A NEW PROOF OF AN

ARITHMETIC THEOREM

A U T H O R

CARL FRIEDRICH GAUSS

PRESENTED TO THE ROYAL SOCIETY OF SCIENCE JAN. 15, 1808

Commentationes societatis regiae scientiarum Gottingensis. Vol. XVI.
Göttingen 1808.

A NEW PROOF OF AN

ARITHMETIC THEOREM

1.

Questions in higher arithmetic lead frequently to singular phenomena, much more so than in analysis, and this contributes a great deal to their allure. In analytical investigations it is evidently impossible to discover new truths, unless the way to them has been revealed by our mastery of their underlying principles. On the other hand, in arithmetic it is very often the case that, through induction and by some unexpected fortune, the most elegant new truths spring up, the demonstrations of which are so deeply hidden and shrouded in so much darkness, that they elude all efforts, and deny access to the keenest investigations. Furthermore, there are so many surprising connections between arithmetic truths, which are at first sight most heterogeneous, that we not infrequently arrive at a demonstration much desired and sought after through long meditations by a path very different from that which had been expected, while we are looking for something quite different. Generally speaking, truths of this kind are of such a nature that they can be approached by several very different paths, and it is not always the shortest paths that present themselves at first. With such a truth, which has been demonstrated through the most abstruse detours, it is certainly valuable if one happens to discover a simpler and more genuine explanation.

2.

Among the questions mentioned in the preceding article, a prominent place is held by the theorem containing almost all the theory of quadratic residues, which in *Disquisitiones Arithmeticae* (Sect. IV) is distinguished by the name *fundamental theorem.* LEGENDRE is undoubtedly to be regarded as the *first* discoverer of this

most elegant theorem, although the great geometers EULER and LAGRANGE had long before discovered several of its special cases by induction. I will not dwell here on enumerating the efforts of these men to find a demonstration; the reader is referred to their extensive work which has just been mentioned. However it is permissible to add, in confirmation of what has been stated in the previous article, an account of my own efforts. I had fallen upon the theorem on my own in 1795, at a time when I was completely ignorant of all that had already been discovered in higher arithmetic, and was completely shut out from literary resources. For a whole year it tortured me, and eluded me despite my most strenuous efforts, until at last I received the demonstration that I have delivered in the fourth Section of the aforementioned work. Afterwards, three others presented themselves to me, based on entirely different principles, one of which I delivered in the fifth Section. But all these demonstrations, even if they seem to leave nothing to be desired with regard to rigor, are derived from very heterogeneous principles, except perhaps the first, which nevertheless proceeded by more laborious reasoning, and was burdened by more extensive operations. Therefore, I have no doubt that until now a genuine demonstration has not been given; let it now be up to the experts to judge whether that which has lately been successfully discovered, and which the following pages present, deserves to be decorated with this name.

3.

THEOREM. *Let p be a positive prime number, and let k any integer not divisible by p;*

A the complex of numbers $1, 2, 3 \ldots \frac{1}{2}(p-1)$

B the complex of numbers $\frac{1}{2}(p+1), \frac{1}{2}(p+3), \frac{1}{2}(p+5) \ldots p-1$

Let us consider the minimal positive residues modulo p of the product of k with each of the numbers in A. These will obviously all be different, with some belonging to A and others to B. Now if it is assumed that, among the resulting residues, μ of them belong to B, then k will either be a quadratic residue or a quadratic non-residue modulo p, according as μ is even or odd.

Proof. Let the residues belonging to A be a, a', $a'' \ldots$, and let the remaining residues belonging to B be b, b', $b'' \ldots$. It is clear that the complements of the latter, $p-b$, $p-b'$, $p-b'' \ldots$, are all distinct from the numbers a, a', $a'' \ldots$, and that, taken together, they complete the complex A. We therefore have

$$1.2.3\ldots\tfrac{1}{2}(p-1) = aa'a''\ldots(p-b)(p-b')(p-b'')\ldots$$

Now the latter product clearly becomes

$$\equiv (-1)^{\mu} aa'a''\ldots bb'b''\ldots \equiv (-1)^{\mu} k.2k.3k\ldots\tfrac{1}{2}(p-1)k$$
$$\equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)} 1.2.3\ldots\tfrac{1}{2}(p-1) \pmod{p}$$

Hence we have

$$1 \equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)}$$

or $k^{\frac{1}{2}(p-1)} \equiv \pm 1$, according as μ is even or odd, from which our theorem immediately follows.

4.

The following considerations will be greatly shortened by the introduction of certain notation. We therefore let the symbol (k, p) denote the multitude of residues of the products

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

whose minimal positive residues exceed $\frac{1}{2}p$. Moreover, for any non-integral quantity x, we denote by $[x]$ the greatest integer less than or equal to x, so that $x - [x]$ is always a positive quantity between 0 and 1. We can now develop the following relations with ease:

I. $[x] + [-x] = -1$.

II. $[x] + h = [x + h]$, whenever h is an integer.

III. $[x] + [h - x] = h - 1$.

IV. If $x - [x]$ is a fraction smaller than $\frac{1}{2}$, then $[2x] - 2[x] = 0$; if it is greater than $\frac{1}{2}$, then $[2x] - 2[x] = 1$.

V. If the minimal positive residue of an integer h exceeds $\frac{1}{2}p$ modulo p, then $\left[\frac{2h}{p}\right] - 2\left[\frac{h}{p}\right] = 0$; if it is less than or equal to $\frac{1}{2}p$ modulo p, then $\left[\frac{2h}{p}\right] - 2\left[\frac{h}{p}\right] = 1$.

VI. From this it immediately follows that $(k,p) =$

$$\left[\tfrac{2k}{p}\right] + \left[\tfrac{4k}{p}\right] + \left[\tfrac{6k}{p}\right] \ldots + \left[\tfrac{(p-1)k}{p}\right]$$
$$-2\left[\tfrac{k}{p}\right] - 2\left[\tfrac{2k}{p}\right] - 2\left[\tfrac{3k}{p}\right] \ldots - 2\left[\tfrac{\frac{1}{2}(p-1)k}{p}\right].$$

VII. From VI and I, we can easily deduce

$$(k,p) + (-k,p) = \tfrac{1}{2}(p-1)$$

Hence, it follows that $-k$ has the same or opposite relation to p (insofar as it is a quadratic residue or non-residue) as does $+k$, depending on whether p is of the form $4n+1$ or $4n+3$. In the former case, it is obvious that -1 will be a quadratic residue, while in the latter case, it will be a non-residue modulo p.

VIII. We will transform the formula given in VI as follows. From III, we have

$$\left[\tfrac{(p-1)k}{p}\right] \equiv k-1-\left[\tfrac{k}{p}\right], \left[\tfrac{(p-3)k}{p}\right] = k-1-\left[\tfrac{3k}{p}\right], \left[\tfrac{(p-5)k}{p}\right] = k-1-\left[\tfrac{5k}{p}\right] \ldots$$

Applying these substitutions to $\frac{p\mp 1}{4}$ terms in the series above, we have

first, if p is of the form $4n+1$, then

$$(k,p) = \tfrac{1}{4}(k-1)(p-1)$$
$$-2\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{3k}{p}\right] + \left[\tfrac{5k}{p}\right] \ldots + \left[\tfrac{\frac{1}{2}(p-3)k}{p}\right]\right\}$$
$$-\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{2k}{p}\right] + \left[\tfrac{3k}{p}\right] \ldots + \left[\tfrac{\frac{1}{2}(p-1)k}{p}\right]\right\}$$

second, if p is of the form $4n+3$, then

$$(k,p) = \tfrac{1}{4}(k-1)(p+1)$$
$$-2\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{3k}{p}\right] + \left[\tfrac{5k}{p}\right] \ldots + \left[\tfrac{\frac{1}{2}(p-1)k}{p}\right]\right\}$$
$$-\left\{\left[\tfrac{k}{p}\right] + \left[\tfrac{2k}{p}\right] + \left[\tfrac{3k}{p}\right] \ldots + \left[\tfrac{\frac{1}{2}(p-1)k}{p}\right]\right\}$$

IX. For the special case $k = +2$, it follows from the formulas given above that $(2,p) = \frac{1}{4}(p\mp 1)$, with the sign being taken as $+$ or $-$ depending on whether p is of the form $4n+1$ or $4n+3$. Thus, $(2,p)$ is even and $2Rp$, whenever p is of the form $8n+1$ or $8n+7$; on the contrary, $(2,p)$ is odd and $2Np$, whenever p is of the form $8n+3$ or $8n+5$.

5.

THEOREM. *Let x be a positive non-integer quantity, such that no multiple of x, $2x$, $3x\ldots$ up to nx is an integer. Letting $[nx]=h$, it is easily concluded that no integer can be found among the multiples of the reciprocal quantities $\frac{1}{x}$, $\frac{2}{x}$, $\frac{3}{x}\ldots$ up to $\frac{h}{x}$. Then I say that*

$$\left.\begin{array}{r}[x]+[2x]+[3x]\cdots+[nx]\\ +\left[\frac{1}{x}\right]+\left[\frac{2}{x}\right]+\left[\frac{3}{x}\right]\ldots+\left[\frac{h}{x}\right]\end{array}\right\}=nh$$

Proof. Let Ω represent the series $[x]+[2x]+[3x]\ldots+[nx]$. Then the terms up to the $\left[\frac{1}{x}\right]^{\text{th}}$ term inclusively are clearly all $=0$; the terms up to the $\left[\frac{2}{x}\right]^{\text{th}}$ term inclusively are all $=1$; the terms up to the $\left[\frac{3}{x}\right]^{\text{th}}$ term inclusively are all $=2$ and so on. Hence we have

$$\left.\begin{array}{l}\Omega=0\times\left[\frac{1}{x}\right]\\ \quad+1\times\left\{\left[\frac{2}{x}\right]-\left[\frac{1}{x}\right]\right\}\\ \quad+2\times\left\{\left[\frac{3}{x}\right]-\left[\frac{2}{x}\right]\right\}\\ \quad+3\times\left\{\left[\frac{4}{x}\right]-\left[\frac{3}{x}\right]\right\}\\ \qquad\text{etc.}\\ \quad+(h-1)\left\{\left[\frac{h}{x}\right]-\left[\frac{h-1}{x}\right]\right\}\\ \quad+h\left\{n-\left[\frac{h}{x}\right]\right\}\end{array}\right\}=hn-\left[\frac{1}{x}\right]-\left[\frac{2}{x}\right]-\left[\frac{3}{x}\right]\ldots-\left[\frac{h}{x}\right]$$

Q. E. D.

6.

THEOREM. *Let k, p be any odd positive integers that are prime to each other. Then*

$$\left.\begin{array}{r}\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\\ +\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ldots+\left[\frac{\frac{1}{2}(k-1)p}{k}\right]\end{array}\right\}=\tfrac{1}{4}(k-1)(p-1).$$

Proof. Suppose, which is allowed, that $k<p$. Then $\frac{\frac{1}{2}(p-1)k}{p}$ is smaller than $\frac{1}{2}k$, but larger than $\frac{1}{2}(k-1)$, so $\left[\frac{\frac{1}{2}(p-1)k}{p}\right]=\frac{1}{2}(k-1)$. Hence, it is clear that the current theorem follows immediately from the previous theorem by taking $\frac{k}{p}=x$, $\frac{1}{2}(p-1)=n$, and therefore $\frac{1}{2}(k-1)=h$.

It can be demonstrated in a similar manner that if k is an *even* number, relatively prime to p, then

$$\left.\begin{array}{r}\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\\ +\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ldots+\left[\frac{\frac{1}{2}kp}{k}\right]\end{array}\right\}=\tfrac{1}{4}k(p-1)$$

But we do not dwell on this proposition, which is not necessary for our purposes.

7.

Now, by combining the theorem mentioned above with proposition VIII of article 4, the fundamental theorem immediately follows. Indeed, let k and p be any two distinct positive prime numbers, and let

$$(k,p)+\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]\ldots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]=L$$

$$(p,k)+\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]\ldots+\left[\frac{\frac{1}{2}(k-1)p}{k}\right]=M$$

Then by proposition VIII of article 4, it is clear that L and M are always even. But by the theorem of Article 6, we have

$$L+M=(k,p)+(p,k)+\tfrac{1}{4}(k-1)(p-1)$$

Therefore, when $\frac{1}{4}(k-1)(p-1)$ turns out to be even, which occurs if either both k and p are of the form $4n+1$ or if one of them is of the form $4n+1$, it is necessary that either both (k,p) and (p,k) are even or both are odd. On the other hand, when $\frac{1}{4}(k-1)(p-1)$ is odd, which happens if both k and p are of the form $4n+3$, it is necessary that one of the numbers (k,p) and (p,k) is even and the other is odd. In the former case, then, the relation of k to p and the relation of p to k (insofar as one is a quadratic residue or non-residue modulo the other) will be identical, and in the latter case they will be opposite.

Q. E. D.

SUMMATION OF CERTAIN

SINGULAR SERIES

A U T H O R

CARL FRIEDRICH GAUSS

PRESENTED TO THE SOCIETY ON AUGUST 24, 1808

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. I.

Göttingen, 1811

SUMMATION OF

CERTAIN SINGULAR SERIES.

1.

Among the remarkable truths to which the theory of the division of the circle has opened the way, the summation proposed in *Disquisitiones Arithmeticae* art. 356 claims not the last place for itself, not only because of its particular elegance and wonderful fecundity, which will be explained more fully on another occasion, but also because its rigorous demonstration is not burdened by uncommon difficulties. Of course, this should have been expected, since the difficulties do not fall so much into the theorem itself, but rather into a limitation of the theorem, which was then ignored, but whose demonstration is immediately available and easily derived from the theory explained in the present work. The theorem is presented there in the following form. Supposing n to be a prime number, denoting all of the quadratic residues of n between the limits 1 and $n-1$ (incl.) indefinitely by a, denoting all the non-residues between the same limits by b, denoting by ω the arc $\frac{360^\circ}{n}$, and by k any fixed integer not divisible by n, we have

I. for values of n which are of the form $4m+1$,

$$\begin{aligned} \Sigma \cos ak\omega &= -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{n} \\ \Sigma \cos bk\omega &= -\tfrac{1}{2} \mp \tfrac{1}{2}\sqrt{n}, \text{ and therefore} \\ \Sigma \cos ak\omega - \Sigma \cos bk\omega &= \pm\sqrt{n} \\ \Sigma \sin ak\omega &= 0 \\ \Sigma \sin bk\omega &= 0 \end{aligned}$$

II. for values of n which are of the form $4m+3$,

$$\Sigma \cos ak\omega = -\tfrac{1}{2}$$
$$\Sigma \cos bk\omega = -\tfrac{1}{2}$$
$$\Sigma \sin ak\omega = \pm\tfrac{1}{2}\sqrt{n}$$
$$\Sigma \sin bk\omega = \mp\tfrac{1}{2}\sqrt{n}$$
$$\Sigma \sin ak\omega - \Sigma \sin bk\omega = \pm\sqrt{n}$$

These sums have been demonstrated with all rigor in loc. cit., and the only remaining difficulty is in determining the *sign* to be assigned to the radical quantity. It can easily be shown that this sign depends only on the number k, that the *same* sign must hold for all values of k that are quadratic residues modulo n, and that the opposite sign must hold for all values of k that are non-residues of n. Therefore, the whole matter revolves around the case $k=1$, and it is evident that as soon as the sign for this value is known, the signs for all other values of k will immediately follow. But in this very question, which at first glance seems to be among the easier ones, we encounter unforeseen difficulties and the method with which we have made progress so far completely denies us further help.

2.

It would not be out of place, before we proceed further, to work out some examples of our summation by numerical calculation: however, it will be convenient to preface this with some general observations.

I. If in the case where n is a prime number of the form $4m+1$, all quadratic residues of n lying between 1 and $\frac{1}{2}(n-1)$ (inclusive) are denoted indefinitely by a', and all non-residues between the same limits are denoted by b', it follows that all $n-a'$ lie among the a, and all $n-b'$ lie among the b. Therefore, since a', b', $n-a'$, $n-b'$ together clearly exhaust the entire set of numbers 1, 2, 3, ..., $n-1$, all a' together with all $n-a'$ include all a, and likewise all b' together with all $n-b'$ include all b. Hence we have

$$\Sigma \cos ak\omega = \Sigma \cos a'k\omega + \Sigma \cos(n-a')k\omega$$
$$\Sigma \cos bk\omega = \Sigma \cos b'k\omega + \Sigma \cos(n-b')k\omega$$
$$\Sigma \sin ak\omega = \Sigma \sin a'k\omega + \Sigma \sin(n-a')k\omega$$
$$\Sigma \sin bk\omega = \Sigma \sin b'k\omega + \Sigma \sin(n-b')k\omega$$

Now, considering that $\cos(n-a')k\omega = \cos a'k\omega$, $\cos(n-b')k\omega = \cos b'k\omega$, $\sin(n-a')k\omega = -\sin a'k\omega$, $\sin(n-b')k\omega = -\sin b'k\omega$, it is obvious that

$$\Sigma \sin ak\omega = \Sigma \sin a'k\omega - \Sigma \sin a'k\omega = 0$$
$$\Sigma \sin bk\omega = \Sigma \sin b'k\omega - \Sigma \sin b'k\omega = 0$$

The summation of cosines, on the other hand, takes on the form

$$\Sigma \cos ak\omega = 2\Sigma \cos a'k\omega$$
$$\Sigma \cos bk\omega = 2\Sigma \cos b'k\omega$$

from which it follows that

$$1 + 4\Sigma \cos a'k\omega = \pm\sqrt{n}$$
$$1 + 4\Sigma \cos b'k\omega = \mp\sqrt{n}$$
$$2\Sigma \cos a'k\omega - 2\Sigma \cos b'k\omega = \pm\sqrt{n}$$

II. In the case where n is of the form $4m+3$, the complement of any quadratic residue a modulo n will be a non-residue, and the complement of any non-residue b will be a quadratic residue; therefore, all $n-a$ will coincide with all b, and all $n-b$ will coincide with all a. Hence we conclude

$$\Sigma \cos ak\omega = \Sigma \cos(n-b)k\omega = \Sigma \cos bk\omega$$

and so, since all a and b together cover all the numbers 1, 2, 3, $\ldots n-1$, it follows that

$$\Sigma \cos ak\omega + \Sigma \cos bk\omega = \cos k\omega + \cos 2k\omega + \cos 3k\omega + \text{etc.} + \cos(n-1)k\omega = -1,$$

and the summations

$$\Sigma \cos ak\omega = -\tfrac{1}{2}$$
$$\Sigma \cos bk\omega = -\tfrac{1}{2}$$

are therefore evident. Similarly,

$$\Sigma \sin ak\omega = \Sigma \sin(n-b)k\omega = -\Sigma \sin bk\omega$$

and from this it is clear how the summations

$$2\Sigma \sin ak\omega = \pm\sqrt{n}$$
$$2\Sigma \sin bk\omega = \mp\sqrt{n}$$

depend upon each other.

