Theory of Biquadratic Residues
Second Treatise

Carl Gauss

Commentationes soc. reg. sc. Gotting. recentiores. Vol. VII. Gottingae 1832

24.

That which was requisite for the classification of the number +2 was carried out thoroughly in the first treatise. Namely, if we suppose all the numbers which are not divisible by p (which will be assumed as a prime number of the form $4n+1$) to be distributed into four classes A, B, C, D, according as each number, when raised to the power of the exponent $\frac{1}{4}(p-1)$, will be congruent to the numbers $+1, +f, -1, -f$,relative to modulus p, where f denotes one of the two roots of the congruence $f^2 \equiv -1 \pmod{p}$, then we find that *the decision concerning which complex the number +2 belongs to, depends upon the decomposition of the number p into two squares*, and indeed, that if $p = a^2 + b^2$, where a^2 denotes the odd square, b^2 denotes the even square, and if we further assume that the signs of a, b were taken in the sense that $a \equiv 1 \pmod{4}$, $b \equiv af \pmod{p}$, the number +2 must belong to the complex A, B, C, D according as $\frac{1}{2}b$ is of the form $4n, 4n+1, 4n+2, 4n+3$ respectively.

From this, the rule which serves for the classification of the number -2 is immediately given as well. Namely, since -1 belongs to the class A for an even value of $\frac{1}{2}b$, but to the class C for an uneven value of $\frac{1}{2}b$, then according to the theorem of article 7, the number -2 belongs to the class A, B, C, D, depending on whether $\frac{1}{2}b$ is of the form $4n, 4n+3, 4n+2, 4n+1$ respectively.

These theorems can also be expressed in the following manner:

$+2$	-2	belong to the complex
if b, mod 8, is congruent to		
0	0	A
$2a$	$6a$	B
$4a$	$4a$	C
$6a$	$2a$	D

It is easily seen that the theorems represented in this way no longer depend upon the condition $a \equiv 1 \pmod{4}$, but rather that the theorems also apply if $a \equiv 3 \pmod{4}$, provided that the other condition $af \equiv b \pmod{p}$ remains true.

Likewise, it is easily seen that *the contents of these theorems can be contracted into a single formula* in a more elegant way, namely:

If a and b are taken as positive, then it always holds that:

$$b^{\frac{1}{2}ab} \equiv a^{\frac{1}{2}ab} 2^{\frac{1}{4}(p-1)} \pmod{p}.$$

25.

We will now investigate to what extent induction yields the classification of the number 3. If the table of article 11 is extended further (by always taking the least primitive root), then it shows that +3 belongs

to the complex

A for		
p	a	b
13	− 3	+ 2
109	− 3	+10
181	+ 9	+10
193	− 7	−12
229	−15	+ 2
277	+ 9	+14

B for		
p	a	b
17	+ 1	− 4
29	+ 5	+ 2
53	− 7	+ 2
89	+ 5	− 8
101	+ 1	+10
113	− 7	− 8
137	−11	− 4
197	+ 1	−14
233	+13	+ 8
257	+ 1	−16
269	+13	+ 8
281	+ 5	+16
293	+17	+ 2

C for		
p	a	b
37	+ 1	−6
p	a	b
61	+ 5	−6
73	− 3	−8
97	+ 9	+4
157	−11	−6
241	−15	−4

D for		
p	a	b
5	+ 1	+ 2
41	+ 5	− 4
149	− 7	+10
173	+13	+ 2

At first glance at least, we observe no simple connection between the values of the numbers a, b, which correspond to the complexes of the same $[A, B, C, D]$. If, however, we consider that a similar distinction in the theory of quadratic residues can effect a more simple rule with regard to the number -3 than the number $+3$, then we maintain the hope of a success which is as fortunate in the theory of biquadratic residues. However, we find that -3 belongs to the complex

A for		
p	a	b
37	+ 1	−6
61	+ 5	−6
157	−11	−6
193	− 7	−12

B for		
p	a	b
5	+ 1	+ 2
17	+ 1	− 4
89	+ 5	− 8
113	− 7	− 8
137	−11	− 4
149	− 7	+10
173	+13	+ 2
233	+13	+ 8
257	+ 1	−16
281	+ 5	+16

C for		
p	a	b
13	− 3	+ 2
73	− 3	−8
97	+ 9	+4
109	− 3	+10
181	+ 9	+10
229	−15	+ 2
241	−15	−4
277	+ 9	+14

D for		
p	a	b
29	+ 5	+ 2
41	+ 5	− 4
53	− 7	+ 2
101	+ 1	+10
197	+ 1	−14
269	+13	+ 8
293	+17	+ 2

and hereby, the inductive law becomes immediately apparent. Namely, -3 belongs to the complex
A, when b is divisible by 3,or $b \equiv 0 \pmod 3$
B, when $a + B$ is divisible by 3, or $b \equiv 2a \pmod 3$
C, when a is divisible by 3, or $a \equiv 0 \pmod 3$
D, when $a - b$ is divisible by 3, or $b \equiv a \pmod 3$.

26.

Furthermore, we find that the number $+5$ belongs to the complex
A for $p = 101, 109, 149, 181, 269$
B for $p = 13, 17, 73, 97, 157, 193, 197, 233, 277, 293$
C for $p = 29, 41, 61, 89, 229, 241, 281$
D for $p = 37, 53, 113, 137, 173, 257$.
If we consider the value of the numbers a, b, which correspond to each p, then we recognize the law here just as easily as for the classification of the number -3. Namely, we arrive at the complex
A, when $b \equiv 0 \pmod 5$
B, when $b \equiv a$
C, when $a \equiv 0$
D, when $b \equiv 4a$.

It is apparent that these rules encompass all cases, since were $b \equiv 2a$ or $b \equiv 3a \pmod 5$, then $a^2 + b^2 \equiv 0$, which is absurd, since p is a different prime number than 5 according to the requirements.

27.

Likewise, induction yields the following rules when applied to the numbers $-7, -11, +13, +17, -19, -23$ and extended far enough:

	$For the number - 7$
A	$a \equiv 0$ *or* $b \equiv 0 \pmod 7$
B	$b \equiv 4a$ *or* $b \equiv 5a$
C	$b \equiv a$ *or* $b \equiv 6a$
D	$b \equiv 2a$ *or* $b \equiv 3a$

28.

The special theorems, found by induction in this way, are confirmed [to the same extent that the induction might be carried out,???] and reveals a very handsome form of criteria. However, if they are compared with one another in order to derive general conclusions, then at first glance, the *following observations* are presented.

The criteria which will determine to which class the prime number $\pm q$ will belong, (where the upper or lower sign is to be taken depending on whether q is of the form $4n+1$, or of the form $4n+3$), depends upon the forms of the numbers a, b, if they are compared with one another with reference to modulus q. Namely,

I. If $a \equiv 0 \pmod q$, then $\pm q$ belongs to a determined complex, and it is indeed A for $q = 7, 17, 23$, and C for $q = 3, 11, 13, 19$, according to which it can be conjectured that the former case generally occurs when q is of the form $8n \pm 1$, the latter case, however, when q is of the form $8n \pm 3$. Moreover, the complexes B and D are already excluded without induction for a value of a divisible by q, in which case $p \equiv b^2 \pmod q$, i.e. p is a residue of q, and thereby $\pm q$ must be a quadratic residue of p by virtue of the fundamental theorem.

II. If a is not divisible by q, then the criteria depends upon the value of the expression $\frac{b}{a} \pmod q$. This expression admittedly contains various values of q, namely, the values $0, 1, 2, 3 \ldots, q-1$; however, if q is of the form $4n+1$, then both values of the expression $\sqrt{-1} \pmod q$ are excluded, which could obviously not be values of the expression $\frac{b}{a} \pmod q$, since we always assume that $p = a^2 + b^2$ is a prime number, different from q. Hence, the quantity of the permissable values of the expression $\frac{b}{a} \pmod q$ is equal to $q-2$ for $q \equiv 1 \pmod 4$, whereas it remains equal to q for $q \equiv 3 \pmod 4$.

Now, these values divide into four classes, such that the ones which are undetermined magnitudes, denoted by α, correspond to complex A, others, denoted by β, correspond to complex B, others, called γ, to complex C, and finally, the rest, denoted by δ, to complex D, namely, in such a way that $\pm q$ belongs to complex A, B, C, D, according as $b \equiv \alpha a$, $b \equiv \beta a$, $b \equiv \gamma a$, $b \equiv \delta a \pmod q$.

The law of this division, however, appears to lie quite concealed [ziemlich versteckt], though some general remarks can be made immediately. In three of the classes the quantity is the same, namely, equal to $\frac{1}{4}(q-1)$ or $\frac{1}{4}(q+1)$, while it is smaller in the other by one (and indeed in that which corresponds to the complex with the criteria $a \equiv 0$), such that the quantity of all of the various criteria with regard to individual complexes is the same, namely, equal to $\frac{1}{4}(q-1)$ or $\frac{1}{4}(q+1)$. Furthermore, we note that 0 always appears in the first class (under α), as well as the complements of the numbers α, β, γ, δ, relative to q, namely $q-\alpha$, $q-\beta$, $q-\gamma$, $q-\delta$, are contained in the first, fourth, third, second, respectively. Finally, we see that the values of the expressions $\frac{1}{\alpha}$, $\frac{1}{\beta}$, $\frac{1}{\gamma}$, $\frac{1}{\delta} \pmod q$, belong to the first, fourth, third, second classes, if the criterion $a \equiv 0$ corresponds to the complex A, but to the third, second, first, fourth classes respectively, if the criterion $a \equiv 0$ corresponds to complex C. However, nearly everything which can be reached by induction is limited to this, if we do not wish to presume to have foreseen here that which will be derived below from natural sources.

29.

Before we proceed further, we would like to remark that the criteria for prime numbers (taken as positive if they are of the form $4n+1$, negative, if they are of the form $4n+3$), suffices for the determination of all remaining numbers, [only if the theorem of Article 7 and the criteria for -1 and ± 2 are taken as aids???]. For example, if it is desired to have the criteria for the number $+3$, then the criteria given in article 25, pertaining to the number -3, also apply for the number $+3$, if $\frac{1}{b}$ is a positive number; on the contrary, complexes A, B, C, D must be exchanged with complexes C, D, A, B if $\frac{1}{b}$ is an odd number, so that we obtain the following rules.

[insert table]

Likewise, the criteria for ± 6 is derived from the connection between the criteria for ∓ 2 and -3, namely:

[insert table]

In analogous ways, the criteria for the number 21 consists of the numbers -3 and -7, and the criteria for 105 consists of the criteria for -1, -3, $+5$, -7, etc.

30.

Thus, induction also yields to us a rich harvest of special theorems, which are transformed from the theorem for the number 2; however a common thread is lacking, a strong proof is lacking, since the method by which we have dealt with the number 2 in the first treatise does not permit of a broader application. There is indeed no lack of various methods, by means of which the proofs for special cases can be obtained, in particular those which pertain to the distribution of the quadratic residues between the complexes A and C; [however we will not be satisfied with this, because we are obliged to desire a general theory which encompasses every case.] Having already begun to consider this subject in the year 1805, we soon came to the conviction that *the natural source of a general theory was to be sought in an* **expansion of the field** *of arithmetic*, as we already indicated in article 1.

Namely, while higher arithmetic dealt only with whole real numbers in the questions heretofore treated, the theorems pertaining to the biquadratic residues only appeared in their entire simplicity and natural beauty, if *the field of arithmetic is also extended to the* ***imaginary*** *numbers*, so that without limit, numbers of the form $a+bi$ form the object itself, where, as usual, i denotes the imaginary magnitude $\sqrt{-1}$ and the indeterminates a, b denote all whole real numbers between $-\infty$ and $+\infty$. We will call these types of numbers **complex whole numbers**, indeed, so that the real [numbers] do not oppose the complex numbers, but are rather considered as a special case of them. *The present treatise will contain the elementary doctrine of complex magnitudes, as well as the first beginnings of the theory of biquadratic residues*, whose complete development we set as a task for ourselves in the following $*$) [1]

31.

First of all, we shall begin with a few *denominations*, whose introduction will facilitate a greater brevity and clarity.

The domain of complex numbers a+bi *contains:*

I. The real numbers, in which $b = 0$, and among these, depending on the nature of a
   1) zero,
   2) the positive numbers,
   3) the negative numbers;

II. The imaginary numbers, in which b is different from 0. we will again distinguish here
   1) the imaginary numbers without a real part, i.e. in which $a = 0$,
   2) the imaginary numbers with a real part, i.e. those in which neither b nor a is equal to zero.

If so desired, the former can be called pure imaginary numbers, the others mixed imaginary numbers. In *this theory* we use *four unities*: $+1$, -1, $+i$, $-i$, which should simply be called positive, negative, positive imaginary, negative imaginary unity.

[1] Only incidentally, we will at least remark in passing, that such an expansion of the field is particularly suited to biquadratic residues. The theory of cubic residues must, in a similar way, be founded upon a consideration of of numbers of the form $a+bh$, where h is an imaginary root of the equation $h^3 - 1 = 0$, say $h = -\frac{1}{2} + \sqrt{\frac{3}{4}} \cdot i$, and likewise, the theory of residues of higher powers requires the introduction of other imaginary magnitudes.

We will call the three products of a complex number with -1, $+i$, $-i$ its **associated** *numbers*. Thus, there will *always be four different numbers associated with one another*, with the exception of zero (which is associated with itself).

On the other hand, we will call those numbers which arise with the exchange of i with $-i$, **conjugates**. Thus, the imaginary numbers will thus *always consist of pairs of conjugate numbers*, while the real numbers are self conjugate, provided that it is desired to extend this denomination to these numbers.

We call the product of the complex number and that number conjugate to it a **norm** for each of them. Hence, the square of a real number is considered its norm.

Generally, there are eight numbers which are connected with one another, namely:

[insert table] we hereby see two quaternions of associated numbers and four pairs of conjugate numbers, and their common norm is $a^2 + b^2$. However, the eight numbers reduce to four different ones if $a = \pm b$, or one of the two numbers a, b is equal to 0.

From the given definitions, directly yield the following:

The product of the two conjugate numbers is the conjugate of the product of their conjugate numbers.

The same applies for the product of many factors as well as for the quotients.

The norm of the product of two complex numbers is equal to the product of the norms of those numbers.

This theorem also extends to products of arbitrarily many factors and quotients.

The norm of each complex number (with the exception of 0, which we tacitly exclude [hindenken] here for the most part) *is a postive number.*

Furthermore, our definition does not stand in the way of extending to fractions or irrational values of a, b; however, $a + bi$ *should then only be called a* **complex whole number** *if each of the two numbers* a, b *are whole*, and only then a rational number, if each of the two numbers a, b are rational.

32.

The algorithms of arithmetic operations with respect to complex numbers are generally known; division is reduced to multiplication via the introduction of the norm, since:

[insert equation].

