

A lecture/report from Hofr. GAUSS presented to the Royal Society on the 15th of April titled:

*Theoria residuorum biquadraticorum, Commentatio secunda.*

is the sequel to a treatise already published in the 6th volume of the *Commentationes novae*, of which an announcement was also made in our pages at that time, April 11, 1825. This sequel as well, though more than doubly thicker than the first, still does not exhaust the extremely rich subject, and the consummation of the whole will remain reserved for the first of a projected third treatise.

Although the fundamental concept of this subject and the contents of the first treatise, which has made a field of study out of higher arithmetic, could be supposed to be familiar to all, still we will bring here a short recollection for the convenience of such friends of this part of mathematics, for which the first treatise is not equally at hand.

A number,  $k$ , is called a biquadratic residue with respect to an arbitrary number  $p$ , if it gives numbers of the form  $x^4 - k$ , which are divisible by  $p$ ; otherwise, it is called a biquadratic non-residue of  $p$ . It is sufficient, to restrict ourselves to the case, where  $p$  is a prime number of the form  $4n + 1$  and not divisible by  $k$ , since all other cases are either evident, or derived from these.

For such a *given* value of  $p$ , all numbers not divisible by  $p$  are divided into *four* classes, which are separated such that one contains biquadratic residues, the second contains biquadratic non-residues which are biquadratic residues, and the two remaining contain biquadratic non-residues, which are the also quadratic non-residues. The principle of this division consists in, that always either  $k^n - 1$ ,  $k^n + 1$ ,  $k^n - f$ , or  $k^n + f$  will be divisible by  $p$ , where  $f$  represents a whole number that makes  $ff + 1$  divisible by  $p$ . Anyone to whom the elementary terminologie is known, sees for themselves, how this word definitions are clothed in the same[?].

The theory of this classification, applying not only for the case  $k = -1$  lying on the surface, rather, requiring subtle [?]aid investigations, also for the case  $k = \pm 2$ , occurs in the first treatise entirely complete. The beginning of the present treatise proceeds now to greater values of  $k$ : however, to do so, one needs to next take into consideration only such [numbers], that themselves are prime numbers, and exhibit the outcome, that the most simple results fall out,

when the value is taken as positive or negative, according as they, considered absolute, are of the form  $4m+1$  or  $4m+3$ . Induction at once, with greater ease, gives a rich harvest from new propositions, of which we introduce only a pair here. The numbering of the classes with 1, 2, 3, 4, are based on the cases where  $k^n$  is congruent to the numbers 1,  $f$ ,  $-1$ ,  $-f$ ; similarly the same value assumed is always for the number  $f$ , which makes  $a+bf$  divisible by  $p$ , if  $aa+bb$  represents the decomposition of  $p$  into an even and an odd square. Then one will find, that the number  $-3$  always belongs to the class 1, 2, 3, 4, according as  $b$ ,  $a+b$ ,  $a$ , or  $a-b$  is divisible by 3; that the number  $+5$  belongs to those in turn according as  $b$ ,  $a-b$ ,  $a$ , or  $a+b$  is divisible by 5; that the number 7 falls under class 1 if  $a$  or  $b$ ; class 2 if  $a-2b$  or  $a-3b$ ; class 3 if  $a-b$  or  $a+b$ ; class 4 if  $a+2b$  or  $a+3b$  is divisible by 7. Similar theorems arise in relation to the numbers  $-11$ ,  $+13$ ,  $+17$ ,  $-19$ ,  $-23$  and so on. However easy it may be to discover all similar special theorems by induction, it appears difficult to find a general rule by this method, and still much harder to find the proof for these propositions. The method used in the first treatise for the numbers  $+2$  and  $-2$  is no longer of use here, and if likewise another method could serve to handle that which corresponds to the first and third classes [erledigen-attend/complete/conclude/handle/carry out/ take care of], then it still demonstrates itself to be unqualified for the substantiation of such *complete* proofs.

According to this, it is soon reconized that this rich field of higher arithmetic can only be penetrated by an entirely new method. The author had already given an indication in the first treatise, that to that a peculiar/singular/specific expansion of the whole field of higher arithmetic is fundamentally essential, without explaining then what this constitutes: the present treatise is thereto dedicated to casting light set this subject.

This is none other than the that for the true foundations of the theory of biquadratic residues, the field of higher arithmetic, which otherwise only extended to the real whole numbers, also covers the imaginary, and these must be allowed complete equal citizenship with those [real numbers]. As soon as these have been accepted that theory appears in an entirely new light, and its results attain an extremely surprising simplicity.

However, before the theory of biquadratic residues itself can be developed in this enlarged number domain, must assume this expansion part in those which this theory preceding teachings of higher arithmetic[?], which till now are only considered to treat real numbers. Here we can only give some of these antecedent investigations. The author takes each magnitude  $a+bi$ , where  $a$  and  $b$  represent real magnitudes, and  $i$  is the short hand for  $\sqrt{-1}$ , to be a complex whole number, if  $a$  and  $b$  are likewise whole numbers. Thus the complex magnitudes do not stand contrary to the real magnitudes, rather these are contained within it as a special case, where  $b=0$ . For a convenient application, it was necessary, to attach a specific nomenclature to various concepts[Begriffbildung] pertaining to complex numbers, which we will seek to circumvent in this announcement.