3.

Now here are some examples of numerical computations:

I. For $n = 5$, there is one value of a', namely $a' = 1$, and one value of b', namely $b' = 2$; and these are

$$\cos\omega = +0{,}3090169944 \qquad \cos 2\omega = -0{,}8090169944$$

Hence $1 + 4\cos\omega = +\sqrt{5},\ 1 + 4\cos 2\omega = -\sqrt{5}$.

II. For $n = 13$, there are three values of a', namely 1, 3, 4, and an equal number of values of b', namely 2, 5, 6, from which we compute

$\cos\omega = +0{,}8854560257$	$\cos 2\omega = +0{,}5680647467$
$\cos 3\omega = +0{,}1205366803$	$\cos 5\omega = -0{,}7485107482$
$\cos 4\omega = -0{,}3546048870$	$\cos 6\omega = -0{,}9709418174$
Sum $= +0{,}6513878190$	Sum $= -1{,}1513878189$

Hence $1 + 4\Sigma\cos a'\omega = +\sqrt{13},\ 1 + 4\Sigma\cos b'\omega = -\sqrt{13}$.

III. For $n = 17$, we have four values of a', namely 1, 2, 4, 8, and an equal number of values of b', namely 3, 5, 6, 7. From this, we compute the cosines

$\cos\omega = +0{,}9324722294$	$\cos 3\omega = +0{,}4457383558$
$\cos 2\omega = +0{,}7390089172$	$\cos 5\omega = -0{,}2736629901$
$\cos 4\omega = +0{,}0922683595$	$\cos 6\omega = -0{,}6026346364$
$\cos 8\omega = -0{,}9829730997$	$\cos 7\omega = -0{,}8502171357$
Sum $= +0{,}7807764064$	Sum $= -1{,}2807764065$

Hence $1 + 4\Sigma\cos a'\omega = +\sqrt{17}, 1 + 4\Sigma\cos b'\omega = -\sqrt{17}$.

IV. For $n = 3$, there is one value of a, namely $a = 1$, which corresponds to

$$\sin\omega = +0.8660254038$$

Hence, $2\sin\omega = +\sqrt{3}$.

V. For $n = 7$, there are three values of a, namely 1, 2, 4: hence we have the sines

$$\begin{aligned}
\sin\omega &= +0{,}7818314825\\
\sin 2\omega &= +0{,}9749279122\\
\sin 4\omega &= -0{,}4338837391\\
\hline
\text{Sum} &= +1{,}3228756556, \text{ hence } 2\Sigma\sin a\omega = +\sqrt{7}.
\end{aligned}$$

VI. For $n = 11$, the values of a are 1, 3, 4, 5, 9, which correspond to sines

$$\begin{aligned}
\sin\omega &= +0{,}5406408175\\
\sin 3\omega &= +0{,}9898214419\\
\sin 4\omega &= +0{,}7557495744\\
\sin 5\omega &= +0{,}2817325568\\
\sin 9\omega &= -0{,}9096319954\\
\hline
\text{Sum} &= +1{,}6583123952, \text{ hence } 2\Sigma\sin a\omega = +\sqrt{11}.
\end{aligned}$$

VII. For $n = 19$, the values of a are 1, 4, 5, 6, 7, 9, 11, 16, 17, which correspond to sines

$$\begin{aligned}
\sin\omega &= +0{,}3246994692\\
\sin 4\omega &= +0{,}9694002659\\
\sin 5\omega &= +0{,}9965844930\\
\sin 6\omega &= +0{,}9157733267\\
\sin 7\omega &= +0{,}7357239107\\
\sin 9\omega &= +0{,}1645945903\\
\sin 11\omega &= -0{,}4759473930\\
\sin 16\omega &= -0{,}8371664783\\
\sin 17\omega &= -0{,}6142127127\\
\hline
\text{Sum} &= +2{,}1794494718, \text{ hence } 2\Sigma\sin a\omega = +\sqrt{19}.
\end{aligned}$$

4.

In all these examples the radical quantity obtains a positive sign, and the same is easily confirmed for larger values $n = 23$, $n = 29$, etc., from which a strong likelihood emerges that this holds generally. However, the proof of this phenomenon cannot be sought from the principles set forth in loc. cit., and must be regarded as deserving of a thorough investigation. Therefore, the purpose of this commentary is to present a rigorous proof of this most elegant theorem, which has been attempted in vain in various ways for many years, and was finally achieved successfully through careful and subtle considerations. At the same time, we will bring the theorem itself, with its elegance preserved or rather enhanced, to a much greater generality. Finally, in the conclusion, we will reveal a remarkable and close connection between this summation and another very important arithmetic theorem. We hope that not only will geometers be gratified by the results of these investigations, but also that the methods, which may well be useful on other occasions, will be deemed worth of their attention.

5.

Our proof relies on the consideration of a specific type of progression, whose terms depend on expressions of the form

$$\frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})\ldots(1-x^{m-\mu+1})}{(1-x)(1-xx)(1-x^3)\ldots(1-x^\mu)}$$

For the sake of brevity, we will denote such a fraction by (m, μ), and we will first present some general observations about such functions.

I. Whenever m is a positive integer smaller than μ, the function (m, μ) clearly vanishes, since the numerator involves the factor $1 - x^0$. For $m = \mu$, the factors in the numerator will be identical, but in the reverse order compared to the factors in the denominator, so that $(\mu, \mu) = 1$. Finally, in the case where m is a positive integer greater than μ, we have the formulas

$$(\mu+1, \mu) = \frac{1-x^{\mu+1}}{1-x} = (\mu+1, 1)$$
$$(\mu+2, \mu) = \frac{(1-x^{\mu+2})(1-x^{\mu+1})}{(1-x)(1-xx)} = (\mu+2, 2)$$
$$(\mu+3, \mu) = \frac{(1-x^{\mu+3})(1-x^{\mu+2})(1-x^{\mu+1})}{(1-x)(1-xx)(1-x^3)} = (\mu+3, 3) \text{ etc.}$$

or more generally,

$$(m, \mu) = (m, m - \mu)$$

II. Furthermore, it is easily confirmed that, in general,

$$(m, \mu + 1) = (m - 1, \mu + 1) + x^{m-\mu-1}(m - 1, \mu)$$

and likewise

$$(m-1, \mu+1) = (m-2, \mu+1) + x^{m-\mu-2}(m-2, \mu)$$
$$(m-2, \mu+1) = (m-3, \mu+1) + x^{m-\mu-3}(m-3, \mu)$$
$$(m-3, \mu+1) = (m-4, \mu+1) + x^{m-\mu-4}(m-4, \mu) \text{ etc.}$$

which continues until

$$(\mu+2, \mu+1) = (\mu+1, \mu+1) + x(\mu+1, \mu)$$
$$= (\mu, \mu) + x(\mu+1, \mu)$$

and therefore, as long as m is a positive integer greater than $\mu + 1$,

$$(m, \mu+1) = (\mu, \mu) + x(\mu+1, \mu) + xx(\mu+2, \mu) + x^3(\mu+3, \mu) + \text{etc.} + x^{m-\mu-1}(m-1, \mu)$$

Hence it is clear that if, for any given value of μ the function (m, μ) is integral for all positive integer values of m, then the function $(m, \mu+1)$ must also be integral. Therefore, since this assumption holds for $\mu = 1$, the same will hold for $\mu = 2$, and thus for $\mu = 3$ etc., i.e. in general for any positive integer value of m the function (m, μ) will be integral, or in other words the product

$$(1 - x^m)(1 - x^{m-1})(1 - x^{m-2}) \ldots (1 - x^{m-\mu+1})$$

will be divisible by

$$(1 - x)(1 - x^2)(1 - x^3) \ldots (1 - x^\mu).$$

6.

We will now consider two series, both of which will help us reach our goal. The first series is

$$1-\tfrac{1-x^m}{1-x}+\tfrac{(1-x^m)(1-x^{m-1})}{(1-x)(1-xx)}-\tfrac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-xx)(1-x^3)}+\ldots$$

or

$$1-(m,1)+(m,2)-(m,3)+(m,4)-\ldots$$

which for the sake of brevity we will denote by $f(x,m)$. It is immediately obvious that when m is a positive integer, this series *terminates* after its $m+1^{\text{st}}$ term (which is $=\pm 1$), and therefore in this case, the sum must be a finite integral function of x. Furthermore, according to observation II from article 5, it is clear that generally, for any value of m, we have

$$\begin{aligned}1&=1\\ -(m,1)&=-(m-1,1)-x^{m-1}\\ +(m,2)&=+(m-1,2)+x^{m-2}(m-1,1)\\ -(m,3)&=-(m-1,3)-x^{m-3}(m-1,2)\ldots\end{aligned}$$

and therefore

$$\begin{aligned}f(x,m)=1-x^{m-1}&-(1-x^{m-2})(m-1,1)+(1-x^{m-3})(m-1,2)\\ &-(1-x^{m-4})(m-1.3)+\ldots\end{aligned}$$

But it is clear that

$$\begin{aligned}(1-x^{m-2})(m-1,1)&=(1-x^{m-1})(m-2,1)\\ (1-x^{m-3})(m-1,2)&=(1-x^{m-1})(m-2,2)\\ (1-x^{m-4})(m-1,3)&=(1-x^{m-1})(m-2,3)\ldots\end{aligned}$$

from which we deduce the equation

$$f(x,m)=(1-x^{m-1})f(x,m-2) \qquad [1]$$

7.

Since $f(x,m)=1$ for $m=0$, we obtain, from the formula we have just found,

$$\begin{aligned}f(x,2)&=1-x\\ f(x,4)&=(1-x)(1-x^3)\\ f(x,6)&=(1-x)(1-x^3)(1-x^5)\\ f(x,8)&=(1-x)(1-x^3)(1-x^5)(1-x^7)\ \text{etc.}\end{aligned}$$

or more generally, for any even value of m,

$$f(x,m)=(1-x)(1-x^3)(1-x^5)\ldots(1-x^{m-1}) \qquad [2]$$

On the other hand, since $f(x,m)=0$ for $m=1$, we have

$$f(x,3)=0$$
$$f(x,5)=0$$
$$f(x,7)=0 \text{ etc.}$$

or, in general, for any odd value of m,

$$f(x,m)=0$$

Moreover, the latter sum could have already been derived from the fact that in the series

$$1-(m,1)+(m,2)-(m,3)+\text{etc.}+(m,m-1)-(m,m),$$

the last term destroys the first, the penultimate destroys the second, etc.

8.

For our purpose it suffices to consider the case where m is a positive odd integer. However, due to the singularity of the matter, it will not hurt to add a few remarks about the cases where m is fractional or negative. Clearly in these cases our series will not be interrupted, but will diverge to infinity. Moreover, it is easily seen that it diverges whenever the value of x is less than 1, so its summation should be restricted to values of x which are greater than 1.

According to formula [1] in article 6, we have

$$f(x,-2)=\tfrac{1}{1-\frac{1}{x}}$$
$$f(x,-4)=\tfrac{1}{1-\frac{1}{x}}\cdot\tfrac{1}{1-\frac{1}{x^3}}$$
$$f(x,-6)=\tfrac{1}{1-\frac{1}{x}}\cdot\tfrac{1}{1-\frac{1}{x^3}}\cdot\tfrac{1}{1-\frac{1}{x^5}} \text{ etc.}$$

so that for negative, even, integral values of m, the function $f(x,m)$ can also be assigned a value with finitely many terms. For the remaining values of m, we will convert the function $f(x,m)$ into an *infinite product* using the following method.

As m approaches negative infinity, the function $f(x,m)$ converges to

$$1+\tfrac{1}{x-1}+\tfrac{1}{x-1}\cdot\tfrac{1}{xx-1}+\tfrac{1}{x-1}\cdot\tfrac{1}{xx-1}\cdot\tfrac{1}{x^3-1}+\text{etc.}$$

Therefore, this series is equal to the infinite product

$$\tfrac{1}{1-\frac{1}{x}}\cdot\tfrac{1}{1-\frac{1}{x^3}}\cdot\tfrac{1}{1-\frac{1}{x^5}}\cdot\tfrac{1}{1-\frac{1}{x^7}}\text{etc. to infinity}$$

Moreover, since it is generally true that

$$f(x,m)=f(x,m-2\lambda).(1-x^{m-1})(1-x^{m-3})(1-x^{m-5})\ldots(1-x^{m-2\lambda+1})$$

we have

$$\begin{aligned}f(x,m)&=f(x,-\infty)\cdot(1-x^{m-1})(1-x^{m-3})(1-x^{m-5})\text{ etc. to infinity}\\&=\tfrac{1-x^{m-1}}{1-x^{-1}}\cdot\tfrac{1-x^{m-3}}{1-x^{-3}}\cdot\tfrac{1-x^{m-5}}{1-x^{-5}}\cdot\tfrac{1-x^{m-7}}{1-x^{-7}}\text{ etc. to infinity}\end{aligned}$$

whose factors clearly converge to unity.

The case $m=-1$ deserves special attention. Here we have

$$f(x,-1)=1+x^{-1}+x^{-3}+x^{-6}+x^{-10}+\text{etc.}$$

It follows that this series can be expressed as an infinite product

$$\tfrac{1-x^{-2}}{1-x^{-1}}\cdot\tfrac{1-x^{-2}}{1-x^{-3}}\cdot\tfrac{1-x^{-6}}{1-x^{-5}}\text{ etc.}$$

or, by replacing x with x^{-1},

$$1+x+x^3+x^6+\text{etc.}=\tfrac{1-xx}{1-x}\cdot\tfrac{1-x^4}{1-x^3}\cdot\tfrac{1-x^6}{1-x^5}\cdot\tfrac{1-x^8}{1-x^7}\text{ etc.}$$

This equality between two somewhat complicated expressions, to which we will return on another occasion, is indeed very remarkable.

9.

Secondly, we consider the series

$$1+x^{\frac{1}{2}}\tfrac{1-x^m}{1-x}+x\tfrac{(1-x^m)}{(1-x)}\tfrac{(1-x^{m-1})}{(1-xx)}+x^{\frac{3}{2}}\tfrac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-xx)(1-x^3)}+\text{etc.}$$

or

$$1+x^{\frac{1}{2}}(m,1)+x(m,2)+x^{\frac{3}{2}}(m,3)+xx(m,4)+\text{etc.}$$

which we will denote by $F(x,m)$. We will restrict this discussion to the case where m is a positive integer, so that the series always terminates at the $m+1^{\text{st}}$ term,

which is $= x^{\frac{1}{2}m}(m,m)$. Since

$$(m,m) = 1, \quad (m,m-1) = (m,1), \quad (m,m-2) = (m,2) \text{ etc.}$$

the above series can also be expressed as:

$$F(x,m) = x^{\frac{1}{2}m} + x^{\frac{1}{2}(m-1)}(m,1) + x^{\frac{1}{2}(m-2)}(m,2) + x^{\frac{1}{2}(m-3)}(m,3) + \text{etc.}$$

Hence we have

$$\begin{aligned}(1 + x^{\frac{1}{2}m+\frac{1}{2}})F(x,m) = 1 + x^{\frac{1}{2}}(m,1) + x(m,2) + x^{\frac{3}{2}}(m,3) + \text{etc.} \\ + x^{\frac{1}{2}}.x^m + x.x^{m-1}(m,1) + x^{\frac{3}{2}}.x^{m-2}(m,2) + \text{etc.}\end{aligned}$$

Therefore (article 5, II),

$$\begin{aligned}(m,1) + x^m &= (m+1,1) \\ (m,2) + x^{m-1}(m,1) &= (m+1,2) \\ (m,3) + x^{m-2}(m,2) &= (m+1,3) \text{ etc.},\end{aligned}$$

we obtain the result

$$(1 + x^{\frac{1}{2}m+\frac{1}{2}})F(x,m) = F(x,m+1) \qquad [3]$$

But $F(x,0) = 1$; therefore we have

$$\begin{aligned}F(x,1) &= 1 + x^{\frac{1}{2}} \\ F(x,2) &= (1 + x^{\frac{1}{2}})(1+x) \\ F(x,3) &= (1 + x^{\frac{1}{2}})(1+x)(1+x^3) \text{ etc.},\end{aligned}$$

or in general

$$F(x,m) = (1 + x^{\frac{1}{2}})(1+x)(1+x^{\frac{3}{2}}) \ldots (1 + x^{\frac{1}{2}m}) \qquad [4]$$

10.

Having made these preliminary observations, let us now proceed towards our objective. Since the squares $1,\ 4,\ 9 \ldots (\frac{1}{2}(n-1))^2$ are all incongruent to each other modulo n, it is clear that their minimal residues modulo n must be identical to the numbers a, and therefore

$$\begin{aligned}\Sigma \cos akw &= \cos kw + \cos 4kw + \cos 9kw + \text{etc.} + \cos(\tfrac{1}{2}(n-1))^2 kw \\ \Sigma \sin akw &= \sin kw + \sin 4kw + \sin 9kw + \text{etc.} + \sin(\tfrac{1}{2}(n-1))^2 kw\end{aligned}$$

Similarly, since the same squares $1, 4, 9, \ldots, (\frac{1}{2}(n-1))^2$ are congruent to $(\frac{1}{2}(n+1))^2, (\frac{1}{2}(n+3))^2, (\frac{1}{2}(n+5))^2, \ldots, (n-1)^2$ in reverse order, we have

$$\Sigma \cos ak\omega = \cos(\tfrac{1}{2}(n+1))^2 k\omega + \cos(\tfrac{1}{2}(n+3))^2 k\omega + \text{etc.} + \cos(n-1)^2 k\omega$$
$$\Sigma \sin ak\omega = \sin(\tfrac{1}{2}(n+1))^2 k\omega + \sin(\tfrac{1}{2}(n+3))^2 k\omega + \text{etc.} + \sin(n-1)^2 k\omega$$

Therefore, assuming

$$T = 1 + \cos k\omega + \cos 4k\omega + \cos 9k\omega + \text{etc.} + \cos(n-1)^2 k\omega$$
$$U = \sin k\omega + \sin 4k\omega + \sin 9k\omega + \text{etc.} + \sin(n-1)^2 k\omega$$

we will have

$$1 + 2\Sigma \cos ak\omega = T$$
$$2\Sigma \sin ak\omega = U$$

Hence it is clear that the sums proposed in article 1 depend on the summation of the series T and U. We will therefore adapt our discussion to these, and complete it in a general way that it includes not only prime values of n but composite ones as well. Let us also suppose that the number k is prime to n; for the case where k and n have a common divisor can be reduced to this one without any difficulty.