The extraction of the square root is performed with aid of the formula:

[insert equation],

if b is a positive number, or with aid of the formula:

[insert equation],

if b is a negative number. It is not necessary for us to stop here and consider [aufzuhalten] to what advantage the transformation of the complex magnitude $a + bi$ into $r(cos\phi + i\ sin\phi)$ will serve in simplifying the calculation.

33.

We call a complex whole number which decomposes into two factors differing$*$)[2] from unity a **composite** *complex number*; however, a number which does not admit such a decomposition is called a *complex* **prime number**. Therefore, it follows directly from this that each composite real number is also a composite complex number. *On the other hand, a real prime number can be a composite complex number*, and will indeed apply to the number 2, and to all positive real numbers of the form $4n + 1$, (with the exception of the number 1), since these can be decomposed into two positive squares, as is generally known; e.g. $2 = (1 + i)(1 - i)$, $5 = (1 + 2i)(1 - 2i)$, $13 = (3 + 2i)(3 - 2i)$, $17 = (1 + 4i)(1 - 4i)$, etc.

However, positive real prime numbers of the form $4n + 3$ *are always complex prime numbers as well.* For if such a number $q = (a + bi)(\alpha + \beta i)$, then also $q = (a - bi)(\alpha - \beta i)$, and therefore $q^2 = (a^2 + b^2)(\alpha^2 + \beta^2)$; however, q^2 can only be decomposed into positive factors which are greater than 1 in a unique way, namely, into $q \cdot q$, such that $q = a^2 + b^2 = \alpha^2 + \beta^2$. However, this is absurd, since the sum of two squares can not be of the form $4n + 3$.

[2] or, what is the same, it is such factors whose norms are greater than unity.

The same denomination evidently applies to negative real numbers as to the positive, and the same applies to pure imaginary numbers.

Therefore, it only *remains to be shown, how prime numbers can be distinguished from composite numbers for mixed imaginary numbers*, and this will occur in the following theorem.

Theorem. *Each mixed whole imaginary number $a + bi$ is either a complex prime number or a composite number, depending upon whether its norm is a real prime number or a composite number.*

Proof. I. Since the norm of a composite complex number is always a composite number, than evidently a complex number, whose norm is a real prime number, must neccessarily be a complex prime number. This is the first part of the theorem.

II. If, however, the norm $a^2 + b^2$ is a composite whole number, then let p be a real positive prime number which goes into it. And now two cases are to be distinguished.

1. If p is of the form $4n + 3$, then it is known that $a^2 + b^2$ can only be divisible by p, if p divides a and b simultaneously, so that thus, $a + bi$ will be a composite number.

2. If p is not of the form $4n + 3$, then it can certainly be decomposed into two squares; hence, we set $\alpha^2 + \beta^2$, since

$$(a\alpha + b\beta)(a\alpha - b\beta) = a^2(\alpha^2 + \beta^2) - \beta^2(a^2 + b^2)$$

and hence, is divisible by p, then p will certainly divide one of the factors $a\alpha + b\beta$, $a\alpha - b\beta$, and since further,

$$(a\alpha + b\beta)^2 + (b\alpha - a\beta)^2 = (a\alpha - b\beta)^2 + (b\alpha + a\beta)^2 = (a^2 + b^2)(\alpha^2 + \beta^2)$$

and is consequently divisible by p^2, then evidently $b\alpha - a\beta$ in the former case, and $b\alpha + a\beta$ in the latter case must be divisible by p. Hence, in first case

$$\frac{a + bi}{\alpha + \beta i} = \frac{a\alpha + b\beta}{p} + \frac{b\alpha - a\beta}{p} i$$

however in the latter case

$$\frac{a + bi}{\alpha - \beta i} = \frac{a\alpha - b\beta}{p} + \frac{b\alpha + a\beta}{p} i$$

a whole complex number. Since consequently, the given number is divisible by either $\alpha + \beta i$, or by $\alpha - \beta i$, and according to the requirements, the norm of the quotient, namely $\frac{a^2+b^2}{p}$, differs from unity, it thus follows that $a + bi$ is a compound complex number in both cases. This is the second part of the theorem.

34.

Therefore *the totality of complex prime numbers will be completely exhausted in the four following classes:*

1. The four unities, $1, +i, -1, -i$, which however, whenever we deal with prime numbers, will for the most part be tacitly considered as excluded.

2. The number $1 + i$, with its three associated numbers $-1 + i$, $-1 - i$, $1 - i$.

3). the real positive prime numbers of the form $4n + 3$ with its three associated numbers.

4). the complex numbers, whose norms are real prime numbers of the form $4n + 1$ which are greater than unity. Indeed, each norm of this type corresponds to eight complex prime numbers and no more, since such a norm can only be decomposed into two squares in a unique way.

35.

Just as the real whole numbers are broken up into even and uneven numbers, and the former again into evenly even and unevenly even numbers, so a similarly essential difference is also represented for the complex numbers. Namely, *they are*

either not divisible by $1+i$, e.g. the numbers $a+bi$ where one of the numbers a, b is odd, the other even,

or divisible by $1+i$, *but not by 2,* if both of the numbers a, b are odd.

or divisible by 2, if both of the numbers a, b are even.

The numbers of the first class can fittingly be called **uneven**, *those of the second class* **half even**, *those of the third class* **even** *complex numbers.*

The product of multiple complex numbers is always uneven if all of the factors are uneven; it is half even if one factor is uneven and the remaining are uneven; however, it is even if among the factors, either at least two half even ones appear, or at least one is even.

The norm of every uneven complex number is of the form $4n+1$*; the norm of a half even number is of the form* $8n+2$*; finally, the norm of an even number is the product of a number of the form* $4n+1$ *and the number 4, or a higher power of 2.*

36.

Since the connection between every four associated complex numbers is analogous to the connection between two opposite real numbers (i.e. between two numbers which are considered as absolutely equal, but with opposite signs) Of these, the positive number generally tends to be correctly considered as a sort of primary number, and so the question arises, whether a similar distinction can be established between every set of four associated complex numbers and must be considered advantageous. In order to decide this question, it must be considered that the principle of distinction must be so consituted that the product of two numbers which qualify as a primary among their associates is itself always a primary number amoung its associated numbers. However, we soon convince ourselves that there is no such principle, provided that the distinction is not limited to whole numbers; indeed, a profitable distinction will even be limited only to the odd numbers. However, for this, the goal can be attained in two ways, namely

I. The product of two numbers $a+bi$, $a'+b'i$, which is so constituted that a, a' is of the form $4n+1$ and b, b' are even, will possess the same properties so that thus, the real part $\equiv 1 \pmod 4$, and the imaginary part will be even. And it is easily seen that among four associated uneven numbers, only one is contained under that form.

II. If the number $a+bi$ is so constituted that $a-1$ and b are either at the same time evenly even or at the same time unevenly even, then its product with a complex number of the same form, will have the same property, and it is easily seen that of every four associated uneven numbers, only one is contained under that form.

Of both of these approximately equally suitable principles, we will select the latter; namely, we will consider as the primary number among four associated uneven complex numbers, that which will be congruent to unity with respect to modulus $2+2i$. In such a way, we will be able to express many excellent theorems with greater brevity. Thus, for example, the complex prime numbers $-1+2i,\ -1-2i,\ +3+2i,\ +3-2i,\ +1+4i,\ +1-4i, \ldots$ are primary numbers, likewise, the real [numbers] $-3, -7, -11, -19, \ldots$, which obviously always have a negative sign. The number conjugate to an uneven complex primary number will likewise be a primary number.

For half even and even numbers in general, a distinction would be all too arbitrary and of too little use. From the associated numbers $1+i,\ 1-i\ -1+i,\ -1-i$ we can choose one above all the rest, however we will not extend such a distinction to composite numbers.

37.

If among the factors of a composite complex number, such appear which are themselves composite, and this is again decomposed into its factors, then evidently, prime factors will finally be arrived at, i.e. *every composite number is decomposable into prime factors.* If among these are found those which are not primary numbers, then the product of their associated primary numbers with $i, -1$ or $-i$ are substituted in their place. In this way, it arises that every composite complex M can be reduced to the form:

$$M = i^{\mu} A^{\alpha} B^{\beta} C^{\gamma} \ldots,$$

-

in such a way, that $A, B, C \ldots$ are different prime complex primary numbers, and $\mu = 0, 1, 2$ or 3. To such a decomposition the theorem applies that this can only occur in a unique way, a theorem which could admittedly appear clear in itself after superficial consideration, but which requires a proof in any event. To this the following theorem prepares the way.

Theorem. *The product $M = A^\alpha B^\beta C^\gamma \ldots$, in which $A, B, C, \ldots$ denote various prime complex primary numbers, is not divisible by any primary complex number which is not contained among $A, B, C, \ldots$*

Proof. Let P be a primary complex prime number which is not contained among $A, B, C, \ldots$, and let $p, a, b, c \ldots$ be the norms of the numbers $P, A, B, C \ldots$. From this it easily follows that the norm of the number M is equal to $a^\alpha b^\beta c^\gamma$ such that this number must be divisible by p, were M to be divisible by p. Since the individual norms are either real prime numbers (from the series 2,5,13,17,...) or, squares of real prime numbers (from the series 9,49,121,...), then it is immediately clear that the former can only occur if p is identical to any one of the norms $a, b, c, \ldots$; accordingly, we take $p = a$. However, since by hypothesis P and A are primary complex prime numbers different from one another, then it is easily seen that these [conditions] can only occur simultaneously if P and A are conjugate complex numbers, and consequently $p = a$ is an odd real prime number (not the square of a prime number); hence, we set $A = k + li$, $P = k - li$. According to this (by extending the concept and the notation of congruence to whole complex numbers), $A \equiv 2k \pmod{P}$, wherefrom it easily follows:

$$M \equiv 2^\alpha k^\alpha B^\beta C^\gamma \ldots \pmod{p}.$$

Thus, as soon as M is assumed to be divisible by P, then

$$2^\alpha k^\alpha B^\beta C^\gamma \ldots$$

will be divisible by P as well, and consequently the norm of this number, which is equal to

$$2^2 \alpha k^2 \alpha b^\beta c^\gamma \ldots$$

will be divisible by p as well. However, since 2 and k are themselves not divisible by p, then from this it follows that p must be identical to any one of the numbers $b, c \ldots$. For example, let $p = b$. However, we conclude from this that either $B = k + li$ or $B = k - li$, i.e. either $B = A$ or $B = P$, both of which are contrary to the hypothesis.

From this theorem another is very easily derived, that the decomposition into prime factors is possible only in a unique way, and indeed, appear as completely analogous to the conclusions which we have made use of in the *Disquisitiones Arithmeticae* (Article 16, c.f. pg. 7 above); it would therefore be superfluous for us to pause [aufzuhalten] here.

38.

We now proceed to *the congruence of numbers according to the complex modulus.* Upon entering this investigation, however, it is convenient to indicate the way in which the complex numbers could be imagined.

Just as every real magnitude can be represented by part of a straight line extended infinitely on both sides, taken from an arbitrary origin, and consequently by the other endpoint of that line, and measured according to an arbitrary segment taken as unity, in such a way that the points on one side of the origin represent the positive magnitudes, the points on the other side the negative magnitudes, so also each complex magnitude is represented by some point in an infinite plane in which a determined line serves as a representation of the real magnitudes, namely the complex magnitude $x + iy$ by a point whose abscissa is equal to x, and whose ordinate (taken as positive on one side of the line of abscissas, and negative on the other) is equal to y. In this way, it can be said that any complex number whatsoever measures the difference between the position of the point to which it belongs and the position of the origin, if the positive unit denotes an arbitrary but determined deflection [angle] from an arbitrary but determined direction, the negative unit just as great a deflection from the direction of opposite sign, and finally, the imaginary unit just as great a deflection from two directions proceeding perpendicularly from both sides.

In this way, the metaphysics of magnitudes which we call imaginary is placed in an outstanding light. If the origin is denoted by (0) and the two complex magnitudes m, m' are drawn through the points M, M' whose position is expressed in relation to the point (0), then the difference $m - m'$ is expressed as nothing other than the position of the point M in relation to the point M'; on the other hand, if the product mm' represents the position of the point N in relation to (0), it will be easily perceived that this position will be just as determined by the position of point M in relation to (0), as the position of the point M' will be determined by the position of same point which corresponds to the positive unit, so that it is not unsuitable to say that the positions of the complex magnitudes corresponding to the points mm', m, 1 form a proportion. However we reserve a more detailed treatment of the subject for another occasion. The difficulty which is believed to surround the theory of imaginary magnitudes is based, for the most part, upon inappropriate denominations (they have even been given [belegen] the discordant name of impossible magnitudes by some). Were the positive magnitudes to have been named direct, the negative inverse, and the imaginary lateral magnitudes, proceeding from the representation which is presented by manifolds of two dimensions (as they would be regarded in the greatest purity for spacial representations [intuitionibus]), then simplicity instead of confusion, clarity instead of obscurity would have been the result.

39.

The discussion of the previous article pertains to continuous complex magnitudes; in arithmetic, which is only concerned with whole numbers, the schema of complex numbers is a system of equidistant points which are laid on equidistant straight lines such that the infinite plane is decomposed into infinitely many squares. Every number which is divisible by a complex number $a + bi = m$ will likewise form infinitely many squares, whose sides are equal to $\sqrt{a^2 + b^2}$ or whose area is equal to $a^2 + b^2$; the latter squares will have an inclined position to the former if neither of the two numbers a, b are equal to zero. Every number which is not divisible with respect to modulus m will correspond to a point, which lies either within such a square, or on the boundary line of two squares; the latter case, however, can only occur if a, b have a common divisor; further, it is clear that numbers congruent relative to modulus m, occupy congruent positions in their [respective] squares. From this it easily follows that if numbers lying inside of a determined square are collected so that all those which lie, for instance, on two adjacent sides of the square, and finally, to add to this the number divisible by m, a complete system of incongruent residues with respect to modulus m is obtained, i.e. that every whole number must be congruent to one, and only one of them. It would also not be difficult to show that the quantity of these residues equals the norm of the modulus, namely, is equal to $a^2 + b^2$. However, it appears advisable to prove this very important theorem in another purely arithmetic way.

40.

Theorem. *Relative to a given complex modulus $m = a + bi$, whose norm is $a^2 + b^2 = p$ and for which a, b are relatively prime numbers, every whole complex number whatsoever will be congruent to one residue in the series $0, 1, 2, 3, \ldots, p - 1$ and not to any other.*

Proof. I. If α, β are whole numbers, for which $\alpha a + \beta b = 1$, then:

$$i = \alpha b - \beta a + m\beta + \alpha i.$$

Hence, if a whole complex number $A + Bi$ is given, we have:

$$A + Bi = A + (\alpha b - \beta a)B + m(\beta B + \alpha Bi).$$

Therefore, if by h is denoted the least positive residue of the number $A + (\alpha b - \beta a)B$ with respect to modulus p, and:

$$A + (\alpha b - \beta a)B \text{ is set } = h + kp = h + m(ak - bki),$$

thus:

$$A + Bi = h + m[\beta B + ak + (\alpha B - bk)i]$$

or:

$$A + Bi \equiv h \pmod{m}.$$

With that, the first part of the theorem is proven.