Just as in arithmetic, it is said that the real numbers [have] only two unities, positive and negative, we have in the arithmetic of complex numbers four unities  $+1$ ,  $-1$ ,  $+i$ ,  $-i$ . A complex whole number is called *composite*, if it is the product

of two whole factors differing by unity; a complex number, on the other hand, which does not admit *such* a decomposition into factors, is called a complex prime number. Thus for example, the real number 3, considered as a complex number, is also a prime number, whereas 5 as a compounded complex number  $= (1 + 2i)(1 - 2i)$ . Just as in the higher arithmetic of real numbers, prime numbers play a leading role in the expanding field of this science.

If a complex whole number  $a+bi$  is taken as the modulus, then  $aa+bb$  incongruent and non-repeating complex numbers can be assembled, to one of which every given complex whole number must be congruent, and which can be called a complete system of incongruent residues. The so-called least and absolute least residues in the arithmetic of real numbers also have here their complete analogy. Thus for example, for the modulus  $1 + 2i$  the complete system of absolute least residues consists of the numbers  $0, 1, i, -1$  and  $-i$ . Almost all investigations of the first four sections of the *Disquisitiones Arithmeticae* also finds their place, with some modification, in the expanded[erweiterten] arithmetic. For example, the famous Fermat's theorem assumes here the following form: If  $a + bi$  is a complex prime number, and  $k$  a complex number not divisible by it, then always  $k^{aa+bb-1} \equiv 1$  for the modulus  $a + bi$ . However, it is particularly noteworthy, that the fundamental theorem for quadratic residues in the arithmetic of complex numbers has its perfect, only still more simple here, counterpart; namely if  $a + bi, A + Bi$  are complex prime numbers, so that  $a$  and  $A$  are odd,  $b$  and  $B$  even, then the first is a quadratic residue of second, if the second is a quadratic residue of the first, otherwise the first is a quadratic non residue of the second, if the second is a quadratic non residue of the first.

While the treatise according to these pre-examinations to the doctrine of from the biquadratic residues themselves [uebergeht], instead of the mere distinction between biquadratic residues and non-residues will foremost stipulate a division of the numbers not divisible by the modulus into four classes. Namely, if the modulus is a complex prime number  $a + bi$  where  $a$  is always presumed odd, and  $b$  even, and for short  $p$  will be written in place of  $aa+bb$ , and  $k$  will be a complex number not divisible by  $a+bi$ , then  $k^{\frac{1}{4}(p-1)}$  will always be congruent to one of the numbers  $+1, +i, -1, -i$ , and by that a division of all numbers by  $a+bi$  into four classes founded[begrundet], [denen] of the series will be arranged according to the biquadratic character 0,1, 2, 3. Evidently the character 0 relates to the biquadratic residues, the rest to the biquadratic non residues, and indeed, so that likewise the character 2 represents quadratic residues, the character 1 and 3 on the other hand correspond to quadratic non residues.

It is easily known, that it generally [hauptsachlich] appears such that, these characters merely for such values of  $k$  determine [zu koennen], which themselves are complex prime numbers, and here lead similarly the induction to highest simple results.

if first is set  $k = 1 + i$ , then it appears, that the character of this number is always  $\equiv \frac{1}{8}(-aa + 2ab - 3bb + 1) \pmod{4}$ , and similar expression is found for the cases  $k = 1 - i, k = 1 + i, k = -1 - i$ .

On the other hand if  $k = \alpha + \beta$  is a such prime number, where  $\alpha$  is even and  $\beta$  odd, then a very easy fundamental theorem for biquadratic residues

entirely analogous reciprocity law arises by induction , which can be most simply expressed in the following way:

If both  $\alpha + \beta - 1$  and  $a + b - 1$  are divisible by 4 (of which case all remaining can be easily reduced), and the character of the number  $\alpha + \beta i$  in relation to the modulus  $a + bi$  is represented by  $\lambda$ , on the other hand the character of  $a + bi$  in relation to the modulus  $\alpha + \beta i$  by  $l$ : then  $\lambda = l$ , if similarly one of the numbers  $\beta, b$  (or both) is divisible by 4, on the other hand  $\lambda = l \pm 2$ , if none neither of the numbers  $\beta b$  is divisible by 4.

This theorem contains in foundation of all fundamentals of the theory of biquadratic residues in it: however, as easy as it was to discover it by induction, it is as difficult to give a strict proof for it, especially for the second, the fundamental theorem of biquadratic residues. Concerning the great depth [Umfangs], to which already the present treatise is accrued, [sah sich] the author constrained, the representation of the proof for the last theorem, in his possession is 20 years ago, to leave for a future third treatise. On the other hand, in present treatise still the complete proof for the first theorem relevant to the number  $1 + i$  (of which the other for  $1 - i, -1 + i, -1 - i$  are dependent) is communicated, which can already give a few concepts of the complexity of the subject.