11.

Let us denote the imaginary quantity $\sqrt{-1}$ by i, and let

$$\cos k\omega + i \sin k\omega = r$$

so that $r^n = 1$, or r is a root of the equation $r^n - 1 = 0$. It is easy to see that all the numbers k, $2k$, $3k, \ldots, (n-1)k$ are not divisible by n and are incongruent to each other modulo n: therefore, the powers of r

$$1, r, r^2, r^3 \ldots r^{n-1}$$

will all be distinct, and each of them will satisfy the equation $x^n - 1 = 0$. For this reason, these powers will represent all the roots of the equation $x^n - 1 = 0$.

These conclusions would be invalid if k had a common divisor with n. For if ν were such a common divisor, then $k.\frac{n}{\nu}$ would be divisible by n, and hence it would be a power less than r^n, say $r^{\frac{n}{\nu}}$, would equal to unity. In this case, therefore, the powers of r up to the $\frac{n}{\nu}^{th}$ will all be roots of the equation $x^n - 1 = 0$, and indeed they are all the distinct roots, if ν is the *greatest* common divisor of k and n. In

our case, where k and n are assumed to be prime to each other, r can conveniently be called a *proper root* of the equation $x^n - 1 = 0$. In the other case, where k and n have a (greatest) common divisor ν, we will say that r is an *improper root* of that equation. Clearly in the latter case, r would be the proper root of the equation $x^{\frac{n}{\nu}} - 1 = 0$. The simplest improper root is the unity, and in the case where n is a prime number, there are no other improper roots whatsoever.

12.

If we now set

$$W = 1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2}$$

it is clear that $W = T + iU$, so that T is the real part of W itself, and U arises from the imaginary part of W by suppressing the factor i. The whole matter is therefore reduced to finding the sum W: for this purpose either the series considered in article 6, or the one we have shown how to sum in article 9, can be used, although the former is less suitable in the case where n is an even number. Nevertheless, we hope that it will be agreeable to the reader if we treat the case where n is odd according to both methods.

Let us suppose first that n is an odd number, that r is any proper root of the equation $x^n - 1 = 0$, and that in the function $f(x, m)$ we set $x = r$ and $m = n - 1$. Then clearly

$$\begin{aligned}
\tfrac{1-x^m}{1-x} &= \tfrac{1-r^{-1}}{1-r} = -r^{-1} \\
\tfrac{1-x^{m-1}}{1-xx} &= \tfrac{1-r^{-2}}{1-rr} = -r^{-2} \\
\tfrac{1-x^{m-2}}{1-x^3} &= \tfrac{1-r^{-3}}{1-r^3} = -r^{-3} \quad \text{etc.}
\end{aligned}$$

up to

$$\tfrac{1-x}{1-x^m} = \tfrac{1-r^{-m}}{1-r^m} = -r^{-m}$$

(It will not be superfluous to mention that these equations are valid only to the extent that r is assumed to be a proper root: for if r were an improper root, the numerator and denominator of some of these fractions would simultaneously vanish, and thus the fractions would become indeterminate).

From here, we derive the following equation:

$$f(r,n-1) = 1 + r^{-1} + r^{-3} + r^{-6} + \text{etc.} + r^{-\frac{1}{2}(n-1)n}$$
$$= (1-r)(1-r^3)(1-r^5)\ldots(1-r^{n-2})$$

The same equation will still hold if we substitute r^λ for r, where λ is any arbitrary integer relatively prime to n, for then r^λ will also be a proper root of the equation $x^n - 1 = 0$. Let us write r^{n-2} instead of r, or equivalently r^{-2}. This gives

$$1 + r^2 + r^6 + r^{12} + \text{etc.} + r^{(n-1)n} = (1-r^{-2})(1-r^{-6})(1-r^{-10})\ldots(1-r^{-2(n-2)})$$

Now, let's multiply both sides of this equation by

$$r \cdot r^3 \cdot r^5 \ldots \cdot r^{(n-2)} = r^{\frac{1}{4}(n-1)^2}$$

and because

$$r^{2+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n-3)^2}, \qquad r^{(n-1)n+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n+1)^2}$$
$$r^{6+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n-5)^2}, \quad r^{(n-2)(n-1)+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n+3)^2}$$
$$r^{12+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n-7)^2}, \quad r^{(n-3)(n-2)+\frac{1}{4}(n-1)^2} = r^{\frac{1}{4}(n+5)^2} \text{ etc.}$$

we get the following equation

$$r^{\frac{1}{4}(n-1)^2} + r^{\frac{1}{4}(n-3)^2} + r^{\frac{1}{4}(n-5)^2} + \text{etc.} + r + 1$$
$$+ r^{\frac{1}{4}(n+1)^2} + r^{\frac{1}{4}(n+3)^2} + r^{\frac{1}{4}(n+5)^2} + \text{etc.} + r^{\frac{1}{4}(2n-2)^2}$$
$$= (r - r^{-1})(r^3 - r^{-3})(r^5 - r^{-5})\ldots(r^{n-2} - r^{-n+2})$$

or, by rearranging the terms of the first member,

$$1 + r + r^4 + \text{etc.} + r^{(n-1)^2} = (r - r^{-1})(r^3 - r^{-3})\ldots(r^{n-2} - r^{-n+2}) \qquad [5]$$

13.

The factors of the second member of the equation [5] can also be represented as

$$r - r^{-1} = -(r^{n-1} - r^{-n+1})$$
$$r^3 - r^{-3} = -(r^{n-3} - r^{-n+3})$$
$$r^5 - r^{-5} = -(r^{n-5} - r^{-n+5}) \text{ etc.}$$

up to

$$r^{n-2} - r^{-n+2} = -(r^2 - r^{-2})$$

in which case this equation takes the following form:

$$W = (-1)^{\frac{1}{2}(n-1)}(r^2 - r^{-2})(r^4 - r^{-4})(r^6 - r^{-6}) \ldots (r^{n-1} - r^{-n+1})$$

Multiplying this equation by [5] in its original form, we obtain

$$W^2 = (-1)^{\frac{1}{2}(n-1)}(r - r^{-1})(r^2 - r^{-2})(r^3 - r^{-3}) \ldots (r^{n-1} - r^{-n+1})$$

where $(-1)^{\frac{1}{2}(n-1)}$ is either $+1$ or -1, depending on whether n is of the form $4\mu+1$ or $4\mu+3$. Therefore,

$$W^2 = \pm r^{\frac{1}{2}n(n-1)}(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \ldots (1 - r^{-2(n-1)})$$

But it is clear that r^{-2}, r^{-4}, $r^{-6} \ldots r^{-2n+2}$ are precisely the roots of the equation $x^n - 1 = 0$, except for the root $x = 1$. Hence the following equation must hold

$$(x - r^{-2})(x - r^{-4})(x - r^{-6}) \ldots (x - r^{-2n+2}) = x^{n-1} + x^{n-2} + x^{n-3} + \text{etc.} + x + 1$$

and setting $x = 1$, we find that

$$(1 - r^{-2})(1 - r^{-4})(1 - r^{-6}) \ldots (1 - r^{-2n+2}) = n$$

Since it is evident that $r^{\frac{1}{2}n(n-1)} = 1$, our equation becomes:

$$W^2 = \pm n \qquad [6]$$

In the case where n is of the form $4\mu+1$, we have:

$$W = \pm\sqrt{n}, \text{ and therefore } T = \pm\sqrt{n}, \quad U = 0$$

On the other hand, in the case where n is of the form $4\mu+3$, we have:

$$W = \pm i\sqrt{n}, \text{ therefore } T = 0, \quad U = \pm\sqrt{n}$$

14.

The method of the previous article determines only the absolute values of T and U, and leaves their signs ambiguous, so it is necessary to establish that T is equal to $+\sqrt{n}$ in the former case and U is equal to $-\sqrt{n}$ in the latter case. However, at least for the case $k = 1$, this can be deduced from equation [5] in the following way. Whereas, for $k = 1$,

$$r - r^{-1} = 2i \sin \omega$$
$$r^3 - r^{-3} = 2i \sin 3\omega$$
$$r^5 - r^{-5} = 2i \sin 5\omega \text{ etc.},$$

this equation is transformed into

$$W = (2i)^{\frac{1}{2}(n-1)} \sin\omega \sin 3\omega \sin 5\omega \ldots \sin(n-2)\omega$$

Now, in the case where n is of the form $4\mu+1$, in the series of odd numbers

$$1, 3, 5, 7 \ldots \tfrac{1}{2}(n-3), \tfrac{1}{2}(n+1) \ldots (n-2)$$

there can be found $\frac{1}{4}(n-1)$ which are less than $\frac{1}{2}n$, and these clearly correspond to positive sines. On the other hand, the remaining $\frac{1}{4}(n-1)$ will be larger than $\frac{1}{2}n$, and these correspond to negative sines. Therefore, the product of all the sines must be equal to a product of a positive quantities, multiplied by the factor $(-1)^{\frac{1}{4}(n-1)}$, and thus W will be equal to the product of a positive real quantity with i^{n-1}, or 1, since $i^4 = 1$ and $n-1$ is divisible by 4. That is, the quantity W will be a positive real quantity, and hence we must necessarily have

$$W = +\sqrt{n}, \quad T = +\sqrt{n}$$

In the second case, where n is of the form $4\mu+3$, in the series of odd numbers

$$1, 3, 5, 7 \ldots \tfrac{1}{2}(n-1), \tfrac{1}{2}(n+3) \ldots (n-2)$$

the first $\frac{1}{4}(n+1)$ will be smaller than $\frac{1}{2}n$, and the remaining $\frac{1}{4}(n-3)$ will be larger. Among the sines of the arcs $\omega, 3\omega, 5\omega \ldots (n-2)\omega$, therefore, $\frac{1}{4}(n-3)$ will be negative, and thus W will be the product of $i^{\frac{1}{2}(n-1)}$ with a positive real quantity and $(-1)^{\frac{1}{4}(n-3)}$; the third factor is $= i^{\frac{1}{2}(n-3)}$, which when combined with the first, gives $i^{n-2} = i$, since $i^{n-3} = 1$. Therefore we necessarily have

$$W = +i\sqrt{n}, \text{ and } U = +\sqrt{n}$$

15.

We will now show how the same conclusions can be deduced from the progression considered in article 9. Let us write $-y^{-1}$ in place of $x^{\frac{1}{2}}$ equation [4], so it becomes

$$1 - y^{-1}\tfrac{1-y^{-2m}}{1-y^{-2}} + y^{-2}\tfrac{(1-y^{-2m})(1-y^{-2m+2})}{(1-y^{-2})(1-y^{-4})} - y^{-3}\tfrac{(1-y^{-2m})(1-y^{-2m+2})(1-y^{-2m+2})}{(1-y^{-2})(1-y^{-4})(1-y^{-6})} + \text{etc.}$$

up to the $m+1^{\text{st}}$ term

$$= (1-y^{-1})(1+y^{-2})(1-y^{-3})(1+y^{-4})\ldots(1\pm y^{-m}) \qquad [7]$$

If we take y to be a proper root of the equation $y^n - 1 = 0$, say r, and at the same time we set $m = n-1$, then we have

$$\tfrac{1-y^{-2m}}{1-y^{-2}} = \tfrac{1-r^2}{1-r^{-2}} = -r^2$$
$$\tfrac{1-y^{-2m+2}}{1-y^{-4}} = \tfrac{1-r^4}{1-r^{-4}} = -r^4$$
$$\tfrac{1-y^{-2m+4}}{1-y^{-6}} = \tfrac{1-r^6}{1-r^{-6}} = -r^6 \text{ etc.}$$

up to

$$\tfrac{1-y^{-2}}{1-y^{-2m}} = \tfrac{1-r^{2n-2}}{1-r^{-2n+2}} = -r^{2n-2}$$

where it should be noted that no denominators $1-r^{-2}$, $1-r^{-4}$ etc. will be $= 0$. Hence equation [7] takes the form

$$1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2} = (1-r^{-1})(1+r^{-2})(1-r^{-3})\ldots(1+r^{-n+1})$$

in the second member of this equation, if we multiply the first term by the last, the second term by the penultimate, etc., then we have

$$(1-r^{-1})(1+r^{-n+1}) = r - r^{-1}$$
$$(1+r^{-2})(1-r^{-n+2}) = r^{n-2} - r^{-n+2}$$
$$(1-r^{-3})(1+r^{-n+3}) = r^3 - r^{-3}$$
$$(1+r^{-4})(1-r^{-n+4}) = r^{n-4} - r^{-n+4} \text{ etc.}$$

From these products, it is easily seen that the product

$$(r-r^{-1})(r^3-r^{-3})(r^5-r^{-5})\ldots(r^{n-4}-r^{-n+4})(r^{n-2}-r^{-n+2})$$

will be

$$= 1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2} = W$$

This equation is identical to equation [5] in article 12, which was derived from the first series, so the rest of the argument can be carried out in the same way as in articles 13 and 14.

16.

We now move on to another case, where n is an even number. First let n be of the form $4\mu+2$, or equivalently an oddly even number. It is clear that the numbers $\frac{1}{4}nn$, $(\frac{1}{2}n+1)^2-1$, $(\frac{1}{2}n+2)^2-4$, etc., or more generally $(\frac{1}{2}n+\lambda)^2-\lambda\lambda$ can be divided by $\frac{1}{2}n$ to produce odd quotients, and thus they are congruent to $\frac{1}{2}n$ modulo n. Hence, if r is a proper root of the equation $x^n-1=0$, and thus $r^{\frac{1}{2}n}=-1$, it follows that

$$\begin{aligned} r^{(\frac{1}{2}n)^2} &= -1 \\ r^{(\frac{1}{2}n+1)^2} &= -r \\ r^{(\frac{1}{2}n+2)^2} &= -r^4 \\ r^{(\frac{1}{2}n+3)^2} &= -r^9 \text{ etc.} \end{aligned}$$

Hence, in the progression

$$1+r+r^4+r^9+\text{etc.}+r^{(n-1)^2}$$

the term $r^{(\frac{1}{2}n)^2}$ destroys the first term, the following term destroys the second term, etc., so we will have

$$W=0, \quad T=0, \quad U=0$$

17.

There remains the case where n is of the form 4μ, or evenly even. Here, in general, $(\frac{1}{2}n+\lambda)^2-\lambda\lambda$ will be divisible by n, and therefore

$$r^{(\frac{1}{2}n+\lambda)^2}=r^{\lambda\lambda}$$

Hence, in the series

$$1+r+r^4+r^9+\text{etc.}+r^{(n-1)^2}$$

the term $r^{(\frac{1}{2}n)^2}$ will be equal the first term, the following term will be the second term, etc., so that

$$W=2(1+r+r^4+r^9+\text{etc.}+r^{(\frac{1}{2}n-1)^2})$$

Let us now suppose that in equation [7] article 15, we set $m=\frac{1}{2}n-1$, and for y we substitute a proper root r of the equation $y^n-1=0$. Then just as in article 15, the equation takes the form

$$1+r+r^4+\text{etc.}+r^{(\frac{1}{2}n-1)^2}=(1-r^{-1})(1+r^{-2})(1-r^{-3})\ldots(1-r^{-\frac{1}{2}n+1})$$

or

$$W = 2(1-r^{-1})(1+r^{-2})(1-r^{-3})(1+r^{-4})\dots(1-r^{-\frac{1}{2}n+1}) \qquad [8]$$

Furthermore, since $r^{\frac{1}{2}n} = -1$, we have

$$1+r^{-2} = -r^{\frac{1}{2}n-2}(1-r^{-\frac{1}{2}n+2})$$
$$1+r^{-4} = -r^{\frac{1}{2}n-4}(1-r^{-\frac{1}{2}n+4})$$
$$1+r^{-6} = -r^{\frac{1}{2}n-6}(1-r^{-\frac{1}{2}n+6}) \text{ etc.}$$

and the product of the factors $-r^{\frac{1}{2}n-2}$, $-r^{\frac{1}{2}n-4}$, $-r^{\frac{1}{2}n-6}$ etc. up to $-r^2$ becomes $= (-1)^{\frac{1}{4}n-1} r^{\frac{1}{16}nn-\frac{1}{4}n}$. The previous equation can also be expressed as

$$W = 2(-1)^{\frac{1}{4}n-1} r^{\frac{1}{16}nn-\frac{1}{4}n}(1-r^{-1})(1-r^{-2})(1-r^{-3})(1-r^{-4})\dots(1-r^{-\frac{1}{2}n+1})$$

Considering that

$$1-r^{-1} = -r^{-1}(1-r^{-n+1})$$
$$1-r^{-2} = -r^{-2}(1-r^{-n+2})$$
$$1-r^{-3} = -r^{-3}(1-r^{-n+3}) \text{ etc.}$$

we have

$$(1-r^{-1})(1-r^{-2})(1-r^{-3})\dots(1-r^{-\frac{1}{2}n+1})$$
$$= (-1)^{\frac{1}{2}n-1} r^{-\frac{1}{8}nn+\frac{1}{4}n}(1-r^{-\frac{1}{2}n-1})(1-r^{-\frac{1}{2}n-2})(1-r^{-\frac{1}{2}n-3})\dots(1-r^{-n+1})$$

and thus

$$W = 2(-1)^{\frac{3}{4}n-2} r^{-\frac{1}{16}nn}(1-r^{-\frac{1}{2}n-1})(1-r^{-\frac{1}{2}n-2})(1-r^{-\frac{1}{2}n-3})\dots(1-r^{-n+1})$$

Multiplying this value of W by the one we previously found, and adjoining the factor $1-r^{-\frac{1}{2}n}$ to both sides, we get

$$(1-r^{-\frac{1}{2}n})W^2 = 4(-1)^{n-3} r^{-\frac{1}{4}n}(1-r^{-1})(1-r^{-2})(1-r^{-3})\dots(1-r^{-n+1})$$

But we have

$$1-r^{-\frac{1}{2}n} = 2$$
$$(-1)^{n-3} = -1$$
$$r^{-\frac{1}{4}n} = -r^{\frac{1}{4}n}$$
$$(1-r^{-1})(1-r^{-2})(1-r^{-3})\dots(1-r^{-n+1}) = n$$

From which it finally follows that

$$W^2 = 2r^{\frac{1}{4}n}n \qquad [9]$$

Now it can be easily seen that $r^{\frac{1}{4}n}$ is either $= +i$ or $= -i$, depending on whether k is of the form $4\mu+1$ or $4\mu+3$. And since

$$2i = (1+i)^2, \quad -2i = (1-i)^2$$

we will have, in the case where k is of the form $4\mu+1$,

$$W = \pm(1+i)\sqrt{n}, \text{ and thus } \quad T = U = \pm\sqrt{n}$$

and in the other case, where k is of the form $4\mu+3$,

$$W = \pm(1-i)\sqrt{n}, \text{ and thus } \quad T = -U = \pm\sqrt{n}$$

18.