II. If the same complex number is congruent to two real numbers h, h' relative to modulus m, then these will also be congruent to each other. If we set $h - h' = m(c + di)$, then:

$$(h - h')(a - bi) = p(c + di)$$

and hence:

$$(h - h')a = pc,\ (h - h')b = -pd,$$

and further, on account of $a\alpha + b\beta = 1$:

$$h - h' = p(c\alpha - d\beta),\ \text{i.e. } h \equiv h' \pmod{p}.$$

Consequently, insofar as they are unequal, h and h' cannot both simultaneously be contained in the complex of numbers $0, 1, 2, 3, \ldots, p - 1$. With that, the second part of the theorem is proven.

41.

Theorem. *Relative to the complex modulus $m = a + bi$, whose norm $a^2 + b^2 = p$ and for which a, b are not prime relative to one another, but have a greatest common divisor λ (which is assumed to be positive), every complex number whatsoever is congruent to a residue $x + iy$ of such quality, that x is any one of the numbers $0, 1, 2, 3, \ldots, \frac{p}{\lambda} - 1$ and y is any one of the numbers $0, 1, 2, 3, \ldots, \lambda - 1$, and indeed only a single one among all p residues exhibits such a form.*

Proof. I. If α, β are assumed in such a way that $\alpha a + \beta b = \lambda$, then:

$$\lambda i = \alpha b - \beta a + m(\beta + \alpha i).$$

Now, if $A + Bi$ is the given complex number, and further y is the least positive residue of B relative to modulus λ and x is the least positive residue of $A + (\alpha b - \beta a)\frac{B-y}{\lambda}$ relative to the modulus $\frac{p}{\lambda}$, and:

$$A + (\alpha b - \beta a)\frac{B - y}{\lambda} = x + \frac{p}{\lambda} \cdot k,$$

then

$$\begin{aligned} A + Bi - (x + yi) &= \frac{p}{\lambda} \cdot k + (B - y)i - (\alpha b - \beta a)\frac{B - y}{\lambda} \\ &= \frac{p}{\lambda} \cdot k + \frac{B - y}{\lambda} \cdot m(\beta + \alpha i) \\ &= (\frac{a}{\lambda} - \frac{b}{\lambda}i)km + \frac{B - y}{\lambda}(\beta + \alpha i)m, \end{aligned}$$

i.e. is divisible by m, or $A + Bi \equiv x + yi \pmod{m}$. With that, the first part of the theorem is proven.

II. If we assume that, relative to modulus m, the same complex number were congruent to two numbers $x + yi$ and $x' + y'i$, then these same numbers are congruent to each other relative to modulus m. Thus, all the more will they be congruent relative to the modulus λ and hence, $y \equiv y' \pmod{\lambda}$. If it is assumed that of the numbers y, y' are contained among the numbers $0, 1, 2, 3, \ldots, \lambda - 1$, then, necessarily, y must $= y'$. However, in this way x will also be $\equiv x' \pmod{m}$, i.e. $x - x'$ will be divisible by m and hence, $\frac{x-x'}{\lambda}$ will be a whole number divisible by $\frac{a}{\lambda} + \frac{b}{\lambda}i$, or, in other words:

$$\frac{x - x'}{\lambda} \equiv 0 \pmod{\frac{a}{\lambda} + \frac{b}{\lambda}i}.$$

However, it follows from this that, since $\frac{a}{\lambda}$, $\frac{b}{\lambda}$ are prime relative to each other, according to the second part of the previous theorem, $\frac{x-x'}{\lambda}$ is also divisible by the norm of the number $\frac{a}{\lambda} + \frac{b}{\lambda}i$, i.e. by the number $\frac{p}{\lambda^2}$, and consequently, $x - x'$ is also divisible by $\frac{p}{\lambda}$. Hence, if it is assumed that both of the numbers x, x' belong to the complex of numbers $0, 1, 2, 3, \ldots, \frac{p}{\lambda} - 1$, necessarily $x = x'$ or, the residues $x + yi$, $x' + y'i$ will be identical. With that, the second part of the theorem is proven.

Moreover it is immediately clear, that included in this is the case, where the modulus is a real number, thus $b = 0$ and consequently $\lambda = \pm a$, likewise the case where the modulus is a pure imaginary number, thus $a = 0$ and consequently $\lambda = \pm b$. In both cases, $\frac{p}{\lambda} = \lambda$.

42.

Hence, if one refers all complex numbers that are congruent to each other relative to a given modulus to the same class, incongruent ones to different classes, then p classes will be given in general, which exhausts the totality of the whole numbers, if p represents the norm of the modulus. The complex of just as many numbers taken from the individual classes will represent a complete system of incongruent residues, as we had determined in articles 40 and 41. And, indeed, in those systems, the choice of those residues which represent, so to speak, the classes in question is based on the principle that, in each class, such a residue $x+yi$ should be found for which y has the smallest value, and among all those in which the same least value of y appears, that for which the value of x is the smallest, excluding however negative values for x as well as for y. For other purposes, however, it will be convenient to use other principles, and indeed we will note in particular the method in which such residue is taken, which, when divided by the modulus, presents the simplest quotients. It is manifest that, if $\alpha + \beta i$, $\alpha' + \beta' i$, $\alpha'' + \beta'' i \ldots$ are the quotients, which arise from the division of congruent numbers by the modulus,The differences of the magnitudes $\alpha, \alpha', \alpha'', \ldots$ among themselves as well as the differences between the magnitudes $\beta, \beta', \beta'', \ldots$ will be whole numbers, and it is clear that a residue always exists, for which α and β lie between the limits 0 and 1, the former limit is included, the latter excluded; we will simply call such a residue the **least residue**. If it is preferred, in place of those limits can be adopted $\frac{-1}{2}$ and $\frac{+1}{2}$ (the former included, the latter excluded). We call one of the the residues corresponding to these limits the **absolute least residue**.

In reference to these least residues, the following problems present themselves.

43.

The least residue of a civen complex number $A + Bi$ with respect to modulus $a + bi$, whose norm is equal to p, is found in the following way.

If $x + yi$ is the sought least residue, then $(x + yi)(a - bi)$ will be the least residue of the product $(A + Bi)(a - bi)$ with respect to modulus $(a + bi)(a - bi)$, i.e. with respect to modulus p. Thus, set:

$$aA + bB = Fp + f,\ aB - bA = Gp + g,$$

so that f, g are the least residues of the numbers $aA + bB, aB - bA$ with respect to modulus p, then:

$$x + yi = \frac{f + gi}{a - bi}$$

or:

$$x = \frac{af - bg}{p} = A - aF + bG$$

$$y = \frac{ag + bf}{p} = B - aG - bF.$$

It is manifest that the least residues f, g must be taken between the limits 0 and $p - 1$ or between the limits $-\frac{1}{2}p$ and $+\frac{1}{2}p$, according as whether simply the least residue or the absolute least residue of the complex number is desired.

44.

The construction of the complete system of least residues for a given modulus can be carried out in several ways. The first method proceeds in this way: first, those limits are determined, between which the real terms must lie, and then, for the individual values lying between these limits, those limits for the imaginary parts must be assigned. For a least residue $x+yi$ of a modulus $a+bi$, the general criterion exists that $ax + by = \xi$ as well as $ay - bx = \eta$ lies between the limits 0 and $a^2 + b^2$, if it concerns

simply the least residues, or, it lies between the limits $-\frac{1}{2}(a^2+b^2)$ and $+\frac{1}{2}(a^2+b^2)$ if the absolute least residue is desired, whereby the second limit is excluded. The distinction of the cases, which determine the variety of signs of the numbers a, b, requires special rules, whose development requires little difficulty, which however, we here forego: let it suffice to have the nature of the procedure set forth with a single **example**.

For the modulus $5+2i$, the simple least residue $x+yi$ must be so constituted, that $5x+2y=\xi$ as well as $5y-2x=\eta$ are equal to some one of the numbers $0, 1, 2, 3, \ldots, 28$. The equation $29x = 5\xi - 2\eta$ shows that the positive value of x can not be greater than $\frac{5\cdot 28}{29}$, and the negative, disregarding the sign, can not be greater than $\frac{2\cdot 28}{29}$. Hence, all the permissible values for x are as follows: $-1, 0, 1, 2, 3, 4$. For $x=-1$, $2y$ must be equal to one of the values $5, 6, 7, \ldots, 33$, and $5y$ must be equal to one of the values $-2, -1, 0, 1, \ldots, 26$; therefore, the least value for y must be equal to $+3$, and the greatest equal to $+5$. If the remaining values are similarly examined, then the following scheme of all least residues arises:

x	y
-1	3, 4, 5
0	0, 1, 2, 3, 4, 5
$+1$	1, 2, 3, 4, 5, 6
$+2$	1, 2, 3, 4, 5, 6
$+3$	2, 3, 4, 5, 6
$+4$	2, 3, 4.

In a similar manner, the absolute least residues ξ and η must be equal to one of the numbers $-14, -13, -12, \ldots, +14$; accordingly, $29x$ cannot lie outside the limits $-7\cdot 14$ and $+7\cdot 14$, and hence x must be equal to one of the numbers $-3, -2, -1, 0, 1, 2, 3$. For $x=-3$, $2y = \xi - 5x = \xi + 15$ equals one of the numbers $1, 2, 3, \ldots, 29$, but $5y = \eta + 2x = \eta - 6$ one of the numbers $-20, -19, -18, \ldots, +8$. Hence, this gives for y the single value $+1$. If the remaining values are examined in the same fashion, then we have the scheme of all absolute least residues:

x	y
-3	$+1$,
-2	-2, -1, 0, $+1$, $+2$,
-1	-3, -2, -1, 0, $+1$, $+2$
0	-2, -1, 0, $+1$, $+2$,
$+1$	-2, -1, 0, $+1$, $+2$, $+3$
$+2$	-2, -1, 0, $+1$, $+2$
$+3$	-1.

45.

By the application of the second method, it is convenient to distinguish between two cases.

In the first case, where a and b do not have a common divisor, let $\alpha a + \beta b$ be set $= 1$, and let k be the least positive residue of $\beta a - \alpha b$ relative to modulus p. Hence, the identical equations

$$a(\beta a - \alpha b) = \beta p - b(\alpha a + \beta b),\ b(\beta a - \alpha b) = -\alpha p + a(\alpha a + \beta b),$$

show that $ak \equiv -b,\ bk \equiv a \pmod{p}$. Therefore, setting as above $ax + by = \xi,\ ay - bx = \eta$, then $\eta \equiv k\xi,\ \xi \equiv -k\eta \pmod{p}$. Consequently, we obtain all numbers $\xi + \eta i$, which correspond to the simple least residues $x + yi$, if either the values $0, 1, 2, 3, \ldots, p-1$ are taken for ξ and the least positive residue for the product $k\xi$ is taken relative to the modulus p, or conversely, those values are taken for η and the least residue of the product $-k\eta$ is taken for ξ. Then, from the individual $\xi + \eta i$, the corresponding $x + yi$ is found according to the formula:

$$x + yi = \frac{\xi + \eta i}{a - bi} = \frac{a\xi - b\eta}{p} + \frac{a\eta + b\xi}{p} i.$$

Furthermore it is clear, that η, while ξ increases by a unit, incurs either the increment k or the decrement $p-k$, and hence $x+yi$ incurs a change of

$$\text{either} \qquad \frac{a-kb}{p}+\frac{ak+b}{p}i$$

$$\text{or} \quad \frac{a-kb}{p}+b+\left(\frac{ak+b}{p}-a\right)i,$$

which observation serves to facilitate the construction [of the table].

Finally, if the absolute least residue $x+yi$ is desired, these precepts only need to change in that, now, the values within the limits $-\frac{1}{2}p$ and $+\frac{1}{2}p$ are given sequentially to ξ, while for η, the absolute least residue of the product $k\xi$ must be taken. Behold, the conspectus of minimum residues for modulus $5+2i$.

Simple Least Residues.

$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$
0	0	$10+25i$	$+5i$	$20+21i$	$+2+5i$
$1+17i$	$-1+3i$	$11+13i$	$+1+3i$	$21+9i$	$+3+3i$
$2+5i$	$+i$	$12+i$	$+2+i$	$22+26i$	$+2+6i$
$3+22i$	$-1+4i$	$13+18i$	$+1+4i$	$23+14i$	$+3+4i$
$4+10i$	$+2i$	$14+6i$	$+2+2i$	$24+2i$	$+4+2i$
$5+27i$	$-1+5i$	$15+23i$	$+1+5i$	$25+19i$	$+3+5i$
$6+15i$	$+3i$	$16+11i$	$+2+3i$	$26+7i$	$+4+3i$
$7+3i$	$+1+i$	$17+28i$	$+1+6i$	$27+24i$	$+3+6i$
$8+20i$	$+4i$	$18+16i$	$+2+4i$	$28+12i$	$+4+4i$
$9+8i$	$+1+2i$	$19+4i$	$+3+2i$		

Absolute Least Residues.

$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$	$\xi+\eta i$	$x+yi$
$-14-6i$	$-2-2i$	$-4-10i$	$-2i$	$+5-2i$	$+1$
$-13+11i$	$-3+i$	$-3+7i$	$-1+i$	$+6-14i$	$+2-2i$
$-12-i$	$-2-i$	$-2-5i$	$-i$	$+7+3i$	$+1+i$
$-11-13i$	$-1-3i$	$-1+12i$	$-1+2i$	$+8-9i$	$+2-i$
$-10+4i$	-2	0	0	$+9+8i$	$+1+2i$
$-9-8i$	$-1-2i$	$+1-12i$	$+1-2i$	$+10-4i$	$+2$
$-8+9i$	$-2+i$	$+2+5i$	$+i$	$+11+13i$	$+1+3i$
$-7-3i$	$-1-i$	$+3-7i$	$+1-i$	$+12+i$	$+2+i$
$-6+14i$	$-2+2i$	$+4+10i$	$+2i$	$+13-11i$	$+3-i$
$-5+2i$	-1			$+14+6i$	$+2+2i$

The second case, in which a, b are not relatively prime, can easily lead back to the previous case. Let λ be the greatest common divisor of the numbers a, b, and $a=\lambda a', b=\lambda b'$. Furthermore, the undetermined F denotes the least residue for the modulus λ, as long as the same will be considered a complex number, i.e. the undetermined F represents such a number $x+yi$, which lies either between the limits 0 and λ or between the limits $-\frac{1}{2}\lambda$ and $+\frac{1}{2}\lambda$ (depending on whether we are dealing with the simple or the absolute least residue); finally, the undetermined F' denotes the least residue for the modulus $a'+b'i$. Then, the undetermined $(a'+b'i)F+F'$ is the least residue for modulus $a+bi$, and the complete system of this residue is obtained if all the F are combined with all the F'.

46.

Two complex numbers will be called relatively ***prime***, if they admit no common divisor other than unity; however, whenever such common divisors are available, then that one whose norm is the greatest will be called the greatest common divisor.

