.