The method of the preceding article provides the absolute values of the functions T and U, and assigned the conditions under which equal or opposite signs should be given to them. But the signs themselves are not yet determined at this point. We will supply this for the case $k = 1$, as follows.

Let $\rho = \cos\frac{1}{2}\omega + i\sin\frac{1}{2}\omega$, so that $r = \rho\rho$ and $\rho^n = -1$. It is clear that equation [8], can be expressed as

$$W = 2(1+\rho^{n-2})(1+\rho^{-4})(1+\rho^{n-6})(1+\rho^{-8})\ldots(1+\rho^{-n+4})(1+\rho^2)$$

or, by arranging the factors in a different order,

$$W = 2(1+\rho^2)(1+\rho^{-4})(1+\rho^6)(1+\rho^{-8})\ldots(1+\rho^{-n+4})(1+\rho^{n-2})$$

Now we have

$$\begin{aligned} 1+\rho^2 &= 2\rho\cos\tfrac{1}{2}\omega \\ 1+\rho^{-4} &= 2\rho^{-2}\cos\omega \\ 1+\rho^{+6} &= 2\rho^3\cos\tfrac{3}{2}\omega \\ 1+\rho^{-8} &= 2\rho^{-4}\cos 2\omega \text{ etc.} \end{aligned}$$

up to

$$\begin{aligned} 1+\rho^{-n+4} &= 2\rho^{-\frac{1}{2}n+2}\cos(\tfrac{1}{4}n-1)\omega \\ 1+\rho^{n-2} &= 2\rho^{\frac{1}{2}n-1}\cos(\tfrac{1}{4}n-\tfrac{1}{2})\omega \end{aligned}$$

Therefore, we have:

$$W = 2^{\frac{1}{2}n}\rho^{\frac{1}{4}n}\cos\tfrac{1}{2}\omega\cos\omega\cos\tfrac{3}{2}\omega\ldots\cos(\tfrac{1}{4}n-\tfrac{1}{2})\omega$$

The cosines in this product are manifestly positive, but the factor $\rho^{\frac{1}{4}n}$ becomes $= \cos 45^\circ + i\sin 45^\circ = (1+i)\sqrt{\frac{1}{2}}$. Hence we conclude that W is a product of $1+i$ and a positive real quantity, so we must necessarily have

$$W = (1+i)\cdot\sqrt{n}, \quad T = +\sqrt{n}, \quad U = +\sqrt{n}$$

19.

It will be worthwhile to gather together here all of the summations we have evaluated so far. Namely, in general we have

$T =$	$U =$	as n is of form
$\pm\sqrt{n}$	$\pm\sqrt{n}$	4μ
$\pm\sqrt{n}$	0	$4\mu+1$
0	0	$4\mu+2$
0	$\pm\sqrt{n}$	$4\mu+3$

and in the case where k is assumed to be $=1$, the positive sign must be assigned to the radical quantity. those things which had been noticed by induction in article 3 for the first few values of n have been demonstrated with all rigor, and nothing remains but to determine the signs for other values of k in all cases. But before this task can be undertaken in all generality, it will be necessary to first consider more closely the cases in which n is either a prime number or a power of a prime number.

20.

Let n be a prime odd number. Then it is clear from what was explained in article 10 that $W = 1 + 2\Sigma r^a = 1 + 2\Sigma R^{ak}$, where we set $R = \cos\omega + i\sin\omega$, and a denotes all of the quadratic residues of n between 1 and $n-1$ indefinitely. But if we also denote indefinitely by b all the quadratic non-residues between the same limits, it is seen without any difficulty that all of the numbers ak will become congruent modulo n to either all of a or all of b, without respect to order, depending on whether k is a residue or a non-residue. Therefore, in the former case, we have

$$W = 1 + 2\Sigma R^a = 1 + R + R^4 + R^9 + \text{etc.} + R^{(n-1)^2}$$

and thus $W = +\sqrt{n}$, if n is of the form $4\mu+1$, and $W = +i\sqrt{n}$, if n is of the form $4\mu+3$.

On the other hand, in the case where k is a quadratic non-residue modulo n, we have

$$W = 1 + 2\Sigma R^b$$

Hence, since it is clear that all integers a and b together complete the complex integer numbers 1, 2, 3, ..., and so

$$\Sigma R^a + \Sigma R^b = R + R^2 + R^3 + \text{etc.} + R^{n-1} = -1$$

therefore

$$W = -1 - 2\Sigma R^a = -(1 + R + R^4 + R^9 + \text{etc.} + R^{(n-1)^2})$$

thus $W = -\sqrt{n}$ if n is of the form $4\mu+1$, and $W = -i\sqrt{n}$ if n is of the form $4\mu+3$.

Hence we conclude:

first, if n is of the form $4\mu+1$, and k is a quadratic residue modulo n,

$$T = +\sqrt{n}, \quad U = 0$$

second, if n is of the form $4\mu+1$, and k is a quadratic non-residue modulo n,

$$T = -\sqrt{n}, \quad U = 0$$

third, if n is of the form $4\mu+3$, and k is a quadratic residue modulo n,

$$T = 0, \quad U = +\sqrt{n}$$

fourth, if n is of the form $4\mu+3$, and k is a quadratic non-residue modulo n,

$$T = 0, \quad U = -\sqrt{n}$$

21.

Let n be a power of an odd prime p increased by 2, and let $n = p^{2\chi}q$, where q is either 1 or p. Here, first of all, it is important to observe that if λ is any integer not divisible by p^χ, we have

$$r^{\lambda\lambda} + r^{(\lambda+p^\chi q)^2} + r^{(\lambda+2p^\chi q)^2} + r^{(\lambda+3p^\chi q)^2} + \text{etc.} + r^{(\lambda+n-p^\chi q)^2}$$
$$= r^{\lambda\lambda}\left\{1 + r^{2\lambda p^\chi q} + r^{4\lambda p^\chi q} + r^{6\lambda p^\chi q} + \text{etc.} + r^{2\lambda(n-p^\chi q)}\right\} = \frac{r^{\lambda\lambda}(1-r^{2\lambda n})}{1-r^{2\lambda p^\chi q}} = 0$$

Hence it is easy to see that

$$W = 1 + r^{p^{2\chi}} + r^{4p^{2\chi}} + r^{9p^{2\chi}} + \text{etc.} + r^{(n-p^\chi)^2}$$

The remaining terms of the series

$$1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2}$$

can be distributed into $(p^\chi - 1)q$ partial sums, each with p^χ terms, and is seen to vanish by applying the transformation given above.

Hence it follows, in the case where $q = 1$, or where n is a power of a prime number with an even exponent, that

$$W = p^\chi = +\sqrt{n}, \text{ and therefore } T = +\sqrt{n}, U = 0$$

On the other hand, in the case where $q = p$, or where n is a power of a prime number with an odd exponent, let us set $r^{p^{2\chi}} = \rho$, where ρ will be the proper root of the equation $x^p - 1 = 0$, namely $\rho = \cos\frac{k}{p}360^\circ + i\sin\frac{k}{p}360^\circ$, and then

$$W = 1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(p^{\chi+1}-1)^2} = p^\chi(1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(p-1)^2})$$

But the sum of the series $1 + p + p^4 + p^9 + \text{etc.} + p^{(p-1)^2}$ is determined by the preceding article, from which it is concluded automatically that

$$W = \pm\sqrt{n} = T, \text{ if } p \text{ is of the form } 4\mu + 1$$
$$W = \pm i\sqrt{n} = iU, \text{ if } p \text{ is of the form } 4\mu + 3$$

with a positive or negative sign according to whether k is a quadratic residue or a non-residue modulo p.

22.

The following proposition, which is easily derived from that which has been set forth in articles 20 and 21, will be of considerable use to us below. Let

$$W' = 1 + r^h + r^{4h} + r^{9h} + \text{etc.} + r^{h(n-1)^2}$$

where h is any integer not divisible by p. Then in the case where $n = p$, or where

n is a power of p with an odd exponent, we have

$$W' = W, \text{ if } h \text{ is a quadratic residue modulo } p$$
$$W' = -W, \text{ if } h \text{ is a quadratic non-residue modulo } p$$

For it is clear that W' arises from W if kh is substituted for k. In the former case, k and kh will be similar, in the latter dissimilar, insofar as they are quadratic residues or non-residues modulo p.

However, in the case where n is a power of p with an even exponent, it is clear that $W' = +\sqrt{n}$, and therefore always $W' = W$.

23.

In articles 20, 21, 22 we considered odd prime numbers, and their powers. It remains, therefore, to consider the case where n is a power of two.

For $n = 2$, it is clear that $W = 1 + r = 0$.

For $n = 4$, we obtain $W = 1 + r + r^4 + r^9 = 2 + 2r$. Hence $W = 2 + 2i$, whenever k is of the form $4\mu + 1$, and $W = 2 - 2i$, whenever k is of the form $4\mu + 3$.

For $n = 8$, we have $W = 1 + r + r^4 + r^9 + r^{16} + r^{25} + r^{36} + r^{49} = 2 + 4r + 2r^4 = 4r$. Hence

$$W = (1+i)\sqrt{8}, \text{ whenever } k \text{ is of the form } 8\mu + 1$$
$$W = (-1+i)\sqrt{8}, \text{ whenever } k \text{ is of the form } 8\mu + 3$$
$$W = (-1-i)\sqrt{8}, \text{ whenever } k \text{ is of the form } 8\mu + 5$$
$$W = (1-i)\sqrt{8}, \text{ whenever } k \text{ is of the form } 8\mu + 7$$

If n is a higher power of two, let $n = 2^{2\chi}q$, so that q is either equal to 1 or 2, and χ is greater than 1. Here, first of all, it must be observed that if λ is an integer not divisible by $2^{\chi-1}$, we have

$$r^{\lambda\lambda} + r^{(\lambda+2^\chi q)^2} + r^{(\lambda+2.2^\chi q)^2} + r^{(\lambda+3.2^\chi q)^2} + \text{etc.} + r^{(\lambda+n-2^\chi q)^2}$$
$$= r^{\lambda\lambda}\left\{1 + r^{2^{\chi+1}\lambda q} + r^{2.2^{\chi+1}\lambda q} + r^{3.2^{\chi+1}\lambda q} + \text{etc.} + r^{(2n-2^{\chi+1}q)\lambda}\right\} = \frac{r^{\lambda\lambda}(1-r^{2\lambda n})}{1-r^{2^{\chi+1}\lambda q}} = 0$$

Hence it is easily seen that

$$W = 1 + r^{2^{2\chi-2}} + r^{4.2^{2\chi-2}} + r^{9.2^{2\chi-2}} + \text{etc.} + r^{(n-2^{\chi-1})^2}$$

Let us set $r^{2^{2\chi-2}} = \rho$. Then ρ will be a root of the equation $x^{4q} - 1 = 0$, and specifically $\rho = \cos \frac{k}{4q} 360° + i \sin \frac{k}{4q} 360°$. Thus we have

$$\begin{aligned} W &= 1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(2^{\chi+1}q-1)^2} \\ &= 2^{\chi-1}(1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(4q-1)^2}) \end{aligned}$$

But the sum of the series $1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(4q-1)^2}$ is determined by what we have already explained in the cases $n = 4$, $n = 8$, hence we conclude that
in the case where $q = 1$, or where n is a power of 4,

$$W = (1+i)2^{\chi} = (1+i)\sqrt{n}, \text{ if } k \text{ is of the form } 4\mu+1$$
$$W = (1-i)2^{\chi} = (1-i)\sqrt{n}, \text{ if } k \text{ is of the form } 4\mu+3$$

which are the exact formulas already given for $n = 4$;
in the case where $q = 2$, or where n is a power of two with an odd exponent greater than 3,

$$W = (1+i)2^{\chi}\sqrt{2} \quad = (1+i)\sqrt{n}, \text{ if } k \text{ is of the form } 8\mu+1$$
$$W = (-1+i)2^{\chi}\sqrt{2} = (-1+i)\sqrt{n}, \text{ if } k \text{ is of the form } 8\mu+3$$
$$W = (-1-i)2^{\chi}\sqrt{2} = (-1-i)\sqrt{n}, \text{ if } k \text{ is of the form } 8\mu+5$$
$$W = (1-i)2^{\chi}\sqrt{2} \quad = (1-i)\sqrt{n}, \text{ if } k \text{ is of the form } 8\mu+7$$

which also precisely match the formulas we provided for $n = 8$.

24.

It will also be worth our while to determine the ratio of the sum of the series

$$W' = 1 + r^h + r^{4h} + r^{9h} + \text{etc.} + r^{h(n-1)^2}$$

to W, where h is an arbitrary odd integer. Since W' arises from W by replacing k with kh, the value of W' will depend on the form of the number kh in the same way as W depends on the form of the number k. Let us set $\frac{W'}{W} = l$. Then it is clear that

I. In the case where $n = 4$, or any higher power of two with an even exponent,

$l = 1$, if h is of the form $4\mu+1$
$l = -i$, if h is of the form $4\mu+3$, and k is of the form $4\mu+1$
$l = +i$, if h is of the form $4\mu+3$, and k is of the same form

II. In the case where $n = 8$, or any higher power of two with an odd exponent,

$l = 1$, if h is of the form $8\mu + 1$,

$l = -1$, if h is of the form $8\mu + 5$,

$l = +i$, if either h is of the form $8\mu + 3$, and k is of the form $4\mu + 1$,
or h is of the form $8\mu + 7$, and k is of the form $4\mu + 3$,

$l = -i$, if either h is of the form $8\mu + 3$, and k is of the form $4\mu + 3$,
or h is of the form $8\mu + 7$, and k is of the form $4\mu + 1$.

With this, the determination of W in those cases where n is a prime number or a power of a prime number is complete. It remains, therefore, for us to complete those cases where n is composed of several prime factors, for which purpose the following theorem will pave the way.

25.

THEOREM. *Let n be the product of two relatively prime positive integers a and b, and set*

$$P = 1 + r^{aa} + r^{4aa} + r^{9aa} + \text{etc.} + r^{(b-1)^2 aa}$$
$$Q = 1 + r^{bb} + r^{4bb} + r^{9bb} + \text{etc.} + r^{(a-1)^2 bb}$$

Then I claim that $W = PQ$.

Proof. Let α indefinitely denote any number among 0, 1, 2, $3 \ldots, a-1$, let β indefinitely denote any number among 0, 1, 2, $3 \ldots, b-1$, let ν indefinitely denote any number among 0, 1, 2, $3 \ldots, n-1$. Then it is clear that

$$P = \Sigma r^{aa\beta\beta}, \quad Q = \Sigma r^{bb\alpha\alpha}, \quad W = \Sigma r^{\nu\nu}$$

Thus, we have $PQ = \Sigma r^{aa\beta\beta + bb\alpha\alpha}$, where all possible values of α and β are to be substituted. Furthermore, because $2ab\alpha\beta = 2\alpha\beta n$, we have $PQ = \Sigma r^{(a\beta + b\alpha)^2}$. But it is clearly seen, without difficulty, that the individual values of $a\beta + b\alpha$ is distinct from each others, and each is equal to some value of ν. Thus, we have $PQ = \Sigma r^{\nu\nu} = W$.

It should also be noted that r^{aa} is a proper root of the equation $x^b - 1 = 0$, and r^{bb} is a proper root of the equation $x^a - 1 = 0$.

26.

Now let n be the product of three mutually prime numbers a, b, c. Then clearly if we set $bc = b'$, then a and b' will be relatively prime. Therefore, W is a product of two factors:

$$1 + r^{aa} + r^{4aa} + r^{9aa} + \text{etc.} + r^{(b'-1)^2 aa}$$
$$1 + r^{b'b'} + r^{4b'b'} + r^{9b'b'} + \text{etc.} + r^{(a-1)^2 b'b'}$$

However, since r^{aa} is a proper root of the equation $x^{bc} - 1 = 0$, the first factor will be the product of two factors

$$1 + \rho^{bb} + \rho^{4bb} + \rho^{9bb} + \text{etc.} + \rho^{(c-1)^2 bb}$$
$$1 + \rho^{cc} + \rho^{4cc} + \rho^{9cc} + \text{etc.} + \rho^{(b-1)^2 cc}$$

if we set $r^{aa} = \rho$. Hence it is clear that W is the product of three factors:

$$1 + r^{bbcc} + r^{4bbcc} + r^{9bbcc} + \text{etc.} + r^{(a-1)^2 bbcc}$$
$$1 + r^{aacc} + r^{4aacc} + r^{9aacc} + \text{etc.} + r^{(b-1)^2 aacc}$$
$$1 + r^{aabb} + r^{4aabb} + r^{9aabb} + \text{etc.} + r^{(c-1)^2 aabb}$$

where r^{bbcc}, r^{aacc}, and r^{aabb} are proper roots of the equations $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0$, respectively.

27.

From this it is easily concluded that in general, if n is the product of any prime factors a, b, c, etc., then W will be a product of as many factors

$$1 + r^{\frac{nn}{aa}} + r^{\frac{4nn}{aa}} + r^{\frac{9nn}{aa}} + \text{etc.} + r^{\frac{(a-1)^2 nn}{aa}}$$
$$1 + r^{\frac{nn}{bb}} + r^{\frac{4nn}{bb}} + r^{\frac{9nn}{bb}} + \text{etc.} + r^{\frac{(b-1)^2 nn}{bb}}$$
$$1 + r^{\frac{nn}{cc}} + r^{\frac{4nn}{cc}} + r^{\frac{9nn}{cc}} + \text{etc.} + r^{\frac{(c-1)^2 nn}{cc}} \quad \text{etc.}$$

where $r^{\frac{nn}{ab}}, r^{\frac{nn}{bb}}, r^{\frac{nn}{cc}}$ etc. are proper roots of the equations $x^a - 1 = 0, x^b - 1 = 0$, $x^c - 1 = 0$ etc.