If the two proposed numbers can be resolved into prime factors, then the determination of the greatest common divisor will be carried out in an exact way, as with the real numbers (*Disquisitiones Arithmeticae*, Article 18, cf. p. 8). Simultaneously, it becomes clear that the greatest common divisor found in this way must be comprised of all the common divisors of two proposed numbers. Since it is already self evident that the three associated numbers will also be common divisors, then the four, and no more, must always be called greatest common divisors, and the norm of this will be a multiple of the norms of the other common divisors.

If the two proposed numbers cannot be resolved into simple factors, then, with the aid of an algorithm similar to that we use with real numbers, the greatest common divisor is found. Let m, m' be the two proposed numbers and through repeated division forms the series $m'', m''', \ldots$ such that m'' is the absolute least residue of m relative to modulus m', m''' is the absolute least residue of m' relative to modulus m'', etc. If the norms of the numbers $m,\ m',\ m'',\ m''', \ldots$ are respectively denoted $p,\ p',\ p'',\ p''', \ldots$, then $\frac{p''}{p'}$ is the norm of the quotient $\frac{m''}{m'}$, and, by the definition of the absolute least residue, is certainly not greater than $\frac{1}{2}$; the same holds for $\frac{p'''}{p''}$, etc. Consequently, the positive real whole numbers $p',\ p'',\ p''', \ldots$ become a constantly decreasing series, finally, the term 0 is necessarily arrived at, or, what is the same, the series $m,\ m',\ m'',\ m''', \ldots$ finally arrives at a term into which the preceding term goes without a divisor. Let this term be $m^{(n+1)}$ and we will set:

$$\begin{array}{lcll} m & = & km' & + \ m'' \\ m' & = & k'm'' & + \ m''' \\ m'' & = & k''m''' & + \ m'''' \\ \ldots\ldots\ldots\ldots & & & \text{up to} \\ m^{(n)} & = & k^{(n)}m^{(n+1)}. & \end{array}$$

Passing through this series of equations in inverse order, it arises that $m^{(n+1)}$ divides into each of the individual preceding terms, $m^{(n)}, \ldots,\ m'',\ m',\ m$. However, passing through the same in direct order, it is manifest that each common divisor of the numbers $m,\ m'$ also divides each of the following ones. The former conclusion teaches, that $m^{(n+1)}$ is a common divisor of the numbers $m,\ m'$, but the latter, that this divisor is the greatest.

Moreover, whenever the last residue $m^{(n+1)}$ is equal to one of the four unities $1,\ -1,\ i,\ -i$, then this indicates that m and m' are relatively prime.

47.

If the equations of the previous article, with the exception of the last, are combined with one another in such a way, that $m'',\ m''',\ m'''', \ldots,\ m^{(n)}$ are eliminated, then results an equation of the form:

$$m^{(n+1)} = hm + h'm',$$

where h and h' are whole numbers and indeed, if the nomenclature in the "*Disquisitiones Arithmeticae*," article 27 (cf. p. 12), is made use of, then:

equations

where the top or bottom signs are assigned according as n is even or odd. This theorem we state thus:

The greatest common divisor of two complex numbers $m,\ m'$ can be brought to the form $hm + h'm'$ in such a way that h and h' are whole numbers.

Namely, it is manifest that this applies not only to that greatest common divisor to which the algorithm in the previous article led, but also to the three associated with it, for which we must take either $hi,\ h'i$, or $-h,\ -h'$, or $-hi,\ -h'i$ in place of the coefficients h, h'.

Hence, whenever the numbers $m,\ m'$ are prime relative to each other, the equation

$$1 = hm + h'm'$$

can be satisfied exactly.

For example, let the numbers $31 + 6i = m,\ 11 - 20i = m'$ be given. Here, we find:

$$\begin{array}{llll} k &= & i, & m'' = + 11 - 5i \\ k' &= + 1 - i, & m''' &= + 5 - 4i \\ k'' &= + 2, & m'''' &= + 1 + 3i \\ k''' &= - 1\ 2i, & m''''' &= \quad + i \\ k'''' &= + 3 - i, & & \end{array}$$

and hence:

$$[k',\ k'',\ k'''] = -6 - 5i \tag{1}$$
$$[k,\ k',\ k'',\ k'''] = +4 - 10i, \tag{2}$$
$$\tag{3}$$

and hence:

$$m''''' = i = (6 + 5i)m + (4 - 10i)m',$$

and further:

$$1 = (5 - 6i)m + (-10 - 4i)m',$$

which equations can be easily confirmed through actual calculation.

48.

By the proceeding, everything which is required for the theory of congruences of the first degree in the arithmetic of complex numbers was prepared; however, since it is not essentially different from that which applies to the arithmetic of real numbers, and this has been thouroughly presented in the "*Disquisitiones Arithmeticae*," then it will be sufficient if here we only attach the main points.

I. The congruence $mt \equiv 1 \pmod{m'}$ is equivalent to the indeterminate equation $mt + m'u = 1$, and this is satisfied by the values $t = h,\ u = h'$, then its solution will be generally represented by $t \equiv h \pmod{m'}$. The condition for solvability, however, is that the modulus m' can have no common divisor with the coefficient m.

II. The solution to the congruence $ax + b \equiv c \pmod{M}$ in the cases where a and M are relatively prime, depends on the solution of the following:

$$at \equiv 1 \pmod{M};$$

if this is satisfied by $t = h$, then the general solution of the former is contained in the formula:

$$x \equiv (c - b)h \pmod{M}$$

III. The congruence $ax + b \equiv c \pmod{M}$ in the case where a and M have a common divisor λ, is equivalent to the following:

$$\frac{a}{\lambda}x \equiv \frac{c - b}{\lambda} \pmod{\frac{M}{\lambda}}$$

Hence, whenever the greatest common divisor of the numbers a and M is taken for λ, the solution of the given equation is reduced to the preceding case, and it is clear, that the necessary and sufficient conditions for the solvability of the congruence, is that λ also divide the difference $c - b$.

49.

What we have touched upon so far is only elementary, however, because of its coherence, we should not leave it out. In deeper investigations, the arithmetic of complex numbers is similar to the arithmetic of real numbers, in that the theorems become simpler and more elegant, if only such moduli that are prime numbers are allowed; in truth, the extension of the same to composite moduli is in most cases more tedious than difficult, and requires more labor than art. On that basis, the discussion shall be primarily on prime number moduli in what follows.

50.

If X denotes a function of the indeterminate x of the form:

$$Ax^n + Bx^{n-1} + Cx^{n-2} + \ldots + Mx + N,$$

where n is a real positive whole number, $A, B, C, \ldots$ are real or imaginary whole numbers, and if m is a whole complex number, then we will also call here the **root** *of the congruence* $X \equiv 0 \pmod{m}$ each arbitrary whole number which, substituted for x, produces a value for X divisible by the modulus m. We will not consider as different those solutions by roots which are congruent relative to the modulus.

If the modulus is a prime number, then such a congruence of the order n can also not have more than n different solutions. If α denotes each determined (complex) whole number, then X can be reduced to an indeterminate of the form $X + (x - \alpha)X' + h$ by means of division by $x - \alpha$, such that h is a determined whole number and X' is a function of the order $n-1$ with integral coefficients. Now, if α is a root of the congruence $X \equiv 0 \pmod{m}$, then it is manifest that h is divisible by m, in other words, for each value of x the congruence will be had: $X \equiv (x - \alpha)X' \pmod{m}$.

Likewise, if β denotes a determined whole number, X' is reduced to the form: $(x-\beta)X'' + h'$, where X'' is a function of the order $(n-2)$ with integral coefficients. However, if it is assumed that β is a root of the congruence $X \equiv 0$, then it must also satisfy the congruence $(\beta - \alpha)X' \equiv 0$, as well as [the congruence] $X' \equiv 0$, so long as the roots α, β are incongruent, from which we conclude that h' must be divisible by m, or the indeterminate X must be $\equiv (x-\alpha)(x-\beta)X'' \pmod{m}$.

In an analogous way, if a third root γ is introduced which is incongruent to the first two, we obtain $X \equiv (x-\alpha)(x-\beta)(x-\gamma)X'''$, such that X''' is a function of the order $n-3$ with integral coefficients. In the same way, this can be carried further, and at the same time it is clear that the coefficient in the highest term in the single function is equal to A, which may not be assumed as divisible by m, since otherwise the congruence $X \equiv 0$ would then actually be referred to a lower order. Hence there are n incongruent roots, namely $\alpha, \beta, \gamma, \ldots, \nu$, then we have the indeterminate:

$$X = A(x-\alpha)(x-\beta)(x-\gamma)\ldots(x-\nu) \pmod{m};$$

consequently, the substitution of a new value for X, incongruent with each of the magnitudes $\alpha, \beta, \gamma, \ldots, \nu$, would surely yield a value not divisible by m, from which the truth of our theorem automatically follows.

Moreover, this proof essentially agrees overall with that which we had imparted in the "*Disquisitiones Arithmeticae*" article 43 (c.f. pg. 27 above), and whose individual points we apply for real as well as for complex numbers.

51.

That which has been imparted in the third section of the "*Disquisitiones Arithmeticae*" pertaining to the residues of powers, applies for the most part to the arithmetic of complex numbers with only minor changes; and indeed, even the proofs of the theorems could be retained in most cases. However, in order to leave nothing out, we wish to put forward the main theorems, established with concise proofs, where the modulus is always considered as a prime number.

Theorem. *If k denotes a whole number which is not divisible by modulus m, whose norm is equal to p, then $k^p - 1 \equiv 1 \pmod{m}$.*

Proof. Let $a, b, c, \ldots$ form a complete system of incongruent residues of modulus m, however, so that the residue which is divisible by m is omitted, and therefore the quantity of those numbers whose complex we denote by C is equal to $p-1$. Further, let C' be the complex of the products ka, kb, kc, ... None of these products will be divisible by m by hypothesis, thus they will each have a single residue congruent to themselves in complex C, thus $ak \equiv a', bk \equiv b', ck \equiv c', \ldots \pmod{m}$ can be set in such a way that the numbers $a', b', c', \ldots$ will appear in complex C. We denote the complex of the numbers $a', b', c', \ldots$ by C''. Further, let P, P', P'' be the product of the individual numbers of the complex C, C', C'', or:

$$P = abc\ldots$$

$$P' = k^p - 1abc\ldots = k^p - 1P$$
$$P'' = a'b'c'\ldots$$

Since the numbers of the complex C are sequentially congruent to the numbers of the complex C', then $P'' \equiv P'$ or $P'' \equiv k^p - 1P$. Since, however, it is easily seen that any two numbers of the complex C'' are incongruent with one another, and therefore all are different from one another, then neccessarily, the numbers of the complex C'' entirely agree, except for order, with the numbers of the complex C, and therefore $P'' = P$. Therefore $(k^p - 1 - 1)P$ is a number divisible by m, whereby it neccessarily follows that since m is a prime number which cannot divide the individual factors of P, $k^p - 1 - 1$ must neccessarily be divisible by m.

52.

Theorem. *If k denotes a whole number not divisible by m as in the preceding article, and t the smallest exponent (except for 0), for which $k^t \equiv 1 \pmod{m}$, then t is a divisor of every other exponent u, for which $k^u \equiv 1 \pmod{m}$.*

Proof. If t were not a divisor of u, then let gt be the next multiple of t larger than u, and hence, $gt - u$ will be a whole positive number smaller than t. From $k^t \equiv 1$, $k^u \equiv 1$ it follows that $0 \equiv k^g t - k^u \equiv k^u(k^g t - u - 1)$ and hence $k^g t - u \equiv 1$, i.e. k can be given as an exponent less than t, which is congruent to 1, contrary to the hypothesis.

It follows from this as a *corollary that t certainly divides $p - 1$.*

Such numbers k for which $t = p - 1$ we will also call **primitive** *roots* of the modulus m. *We will now show that these actually exist.*

53.

The number $p - 1$ is decomposed into its prime factors such that:

$$p - 1 = a^\alpha b^\beta c\gamma\ldots,$$

where $a, b, c, \ldots$ *denote positive real numbers which are different from one another. Further, let $A, B, C, \ldots$ be whole (complex) numbers not divisible by m, which do* ***not*** *sufficiently yield the congruences*

$$x^{\frac{p-1}{a}} \equiv 1,\ x^{\frac{p-1}{b}} \equiv 1,\ x^{\frac{p-1}{c}} \equiv 1,\ \ldots$$

respectively, according to modulus m; that that such numbers exist is apparent from article 50 . Finally, let h be congruent to the product

$$A^{\frac{p-1}{a^\alpha}} \cdot B^{\frac{p-1}{b^\beta}} \cdot C^{\frac{p-1}{c^\gamma}} \ldots.$$

relative to modulus m. Then I maintain, that h is a primitive root.

Proof. If t denotes the exponent of the lowest power h^t congruent to unity, then t is a divisor of $p-1$ or in other words, $\frac{p-1}{t}$ is a whole number, larger than unity, if h were not a primitive root. Evidently, the real prime factors of these whole numbers are found among the numbers $a, b, c, \ldots$. Therefore we assume (which is permitted), that $\frac{p-1}{t}$ is divisible by a, and we set $p - 1 = atu$. Therefore, since $h^t \equiv 1$, then also $h^t u \equiv 1$, or in other words

$$A^{\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \cdot B^{\frac{p-1}{b^\beta}\cdot\frac{p-1}{a}} \cdot C^{\frac{p-1}{c^\gamma}\cdot\frac{p-1}{a}} \ldots. \equiv 1.$$

However, $\frac{p-1}{ab^\beta}$ is evidently a whole number, and consequently

$$B^{\frac{p-1}{b^\beta}\cdot\frac{p-1}{a}} = (B^{p-1})^{\frac{p-1}{ab^\beta}} \equiv 1;$$

likewise:

$$C^{\frac{p-1}{c^\gamma}\cdot\frac{p-1}{c}} \equiv 1$$

etc. Consequently:

$$A^{\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \equiv 1.$$

Now a positive whole number λ is determined in such a way that

$$\lambda b^\beta c^\gamma \ldots . \equiv 1 \pmod{a}$$

which is possible, since the prime number a does not go into the number $b^\beta c^\gamma \ldots$, and $\lambda b^\beta c^\gamma \ldots$ is set $= 1 + a\mu$. Then evidently: $A^{\lambda\cdot\frac{p-1}{a^\alpha}} \equiv 1$, or, since $\lambda \cdot \frac{p-1}{a^\alpha} \cdot \frac{p-1}{a} = (1+a\mu)\frac{p-1}{a} = (p-1)\mu + \frac{p-1}{a}$:

$$A^{(p-1)\mu} \cdot A^{\frac{p-1}{a}} \equiv 1,$$

and from this it follows, since $A^{(p-1)\mu} \equiv 1$, then also $A^{\frac{p-1}{a}} \equiv 1$, which is contrary to the hypothesis. Consequently, the assumption that t is a submultiple of $p-1$ cannot exist, and consequently, h is neccessarily a primitive root.

54.