28.

From these principles, the passage to the complete determination of W for any given value of n is now clear. Let n be decomposed into factors a, b, c, etc.,

which are either distinct prime numbers or powers of distinct prime numbers. Let $r^{\frac{nn}{aa}} = A$, $r^{\frac{nn}{bb}} = B$, $r^{\frac{nn}{cc}} = C$, etc., and let A, B, C, etc. be the respective roots of the equations $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0$, etc. Then W is the product of the factors

$$1 + A + A^4 + A^9 + \text{etc.} + A^{(u-1)^2}$$
$$1 + B + B^4 + B^9 + \text{etc.} + B^{(b-1)^2}$$
$$1 + C + C^4 + C^9 + \text{etc.} + C^{(c-1)^2} \text{ etc.}$$

But each of these factors can be determined by the methods explained in articles 20, 21, 23. Hence, the value of the product can also be known. It will be useful to collect the rules for determining these factors here. When the root A is $= \frac{kn}{a} \cdot \frac{360^0}{a}$, the sum $1+A+A^4+A^9+\text{etc.}+A^{(a-1)^2}$, which we shall denote by L, will be determined by the number $\frac{kn}{a}$, in the same way that W was determined by k in our general discussion. We have already distinguished twelve cases:

I. If a is a prime number of the form $4\mu+1$, say $= p$, or a power of such a prime number with an odd exponent, and at the same time $\frac{kn}{a}$ is a quadratic residue modulo p, then $L = +\sqrt{a}$.

II. If $\frac{kn}{a}$ is a quadratic non-residue modulo p, then $L = -\sqrt{a}$.

III. If a is a prime number of the form $4\mu+3$, say $= p$, or a power of such a prime number with an odd exponent, and at the same time $\frac{kn}{a}$ is a quadratic residue modulo p, then $L = +i\sqrt{a}$.

IV. If, with the rest of the assumptions as in III, $\frac{kn}{a}$ is a quadratic non-residue modulo p, then $L = -i\sqrt{a}$.

V. If a is a square number, or a higher power of a prime number (with an even exponent), then $L = +\sqrt{a}$.

VI. If $a = 2$, then $L = 0$.

VII. If $a = 4$ or a higher power of two with an even exponent, and also $\frac{kn}{a}$ is of the form $4\mu+1$, then $L = (1+i)\sqrt{a}$.

VIII. If, with the rest of the assumptions as in VII, $\frac{kn}{a}$ is of the form $4\mu+3$, then $L = (1-i)\sqrt{a}$.

IX. If $a = 8$, or a higher power of two with an odd exponent, and at the same time $\frac{kn}{a}$ is of the form $8\mu+1$, then $L = (1+i)\sqrt{a}$.

X. If, with the rest of the assumptions as in IX, $\frac{kn}{a}$ is of the form $8\mu+3$, then $L=(-1+i)\sqrt{a}$.

XI. If, with the rest of the assumptions as in IX, $\frac{kn}{a}$ is of the form $8\mu+5$, then $L=(-1-i)\sqrt{a}$.

XII. If, with the rest of the assumptions as in IX, $\frac{kn}{a}$ is of the form $8\mu+7$, then $L=(1-i)\sqrt{a}$.

29.

For example, let $n=2520=8.9.5.7$ and $k=13$. In this case, we have

for $a=8$, by case XII, $L=(1-i)\sqrt{8}$
for the factor 9, by case V, the corresponding sum will be $=\sqrt{9}$
for the factor 5, by case II, the corresponding sum will be $=-\sqrt{5}$
for the factor 7, by case III, the corresponding sum will be $=+i\sqrt{7}$

Hence, we get $W=(1-i)\cdot(-i)\cdot\sqrt{2520}=(-1-i)\sqrt{2520}$.

If, for the same value of n, we set $k=1$, then

for the factor 8, the sum is $(-1+i)\sqrt{8}$
for the factor 9, the sum is $\sqrt{9}$
for the factor 5, the sum is $\sqrt{5}$
for the factor 7, the sum is $-i\sqrt{7}$

Hence, the product is $W=(1+i)\sqrt{2520}$.

30.

Another method of finding the sum W in a general manner is suggested by that which was set forth in articles 22 and 24. Set $\cos\omega+i\sin\omega=\rho$, and

$$\rho^{\frac{nn}{aa}}=\alpha,\quad \rho^{\frac{nn}{bb}}=\beta,\quad \rho^{\frac{nn}{cc}}=\gamma \text{ etc.}$$

so that we have $r=\rho^k$, $A=\alpha^k$, $B=\beta^k$, $C=\gamma^k$ etc. Then

$$1+\rho+\rho^4+\rho^9+\text{etc.}+\rho^{(n-1)^2}$$

will be a product of factors

$$1+\alpha+\alpha^4+\alpha^9+\text{etc.}+\alpha^{(a-1)^2}$$
$$1+\beta+\beta^4+\beta^9+\text{etc.}+\beta^{(b-1)^2}$$
$$1+\gamma+\gamma^4+\gamma^9+\text{etc.}+\gamma^{(c-1)^2}\text{ etc.}$$

and therefore W will be a product of factors

$$w = 1 + \rho + \rho^4 + \rho^9 + \text{etc.} + \rho^{(n-1)^2}$$
$$\mathfrak{A} = \frac{1+A+A^4+A^9+\text{etc.}+A^{(a-1)^2}}{1+\alpha+\alpha^4+\alpha^9+\text{etc.}+a^{(a-1)^2}}$$
$$\mathfrak{B} = \frac{1+B+B^4+B^9+\text{etc.}+B^{(b-1)^2}}{1+\beta+\beta^4+\beta^9+\text{etc.}+\beta^{(b-1)^2}}$$
$$\mathfrak{C} = \frac{1+C+C^4+C^9+\text{etc.}+C^{(c-1)^2}}{1+\gamma+\gamma^4+\gamma^9+\text{etc.}+\gamma^{(c-1)^2}} \text{ etc.}$$

Now, the first factor w is determined by the above discussion (article 19); the remaining factors $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ etc. come from the formulas of articles 22 and 24, which are collected here again so that they can all be considered together[1]. Twelve cases must be distinguished here, namely

I. If a is a prime number (odd) $= p$, or a power of such a number with an odd exponent, and k is a quadratic residue modulo p, then the corresponding factor will be $\mathfrak{A} = +1$.

II. If, with the rest of the assumptions as in I, k is a quadratic non-residue modulo p, then $\mathfrak{A} = -1$.

III. If a is the square of an odd prime number, or a higher power with an even exponent, then $\mathfrak{A} = +1$.

IV. If a is $= 4$, or a higher power of two with an even exponent, and k is of the form $4\mu + 1$, then $\mathfrak{A} = +1$.

V. If, with the rest of the assumptions as in IV, k is of the form $4\mu + 3$, and $\frac{n}{a}$ is of the form $4\mu + 1$, then $\mathfrak{A} = -i$.

VI. If, with the rest of the assumptions as in IV, k is of the form $4\mu + 3$, and $\frac{n}{a}$ is of the form $4\mu + 3$, then $\mathfrak{A} = +i$.

VII. If a is $= 8$, or a higher power of two with an odd exponent, and k is of the form $8\mu + 1$, then $\mathfrak{A} = +1$.

VIII. If, with the rest of the assumptions as in VII, k is of the form $8\mu + 5$, then $\mathfrak{A} = -1$.

IX. If, with the rest of the assumptions as in VII, k is of the form $8\mu + 3$, and $\frac{n}{a}$ is of the form $4\mu + 1$, then $\mathfrak{A} = +i$.

[1] Clearly, what was k and h there, will here be $\frac{n}{a}$ and k in the second factor, $\frac{n}{b}$ and k in the third factor etc.

X. If, with the rest of the assumptions as in VII, k is of the form $8\mu+3$, and $\frac{n}{a}$ is of the form $4\mu+3$, then $\mathfrak{A}=-i$.

XI. If, with the rest of the assumptions as in VII, k is of the form $8\mu+7$, and $\frac{n}{a}$ is of the form $4\mu+1$, then $\mathfrak{A}=-i$.

XII. If, with the rest of the assumptions as in VII, k is of the form $8\mu+7$, and $\frac{n}{a}$ is of the form $4\mu+3$, then $\mathfrak{A}=+i$.

We omit the case where $a=2$; indeed, in this case $\mathfrak{A}$ would be $\frac{0}{0}$, or indeterminate, but then $W=0$ always.

The remaining factors $\mathfrak{B}$, $\mathfrak{C}$, etc. depend in the same way on b, c, etc., as $\mathfrak{A}$ depends on a.

31.

According to this second method, the first example in article 29 is as follows:

The factor w becomes $=(1+i)\sqrt{2520}$
For $a=8$, the corresponding factor $\mathfrak{A}$ becomes, by case VIII, $=-1$
The second factor 9 corresponds to factor $+1$ (by case III)
The factor 5 corresponds to factor -1 (by case II)
The factor 7 corresponds to factor -1 (by case II)

Hence, the product $W=(-1-i)\sqrt{2520}$ is obtained, as in article 29.

32.

Since the value of W can be determined using two methods, one of which is based on the relations of the numbers $\frac{nk}{a}$, $\frac{nk}{b}$, $\frac{nk}{c}$, etc. with the numbers a, b, c, etc., and the other depending on the relations of k with the numbers a, b, c, etc., there must be a certain conditional connection between all these relations, so that each of them must be determinable from the others. Let us suppose that all the numbers a, b, c, etc. are odd prime numbers, and take $k=1$. Let the factors a, b, c, etc. be distributed into two classes, one of which contains those that are of the form $4\mu+1$, and which are denoted by p, p', p'', etc., and the other consisting of those that are of the form $4\mu+3$, and which are denoted by q, q', q'', etc. We will designate the multitude of the latter by m. Having done this, we observe first that n will be of the form $4\mu+1$, when m is even (which also applies to the case where the factors of the other class are completely absent, or where $m=0$), whereas n will be of the form $4\mu+3$, when m is odd. Now the determination of W is achieved

by the first method as follows. Let numbers P, P', P'', etc., Q, Q', Q'', etc. be determined from the relations between the numbers $\frac{n}{p}$, $\frac{n}{p'}$, $\frac{n}{p''}$ etc., $\frac{n}{q}$, $\frac{n}{q'}$, $\frac{n}{q''}$ and the numbers p, p', p'', etc., q, q', q'', etc., respectively, by setting

$$P = +1, \text{ if } \tfrac{n}{p} \text{ is a quadratic residue modulo } p$$

$$P = -1, \text{ if } \tfrac{n}{p} \text{ is a quadratic non-residue modulo } p$$

and likewise for the rest. Then W will be the product of the factors $P\sqrt{p}$, $P'\sqrt{p'}$, $P''\sqrt{p''}$, etc., $iQ\sqrt{q}$, $iQ'\sqrt{q'}$, $iQ''\sqrt{q''}$, etc., and hence

$$W = PP'P'' \ldots QQ'Q'' \ldots i^m \sqrt{n}$$

By the second method, or rather directly by the rules from article 19, it will be

$$W = +\sqrt{n}, \text{ if } n \text{ is of the form } 4\mu+1, \text{ or equivalently, if } m \text{ is even}$$
$$W = +i\sqrt{n}, \text{ if } n \text{ is of the form } 4\mu+3, \text{ or if } m \text{ is odd}$$

Both cases may be included together in the following formula:

$$W = i^{mm}\sqrt{n}$$

Hence it follows that

$$PP'P'' \ldots QQ'Q'' \ldots = i^{mm-m}$$

But i^{mm-m} is $=1$ whenever m is of the form 4μ or $4\mu+1$, and $=-1$ whenever m is of the form $4\mu+2$ or $4\mu+3$, from which we deduce the following very elegant

THEOREM. *Let a, b, c, etc. denote positive odd prime numbers that are not equal to each other, and let their product be denoted $= n$. Let m be the number of the form $4\mu+3$ among them, and let the other numbers be of the form $4\mu+1$. Then the multitude of those numbers among a, b, c, etc., whose residues are not equal to $\frac{n}{a}$, $\frac{n}{b}$, $\frac{n}{c}$, etc., will be even whenever m is of the form 4μ or $4\mu+1$, but odd whenever m is of the form $4\mu+2$ or $4\mu+3$.*

By setting e.g. $a=3$, $b=5$, $c=7$, $d=11$, we have three numbers of the form $4\mu+3$, namely 3, 7, and 11; and we have $5.7.11R3$; $3.7.11R5$; $3.5.11R7$; $3.5.7N11$, so there is a unique $\frac{n}{d}$ which is a quadratic non-residue modulo d.

33.

The celebrated *fundamental theorem* concerning quadratic residues is nothing but a special case of the theorem just developed. By limiting the multitude of the

numbers a, b, c, etc. to *two*, it is evident that if only one of them, or neither, is of the form $4\mu+3$, then we must have simultaneously aRb, bRa, or simultaneously aNb, bNa. On the other hand, if both are of the form $4\mu+3$, then one of them must be a quadratic non-residue modulo the other, and the other a quadratic residue modulo the one. And so the fourth demonstration has been given for this most important theorem, the first and second demonstration of which we have recently given in Disquisitiones Arithmeticae, and the third in a special commentary (*Commentt. T. XVI*). We will present two other proofs in the future, based again on completely different principles. It is exceedingly surprising that this most beautiful theorem, which at first so obstinately eluded all attempts, could be approached later by methods so very distant from one other.

34.

Moreover, the remaining theorems, which act as a supplement to the fundamental theorem, that is, by which the prime numbers for which -1, 2, and -2 are quadratic residues or non-residues may be identified, can be derived from the same principles. Let us start with the residue $+2$.

Set $n = 8a$, where a is a prime number, and let $k = 1$. Then by the method of article 28, W will be the product of two factors, of which one will be $+\sqrt{a}$ or $+i\sqrt{a}$, if 8, or equivalently 2, is a quadratic residue modulo a; or else $-\sqrt{a}$ or $-i\sqrt{a}$, if 2 is a quadratic non-residue modulo a. The second factor is

$$\begin{aligned}
&(1+i)\sqrt{8}, \text{ if } a \text{ is of the form } 8\mu+1\\
&(-1+i)\sqrt{8}, \text{ if } a \text{ is of the form } 8\mu+3\\
&(-1-i)\sqrt{8}, \text{ if } a \text{ is of the form } 8\mu+5\\
&(1-i)\sqrt{8}, \text{ if } a \text{ is of the form } 8\mu+7
\end{aligned}$$

But by article 18, we will always have $W = (1+i)\sqrt{n}$. Dividing this value by the four values of the second factor, it is clear that the first factor must be

$$\begin{aligned}
&+\sqrt{a}, \text{ if } a \text{ is of the form } 8\mu+1\\
&-i\sqrt{a}, \text{ if } a \text{ is of the form } 8\mu+3\\
&-\sqrt{a}, \text{ if } a \text{ is of the form } 8\mu+5\\
&+i\sqrt{a}, \text{ if } a \text{ is of the form } 8\mu+7
\end{aligned}$$

From this it follows automatically that 2 must be a quadratic residue modulo a in the first and fourth cases, and in the second and third cases it must be a quadratic non-residue.

35.

Prime numbers for which -1 is a quadratic residue or non-residue are easily recognized with the help of the following theorem, which is also quite memorable by itself.

THEOREM. *The product of the two factors*

$$W' = 1 + r^{-1} + r^{-4} + \text{etc.} + r^{-(n-1)^2}$$
$$W = 1 + r + r^4 + \text{etc.} + r^{(n-1)^2}$$

is $= n$, *if* n *is odd, or* $= 0$, *if* n *is odd even, or* $= 2n$, *if* n *is evenly even.*

Proof. Since it is clear that

$$\begin{aligned} W &= r + r^4 + r^9 + \text{etc.} + r^{nn} \\ &= r^4 + r^9 + \text{etc.} + r^{(n+1)^2} \\ &= r^9 + \text{etc.} + r^{(n+2)^2} \ \text{ etc.} \end{aligned}$$

the product WW' can also be presented as

$$\begin{aligned} & 1 + r + r^4 + r^9 + \text{etc.} + r^{(n-1)^2} \\ & + r^{-1}(r + r^4 + r^9 + r^{16} + \text{etc.} + r^{nn}) \\ & + r^{-4}(r^4 + r^9 + r^{16} + r^{25} + \text{etc.} + r^{(n+1)^2}) \\ & + r^{-9}(r^9 + r^{16} + r^{25} + r^{36} + \text{etc.} + r^{(n+2)^2}) \\ & \text{etc.} \\ & + r^{-(n-1)^2}(r^{(n-1)^2} + r^{nn} + r^{(n+1)^2} + r^{(n+2)^2} + \text{etc.} + r^{(2n-2)^2}) \end{aligned}$$

which, when vertically summed, produces

$$\begin{aligned} & n \\ & + r(1 + rr + r^4 + r^6 + \text{etc.} + r^{2n-2}) \\ & + r^4(1 + r^4 + r^8 + r^{12} + \text{etc.} + r^{4n-4}) \\ & + r^9(1 + r^6 + r^{12} + r^{18} + \text{etc.} + r^{6n-6}) \\ & + \text{etc.} \\ & + r^{(n-1)^2}(1 + r^{2n-2} + r^{4n-4} + r^{6n-6} + \text{etc.} + r^{2(n-1)^2}) \end{aligned}$$

Now if n is odd, each part of this sum, except the first n, will be $= 0$. For the second part manifestly becomes $\frac{r(1-r^{2n})}{1-rr}$, the third $\frac{r^4(1-r^{4n})}{1-r^4}$, etc. When n is even, it is also be necessary to study the part

$$r^{\frac{1}{4}nn}(1+r^n+r^{2n}+r^{3n}+\text{etc.}+r^{nn-n})$$

which becomes $=nr^{\frac{1}{4}nn}$. In the former case, we therefore obtain $WW'=n$, but in the latter, $=n+nr^{\frac{1}{4}nn}$. But $r^{\frac{1}{4}nn}$ becomes $=+1$, if n is evenly even, and thus $WW'=2n$. On the other hand, if n is oddly even, then $r^{\frac{1}{4}nn}=-1$, and thus $WW'=0$. Q. E. D.