If h denotes a primitive root for modulus m, whose norm is equal to p, then the terms of the series

$$1, h, h^2, h^3, \ldots, h^{p-2}$$

will be incongruent to one another, from which it follows easily, that every whole number not divisible by the modulus must be congruent to one of those numbers or that that series represents a complete system of incongruent residues with the exception of zero. *The exponent of that power which is congruent to a given number can be called the* ***index*** *of the number, if* h *in considered the* ***base***. We give here a few examples, where beside each index we have placed the absolute least residue.

First Example

$$m = 5 + 4i, p = 41, h = 1 + 2i$$

Index	Residue	Index	Residue	Index	Residue	Index	Residue	Index	Residue
0	$+1$	8	-4	16	$-2+2i$	24	$+2i$	32	$+1+i$
1	$+1+2i$	9	$-3+i$	17	$-1+2i$	25	$-3i$	33	$+1+3i$
2	$+1-i$	10	$-i$	18	$+4i$	26	$+2+2i$	34	$+2$
3	$+3+i$	11	$+2-i$	19	$+1+3i$	27	$+2+i$	35	-3
4	$-2i$	12	$-1-i$	20	-1	28	$+4$	36	$+2-2i$
5	$+3i$	13	$+1-3i$	21	$-1-2i$	29	$+3-i$	37	$+1-2i$
6	$-2-2i$	14	-2	22	$-1+i$	30	$+i$	38	$-4i$
7	$-2-i$	15	$+3$	23	$-3-i$	31	$-2+i$	39	$-1-3i$

Second Example

$$m = 7,\ p = 49,\ h = 1 + 2i$$

Index	Residue	Index	Residue	Index	Residue	Index	Residue	Index	Residue
0	$+1$	10	$-1-i$	20	$+2i$	30	$+2-2i$		
1	$+1+2i$	11	$+1-3i$	21	$+3+2i$	31	$-1+2i$	40	$+3$
2	$-3-3i$	12	$-i$	22	$-1+i$	32	$+2$	41	$+3-i$
3	$+3-2i$	13	$+2-i$	23	$-3-i$	33	$+2-3i$	42	$-2-2i$
4	$3\ i$	14	$-3+3i$	24	-1	34	$+1+i$	43	$+2+i$
5	$-1-3i$	15	$-2-3i$	25	$-1-2i$	35	$-1+3i$	44	$-2i$
6	$-2+2i$	16	-3	26	$+3+3i$	36	$+i$	45	$-3-2i$
7	$+1-2i$	17	$-3+i$	27	$-3+2i$	37	$-2+i$	46	$+1-i$
8	-2	18	$+2+2i$	28	$+3i$	38	$+3-3i$	47	$+3+i$
9	$-2+3i$	19	$-2-i$	29	$+1+3i$	39	$+2+3i$		

55.

We add a few remarks concerning primitive roots and the algorithm of the indices, ommitting the proofs on account of their simplicity. I. In a given system, indices congruent with respect to modulus $(p-1)$ correspond to residues congruent with respect to modulus m and $vice-versa$. II. Residues which correspond to indices which are prime with respect to $p-1$ are likewise primitive roots, and $vice-versa$. III. If a primitive root h is taken as base, and t is the index of another primitive root h', and conversely t' is the index of h, then, if h' is taken as base, $tt' \equiv 1 \pmod{p-1}$; and if under the same premises the indices of some other number in these two systems are u and u' respectively, then $tu' \equiv u$, and $t'u \equiv u' \pmod{p-1}$. IV. If the numbers 1, $1+i$ and each of their three associated numbers are excluded (as too trivial) from the moduli which we are to consider, then what remains will be those prime numbers which we listed under 3. and 4. in article 34. The norms of the latter are real prime numbers of the form $4n+1$; the norms of the former, hoewever, are squares of the odd real prime numbers; in both cases, $p-1$ is divisible by 4. V. If the index of the number -1 is denoted by u, then $2u \equiv 0 \pmod{p-1}$, and therefore either $u \equiv 0$ or $u \equiv \frac{1}{2}(p-1)$; however, since the index 0 corresponds to the residue +1, the index of the number -1 must necessarily be $\frac{1}{2}(p-1)$. VI.Likewise, if the index of the number i is denoted by u, then $2u \equiv \frac{1}{2}(p-1) \pmod{p-1}$, and therefore either $u \equiv \frac{1}{4}(p-1)$ or $u \equiv \frac{3}{4}(p-1)$. However this ambiguity depends on the choice of primitive roots. That is to say, that if the primitive root h is taken as the base, and the index of the number i will be equal to $\frac{1}{4}(p-1)$, then the index will be $\frac{3}{4}(p-1)$ if h^μ is taken as base, where μ denotes a positive integer of the form $4n+3$ and relatively prime to $(p-1)$, e.g. the very number $p-2$, and *vice-versa*. Thus half of the primitive roots yield the index $\frac{1}{4}(p-1)$ for the number i, the other half yield $\frac{3}{4}(p-1)$, and evidently the former will have the index $\frac{3}{4}(p-1)$ for $-i$, and the the latter however will have the index $\frac{1}{4}(p-1)$. VII. If the modulus is a positive real prime number of the form $4n+3$, let us suppose it equal to q, and hence $p = q^2$, then the indices of all real numbers will be divisible by $q+1$. Denoting by t the index of the real number k, then because $k^{q-1} \equiv 1 \pmod{q}$, $(q-1)t \equiv 0 \pmod{q^2-1}$ and hence $\frac{t}{q+1}$ is a whole number. Likewise the indices of the pure imaginary numbers like ki are divisible by $\frac{1}{2}(q+1)$. Therefore the primitive roots for such moduli need only be sought among the mixed imaginary numbers. VIII. On the contrary, for a modulus m which is a mixed complex prime number (whose norm is consequently a real prime number of the form $4n+1$), any primitive root whatever can also be found among the real numbers, because an entire system of incongruent residues can be found among the real numbers (article 40). However it is manifest that every real number which is a primitive root of the complex modulus m is also simultaneously a a primitive root of the modulus p in the arithmetic of real numbers, and *vice-versa*.

56.

Although the theory of quadratic residues and nonresidues in the arithmetic of complex numbers is contained under the theory of biquadratic residues, we will however here present the most fundamental theorems of the former seperately before we go over to the latter; on account of brevity however, we will here discuss only the principle case, where the modulus is a complex uneven prime number. Let m be such a number and p its norm. It is evident that every integer (not divisible by m, as will here always be considered to be the case) can be either congruent or non-congruent to a square with respect to modulus m depending on whether its index, having taken any primitive root as base, is even or uneven; in the first case those integers will be called quadratic residues of m, and the latter, quadratic non-residues. It follows from this that among the $p-1$ numbers which represent a complete system of incongruent residues (not divisible by m), one half belongs to the quadratic residues, and the other half to the quadratic non-residues. Every other number which does not appear in this system is however in this respect to be assigned the same character as the number has which is congruent to it in the system. From the same, it follows that the product of two quadratic residue, as well as the product of two quadratic non-residues, is a quadratic residue, whereas the product of a quadratic residue and a quadratic nonresidue is a nonresidue; and in general the product of arbitrarily many factors is a quadratic residue or nonresidue, according as the number of nonresidues among those factors is evenn or odd. In order to distinguish the quadratic residues from the quadratic nonresidues, the following general criterion immediately presents itself: The number k , not divisible by the modulus, is a quadratic residue or nonresidue of that modulus, depending on whether $k^{\frac{1}{2}(p-1)} \equiv 1$ or $k^{\frac{1}{2}(p-1)} \equiv -1$. The validity of this

theorem follows immediately from the fact that, provided an arbitrary primitive root is taken as base, the index of the power $k^{\frac{1}{2}(p-1)}$ is either $\equiv 0$ or $\equiv \frac{1}{2}(p-1)$ depending on whether the index of the number k is even or uneven.

57.

It is indeed easy to divide the complete system of incongruent residues for a given modulus into two classes, namely into quadratic residues and nonresidues, in this way the classes to which the remaining numbers belong are also automatically determined; far more difficult however is the question of the criteria by which those moduli for which a given number is a quadratic residue can be distinguished from those for which it is a nonresidue. As for the real units +1 and -1, these are squares [themselves-*selbst* indeed-*reapse*], and are consequently quadratic residues for *every* modulus. It follows equally as easily from the criteria of the preceding pragraphs, that the number i (and likewise $-i$) is a quadratic residue of every modulus whose norm p is of the form $8n+1$, and on the contrary a quadratic nonresidue of every modulus whose norm is of the form $8n+5$. Since it is evidently of no consequence whether the number m or one of the numbers $im, -m, -im$ associated with it is taken as a modulus, it may be assumed that the modulus would be the primary number (article 36, II) among the associates and consequently, if the modulus is set equal to $a+bi$, a would be odd and b even. Since according to this a^2 is always $\equiv 1 \pmod 8$ but b^2 is either $\equiv 0$ or $\equiv 4 \pmod 8$, depending on whether b is evenly even or unevenly even, then it is clear that the numbers $+i$ and $-i$ will be in the first case quadratic residues of the modulus and in the second, quadratic nonresidues.

58.

Since the decision concerning the character of a composite number, whether it is a quadratic residue or nonresidue, depends on the character of its factors, it will evidently be sufficient if we limit the development of the criteria for the distinguishing of those moduli for which a given number k is a quadratic residue from those for which it is a nonresidue to such values of k which are prime numbers and moreover are the primary number amongst those numbers to which it is associated. In this this investigation induction immediately yields to us most elegant theorems. We begin with the number $1+i$, which is found to be a quadratic residue of the moduli

$$-1+2i, +3-2i, -5-2i, -5-2i, -1-6i, +5+4i, +5-4i, -7, +7+2i, -5+6i, \ldots,$$

however a nonresidue of the following

$$-1-2i, -3, +3+2i, +1+4i, +1-4i, -5+2i, -1+6i, +7-2i, -5-6i, -3+8i, -3-8i, +5+8i, +5-8i, +9+4i, +9-4i, \ldots$$

If we carefully consider this conspectus, in which we have always taken the primary among each four associated moduli, we easily note that the moduli $a+bi$ in the first class are all so composed that for them $a+b \equiv 1 \pmod 8$, while those in the latter class are so composed that for them $a+b \equiv -3 \pmod 8$. Evidently, if we take instead of the primary modulus m the associated $-m$, this criterion must be modified such that for moduli of the first class $a+b \equiv -1 \pmod 8$, but for the latter class $a+b \equiv +3 \pmod 8$. Hence, if our induction has otherwise not decieved us, and if $a+bi$ denotes a prime number in which a is odd and b is even, $1+i$ will be a quadratic residue or nonresidue of that prime number depending on whether $a+b \equiv \pm 1$ or $\equiv \pm 3 \pmod 8$. The same rule holds for $-1-i$ as for $1+i$. On the contrary, considering $1-i$ as the product of $-i$ and $1+i$ it is clear that the number $1-i$ has the same character as $1+i$ if b is evenly even; on the contrary it has the opposite character if b is unevenly even, from which it easily follows that $1-i$ is a quadratic residue of the prime number $a+bi$ if $a-b \equiv \pm 1$ but a quadratic nonresidue if $a-b \equiv \pm 3 \pmod 8$, always supposing a to be odd and b to be even. Moreover this second theorem can also be derived from the first by aid of a more general theorem which we express thus: In the theory of quadratic residues the character of the number $\alpha+\beta i$ with respect to the number $a+bi$ is the same as the character of the number $\alpha-\beta i$ with respect to the modulus $a-bi$. The proof of this theorem is derived from the fact that both moduli have the same norm, p, and so that as long as $(\alpha+\beta i)^{\frac{1}{2}(p-1)}-1$ is divisible by $a+bi$, $(\alpha-\beta i)^{\frac{1}{2}(p-1)}-1$ is also divisible by $a-bi$, however whenever $(\alpha+\beta i)^{\frac{1}{2}(p-1)}+1$ can be divided by $a-bi$, $(\alpha-\beta i)^{\frac{1}{2}(p-1)}+1$ must be divisible by $a-bi$.

59.

We proceed now to the uneven prime numbers. We find that the number -1+2i is a quadratic residue of the moduli:

$$+3+2i, +1-4i, -5+2i, -5-2i, -1-6i, +7-2i, -3+8i, +5+8i, +5-8i, +9+4i, \ldots,$$

however a nonresidue of the moduli:

$$-1-2i, -3, +3-2i, +1+4i, -1+6i, +5+4i, +5-4i, -7, +7+2i, -5+6i, -5-6i, -3-8i, +9-4i, \ldots$$

Reducing the moduli of the first class to their absolute least residue relative to the modulus $-1+2i$ then only the residues +1 and -1 will appear; that is $+3+2i \equiv -1, +1-4i \equiv -1, -5+2i \equiv +1, -5-2i \equiv -1$, etc. On the other hand it is found that all moduli of the latter class relative to moduli $-1+2i$ are either congruent to $+i$ or $-i$. However +1 and -1 are themselves quadratic residues of the modulus $-1+2i$ and $+i$ and $-i$ are quadratic nonresidues: wherefore, so far as the induction may be believed, the following theorem arises: The number $-1+2i$ is a quadratic residue or nonresidue of a prime number $a+bi$ depending on whether the latter is a quadratic residue or nonresidue of $-1+2i$, provided that $a+bi$ is the primary among its four associates, or better said, if a is odd and b is even. Further analogous theorems for the numbers $+1-2i, -1-2i, +1+2i$ follow automatically from this theorem.

60.

Employing a similar induction with respect to the number -3 or +3, we find that each of the two will be a quadratic residue of the moduli

$$+3+2i, +3-2i, -1+6i, -1-6i, -7, -5+6i, -5-6i, -3+8i, -3-8i, +9+4i, +9-4i, \ldots$$

but a quadratic nonresidue of the moduli

$$-1+2i, -1-2i, +1+4i, +1-4i, -5+2i, -5-2i, +5+4i, +5-4i, +7+2i, +7-2i, +5+8i, +5-8i, \ldots$$

The former are congruent to some one of the four numbers $+1, -1, +i, -i$ with respect to modulus 3; the latter however are congruent to some one of $+1+i, +1-i, -1+i, -1-i$. The former are themselves quadratic residues of three, and the latter nonresidues. This induction therefore shows that the prime number $a+bi$, assuming always that a is odd and b is even, has the same relation to the number -3 (and likewise +3) as the latter to the former, that is, whether one is a quadratic residue or nonresidue of the other. Extending the same induction to the other prime numbers, it is found that this most elegent law of reciprocity everywhere holds and we thus arrive at the following fundamental theorem regarding quadratic residues in the arithmetic of complex numbers: *If a+bi and A+Bi are prime numbers such that a, A are odd and b, B are even: then either each will be a quadratic residue or each will be quadratic nonresidue of the other.* However, despite the great simplicity of the theorem, great difficulties underlie its proof, which we will not dwell on here, since the theorem is itself only a special case of a more general theorem which contains the whole theory of biquadratic residues in itself. We will now proceed to this.

61.

That which was adduced in article 2 of the earlier treatise on the concept of quadratic and biquadratic residues, we now extend also to the arithmetic of the complex numbers and likewise here also limit the investigation to such moduli as are prime numbers; at the same time it will be tacitly assumed, that the modulus is taken in such a way that is the primary among its four associated numbers, that is $\equiv 1$ relative to the modulus $2+2i$, and that the numbers whose character (insofar as they are quadratic residues or nonresidues) is being considered, are not divisble by the modulus. Thus for a given modulus, the numbersnot divisble by it can be seperated into three classes, of which the first are the biquadratic residues, the second are biquadratic nonresidues which are quadratic residues, and finally the third which are quadratic nonresidues. However here also it is more advantageous to replace the third class with two, so that there are four classes in all. If any one primitive root is taken as the base, then the

biquadratic residues will have indices which are divisible by 4, or of the form $4n$; those nonresidues which are quadratic residues, will have indices of the form $4n+2$; finally the indices of quadratic nonresidues will be in part of the form $4n+1$, and in part of the form $4n+3$. In this way four classes would indeed emerge, however the difference between the two latter classes would not be absolute, but rather dependent upon the choice of primitive root taken as the basis. Then it is easily seen, that for one half of the primitive roots a given quadratic residue corresponds to an index of the form $4n+1$; and of the form $4n+3$ for the other half. In order to remedy this ambiguity, we will assume that such a primitive root will always be chosen for which the index $\frac{1}{4}(p-1)$ belongs to the number $+i$ (cf. article 55, VI). In this way a classification arises which we can represent more concisely in the following way, independent of the primitive root: The *first* class contains those numbers k, for which $k^{\frac{1}{4}(p-1)} \equiv 1$; these numbers are the biquadratic residues of the modulus. The *second* class contains those numbers for which $k^{\frac{1}{4}(p-1)} \equiv i$. The *third* class contains those numbers for which $k^{\frac{1}{4}(p-1)} \equiv -1$. The *fourth* class contains those numbers for which $k^{\frac{1}{4}(p-1)} \equiv -i$. The third class will contain those biquadratic nonresidues which are quadratic residues; the quadratic nonresidues are divided between the second and fourth class. To the numbers of these classes we attach the *biquadratic characters* 0, 1, 2, 3 respectively. If we define the character λ of a number k with respect to modulus m such that it is to be the exponent of that power of i to which the number $k^{\frac{1}{4}(p-1)}$ is congruent, then it is manifest that the characters which are congruent with respect to modulus 4 are to be considered as equivalent. Moreover, this concept will for time being be limited to those moduli which are prime numbers; in the course of this investigation, we will show how it will also be adapted to composite moduli.

62.

In order to the more easily employ a detailed induction with regard to the characters of the moduli, we append here an extensive table, with whose aid the character with respect to a modulus of every given number whose norm does not exceed 157 can be obtained with less effort, provided that the following observations are kept in mind. Since the character of a composite number is equal (or congruent with respect to modulus 4) to the aggregate of the characters of its factors, it will suffice if we can determine the character of the prime numbers for any given modulus. Further, since the character of the units $+1, -1, +i, -i$ are evidently congruent to the numbers $\frac{1}{2}(p-1)$, $\frac{1}{4}(p-1)$, $\frac{3}{4}(p-1)$, with respect to modulus 4, then it will also suffice if only the character of the primary number among its associates is represented. FInally, since the numbers congruent with respect to modulus m have the same character, it will suffice to include in the table the characters of such numbers as are contained in the system of absolute least residues. Furthermore, it is demonstrated by a similar line of reasoning to that employed in article 58, that if for the modulus $a+bi$ the character of the number $A+Bi$ is equal to λ, and for the modulus $a-bi$ however the character of the number $A-Bi$ is equal to λ',then we will always have $\lambda \equiv -\lambda' \pmod 4$ or $\lambda+\lambda'$ is divisible by 4; consequently it is sufficient to include in the table only moduli for which b is either positive or equal to 0. If for example we seek the character of the number $11-6i$ with respect to the modulus $-5-6i$, thus can we substitute $11+6i, -5+6i$ for these numbers; then we determine (article 43) the absolute least residue of the number $11+6i$ relative to the modulus $-5+6i$, which is $-1-4i = -1 \times (1+4i)$. Consequently, since for the modulus $-5+6i$ the character of -1 is equal to 30, but the character of the number $1+4i$ is 2 according to the table, and the character of the number $11+6i$ is 32 or 0 for the modulus $-5+6i$ and consequently by the last observation 32 or 0 is also the character of the number $11-6i$ for the modulus $-5-6i$. Similarly, if the character of the number $-5+6i$ with respect to the modulus $11+6i$ is sought, the absolute least residue of $1-5i$ is decomposed into the factors $-i, 1+i, 3-2i$, to which the characters 117, 0, 1 correspond, so that the sought character is 118 or 2; the same character is attached to the number $-5-6i$ as well, with respect to the modulus $11-6i$.

Modulus	*Character*	*Number*
$-\ 3$	3	$1+i$
$+\ 3\ +\ 2i$	3	$1+i$
$+\ 1\ +\ 4i$	1	$-1+2i$
	3	$1+i$
$-\ 5\ +\ 2i$	0	$-1-2i$
	1	$1+i$
	2	$-1+2i$
$-\ 1\ +\ 6i$	0	-3
	1	$1+i,\quad -1+2i$
	2	$-1-2i$
$+\ 5\ +\ 4i$	0	$1+i$
	1	-3
	3	$-1+2i,\quad -1-2i$
$-\ 7$	0	-3
	1	$-1+2i,\quad 3-2i$
	2	$1+i$
	3	$-1-2i,\quad 3+2i$
$+\ 7\ +\ 2i$	0	$1+i,\quad 3+2i,\quad 3-2i,\quad 1-4i$
	1	-3
	2	$-1-2i,\quad 1+4i$
	3	$-1+2i$
$-\ 5\ +\ 6i$	0	$1+i,\quad -3,\quad 3+2i,\quad 3-2i$
	1	$1-4i$
	2	$1+4i$
	3	$-1+2i,\quad -1-2i$
$-\ 3\ +\ 8i$	0	$-1+2i,\quad 3-2i,\quad 1-4i$
	1	$1+i,\quad 3+2i$
	2	-3
	3	$-1-2i,\quad 1+4i,\quad -5+2i$
$+\ 5\ +\ 8i$	0	$-1-2i$
	1	$-5-2i,\quad -1+6i$
	2	$-1+2i,\quad 3-2i$
	3	$1+i,\quad -3,\quad 3+2i,\quad 1+4i,\quad 1-4i$
$+\ 9\ +\ 4i$	0	$-1+2i,\quad 3+2i$
	1	$1+i,\quad -1-2i,\quad 3-2i$
	2	$-3,\quad 1+4i$
	3	$1-4i,\quad -5+2i$
$-\ 1\ +\ 10i$	0	$1+i,\quad -1+2i,\quad -1-2i,\quad 3+2i$
	1	-3
	2	$3-2i,\quad -5+2i,\quad 5-4i$
	3	$1+4i,\quad 1-4i$
$+\ 3\ +\ 10i$	1	$1+i,\quad -1-2i,\quad 1-4i$
	2	$-3,\quad 3+2i,\quad 1+4i,\quad -5-2i$
	3	$-1+2i,\quad 3-2i$
$-\ 7\ +\ 8i$	0	$1+i,\quad -7$
	1	$3+2i,\quad 3-2i,\quad 1-4i,\quad -5-2i$
	2	$-1-2i,\quad 1+4i,\quad -5+2i,\quad -1-6i$
	3	$-1+2i,\quad -3,\quad -1+6i$

Modulus	*Character*	*Number*
$-\ 11$	0	-3
	1	$1+i,\quad 3-2i,\quad 1+4i,\quad -5+2i,\quad 5+4i$
	2	$-1+2i,\quad -1-2i$
	3	$3+2i,\quad 1-4i,\quad -5-2i,\quad 5-4i$
$-\ 11\ +\ 4i$	0	$1+i,\quad -1+2i,\quad 3+2i,\quad 5+4i$
	1	$-1-2i,\quad -1+6i$
	2	$-5+2i$
	3	$-3,\quad 3-2i,\quad 1+4i,\quad 1-4i,\quad -5-2i$
$+\ 7\ +\ 10i$	0	$1+4i,\quad 1-4i,\quad -1+6i,\quad -1-6i$
	1	$-1+2i,\quad 3+2i,\quad -5+2i$
	2	$1+i,\quad 3-2i$
	3	$-1-2i,\quad -3,\quad -5-2i$
$+\ 11\ +\ 6i$	0	$1+i,\quad -1+2i,\quad -3,\quad 1+4i,\quad 1-4i,\quad -7$
	1	$-1-2i,\quad 3+2i,\quad 3-2i$
	2	$-5-2i,\quad -1+6i,\quad 5-4i$
	3	$-5+2i,\quad 5+4i,\quad 7-2i$

63.

We will now attempt to discover through induction the common criteria of the moduli for which a given prime number has the same character. We always suppose the modulus to be the primary among its associated numbers. Let such a number be $a+bi$ for which either $a \equiv 1, b \equiv 0$ or $a \equiv 3, b \equiv 2 \pmod 4$. With respect to the number $1+i$, with which we make our beginning, the inductive law is more easily arrived at if we seperate the moduli of the first type (for which $a \equiv 1, b \equiv 0$) from those of the second (for which $a \equiv 3, b \equiv 2$). By aid of the table in the preceding article, we the corresponding

character	$for the modulio f the first type:$
0	$5+4i,\quad -7+8i,\quad -7-8i,\quad -11+4i$
1	$1-4i,\quad -3+8i,\quad -3-8i,\quad 9+4i,\quad -11$
2	$5-4i,\quad -7,\quad -11-4i$
3	$-3,\quad 1+4i,\quad 5+8i,\quad 5-8i,\quad 9-4i$

If we carefully consider these seventeen examples, we find that the character of every number is $\equiv \frac{1}{4}(a-b-1) \pmod 4$. Likewise correspond

character	$for the modulio f the second type:$
0	$3-2i,\quad -1-6i,\quad 7+2i,\quad -5+6i,\quad -1+10i,\quad 11+6i$
1	$-5+2i,\quad -1+6i,\quad 7-2i,\quad -1-10i,\quad 3+10i$
2	$-1+2i,\quad -5-2i,\quad 3-10i,\quad 7+10i$
3	$-1-2i,\quad 3+2i,\quad -5-6i,\quad 7-10i,\quad 11-6i$

With a little attentiveness, in all these twenty examples it can be found that the character is $\equiv \frac{1}{4}(a-b-5) \pmod 4$. These two rules can easily be combined into one which applies to both types of modulus, if it is considered that $\frac{1}{4}b^2$ is $\equiv 0$ for moduli of the first type, and $\equiv 1 \pmod 4$ for moduli of the second. Thus, the character of the number $1+i$ with respect to each prime that is also primary among its associated numbers, is $\equiv \frac{1}{4}(a-b-1-b^2) \pmod 4$. We will additionally remark here that since $(b+1)^2$ is always of the form $8n+1$ or $\frac{1}{4}(2b+b^2)$ is even, that [?] character is always even or odd depending upon whether $\frac{1}{4}(a+b-1)$ is even or odd, which agrees with the rulegiven for quadratic characters in article 58. Since $\frac{1}{4}(a-b-1), \frac{1}{4}(a-b+3)$ are integers, of which the one is even and the other odd, their product will be even or $\frac{1}{8}(a-b-1)(a-b+3) \equiv 0 \pmod 4$. It follows from this that in place of the given expression for the quadratic character the following can also be taken:

$$\frac{1}{4}(a-b-1-b^2) - \frac{1}{8}(a-b-1)(a-b+3) = \frac{1}{8}(-a^2+2ab-3b^2+1),$$

which form is also recommended by the fact that it is not limited to primary moduli, but rather only assumes that a is odd and b is even; then it is evident that under this supposition either $a+bi$ or $a-bi$

will be the primary among the associated numbers, and the value of that formula is the same for both moduli.

64.

Proceeding from the last law found in the preceeding article we find

for the number	the character is $\equiv$
$-\ 1\ +\ i$	$\frac{1}{8}($ $a^2 + 2ab - b^2 - 1)$
$-\ 1\ -\ i$	$\frac{1}{8}($ $-a^2 + 2ab + b^2 + 1)$
$+\ 1\ -\ i$	$\frac{1}{8}($ $a^2 + 2ab + 3b^2 - 1)$

This follows directly from the fact that the character of i is $\frac{1}{4}(a^2 + b^2 - 1)$, but the character of -1 is $\frac{1}{2}(a^2 + b^2 - 1) \equiv \frac{1}{2}b^2$, since $a^2 - 1$ is always of the form $8n$. Although they have been hitherto only obtained through induction, these four rules are evidently bound together in such a way that as soon as the proof of one of them is carried out, the three remaining are simultaneously proven. It is scarcely necessary to point out that in this rule it is also supposed that a is odd and b is even. If it is desired to employ the formulae which are limited to primary moduli, the following form can be utilized.

For the number	the character is $\equiv$
$-\ 1\ +\ i$	$\frac{1}{4}($ $-a - b + 1 - b^2)$
$-\ 1\ -\ i$	$\frac{1}{4}($ $a - b - 1 + b^2)$
$+\ 1\ -\ i$	$\frac{1}{4}($ $-a - b + 1 + b^2)$

The simplest formulae arise if we distinguish moduli of the first and second types as we did at the beginning of our induction. That is to say

For the number	the character is $\equiv$	
$-\ 1\ +\ i$	$\frac{1}{4}($ $-a - b + 1)$	$\frac{1}{4}($ $-a - b - 3)$
$-\ 1\ -\ i$	$\frac{1}{4}($ $a - b - 1)$	$\frac{1}{4}($ $a - b + 3)$
$+\ 1\ -\ i$	$\frac{1}{4}($ $-a - b + 1)$	$\frac{1}{4}($ $-a - b + 5)$

65.

For the number $-1 + 2i$ to which we now proceed, we will likewise make the distinction between those moduli $a + bi$ for which $a \equiv 1$, $b \equiv 0$ and those for which $a \equiv 3$, $b \equiv 2$. The table of article 62 shows that with respect to that number

the character	corresponds to the moduli of the first type:
0	$-3+8i$, $+5-8i$, $+9+4i$, $-11+4i$
1	$+1+4i$, $+5-4i$, -7, $-3-8i$
2	$+1-4i$, $+5+8i$, $-7-8i$, -11
3	-3, $+5+4i$, $+9-4i$, $-7+8i$, $-11-4i$

If we reduce these individual moduli to their absolute least residues relative to modulus $-1 + 2i$, we observe that all those [for which $-1 + 2i$ has the character] 0, are $\equiv 1$, and those [for which it has] the character 1 are $\equiv i$, those where the character is 2, $\equiv -1$, and finally those giving character 3 will be $\equiv -i$. But the characters of the numbers $1, i, -1, -i$ for the modulus $-1 + 2i$ are just 0, 1, 2 ,3 respectively; consequently in all these seventeen examples the character of the number $-1 + 2i$ relative to moduli of the first type $a + bi$ is identical with the character of this number with respect to the modulus $-1 + 2i$. It is likewise found by aid of the table that

the character	corresponds to the moduli of the second type:
0	$+3+2i$, $-5-2i$, $-1+10i$, $-1-10i$ $+11+6i$
1	$+3-2i$, $-1+6i$, $-5-6i$, $+7+10i$ $+7-10i$
2	$-5+2i$, $-1-6i$, $+7-2i$
3	$-1-2i$, $+7+2i$, $-5+6i$, $+3+10i$, $+3-10i$, $+11-6i$

If we these moduli to their absolute least residues with respect to modulus $-1+2i$ then it is found that all of the numbers [for which $-1+2i$ has the character] 0, 1, 2, 3 are congruent to the numbers $-1, -i, +1, +i$ respectively; however these [unit] numbers have the characters 2, 3, 0, 1 respectively, if inversely $-1+2i$ is taken as modulus. Consequently in all of these 19 examples, the character of the number $-1+2i$ with respect to a modulus of the second type, differes by two units from the character of this number with respect to the modulus $-1+2i$. It can be seen with no effort that something entirely similar will occur with respect to the number $-1-2i$.