36.

Already from article 22, it is clear that if n is an odd prime number, then $\frac{W'}{W}$ will be equal to $+1$ or -1, according as -1 is a quadratic residue or a non-residue modulo n. Hence in the former case, we must have $W^2=+n$, in the latter $W^2=-n$; wherefore, by article 13, we conclude that the former case can only occur when n is of the form $4\mu+1$, and the latter case when n is of the form $4\mu+3$.

Finally, from the combination of conditions for the residues $+2$ and -1, it naturally follows that -2 is a quadratic residue modulo any prime number of the form $8\mu+1$ or $8\mu+3$, and a quadratic non-residue modulo any prime number of the form $8\mu+5$ or $8\mu+7$.

NEW DEMONSTRATIONS AND EXTENSIONS

OF THE FUNDAMENTAL THEOREM

IN

THE THEORY OF QUADRATIC RESIDUES

A U T H O R

CARL FRIEDRICH GAUSS

SUBMITTED TO THE ROYAL SOCIETY OF SCIENCES 1817, FEBRUARY 10.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. IV.
Göttingen 1818.

NEW DEMONSTRATIONS AND EXTENSIONS OF THE FUNDAMENTAL THEOREM IN THE THEORY OF QUADRATIC RESIDUES

The fundamental theorem of quadratic residues, which is considered among the most beautiful truths of higher arithmetic, has indeed been easily discovered through induction, but has proven to be much more difficult to demonstrate. It often happens in this kind of scenario that the demonstrations of very simple truths, which seem to offer themselves readily to the inquirer through induction, are deeply hidden, and after many futile attempts, a path very different from the one sought may finally come to light. Then it often happens that once one path is discovered, several others are also revealed leading to the same goal, some more briefly and more directly, others seemingly obliquely and beginning from very different principles, among which you would scarcely have suspected any connection to the proposed question. Such a marvelous connection between more abstruse truths not only adds a certain peculiar beauty to these contemplations, but also merits diligent investigation and unraveling, because not infrequently new supports or increments to the very science itself come from there.

Therefore, although the arithmetic theorem which is to be discussed here may seem to be fully completed by previous efforts, which provided four entirely different demonstrations[2], I nonetheless return again to the same theme, and add two more

[2]Two have been set forth in the Disquisitiones Arithmeticae Sections four and five; the third in a separate treatise (Commentt. Soc. Gotting. Vol. XVI), the fourth is included in the treatise: Summation of certain singular series (Commentt. Recentiores, Vol. I).

demonstrations, which will certainly shed new light on this matter. The first is in a certain way related to the third, as it proceeds from the same lemma; afterwards, however, it follows a different course, so that it can well be considered a new proof, which will be seen to be, if not superior, at least not inferior to the third one, in its very conciseness. On the other hand, the sixth demonstration is based on a completely different and more subtle principle and provides a new example of the astonishing connection between arithmetic truths that, at first glance, appear to be very far apart. To these two demonstrations, a very simple new algorithm is added to determine whether a given integer is a quadratic residue modulo a given prime or not.

There was yet another reason, which prompted me to announce the new demonstrations at this particular moment, although they had been promised nine years ago. Namely, from 1805, when I began to investigate the theory of cubic and biquadratic residues, which is a much more difficult subject, I experienced almost the same fate as I once had in the theory of quadratic residues. Indeed, those theorems, which entirely exhaust these questions, and in which a remarkable analogy with the theorems pertaining to quadratic residues shines forth, were immediately discovered by induction as soon as a suitable approach had been found. However, all efforts to obtain them, with their demonstrations perfected in every aspect, remained fruitless for a long time. This was the very incentive for me to add more and more demonstrations to those already known about quadratic residues, supported by the hope that among many diverse methods, one or another might do something to illuminate an analogous line of reasoning. This hope was by no means in vain, and tireless labor was finally followed by prosperous success. It will soon be possible to bring the fruits of this vigilance to public light; but before embarking on this arduous task, I decided to return once more to the theory of quadratic residues, to complete all that still remained of that agenda, and thus to bid farewell to this sublime part of arithmetic.

FUNDAMENTAL THEOREM OF THE THEORY OF QUADRATIC RESIDUES, FIFTH PROOF

1.

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

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

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

be taken. Some of these will be less than $\frac{1}{2}m$ and some will be greater; let the multitude of the latter $= n$. Then M will be a quadratic residue or non-residue modulo m, depending on whether n is even, or odd.

PROOF. Let those residues which are less than $\frac{1}{2}m$ be denoted by a, b, c, d, etc., and let the rest, which are greater than $\frac{1}{2}m$, be denoted by a', b', c', d', etc. The complements to m of the latter, $m-a'$, $m-b'$, $m-c'$, $m-d'$, etc., will evidently all be less than $\frac{1}{2}m$, and they will be distinct both among themselves and from the residues a, b, c, d, etc. Therefore they will be identical, though in a different order, with the numbers 1, 2, 3, 4, ..., $\frac{1}{2}(m-1)$. So, if we set

$$1 \times 2 \times 3 \times 4 \ldots \tfrac{1}{2}(m-1) = P$$

then

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

and thus

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

Furthermore, we have

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

modulo m, so

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

Hence $M^{\frac{1}{2}(m-1)} \equiv \pm 1$, where the sign is positive if n is even and negative if n is odd. Therefore, with the help of the theorem demonstrated in *Disquisitiones Arithmeticae* art. 106, the truth of the lemma is immediately apparent.

2.

THEOREM. *Let m, M be positive odd relatively prime integers, and let n be the multitude of numbers in the sequence*

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

whose minimal positive residues modulo m are greater than $\frac{1}{2}m$. Similarly, let N be the multitude of numbers in the sequence

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

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

PROOF. Let us denote

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

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

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

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

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

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

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

Since every integer not divisible by m must be congruent, modulo m, to a residue from the complex f or from the complex f', and similarly every integer not divisible by M must be congruent to a residue from the complex F or from the complex F', it follows that all the numbers φ, among which obviously no one is divisible by both m and M, can be distributed into eight classes in the following way.

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

II. Numbers congruent to numbers from f, F' modulo m, M, respectively, the multitude of which we set $= \beta$.

III. Numbers congruent to numbers from f', F modulo m, M, respectively, the multitude of which we set $= \gamma$.

IV. Numbers congruent to numbers from f', F' modulo m, M, respectively, the multitude of which shall be $= \delta$.

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

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

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

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

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

Similarly, all the numbers φ' will be distributed into eight classes IX - XVI. If we maintain the same order, then it is easy to see that the numbers in the classes

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

are the complement to mM of the numbers in the classes

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

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

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

and by a similar argument

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

By joining all numbers of classes II, IV, VI, we will clearly have all numbers below $\frac{1}{2}mM$, which are congruent to some residue from F' modulo M. Moreover, these same numbers can also be presented as follows:

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

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

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

Similarly, by joining the classes III, IV, VIII, it follows that

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

From all this the following four equations arise:

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

each of which demonstrates the truth of the theorem.

3.

If we now assume that m and M are prime numbers, the combination of the previous theorem with the lemma of article 1 immediately yields the fundamental theorem. For it is clear that,

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

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

FUNDAMENTAL THEOREM OF THE THEORY OF QUADRATIC RESIDUES, SIXTH PROOF.

1.

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

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

will be divisible by

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

PROOF. Let g be a positive integer such that $gn \equiv 1 \pmod{p}$, and let $gn = 1 + hp$. Then we have

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

and therefore the function is clearly integral. Q. E. D.

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

2.

Let α denote a positive primitive root modulo p, i.e., let α be a positive integer such that the minimal positive residues of the powers 1, α, $\alpha\alpha$, α^3, ..., α^{p-2} modulo p are identical, without respect to order, with the numbers 1, 2, 3, 4, ..., $p-1$. Further denote by $f(x)$ the function

$$x + x^\alpha + x^{\alpha\alpha} + x^{\alpha^3} + \ldots + x^{\alpha^{p-2}} + 1$$

It is clear that $f(x) - 1 - x - xx - x^3 - \ldots - x^{p-1}$ will be divisible by $1 - x^p$, and therefore a fortiori by $\frac{1-x^p}{1-x} = 1 + x + xx + x^3 + \ldots + x^{p-1}$. From this it follows, since x is an indeterminate quantity, that $f(x^n)$ will also be divisible by $\frac{1-x^{np}}{1-x^n}$ and consequently (by the previous article) also by $\frac{1-x^p}{1-x}$, as long as n is an integer not divisible by p. Conversely, whenever n is an integer divisible by p, each part of the function $f(x^n)$, reduced by unity, will be divisible by $1 - x^p$. Therefore in this case,

$f(x^n)-p$ will also be divisible by $1-x^p$, and consequently also by $\frac{1-x^p}{1-x}$.

3.

THEOREM. *If we set*

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

then $\xi\xi\mp p$ *will be divisible by* $\frac{1-x^p}{1-x}$, *if we take the upper sign whenever* p *is of the form* $4k+1$ *and the lower sign whenever* p *is of the form* $4k+3$.

PROOF. It can easily be seen that, of the $p-1$ functions

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

etc. up to

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

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

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

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

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

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

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

remains divisible by $\frac{1-x^p}{1-x}$. Above the sign will be positive or negative, depending

on whether p is of the form $4k+1$ or $4k+3$. And since $f(x^{\alpha^{\frac{1}{2}(p-1)}+1})-p$ is divisible by $\frac{1-x^p}{1-x}$, it follows that $\xi\xi\mp p$ will also be divisible by $\frac{1-x^p}{1-x}$. Q.E.D.

To avoid any ambiguity from the double sign, we will denote by ε the number $+1$ or -1, according to whether p is of the form $4k+1$ or $4k+3$. Therefore,

$$\frac{(1-x)(\xi\xi-\varepsilon p)}{1-x^p}$$

will be an integral function of x, which we will denote by Z.

4.

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

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

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

5.

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

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

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

$$\begin{gathered}x^q-x^{\alpha^\mu}\\ x^{q\alpha}-x^{\alpha^{\mu+1}}\\ x^{q\alpha\alpha}-x^{\alpha^{\mu+2}}\\ x^{q\alpha^3}-x^{\alpha^{\mu+3}}\\ \vdots\end{gathered}$$

$$\begin{gathered} x^{q\alpha^{p-\mu-2}} - x^{\alpha^{p-2}} \\ x^{q\alpha^{p-\mu-1}} - x \\ x^{q\alpha^{p-\mu}} - x^{\alpha} \\ x^{q\alpha^{p-\mu+1}} - x^{\alpha\alpha} \\ \vdots \\ x^{q\alpha^{p-2}} - x^{\alpha^{\mu-1}} \end{gathered}$$

will all be divisible by $1 - x^p$. Taking these quantities alternately positive and negative, and adding them up, it is clear that the function

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

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

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

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

6.

Having made these preparations, we deduce by combining the preceding equations that

$$q\xi X = \varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma) + \tfrac{1-x^p}{1-x} \cdot (Z(\delta p^{\frac{1}{2}(q-1)} - \gamma) + Y\xi\xi - W\xi(1-x))$$

Suppose that upon dividing the function ξX by

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

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

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

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

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

which is obviously false unless both the left member and the right member vanish separately. Therefore $\varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)$ will be divisible by q, and also $\delta p^{\frac{1}{2}(q-1)} - \gamma$,

and therefore, because $\delta\delta = 1$, the number $p^{\frac{1}{2}(q-1)} - \gamma\delta$ will be divisible by q.

Now if β denotes a positive or negative unit, depending on whether p is a quadratic residue or non-residue modulo q, then $p^{\frac{1}{2}(q-1)} - \beta$ will be divisible by q, and therefore so will be $\beta - \gamma\delta$, which cannot happen unless $\beta = \gamma\delta$. Hence, the fundamental theorem follows automatically. Namely,

I. Whenever both p, q, or one of them alone, is of the form $4k+1$, and consequently $\delta = +1$, we will have $\beta = \gamma$, and thererfore either q is a quadratic residue mduloo p, and p is simultaneously a quadratic residue modulo q, or q is a quadratic non-residue modulo p, and simultaneously p is a quadratic non-residue modulo q.

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

A new algorithm for determining whether a given positive integer is a quadratic residue or non-residue modulo a given prime.

1.

Before we present a new solution to this problem, we will briefly repeat the solution given in *Disquisitiones Arithmeticae*, which is accomplished quite expediently with the help of the fundamental theorem and the following well-known theorems:

I. The relation of a number a to a number b (insofar as the former is a quadratic residue or non-residue modulo the latter) is the same as the relation of a number c to b, if $a \equiv c \pmod{b}$.

II. If a is a product of factors α, β, γ, δ, etc., and b is a prime number, then the relation of a to b will depend on the relation of these factors to b, so that a will be a quadratic residue or non-residue depending on whether there is an even or odd number of such factors which are quadratic non-residues modulo b. Thus, whenever any factor is a square, it will not be considered at all in this examination; but if any factor is a power of an integer with an odd exponent, it can be replaced with that integer instead.

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

Therefore, given a number a whose relation to the prime number b is sought, we first substitute the minimal positive residue of a modulo b in place of a. Then, after resolving this residue into its prime factors, the problem is reduced by theorem II to the determination of the relations of each of these factors to b. The relation of the factor 2 (if it is present an odd number of times) to b is known by theorem III. The relations of the remaining factors to b is known by the fundamental theorem. In this way, instead of finding the relation of the given number to the prime number b, the relations of the number b to some other odd primes smaller than b must now been investigated, and these problems will be reduced in the same way to smaller moduli, and is clear that these successive reductions will eventually be exhausted.

2.

To illustrate this solution by an example, let us seek the relation of the number 103 to 379. Since 103 is already less than 379, and is itself a prime number, the fundamental theorem must be applied immediately, which tells us that the relation we seek is the opposite of the relation of the number 379 to 103. This in turn is equal to the relation of the number 70 to 103, which depends on the relations of the numbers 2, 5, 7 to 103. The first of these relations is revealed by theorem III. The second, by the fundamental theorem, depends on the relation of the number 103 to 5, which by theorem I is equal to the relation of the number 3 to 5; this, in turn, by the fundamental theorem, depends on the relation of the number 5 to 3, which by theorem I is equal the relation of the number 2 to 3, which is known by theorem III. Likewise, the relation of the number 7 to 103 depends, by the fundamental theorem, on the relation of the number 103 to 7, which by theorem I is equal to the relation of the number 5 to 7; this, in turn, by the fundamental theorem, depends on the relation of the number 7 to 5, which is equal, by theorem I, to the relation of the number 2 to 5, which is known by theorem III. If one prefers to transform this analysis into a synthesis, the decision of the question will be referred to the fourteen points, which we present here in full, so that the greater conciseness of the new solution may be the more clearly understood.

1. The number 2 is a quadratic residue modulo 103 (theorem III).
2. The number 2 is a quadratic non-residue modulo 3 (theorem III).
3. The number 5 is a quadratic non-residue modulo 3 (by 1 and 2).
4. The number 3 is a quadratic non-residue modulo 5 (fund. thm. and 3).
5. The number 103 is a quadratic non-residue modulo 5 (1 and 4).

6. The number 5 is a quadratic non-residue modulo 103 (fund. thm. and 5).

7. The number 2 is a quadratic non-residue modulo 5 (theorem III).

8. The number 7 is a quadratic non-residue modulo 5 (1 and 7).

9. The number 5 is a quadratic non-residue modulo 7 (fund. thm. and 8).

10. The number 103 is a quadratic non-residue modulo 7 (1 and 9).

11. The number 7 is a quadratic residue modulo 103 (fund. thm. and 10).

12. The number 70 is a quadratic non-residue modulo 103 (II, 1, 6, 11).

13. The number 379 is a quadratic non-residue modulo 103 (1 and 12).

14. The number 103 is a quadratic residue modulo 379 (fund. thm. and 13).

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

3.

PROBLEM. *If a and b are positive integers which are relatively prime to each other, and $\left[\frac{1}{2}a\right] = a'$, evaluate the sum*

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

SOLUTION. For the sake of brevity, let us denote the sum in question by $\varphi(a, b)$, so that

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

if we set $\left[\frac{1}{2}b\right] = b'$. In the demonstration of the third fundamental theorem, it was shown that, in the case where a and b are both odd, we have

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

By following the same method, the truth of this proposition can also be extended to the case where only one of the numbers a, b is odd, as we already mentioned there. Let a be divided by b in a manner analogous to the method by which the greatest common divisor of two integers is investigated, let β be the quotient, and let c be the remainder; then divide b by c and so on in a similar manner, so as to obtain equations

$$a = \beta b + c$$
$$b = \gamma c + d$$
$$c = \delta d + e$$
$$d = \varepsilon e + f \text{ etc.}$$

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

$$k = \lambda l + 1$$

We clearly have

$$\left[\tfrac{a}{b}\right] = \left[\beta + \tfrac{c}{b}\right] = \beta + \left[\tfrac{c}{b}\right]$$
$$\left[\tfrac{2a}{b}\right] = \left[2\beta + \tfrac{2c}{b}\right] = 2\beta + \left[\tfrac{2c}{b}\right]$$
$$\left[\tfrac{3a}{b}\right] = \left[3\beta + \tfrac{3c}{b}\right] = 3\beta + \left[\tfrac{3c}{b}\right]$$

etc., so

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

and therefore

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

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

$$\varphi(b,c) = b'c' - \tfrac{1}{2}\gamma(c'c' + c') - \varphi(a,d)$$
$$\varphi(c,d) = c'd' - \tfrac{1}{2}\delta(d'd' + d') - \varphi(d,e)$$
$$\varphi(d,e) = d'e' - \tfrac{1}{2}\varepsilon(e'e' + e') - \varphi(e,f)$$

etc. up to

$$\varphi(k,l) = k'l' - \tfrac{1}{2}\lambda(l'l' + l') - \varphi(l,1)$$

Therefore, since it is obvious that $\varphi(l,1) = 0$, we obtain the formula

$$\varphi(a,b) = a'b' - b'c' + c'd' - d'e' + \text{etc.} \pm k'l'$$
$$- \tfrac{1}{2}\beta(b'b' + b') + \tfrac{1}{2}\gamma(c'c' + c') - \tfrac{1}{2}\delta(d'd' + d') + \tfrac{1}{2}\varepsilon(e'e' + e') - \text{etc.} \mp \tfrac{1}{2}\lambda(l'l' + l')$$

4.