66.

For the number -3, we omit the distinction between moduli of the first and second type, since the results show, that it is superfluous here. Hence

the character	corresponds to the moduli				
0	$-3+8i$,	$+5-8i$,	$+9+4i$,	$-11+4i$	
1	$+1+4i$,	$+5-4i$,	-7,	$-3-8i$	
2	$+1-4i$,	$+5+8i$,	$-7-8i$,	-11	
3	-3,	$+5+4i$,	$+9-4i$,	$-7+8i$,	$-11-4i$

If we reduce these moduli to their least residues relative to modulus 3, we see that those [for which -3 has the character] 0 are in part $\equiv 1$, in part $\equiv -1$, those [for which it has the character] 1 are either $\equiv 1-i$ or $\equiv -1+i$, those for which [-3 has the character] 2, are either $\equiv i$ or $\equiv -i$, and finally those [for which it has the character] 3 are either $\equiv 1+i$ or $\equiv -1-i$. Thus from this induction we conclude that the character of the number -3 for a prime primary modulus is identical with the character of this modulus if 3 or, what amounts to the same thing, -3 is considered as the modulus.

67.

If a similar induction is employed with respect to other prime numbers, it is found that the numbers $3\pm 2i, -1\pm 6i, 7\pm 2i, -5\pm 6i, \ldots$ furnish similar theorems to those which we obtained in article 65 with respect to the number $-1+2i$, [but that] on the other hand the numbers $1\pm 4i, 5\pm 4i, -3\pm 8i, 5\pm 8i, 9\pm 4i, \ldots$ behave like the number -3. The induction thus leads to a most elegant theorem which, by analogy with the theory of quadratic residues in the arithmetic of real numbers, can be called the FUNDAMENTAL THEOREM of biquadratic residues, viz.:

If $a+bi, a'+b'i$ denote two different prime primary numbers, i.e. prime numbers congruent to unity relative to modulus $2+2i$, then the biquadratic character of the number a+bi with respect to the modulus a'+b'i is identical with the character of the number a'+b'i with respect to the modulus a+bi, if either each or at least one of the two numbers $a+bi, a'+b'i$ belongs to the first type, i.e. is congruent to unity with respect to modulus 4; on the other hand, those characters will differ by two units if neither of the numbers $a+bi, a'+b'i$ belong to the first type, i.e. if both are congruent to the number 3+2i with respect to modulus 4.

Despite the great simplicity of this theorem however, its proof belongs to the most hidden secrets of higher arithmetic, so that, at least so far as things stand, can be carried out only by means of the most subtle investigations which far surpass the limits of this treatise. Thus, we reserve the publication of this proof, as well as the the development between this theorem and those that we set out to establish by induction at the beginning of this treatise, for a third treatise. To conclude [coronidis tamen loco] we here present that which is necessary for the proof of the theorem put forward in articles 63 and 64.

68.

We begin with those prime numbers $a+bi$ for which $b=0$ (from the third type of article 34), where consequently (in order that the number be primary among its associates) a must be a real negative prime number of the form $-(4n+3)$, which we will write as $-q$. The numbers -3, -7, -11, -19, . . . are of such a type. Denoting by λ the character of the number $1+i$, then taking that number as the modulus, we must have

$$i^\lambda \equiv (1+i)^{\frac{1}{4}(q^2-1)} \equiv 2^{\frac{1}{8}(q^2-1)} \cdot i^{\frac{1}{8}(q^2-1)} \pmod{q}$$

But as is well known, 2 is a quadratic residue or nonresidue of q, depending on whether q is of the form $8n+7$ or $8n+3$, whereby it follows, that in general

$$2^{\frac{1}{2}(q-1)} \equiv (-1)^{\frac{1}{4}(q+1)} \equiv i^{\frac{1}{2}(q+i)} \pmod{q}$$

and therefore, raising to the power $\frac{1}{4}(q+1)$,

$$2^{\frac{1}{8}(q^2-1)} \equiv i^{\frac{1}{8}(q+i)^2} \pmod{q}.$$

Hence the preceding equation assumes the following form:

$$i^\lambda \equiv i^{\frac{1}{8}(q+1)^2+\frac{1}{8}(q^2-1)} \equiv i^{\frac{1}{4}(q^2+q)} \pmod{q}$$

and it follows from that, that

$$\lambda \equiv \frac{1}{4}(q^2+q) \equiv \frac{1}{4}(q+1)^2 - \frac{1}{4}(q+1) \pmod{4}$$

or, since $\frac{1}{4}(q+1)^2 \equiv 0 \pmod{4}$:

$$\lambda \equiv -\frac{1}{4}(q+1) \equiv \frac{1}{4}(a-1) \pmod{4}$$

This is the theorem of article 63 for the case $b=0$.

69.

But indeed it is far more difficult to carry this out for the moduli $a+bi$, for which b is not equal to zero (the numbers of the fourth type, article 34), and must first be preceeded by several investigations. The norm a^2+b^2, which is a real prime number of the form $4n+1$, we denote by p. The complex of all simple least residues for the modulus $a+bi=m$ with the exception of zero, may be denoted by S, so that the quantity of the numbers contained in S is equal to $p-1$. Further, $x+yi$ denotes any one undetermined number of the system, and $ax+by=\xi, ay-bx=\eta$. ξ and η are integers which are contained between the limits 0 and p, *exclusive*: since in the case at hand, where a and b are relatively prime, the formulae of article 45, namely $\eta \equiv k\xi, xi \equiv k\eta \pmod{p}$, show that neither of the numbers ξ, η can be equal to 0, if the other does not vanish simultaneously and consequently $x=0, y=0$, a combination which we have already excluded. Thus, the criterion for the number $x+yi$ to be contained in S is that the four numbers $\xi, \eta, p-\xi, p-\eta$ must be positive. We observe further that for no such number can $\xi=\eta$ since it would follow from this that $p(x+y)=a(\xi+eta)+b(\xi-\eta)=2a\xi$ which is absurd, since none of the factors $2, a, \xi$ is divisible by p. In a similar way the equation $p(x-y+a+b)=2a\xi+(a+b)(p-\xi-\eta)$ shows that $\xi+\eta$ cannot be equal to p. Therefore, since $\xi-\eta, p-\xi-\eta$ must be either positive or negative, we obtain from this a distribution of the system S into four complexes C, C', C'', C''' in such a way that

in the complex	we put the numbers for which			
C	$\xi-\eta$	is positive,	$p-\xi-\eta$	is positive
C'	$\xi-\eta$	is positive,	$p-\xi-\eta$	is negative
C''	$\xi-\eta$	is negative,	$p-\xi-\eta$	is negative
C'''	$\xi-\eta$	is negative,	$p-\xi-\eta$	is positive

The criterion for a number of the complex C is properly sixfold, namely, the six numbers $\xi, \eta, p-\xi, p-\eta, \xi-\eta, p-\xi-\eta$ must be positive; but it is evident that the second, fifth and sixth conditions automatically imply the others. Something similar holds for the complexes C', C'', C''', so that the complete criteria are threefold. Namely

for the complex	these numbers must be positive		
C	$\eta,$	$\xi-\eta,$	$p-\xi\eta$
C'	$p-\xi,$	$\xi-\eta,$	$\xi+\eta-p$
C''	$p-\eta,$	$\eta-\xi,$	$\xi+\eta-p$
C'''	$\xi,$	$\eta-\xi,$	$p-\xi-\eta.$

It will further be easily recognized that in the geometric representation of complex numbers (cf. article 39) the numbers of the system S are contained within a square whose sides connect the points which represent the numbers $0, a+bi, (1+i)(a+bi), i(a+bi)$, and that the distribution of the system S corresponds to the division of the square along its diagonals. However here we prefer to make use of pure arithemtic conclusions, meanwhile we leave the illustration by a pictoral representation to the experienced reader.

70.

If the four complex numbers

$$r = x+yi, r' = x'+y'i, r'' = x''+y''i, r''' = x'''+y'''i$$

are related to one another in such a way that

$$r' = m+ir, r'' = m+ir' = (1+i)m-r, r''' = m+ir'' = im-ir$$

and it is assumed that the first r belongs to the complex C then the remaining r', r'', r'' will belong to the complexes C', C'', C''' respectively. Then, setting

$$\begin{array}{rclcrcrcl} \xi & = & ax & + & by, & \eta & = & ay & - & bx \\ \xi' & = & ax' & + & by', & \eta' & = & ay' & - & bx' \\ \xi'' & = & ax'' & + & by'', & \eta'' & = & ay'' & - & bx'' \\ \xi''' & = & ax''' & + & by''', & \eta''' & = & ay''' & - & bx''', \end{array}$$

it is found that

$$\eta = p-\xi' = p-\eta'' = \xi'''\xi-\eta = \xi'+\eta'-p = \eta''-\xi'' = p-\xi'''-\eta'''p-\xi-\eta = \xi'-\eta' = \xi''+\eta''-p = \eta'''-\xi''',$$

from which, by aid of the criterion for the individual complexes [?] the correctness of the theorem is automatically yielded. And since again $r = m+ir'''$, it is easily seen that if r is assumed to belong to the complex C', the numbers r', r'', r''', belong to C'', C''', C respectively; if the former belongs to C'', the latter belong to C''', C, C'; and finally if the former belongs to C''', then the latter belong to C, C', C''. At the same time it follows from this that in the individual complexes C, C', C'', C''' an equal amount of numbers is contained, that is $\frac{1}{4}(p-1)$.

71.

theorem. *If the inividual numbers of the complexe C are multiplied by k, where k denotes an integer not divisible by m, and according as the simple least residues of these products with respect to modulus m are distributed amoung the complexes C, C', C'', C''', the quantity of those, which belong the the inviludal complexes, will be denoted with c, c', c'', c''' respectively, then the character of the number k with respect to the modulus m is congruent to $c'+2c''+3c'''$* (mod 4).

Proof. Let the c least residues belonging to C be $\alpha, \beta, \gamma, \delta, ...$, the c' residues belonging to C' be $m+i\alpha', m+i\beta', m+i\gamma', m+i\delta', ...$, and further the c'' residues belonging to C'' are $(1+i)m-\alpha'', (1+i)m-\beta'', (1+i)m-\gamma'', (1+i)m-\delta'', ...$, finally the c''' residues belonging to C'''' are $im-i\alpha''', im-i\beta''', im-i\gamma''', im-i\delta''', ...$ We now observe four products, namely:

1. the product of all $\frac{1}{4}(p-1)$ constituent numbers of the complex C,

2. the product of the products, which arise from the multiplication of these individual numbers with k,

3. the product of the least residues of these products, namely of the numbers $\alpha, \beta, \gamma, \delta, ..., m+i\alpha', m+i\beta', ...$

4. the product of all $c+c'+c''+c'''$ numbers $\alpha, \beta, \gamma, \delta, ...,\ \alpha', \beta', \gamma', \delta', ...,\ \alpha'', \beta'', \gamma'', \delta'', ...$

If these four products are denoted in succession with P, P', P'', P''', then evidently:

$$P' = k^{\frac{1}{4}(p-1)}P,\ P' \equiv P'',\ P'' \equiv P'''i^{c'+2c''+3c'''} \pmod{m}$$

and consequently:

$$Pk^{\frac{1}{4}(p-1)} \equiv Pi^{c'+2c''+3c'''} \pmod{m}$$

However, it is easily seen thatthe numbers $\alpha, \beta, \gamma, \delta, ...,\ \alpha', \beta', \gamma', \delta', ...,\ \alpha'', \beta'', \gamma'', \delta'', ...$ all belong to the complex C and different from each other as well from $\alpha, \beta, \gamma, \delta, ...,$ just as the latter differ from one another. Therefore all these numbers taken together must be completely identical with all the numbers which form the complex C irrespctive of order, from which it follows $P = P'''$ and therefore":

$$k^{\frac{1}{4}(p-1)} \equiv i^{c'+2c''+3c'''} \pmod{m}$$

so that $c'+2c''+3c'''$ is the character of the number k with respect to modulus m.

72.

In order to be able to apply the general theorem of the preceeding article to the number $1+i$, we must again divide the complex C into two smaller complexes G and G', and we will include those numbers $x+yi$ for which $ax+by=\xi$ is smaller than $\frac{1}{2}p$ in complex G, but those numbers for which ξ is greater than $\frac{1}{2}p$ we will include in the complex G'; the quantity of numbers contained in the complexes G and G' we will denote by g and g' so that $g+g' = \frac{1}{4}(p-1)$.

The complete criterion of the numbers belonging to complex G is consequently that the three numbers $\eta, \xi-\eta, p-2\xi$ are positive; since the third condition for the complex C according to which $p = \xi-\eta$ should be positive is already implicitly contained in the former, since $p = \xi-\eta = (\xi-\eta)+(p-2\xi)$. Likewise, the complete criterion for the numbers which belong to G' consist in the positive in the positives of the three numbers $\eta, p-\xi-\eta, 2\xi-p$.

From this it easily follows that the product of each number of the complex G and the number $1+i$ belongs to complex C'''. Since if we set:

$$(x+yi)(1+i) = x'+y'i \text{ and } ax'+by' = \xi', ay'-bx' = \eta'$$

then it is found:

$$\xi' = \xi-\eta, \eta'-\xi' = 2\eta, p-\xi'-\eta' = p-2\xi,$$

i.e. the criterion for the number $x+yi$ belonging to complex G is identical with the criterion for the number $x'+y'i$ belonging to complex C'''.

In a completely similar way, it is shown that the product of any number of the complex G' with $1+i$ belongs to complex C''.

Therefore, if in the preceeding aricle we give k the value $1+i$ we will have $c=0, c'=0, c''=g', c'''=g$ and consequently, the character of the number $1+i$ becomes $3g+2g' = \frac{1}{2}(p-1)+g$. And since the characters of the numbers $i, -1$ are $\frac{1}{4}(p-1), \frac{1}{2}(p-1)$ respectively, the characters of the numbers $-1+i, -1-i, 1-i$ will be $\frac{3}{4}(p-1)+g, g, \frac{1}{4}(p-1)+g$ repectively. Therefore the whole thing hinges now on ascertaining the number g.

73.

That which we have exposited in aricles 69 to 72 is actually independent of the supposition that m be a primary number; from now on, however, we will at least assume that a be odd and b be even, and futhermore, that a, b and $a-b$ be positive numbers. First of all, we must establish the limits of the value of x in the complex G.

Setting:

$$ay - bx = \eta, (a+b)x - (a-b)y = \zeta, p - 2ax - 2by = \theta,$$

the criterion of the number $x + yi$ belonging to complex G consists in the three conditions, that η, ζ, θ be positive numbers. Since $px = (a-b)\eta + a\zeta, p(a-2x) = a\theta + 2b\eta$, then evidently x and $2a - x$ must be positive numbers, or x must be equal to one of the numbers $1, 2, 3, ..., \frac{1}{2}(a-1)$. Since further $(a-b)\theta = 2b\zeta + p(a-b-2x)$ it is clear, that whenever x is smaller than $\frac{1}{2}(a-b)$, the second condition (by which ζ should be positive) already contains a third (that θ must be positive) and that, on the other hand, whenever x is greater than $\frac{1}{2}(a-b)$, the second condition is already contained under the third. Consequently, care only has to be taken that for the following values of x, namely $1, 2, 3, ..., \frac{1}{2}(a-b-1)$, that η and ζ become positive, or that y be greater than $fracbxa$ and less than $\frac{(a+b)x}{a-b}$. Therefore, for such a given value of x, there are in all

$$\left[\frac{(a+b)x}{a-b}\right] - \left[\frac{bx}{a}\right],$$

numbers $x + yi$, if the brackets signify the same as we have used them elsewhere in the past [cf. *"'New Proof of an Arithmetic theorem"'*, Art. 4 and *"'New Proof and Expansions of the Fundamental theorem in the Theory of Quadratic Residues", "New Algorithms e/t/c.* Article 3]. On the contrary, it is sufficient for the following values of x: $\frac{1}{2}(a-b+1), \frac{1}{2}(a-b+3), ..., \frac{1}{2}(a-1)$, if η and θ recieve positive values, or if y becomes greater than $\left[\frac{bx}{a}\right]$ and less than $\frac{p-2ax}{2b}$; consequently, for such a given value of x there are in all

$$\left[\frac{1}{2}b + \frac{a^2-2ax}{2b}\right] - \left[\frac{bx}{a}\right].$$

numbers $x + yi$.

Thus we conclude from this, that the quantitu of number of the complex G is g:

$$g = \sum\left[\frac{(a+b)x}{a-b}\right] + \sum\left[\frac{1}{2}b + \frac{a^2-2ax}{2b}\right] - \sum\left[\frac{bx}{a}\right],$$

where in the first term, the summation is to be extended over all integer values of x from 1 to $\frac{1}{2}(a-b-1)$ in the second, from $\frac{1}{2}(a-b+1)$ to $\frac{1}{2}(a-1)$, and in the third, from 1 to $\frac{1}{2}(a-1)$.

If we use the letter ϕ in the same sense as in the referenced locations, namely

$$\phi(t,u) = \left[\frac{u}{t}\right] + \left[\frac{2u}{t}\right] + \left[\frac{3u}{t}\right] + ... + \left[\frac{t'u}{t}\right]$$

where t, u signify any two positive numbers and t' the number $\left[\frac{1}{2}t\right]$, then the first term of the former is equal to $\phi(a-b, a+b)$, third equal to $-\phi(a,b)$, however the second will be equal to

$$\frac{1}{4}b^2 + \sum\left[\frac{a^2-2ax}{2b}\right].$$

However, if we write the terms in inverse order:

$$\sum\left[\frac{a^2-2ax}{2b}\right] = \left[\frac{a}{2b}\right] + \left[\frac{3a}{2b}\right] + \left[\frac{5a}{2b}\right] + ... + \left[\frac{(b-1)a}{2b}\right] = \phi(2b,a) - \phi(b,a),$$

Hence our formula assumes the following form:

$$g = \phi(a-b, a+b) + \phi(2b,a) - \phi(a,b) - \phi(b,a) + \frac{1}{4}b^2.$$

We first consider the term $\phi(a-b, a+b)$, which transforms itself immediately into $\phi(a-b, 2b) + 1 + 2 + 3 + ... + \frac{1}{2}(a-b-1)$, for into

$$\phi(a-b, 2b) + \frac{1}{8}((a-b)^2 - 1).$$

Since by the general theorem $\phi(t,u) + \phi(u,t) = \left[\frac{1}{2}t\right] \cdot \left[\frac{1}{2}u\right]$, we have further, whenever t and u are relatively prime positive integers:

$$\phi(a-b, 2b) = \frac{1}{2}b(a-b-1) - \phi(2b, a-b)$$

and therefore:

$$\phi(a-b,a+b) = \tfrac{1}{8}(a^2+2ab-3b^2-4b-1) - \phi(2b,a-b).$$

If we order the terms $\phi(2b,a-b)$ in the following way:

$$\left[\tfrac{a-b}{2b}\right] + \left[\tfrac{3(a-b)}{2b}\right] + \left[\tfrac{5(a-b)}{2b}\right] + ... + \left[\tfrac{(b-1)(a-b)}{2b}\right] + \left[\tfrac{a-b}{b}\right] + \left[\tfrac{2(a-b)}{b}\right] + \left[\tfrac{3(a-b)}{b}\right] + ... + \left[\tfrac{\frac{1}{2}b(a-b)}{b}\right],$$

the second series will evidently be equal to

$$\phi(b,a-b) = \phi(b,a) - 1 - 2 - 3 - ... - \tfrac{1}{2}b = \phi(b,a) - \tfrac{1}{8}(b^2+2b);$$

however, after inverting the order of the terms, we reprsent the first series thus:

$$\left[\tfrac{1}{2}(a+1-b) - \tfrac{a}{2b}\right] + \left[\tfrac{1}{2}(a+3-b) - \tfrac{3a}{2b}\right] + \left[\tfrac{1}{2}(a+5-b) - \tfrac{5a}{2b}\right] + ... + \left[\tfrac{1}{2}(a-1) - \tfrac{(b-1)a}{2b}\right],$$

and this expression transforms itself into the following, since if t denotes an integer and u denotes a fraction, then generally $[t-u] = t-1-[u]$:

$$\tfrac{1}{8}b(2a-4-b) - \left[\tfrac{a}{2b}\right] - \left[\tfrac{3a}{2b}\right] - \left[\tfrac{5a}{2b}\right] - ... - \left[\tfrac{(b-1)a}{2b}\right] = \tfrac{1}{8}b(2a-4-b) - \phi(2b,a) + \phi(b,a).$$

Hence:

$$\phi(2b,a-b) = 2\phi(b,a) - \phi(2b,a) + \tfrac{1}{4}b(a-3-b)$$

and consequently:

$$\phi(a-b,a+b) = \phi(2b,a) - 2\phi(b,a) + \tfrac{1}{8}(a^2-b^2+2b-1)$$

If this value is substituted into the formula for g given above and moreover we set $\phi(a,b)+\phi(b,a) = \frac{1}{4}b(a-1)$, then we obtain:

$$g = 2\phi(2b,a) - 2\phi(b,a) + \tfrac{1}{8}(a^2-2ab+b^2+4b-1).$$

74.

The case where a,b still remain positive, but $a-b$ is negative or $b-a$ positive, is dealt with by an entirely simiar line of reasoning. The equations $p(a-2x) = 2b\eta + a\theta, p(b-a+2x) = 2b\zeta + (b-a)\theta$ show that $\frac{1}{2}a - x$ and $x + \frac{1}{2}$ are positive and consequently x must be equal to one of the numbers $-\frac{1}{2}(b-a-1), \frac{1}{2}(b-a-3), \frac{1}{2}(b-a-5), ..., +\frac{1}{2}(a-1)$. It further follows from the equation $px+(b-a)\eta = a\zeta$ that for negative values of x, the condition according to which η should be positive is already contained under the condition according to which ζ should be positive, such that the opposite occurs, provided x is assigned a positive value. Hence, the value of y for a determined negative value of x must be contained within $\frac{(a+b)x}{a-b}$ and $\frac{p-2ax}{2b}$, but between $\frac{bx}{a}$ and $\frac{p-2ax}{2b}$ for a given positive value of x; evidently, for $x=0$, the limits are 0 and $\frac{p}{2b}$, excluding the value $y=0$.

It follows from this:

$$g = -\sum\left[\tfrac{(a+b))x}{a-b}\right] + \sum\left[\tfrac{1}{2}b + \tfrac{a^2-2ax}{2b}\right] - \sum\left[\tfrac{bx}{a}\right]$$

where in the first term, the summation extendes over all negative values of x from -1 up to $-\frac{1}{2}(b-a-1)$, in the second, over all values of x from $-\frac{1}{2}(b-a-1)$ up to $-\frac{1}{2}(a-1)$, and in the third, over all positive values of x from $+1$ up to $-\frac{1}{2}(a-1)$. In this way the first summation yeilds $-\phi(b-a,b+a)$, the second, just as in the previous article, yeilds $\frac{1}{4}b^2 + \phi(2b,a) - \phi(b,a)$, and finally the third yeilds $-\phi(a,b)$, or we have:

$$g = -\phi(b-a,b+a) + \phi(2b,a) - \phi(b,a) - \phi(a,b) + \tfrac{1}{2}b^2.$$

In a way entirely analogous to the previous article, we now develop:

$$\phi(b-a,b+a) = \phi(b-a,2b) - \tfrac{1}{8}((b-a)^2-1) = \tfrac{1}{8}(3b^2-2ab-a^2-4b+1) - \phi(2b,b-a),$$

just as:

$$\phi(2b,b-a) = \phi(2b,a) - 2\phi(b,a) + \tfrac{1}{4}b(b-1-a)$$

and therefore:

$$\phi(b-a,b+a) = 2\phi(b,a) - \phi(2b,a) + \tfrac{1}{8}(b^2-a^2-2b+1)$$

and finally:

$$g = 2\phi(2b,a) - 2\phi(b,a) + \tfrac{1}{8}(a^2-2ab+b^2+4b-1)$$

Hence it is proven that the same formula applies to g whether $a-b$ is positive or negative, provided only that a and b are positive.

75.

In order to reach a further reduction, we set:

$$\begin{aligned} L &= \left[\tfrac{a}{2b}\right] + \left[\tfrac{2a}{2b}\right] + \left[\tfrac{3a}{2b}\right] + \ldots + \left[\tfrac{\frac{1}{2}ba}{2b}\right] \\ M &= \left[\tfrac{(\frac{1}{2}b+1)a}{2b}\right] + \left[\tfrac{(\frac{1}{2}b+2)a}{2b}\right] + \left[\tfrac{(\frac{1}{2}b+3)a}{2b}\right] + \ldots + \left[\tfrac{ba}{2b}\right] \\ N &= \left[\tfrac{a+b}{2b}\right] + \left[\tfrac{2a+b}{2b}\right] + \left[\tfrac{3a+b}{2b}\right] + \ldots + \left[\tfrac{\frac{1}{2}ba+b}{2b}\right]. \end{aligned}$$

Since it is easily seen, that generally $[u] + \left[u+\frac{1}{2}\right] = [2u]$, whatever real magnitudes u might denote, then $L+N = \phi(b,a)$, and sind evidently $L+M = \phi(2b,a)$, then:

$$\phi(2b,a) - \phi(b,a) = M - N.$$

Further, it is clear that the aggregate of the first term of the series N and the last term of the series M will be $\left[\frac{a+b}{2b}\right] + \left[\frac{(b-1)a}{2b}\right] = \frac{1}{2}(a-1)$, and that the same sum will be formed from the aggregate of the second term of the series N and the second to last term of M e.t.c. Now, since the last term of the series M is also equal to $\frac{1}{2}(a-1)$ but the last term of the series N is equal to $\left[\frac{a+2}{4}\right] = \frac{1}{4}(a \mp 1)$, where the upper or lower sign is used according to whether a is of the form $4n+1$ or $4n-1$, it thus follows:

$$M + N = \tfrac{1}{4}(a-1)b + \tfrac{1}{4}(a \mp 1),$$

and therefore:

$$\phi(2b,a) - \phi(b,a) = \tfrac{1}{4}(a-1)b + \tfrac{1}{4}(a \mp 1) - 2N.$$

Accordingly the formula for g found in aricles 73 and 64 becomes:

$$g = \tfrac{1}{8}((a+b)^2-1) + 2n - 4N,$$

if we set $a \mp 1 = 4n$, where n is an integer. However, since we obtain from this $1 = 16n^2 - 8an + a^2$, then this formula can also be represented as follows:

$$g = \tfrac{1}{8}(-a^2+2ab+b^2+1) + 4(\tfrac{1}{2}(a+1)n - n^2 - N).$$

Now, since g is the character of the number $-1-i$ for the modulus $a+bi$, then accordingly this character will be $\equiv \frac{1}{8}(-a^2+2ab+b^2+1)$ which is the very theorem found through induction above (article 64), and the theorem pertaining to the character of the numbers $1+i, 1-i, -1+i$ proceeds immedeiately from this. Consequently these four theorems for that case in which a and b are positve, have now been rigourously proven.

If b is negative, while a remains positive, then $b = -b'$ such that b' will be positive, now since it is to be proven that for the modulus $a + b'i$ the character of the number $-1 - i$ is congruent to $\frac{1}{8}(-a^2 + 2ab' + b'^2 + 1)$, then the character of the number $-1 + i$ for the modulus $a - b'i$ will be congrent to $\frac{1}{8}(a^2 - 2ab' - b'^2 - 1)$ according to the theorem brought foward in article 62, i.e. the character of the number $-1 + i$ for the modulus $a + bi$ is congruent to $\frac{1}{8}(a^2 + 2ab - b^2 - 1)$; but this is exactly the theorem given in article 64, whereby the three remaining theorems pertaining to the character of the numbers $1 + i, 1 - i, -1 - i$ immediately follow. Consequently, these theorems are also proven for the case where b is negative viz. for all cases in which a is positive.

Finally, if a is negative, then $a = -a', b = -b'$. Now since, by what was already proven, the character of the number $1 + i$ with respect to the modulus $a + b'i$ is $\equiv \frac{1}{8}(-a'^2 + 2a'b' - 3b'^2 + 1) \pmod 4$ and is all the same, whether we have the number $a' + b'i$ or the opposite $-a' - b'i$ as the modulus, the character of the number $1 + i$ in reference to the modulus $a + bi$ is evidently $\equiv \frac{1}{8}(-a^2 + 2ab - 3b^2 + 1) \pmod 4$ and something similar applies regaurding the characters fo the numbers $1 - i, -1 + i, -1 - i$.

Therefore if follows that the proof of the theorems concerning the characters of the numbers $1 + i, 1 - i, -1 + i, -1 - i$ (article 63 and 64) are liable to no further limitation.