It is easily concluded from what was set forth in the third proof, that the relation of the number b to a, whenever a is a prime number, is automatically known from the value of the sum $\varphi(a, 2b)$. Namely, b will be a quadratic residue modulo a

or a non-residue depending on whether this sum is a even or odd number. The sum $\varphi(a,b)$ itself can be used for the same purpose, but with the restriction, however, that the case where b is odd must be distinguished from the case where it is even. Specifically,

I. Whenever b is odd, b will be a quadratic residue or non-residue modulo a, depending on whether $\varphi(a,b)$ is even or odd.

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

All of these are very easily derived from article 4 of the third proof.

5.

Example. If the ratio of the number 103 to the prime number 379 is sought, then to find the sum $\varphi(379,103)$, we first compute

$$\begin{array}{r|l|l} a=379 & a'=189 & \\ b=103 & b'=\ 51 & \beta=3 \\ c=\ 70 & c'=\ 35 & \gamma=1 \\ d=\ 33 & d'=\ 16 & \delta=2 \\ e=\ 4 & e'=\ 2 & \varepsilon=8 \end{array}$$

hence

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

and thus 103 is a quadratic residue modulo 379. If we want to use the sum $\varphi(379,206)$ for the same purpose, we have the following pattern,

$$\begin{array}{r|r|l} 379 & 189 & \\ 206 & 103 & 1 \\ 173 & 86 & 1 \\ 33 & 16 & 5 \\ 8 & 4 & 4 \end{array}$$

from which we deduce

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

and thus 103 is a quadratic residue modulo 379.

6.

Since in order to determine the relation of b to a, it is not necessary to compute each part of the aggregate $\varphi(a, b)$, but rather it is sufficient to know how many of them are odd, our rule can also be expressed as follows:

Let $a = \beta b + c$, $b = \gamma c + d$, $c = \delta d + e$ etc., until the series of numbers a, b, c, d, e etc. reaches unity. Set $\left[\frac{1}{2}a\right] = a'$, $\left[\frac{1}{2}b\right] = b'$, $\left[\frac{1}{2}c\right] = c'$ etc., and let μ be the multitude of odd numbers in the series a', b', c' etc. which are immediately followed by an odd number; further, let ν be the multitude of odd numbers in the series β, γ, δ etc., such that the corresponding number in the series b', c', d' etc. is of the form $4n+1$ or $4n+2$. With this being done, b will be a quadratic residue or non-residue modulo a, depending on whether $\mu+\nu$ is even or odd, except in the case where b is even and a is of the form $8n+3$ or $8n+5$, in which case the opposite rule holds.

In our example, the sequence a', b', c', d', e' has two consecutive pairs of odd numbers, hence $\mu = 2$, and in the series b', c', d', e', there are two odd numbers, but the corresponding numbers in b', c', d', e' are of the form $4n+3$, hence $\nu = 0$. Therefore, $\mu+\nu$ is even, and it follows that 103 is a quadratic residue modulo 379.

THE THEORY OF
BIQUADRATIC RESIDUES

FIRST COMMENTARY

AUTHOR

CARL FRIEDRICH GAUSS

DELIVERED TO THE ROYAL SOCIETY 1825, APRIL 5.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. VI.
Göttingen 1827.

THE THEORY OF BIQUADRATIC RESIDUES.

FIRST COMMENTARY

1.

The theory of quadratic residues has been reduced to a few fundamental theorems, to be numbered among the most beautiful relics of Higher Arithmetic. These were first easily discovered by induction, and then were demonstrated in many ways, so that nothing more was left to be desired.

However, the theory of cubic and biquadratic residues is a far deeper undertaking. When we began to investigate this in the year 1805, some special theorems presented themselves, beyond those which had been placed on the threshold, which were very remarkable owing both to their simplicity and to the difficulty of their demonstrations. We soon found out that the principles of higher arithmetic hitherto used were by no means sufficient for establishing the general theory, and rather this necessarily requires that the field of higher arithmetic be advanced as if to infinity. How this is to be understood will be elucidated clearly in the remainder of these discussions. As soon as we entered this new field, an approach to the knowledge of the simplest theorems was at once obvious, and the whole theory was exhausted by induction. Yet the demonstrations lay so deeply concealed, that it was only after many fruitless attempts that they could at last be brought to light.

Now that we are preparing to publish these lucubrations, we will begin with the theory of biquadratic residues, and indeed in this first commentary we will

describe those investigations which have already been completed within the expanded field of Arithmetic, which paved they way, as it were. At the same time, we will present some new developments in the theory of division of the circle.

2.

We introduced the concept of a biquadratic residue in *Disquisitiones Arithmeticae* art. 115. Specifically, an integer a, positive or negative, is said to be a biquadratic residue modulo p if a is congruent to a biquadrate modulo p, and likewise a non-residue, if no such congruence exists. In all of the following discussions, unless explicitly stated otherwise, we will assume that the modulus p is a prime number (odd positive), and that a is not divisible by p, since all of the remaining cases can easily be reduced to this one.

3.

It is clear that every biquadratic residue modulo p is also a quadratic residue, and therefore every quadratic non-residue is also a biquadratic non-residue. We may also invert this statement whenever p is a prime number of the form $4n+3$. For in this case, if a is a quadratic residue modulo p, we can set $a \equiv bbb \,(\mathrm{mod.}\, p)$, and b will either be a quadratic residue or non-residue modulo p. In the former case, we can set $b \equiv cc$, and hence $a \equiv c^4$, i.e. a will be a biquadratic residue modulo p. In the latter case, $-b$ will be a quadratic residue modulo p (since -1 is a quadratic non-residue of any prime of the form $4n+3$), and setting $-b \equiv cc$, we will have as before $a \equiv c^4$, so a will be a biquadratic residue modulo p. At the same time, it can be easily seen that, aside from the solutions $x \equiv c$ and $x \equiv -c$, no other solutions of the congruence $x^4 \equiv a \,(\mathrm{mod.}\, p)$ can be found in this case. Since these propositions clearly exhaust the entire theory of biquadratic residues for prime moduli of the form $4n+3$, we will exclude such moduli entirely from our investigation, or in other words we will limit ourselves to prime moduli of the form $4n+1$.

4.

Given a prime number p of the form $4n+1$, the converse of the proposition in the previous article is invalid: namely, there can exist quadratic residues that are not at the same time biquadratic residues. Indeed, this happens whenever a quadratic residue is congruent to the square of a quadratic non-residue. For setting $a \equiv bb$, where b is a quadratic non-residue modulo p, if the congruence $x^4 \equiv a$ could be

satisfied by a value $x \equiv c$, then we would have $c^4 \equiv bb$, or the product $(cc-b)(cc+b)$ would be divisible by p. Thus p would divide one of the two factors $cc-b$ or $cc+b$, i.e., either $+b$ or $-b$ would be a quadratic residue modulo p, and therefore (since -1 is a quadratic residue) both would be quadratic residues, contrary to the hypothesis.

Therefore, all integers not divisible by p can be distributed into three classes, the first containing the biquadratic residues, the second containing the biquadratic non-residues which are at the same time quadratic residues, and the third containing the quadratic non-residues. Clearly, it is sufficient to subject only the numbers 1, 2, $3 \ldots p-1$ to this classification, and half of these will be reduced to the third class, whereas the other half will be distributed between the first and second classes.

5.

However, it will be better to establish four classes, whose nature is as follows.

Let A be the complex of all biquadratic residues modulo p that are situated between 1 and $p-1$ (inclusive), and let e be an arbitrary quadratic non-residue modulo p. Let B be the complex of minimal positive residues arising from the products eA taken modulo p, and likewise let C and D be the complexes of minimal positive residues arising from the products eeA, e^3A modulo p. Having done this, it is easy to see that the numbers in B will be distinct from each other, and likewise for C and D. Furthermore, it is clear that all numbers contained in A and C are quadratic residues of p, while all those in B and D are quadratic non-residues, so that certainly the complexes A and C cannot have a number in common with the either of the complexes B or D. Moreover, A cannot have any number in common with C, and B cannot have any number in common with D. For suppose

I. that some number from A, e.g. a, can also be found in C, where it is congruent to a product eea', with a' being a number from the complex A. Let $a \equiv \alpha^4$, $a' \equiv \alpha'^4$, and let an integer Θ be chosen such that $\Theta\alpha' \equiv 1$. Then we have $ee\alpha'^4 \equiv \alpha^4$, and therefore, by multiplying by Θ^4,

$$ee \equiv \alpha^4\Theta^4$$

i.e. ee is a biquadratic residue, and therefore e is a quadratic residue, contrary to the hypothesis.

II. Similarly, suppose that some number is common to the complexes B, D, and that it comes from products ea, e^3a', with a, a' being numbers from the complex A. Then the congruence $ea \equiv e^3a'$ would imply $a \equiv eea'$, hence a number would be obtained, which being a product eea' would originate from C, but at the same time would belong to A, which we have just shown to be impossible.

Furthermore, it is easily shown that *all* quadratic residues modulo p, between 1 and $p-1$ inclusive, must necessarily lie in either A or C, and all quadratic non-residues of p between those limits must necessarily lie in either B or in D. For

I. Every such quadratic residue, which is also a biquadratic residue, is found in A by hypothesis.

II. Given a quadratic residue h (less than p), which is also a biquadratic non-residue, one can find a quadratic non-residue such that h is $\equiv gg$. Find an integer γ such that $e\gamma \equiv g$. Then γ will be a quadratic residue modulo p, which we set $\equiv kk$. Hence

$$h \equiv gg \equiv ee\gamma\gamma \equiv eek^4$$

Therefore, since the minimum residue of k^4 is found in A, the number h, which arises from it by taking the product with ee, must necessarily be contained in C.

III. Let h denote a quadratic non-residue modulo p between the limits 1 and $p-1$, and let g be an integer between the same limits such that $eg \equiv h$. Then g is a quadratic residue, and therefore it is contained in either A or C. In the former case, h will clearly be found among the numbers in B, and in the latter case, it will be found among the numbers in D.

From all this it is deduced that the numbers 1, 2, 3, $\ldots p-1$ are distributed among the four series A, B, C, D in such a way that each of them is found in exactly one of these. Therefore, each series must contain exactly $\frac{1}{4}(p-1)$ numbers. In this classification, classes A and C possess their numbers naturally, but the distinction between classes B and D is arbitrary, insofar as it depends on the choice of the number e, which is always referred to class B. Therefore, if another number from class D is adopted in its place, the classes B and D will be interchanged.

6.

Since -1 is a quadratic residue modulo p, let us set $-1 \equiv ff \pmod{p}$, so that the four roots of the congruence $x^4 \equiv 1$ will be 1, f, -1, $-f$. Then if a is a biquadratic residue modulo p, say $\equiv \alpha^4$, the four roots of the congruence $x^4 \equiv a$

will be α, $f\alpha$, $-\alpha$, $-f\alpha$, which are easily seen to be incongruent to each other. Hence, it is clear that if the least positive residues of the biquadrates 1, 16, 81, $256 \ldots (p-1)^4$ are collected, each will be present four times, so that the $\frac{1}{4}(p-1)$ distinct biquadratic residues forming the complex A will be obtained. If only the minimal residues of biquadrates up to $(\frac{1}{2}p - \frac{1}{2})^4$ are collected, then each will occur twice.

7.

The product of two biquadratic residues is clearly a biquadratic residue, as multiplication of two numbers of class A will always produce a product whose minimal positive residue belongs to the same class. Similarly, products of numbers from B with numbers from D, or numbers from C with numbers from C, will always have their minimal positive residues in A.

Likewise, the residues of the products $A.B$ and $C.D$ fall in B; the residues of the products $A.C$, $B.B$, and $D.D$ fall in C; and finally, the residues of the products $A.D$ and $B.C$ fall in D.

The proofs are so obvious that it suffices to indicate just one. Let e.g. c and d be numbers from C and D, with $c \equiv eea$, $d \equiv e^3a'$, where a and a' are numbers from A. Then e^4aa' will be a biquadratic residue, i.e. its minimal residue will lie in A: thus, since the product cd is $\equiv ee^4aa'$, its minimal residue will lie in B.

At the same time, it can now be easily judged to which class the product of several factors should be referred. Namely, by assigning characters 0, 1, 2, 3 to the classes A, B, C, D respectively, the character of a product will be equal to the sum of the characters, or rather its minimal residue modulo 4.

8.

It seemed worthwhile to develop these elementary propositions without the support of the theory of powers of residues, with whose help it would have been far easier to demonstrate everything thus far.

Let g be a primitive root modulo p, i.e. a number such that in the series of powers g, gg, $g^3, \ldots$ no value before g^{p-1} is congruent to unity modulo p. Then without regard to order, the minimal positive residues of the numbers 1, g, gg, $g^3, \ldots, g^{p-2}$ agree with 1, 2, $3, \ldots, p-1$, and they can be conveniently distributed into four classes in the following manner:

to	the minimal residues of the numbers
A	$1,\ g^4, g^8,\ g^{12}, \ldots, g^{p-5}$
B	$g,\ g^5, g^9,\ g^{13}, \ldots, g^{p-4}$
C	$gg, g^6, g^{10}, g^{14}, \ldots, g^{p-3}$
D	$g^3, g^7, g^{11}, g^{15}, \ldots, g^{p-2}$

Hence all the previous propositions follow automatically.

Moreover, just as here the numbers $1,\ 2,\ 3, \ldots, p-1$ have been distributed into four classes, whose complexes we denoted by A, B, C, D, so may *any* integer not divisible by p be assigned to one of these classes, according to the class of its minimal residue modulo p.

9.

We shall denote by f the minimal residue of the power $g^{\frac{1}{4}(p-1)}$ modulo p. Then it follows that $ff \equiv g^{\frac{1}{2}(p-1)} \equiv -1$ (*Disquis. Arithm.* art. 62), and it is clear that f here has the same meaning as in article 6. Thus for an arbitrary positive integer λ, the power $g^{\frac{1}{4}\lambda(p-1)}$ will be congruent to 1, f, -1, $-f$ modulo p, depending on whether λ takes the form $4m$, $4m+1$, $4m+2$, $4m+3$ resp., or as the minimal residue of g^λ is found in A, B, C, D resp. From this we obtain a very simple criterion for deciding to which class a given number h (not divisible by p) should be referred; namely, h will belong to A, B, C, or D, depending on whether the power $h^{\frac{1}{4}(p-1)}$ turns out to be congruent to 1, f, -1, or $-f$ modulo p.

As a corollary, it follows from this that -1 is always referred to class A whenever p is of the form $8n+1$, and to class C whenever p is of the form $8n+5$. A proof of this theorem which is independent of the theory of residual powers can be easily constructed from what we have shown in *Disquisitionibus Arithmeticis* art. 115, III.

10.

Since *all* primitive roots modulo p come from residues of powers g^λ, by taking for λ all numbers relatively prime to $p-1$, it is easy to see that these will be equally distributed between the sets B and D, with the base g always contained in B. If, instead of the number g, a different primitive root from the set B is chosen as the base, the classification will remain the same; however, if a primitive root from the set D is adopted as the base, the sets B and D will be interchanged.

If the classification criterion is built upon the theorem in the previous article, the distinction between the classes B and D will depend on which root of congruence $xx \equiv -1 \pmod{p}$ we adopt as the characteristic number f.

11.

In order for the more subtle investigations which we are about to undertake to be illustrated by examples, we present here the construction of the classes for all moduli less than 100. We have adopted the smallest primitive root in each case.

$$p = 5$$
$$g = 2, f = 2$$

A	1
B	2
C	4
D	3

$$p = 13$$
$$g = 2, f = 8$$

A	$1, \quad 3, \quad 9$
B	$2, \quad 5, \quad 6$
C	$4, \ 10, \ 12$
D	$7, \quad 8, \ 11$

$$p = 17$$
$$g = 2, f = 12$$

A	$1, \ 4, \ 13, \ 16$
B	$3, \ 5, \ 12, \ 14$
C	$2, \ 8, \quad 9, \ 15$
D	$6, \ 7, \ 10, \ 11$

$$p = 29$$
$$g = 2, f = 12$$

A	$1, \quad 7, \ 16, \ 20, \ 23, \ 24, \ 25$
B	$2, \quad 3, \ 11, \ 14, \ 17, \ 19, \ 21$
C	$4, \quad 5, \quad 6, \quad 9, \ 13, \ 22, \ 28$
D	$8, \ 10, \ 12, \ 15, \ 18, \ 26, \ 27$

$p = 37$

$g = 2, f = 31$

A	$1,\ \ 7,\ \ 9,\ 10,\ 12,\ 16,\ 26,\ 33,\ 34$
B	$2,\ 14,\ 15,\ 18,\ 20,\ 24,\ 29,\ 31,\ 32$
C	$3,\ \ 4,\ 11,\ 21,\ 25,\ 27,\ 28,\ 30,\ 36$
D	$5,\ \ 6,\ \ 8,\ 13,\ 17,\ 19,\ 22,\ 23,\ 35$

$p = 41$

$g = 6, f = 32$

A	$1,\ \ 4,\ 10,\ 16,\ 18,\ 23,\ 25,\ 31,\ 37,\ 40$
B	$6,\ 14,\ 15,\ 17,\ 19,\ 22,\ 24,\ 26,\ 27,\ 35$
C	$2,\ \ 5,\ \ 8,\ \ 9,\ 20,\ 21,\ 32,\ 33,\ 36,\ 39$
D	$3,\ \ 7,\ 11,\ 12,\ 13,\ 28,\ 29,\ 30,\ 34,\ 38$

$p = 53$

$g = 2, f = 30$

A	$1,\ 10,\ 13,\ 15,\ 16,\ 24,\ 28,\ 36,\ 42,\ 44,\ 46,\ 47,\ 49$
B	$2,\ \ 3,\ 19,\ 20,\ 26,\ 30,\ 31,\ 32,\ 35,\ 39,\ 41,\ 45,\ 48$
C	$4,\ \ 6,\ \ 7,\ \ 9,\ 11,\ 17,\ 25,\ 29,\ 37,\ 38,\ 40,\ 43,\ 52$
D	$5,\ \ 8,\ 12,\ 14,\ 18,\ 21,\ 22,\ 23,\ 27,\ 33,\ 34,\ 50,\ 51$

$p = 61$

$g = 2, f = 11$

A	$1,\ 9,\ 12,\ 13,\ 15,\ 16,\ 20,\ 22,\ 25,\ 34,\ 42,\ 47,\ 56,\ 57,\ 58$
B	$2,\ 7,\ 18,\ 23,\ 24,\ 26,\ 30,\ 32,\ 33,\ 40,\ 44,\ 50,\ 51,\ 53,\ 55$
C	$3,\ 4,\ \ 5,\ 14,\ 19,\ 27,\ 36,\ 39,\ 41,\ 45,\ 46,\ 48,\ 49,\ 52,\ 60$
D	$6,\ 8,\ 10,\ 11,\ 17,\ 21,\ 28,\ 29,\ 31,\ 35,\ 37,\ 38,\ 43,\ 54,\ 59$

$p = 73$

$g = 5, f = 27$

A	$1,\ \ 2,\ \ 4,\ \ 8,\ \ 9,\ 16,\ 18,\ 32,\ 36,\ 37,\ 41,\ 55,\ 57,\ 64,\ 65,\ 69,\ 71,\ 72$
B	$5,\ \ 7,\ 10,\ 14,\ 17,\ 20,\ 28,\ 33,\ 34,\ 39,\ 40,\ 45,\ 53,\ 56,\ 59,\ 63,\ 66,\ 68$
C	$3,\ \ 6,\ 12,\ 19,\ 23,\ 24,\ 25,\ 27,\ 35,\ 38,\ 46,\ 48,\ 49,\ 50,\ 54,\ 61,\ 67,\ 70$
D	$11,\ 13,\ 15,\ 21,\ 22,\ 26,\ 29,\ 30,\ 31,\ 42,\ 43,\ 44,\ 47,\ 51,\ 52,\ 58,\ 60,\ 62$

$p = 89$

$g = 3, f = 34$

A	1, 2, 4, 8, 11, 16, 22, 25, 32, 39, 44, 45, 50, 57, 64, 67, 73, 78, 81, 85, 87, 88
B	3, 6, 7, 12, 14, 23, 24, 28, 33, 41, 43, 46, 48, 56, 61, 65, 66, 75, 77, 82 83, 86
C	5, 9, 10, 17, 18, 20, 21, 34, 36, 40, 42, 47, 49, 53, 55, 68, 69, 71, 72, 79 80, 84
D	13, 15, 19, 26, 27, 29, 30, 31, 35, 37, 38, 51, 52, 54, 58, 59, 60, 62, 63, 70 74, 76

$p = 97$

$g = 5, f = 22$

A	1, 4, 6, 9, 16, 22, 24, 33, 35, 36, 43, 47, 50, 54, 61, 62, 64, 73, 75, 81, 88, 91, 93, 96
B	5, 13, 14, 17, 19, 20, 21, 23, 29, 30, 41, 45, 52, 56, 67, 68, 74, 76, 77, 78 80, 83, 84, 92
C	2, 3, 8, 11, 12, 18, 25, 27, 31, 32, 44, 48, 49, 53, 65, 66, 70, 72, 79, 85 86, 89, 94, 95
D	7, 10, 15, 26, 28, 34, 37, 38, 39, 40, 42, 46, 51, 55, 57, 58, 59, 60, 63, 69 71, 82, 87, 90

12.

Since the number 2 is a quadratic residue modulo all prime numbers of the form $8n+1$, and a non-residue modulo all prime numbers of the form $8n+5$, it will be found in classes A or C for prime moduli of the former form, and in classes B or D for prime moduli of the latter form. Since the distinction between classes B and D is not essential, and indeed depends only on the choice of the number f, we will temporarily set aside the moduli of the form $8n+5$. By applying *induction* to moduli of the form $8n+1$, we find that 2 belongs to A for $p = 73$, 89, 113, 233, 257, 281, 337, 353, etc.; on the contrary, 2 belongs to C for $p = 17$, 41, 97, 137, 193, 241, 313, 401, 409, 433, 449, 457, etc.

Moreover, since the number -1 is a biquadratic residue modulo any prime of the form $8n+1$, it is evident that -2 always belongs to the same class as $+2$.

13.

If the examples of the previous article are compared to each other, no simple criterion seems to offer itself, at least at first sight, by which it would be possible to distinguish the former moduli from the latter. Nevertheless, two such criteria can be found, distinguished by their elegance and remarkable simplicity, to which the consideration of the following observations will pave the way.

The modulus p being a prime number of the form$8n+1$, it is reducible, and indeed in only one way, to the form $aa+2bb$ (*Disquiss. Arithm.* art. 182, II); we will assume that roots a, b are taken positively. Clearly a will be odd, and b will be even; let us set $b=2^{\lambda}c$, where c is odd. We now observe

I. By assumption, $p \equiv aa \pmod{c}$, so p is a quadratic residue modulo c, and therefore it is also a quadratic residue modulo each prime factor of c. Therefore, by the fundamental theorem, each of these prime factors will be a quadratic residue modulo p, and therefore also their product c will be a quadratic residue modulo p. Since this also holds for the number 2, it is clear that b is a quadratic residue modulo p, and therefore both bb and $-bb$ are biquadratic residues.

II. It follows that $-2bb$ must belong to the same class as the number 2. Therefore, since $aa \equiv -2bb$, it is clear that 2 will belong to class A or class C, depending on whether a is a quadratic residue or non-residue modulo p.

III. Now let us suppose that a has been resolved into its prime factors, among which those which are of the form $8m+1$ or $8m+7$ are denoted by α, α', α'' etc., and those which are of the form $8m+3$ or $8m+5$ are denoted by β, β', β'' etc. Let the multitude of the latter be $=\mu$. Since $p \equiv 2bb \pmod{a}$, p will be a quadratic residue modulo those prime factors of a for which 2 is a quadratic residue, i.e. the factors α, α', α'' etc.; and it will be a quadratic non-residue modulo those factors for which 2 is a quadratic non-residue, i.e. the factors β, β', β'' etc. Therefore, by the fundamental theorem, each of the numbers α, α', α', α'' etc. will be a quadratic residue modulo p, and each of the numbers β, β', β'' etc. will be a quadratic non-residue. From this it follows that the product a will be a quadratic residue or non-residue modulo p, depending on whether μ is even or odd.

IV. But it is easily confirmed that the product of all α, α', α'' etc. will be of the form $8m+1$ or $8m+7$, and the same holds for the product of all β, β', β'' etc., if the multitude of these is even. So, in this case the product a must necessarily be of the form $8m+1$ or $8m+7$. On the other hand, the product of all β, β', β'' etc., whenever their multitude is odd, will be of the form $8m+3$ or $8m+5$, and the

same holds in this case for the product a.

From all of this, an elegant theorem can be deduced:

When a is of the form $8m+1$ or $8m+7$, the number 2 will be in the complex A; but whenever a is of the form $8m+3$ or $8m+5$, it will be in the complex C.

This is confirmed by the examples enumerated in the preceding article; the former moduli are thus resolved: $73 = 1+2.36$, $89 = 81+2.4$, $113 = 81+2.16$, $233 = 225+2.4$, $257 = 225+2.16$, $281 = 81+2.100$, $337 = 49+2.144$, $353 = 225+2.64$; but the latter thus: $17 = 9+2.4$, $41 = 9+2.16$, $97 = 25+2.36$, $137 = 9+2.64$, $193 = 121+2.36$, $241 = 169+2.36$, $313 = 25+2.144$, $401 = 9+2.196$, $409 = 121+2.144$, $433 = 361+2.36$, $449 = 441+2.4$, $457 = 169+2.144$.

14.

Since the factorization of the number p into a simple and double square has produced such a remarkable connection with the classification of the number 2, it seems worthwhile to investigate whether the decomposition into two squares, to which the number p is equally liable, may provide a similar success. Behold then, the decompositions of the numbers p for which 2 belongs to the class

A	C
$9+64$	$1+16$
$25+64$	$25+16$
$49+64$	$81+16$
$169+64$	$121+16$
$1+256$	$49+144$
$25+256$	$225+16$
$81+256$	$169+144$
$289+64$	$1+400$
	$9+400$
	$289+144$
	$49+400$
	$441+16$

First of all we observe that, of the two squares into which p has been divided, one must be odd, which we set $= aa$, and the other must even, which we set $= bb$. Since aa is of the form $8n+1$, it is clear that the oddly even b correspond to values of p of the form $8n+5$, which are excluded by our induction, since they would have the number 2 in class B or D. For the values of p which are of the form $8n+1$, the value of b must be evenly even, and if we have faith in the induction presented before our eyes, the number 2 must be assigned to class A for all moduli such that b is of the form $8n$, and to class C for all moduli such that b is of the form $8n+4$. But this theorem requires a far deeper investigation than that which we have brought forth in the preceding article, and the demonstration must be preceded by several preliminary investigations regarding the order in which the numbers of the sets A, B, C, D follow each other.

15.

Let us denote the multitude of numbers from the complex A, that are immediately followed by numbers from the complexes A, B, C, D resp., by (00), (01), (02), (03). Likewise, denote the multitude of numbers from complex B that are followed by numbers from complex A, B, C, D resp. by (10), (11), (12), (13); and likewise in the complex C by (20), (21), (22), (23), and in complex D by (30), (31), (32), (33). We propose to determine these sixteen multitudes a priori. In order that the reader can compare the general reasoning with some examples, it was thought to add here the numerical values of the terms in a diagram (S)

$$\begin{array}{c} (00),\ (01),\ (02),\ (03) \\ (10),\ (11),\ (12),\ (13) \\ (20),\ (21),\ (22),\ (23) \\ (30),\ (31),\ (32),\ (33) \end{array}$$

for each modulus for which we have given the classifications in article 11.

$p=5$	$p=13$	$p=17$	$p=29$
0, 1, 0, 0	0, 1, 2, 0	0, 2, 1, 0	2, 3, 0, 2
0, 0, 0, 1	1, 1, 0, 1	2, 0, 1, 1	1, 1, 2, 3
0, 0, 0, 0	0, 1, 0, 1	1, 1, 1, 1	2, 1, 2, 1
0, 0, 1, 0	1, 0, 1, 1	0, 1, 1, 2	1, 2, 3, 1

$p=37$	$p=41$	$p=53$	$p=61$
2, 1, 2, 4	0, 4, 3, 2	2, 3, 6, 2	4, 3, 2, 6
2, 2, 4, 1	4, 2, 2, 2	4, 4, 2, 3	3, 3, 6, 3
2, 2, 2, 2	3, 2, 3, 2	2, 4, 2, 4	4, 3, 4, 3
2, 4, 1, 2	2, 2, 2, 4	4, 2, 3, 4	3, 6, 3, 3

$p=73$	$p=89$	$p=97$
5, 6, 4, 2	3, 8, 6, 4	2, 6, 7, 8
6, 2, 5, 5	8, 4, 5, 5	6, 8, 5, 5
4, 5, 4, 5	6, 5, 6, 5	7, 5, 7, 5
2, 5, 5, 6	4, 5, 5, 8	8, 5, 5, 6

Since the moduli of the form $8n+1$ and $8n+5$ behave in different ways, each must be treated separately: we will begin with the former.

16.

The symbol (00) indicates the multitude of different ways that the equation $\alpha+1=\alpha'$ can be satisfied, where α, α' denote indefinite numbers in the complex A. Whereas for a modulus of the form $8n+1$, such as we understand here, α' and $p-\alpha'$ belong to the same complex, we will say more succinctly that (00) expresses the multitude of different ways to satisfy the equation $1+\alpha+\alpha'=p$. Clearly, this equation can be replaced by the congruence $1+\alpha+\alpha' \equiv 0 \pmod{p}$.

Likewise,

(01) indicates the multitude of solutions of the congruence $1+\alpha+\beta \equiv 0 \pmod{p}$
(02) the multitude of solutions of the congruence $1+\alpha+\gamma \equiv 0$
(03) the multitude of solutions of the congruence $1+\alpha+\delta \equiv 0$
(11) the multitude of solutions of the congruence $1+\beta+\beta' \equiv 0$ etc.

where β and β' are indefinite numbers from the complex B, γ is an indefinite number from the complex C, and δ is an indefinite number from the complex D. Hence we immediately obtain the following six equations:

$$(01)=(10),\ (02)=(20),\ (03)=(30),\ (12)=(21),\ (13)=(31),\ (23)=(32)$$

From any given solution of the congruence $1+\alpha+\beta \equiv 0$, there arises a solution of the congruence $1+\delta+\delta' \equiv 0$, where δ a number within the limits $1 \ldots p-1$ such

that $\beta\delta \equiv 1$ (which is clearly from the complex D), and δ' is the minimal positive residue of the product $\alpha\delta$ (which will also be from the complex D). Likewise it is clear how to return from a given solution of the congruence $1+\delta+\delta' \equiv 0$ to a solution of the congruence $1+\alpha+\beta \equiv 0$, if β is taken in such a way that $\beta\delta \equiv 1$, and we simultaneously let $\alpha \equiv \beta\delta'$. Hence, we conclude that both congruences enjoy an equal multitude of solutions, that is, $(01) = (33)$.

In a similar manner, from the congruence $1+\alpha+\gamma \equiv 0$ we deduce $\gamma'+\gamma''+1 \equiv 0$, if γ' is taken from the complex C in such a way that $\gamma\gamma' \equiv 1$, and γ'' is congruent to the product $\alpha\gamma'$ from the same complex. Hence, we easily infer that these two congruences admit an equal multitude of solutions, that is, $(02) = (22)$.

Similarly, from the congruence $1+\alpha+\delta \equiv 0$ we deduce $\beta+\beta'+1 \equiv 0$, where β, β' are chosen in such a way that $\beta\delta \equiv 1, \beta\alpha \equiv \beta'$. Therefore, $(03) = (11)$.

Finally, from the congruence $1+\beta+\gamma \equiv 0$, we derive in a similar manner h the congruence $\delta+1+\beta' \equiv 0$, and hence also $\gamma'+\delta'+1 \equiv 0$, and thus we conclude that $(12) = (13) = (23)$.

We have thus obtained, among our sixteen unknowns, eleven equations, such that they can be reduced to five, and the scheme S can thus be exhibited as follows:

$$\begin{array}{cccc} h, & i, & k, & l \\ i, & l, & m, & m \\ k, & m, & k, & m \\ l, & m, & m, & i \end{array}$$

Three new conditional equations can now be easily added. For since every number of the complex A, except the final $p-1$, must be followed by a number from one of the complexes A, B, C or D, we will have

$$(00)+(01)+(02)+(03) = 2n-1$$

and similarly

$$(10)+(11)+(12)+(13) = 2n$$
$$(20)+(21)+(22)+(23) = 2n$$
$$(30)+(31)+(32)+(33) = 2n.$$

In terms of the variables we have just introduced, the first three equations supply:

$$h+i+k+l = 2n-1$$
$$i+l+2m = 2n$$
$$k+m = n$$

and the fourth is identical to the second. With the aid of these equations it is

possible to eliminate three of the unknowns, by which means the sixteen unknowns are now reduced to two.

17.

In order to obtain a complete determination, it will be necessary to investigate the number of solutions of the congruence

$$1+\alpha+\beta+\gamma \equiv 0 \,(\text{mod. } p)$$

where α, β, γ denote indefinite numbers from the complex A, B, C. Clearly the value $\alpha = p-1$ is not admissible, since we cannot have $\beta+\gamma \equiv 0$. Therefore, substituting for α the remaining values produces h, i, k, l values of $1+\alpha$ from A, B, C, D respectively. Similarly, for any *given* value of $1+\alpha$ from A, say for $1+\alpha = \alpha^0$, the congruence $\alpha^0+\beta+\gamma \equiv 0$ will admit the same number of solutions as the congruence $1+\beta'+\gamma' \equiv 0$ (by setting $\beta \equiv \alpha^0\beta'$, $\gamma \equiv \alpha^0\gamma'$), i.e. the number of solutions will be $(12) = m$. Likewise, for any given value of $1+\alpha$ from B, say $1+\alpha = \beta^0$, the congruence $\beta^0+\beta+\gamma \equiv 0$ will have as many solutions as the congruence $1+\alpha'+\beta' \equiv 0$ (by setting $\beta \equiv \beta^0\alpha'$, $\gamma \equiv \beta^0\beta'$), i.e. the number of solutions will be $(01) = i$. Similarly, for any given value of $1+\alpha$ from C, say $1+\alpha = \gamma^0$, the congruence $\gamma^0+\beta+\gamma \equiv 0$ has the same number of solutions as the congruence $1+\delta+\alpha' \equiv 0$ (by setting $\beta \equiv \gamma^0\delta$, $\gamma \equiv \gamma^0\alpha'$), i.e. the number of solutions will be $(03) = l$. Finally, for any given value of $1+\alpha$ from D, say for $1+\alpha = \delta^0$, the congruence $\delta^0+\beta+\gamma \equiv 0$ will have as many solutions as the congruence $1+\gamma'+\delta' \equiv 0$ (by setting $\beta \equiv \delta^0\gamma'$, $\gamma \equiv \delta^0\delta'$), i.e. there will be $(23) = m$ solutions. Putting all of this together, it is clear that the congruence $1+\alpha+\beta+\gamma \equiv 0$ will admit

$$hm+ii+kl+lm$$

distinct solutions.

In exactly the same way we can deduce that if each of the numbers from B are substituted for β, then $1+\beta$ obtains resp. (10), (11), (12), (13) or i, l, m, m values from A, B, C, D, and for any *given* value of $1+\beta$ from the relevant complexes, the congruence $\alpha+\beta+\gamma \equiv 0$ admits (02), (31), (20), (13) or k, m, k, m distinct solutions, so that the multitude of all solutions becomes

$$= ik + lm + km + mm$$

We are led to the same value if we apply the same considerations to the values of $1 + \gamma$.

18.

From this double expression of the same multitude we obtain the equation:

$$0 = hm + ii + kl - ik - km - mm$$

and hence, eliminating h with the aid of the equation $h = 2m - k - 1$,

$$0 = (k-m)^2 + ii + kl - ik - kk - m$$

But the last two equations of article 16 yield $k = \frac{1}{2}(l+i)$, and substituting this value for k, $ii + kl - ik - kk$ becomes $\frac{1}{4}(l-i)^2$. Therefore the preceding equation, after multiplying by 4, becomes

$$0 = 4(k-m)^2 + (l-i)^2 - 4m$$

Hence, because $4m = 2(k+m) - 2(k-m) = 2n - 2(k-m)$, it follows that

$$2n = 4(k-m)^2 + 2(k-m) + (l-i)^2$$

or

$$8n + 1 = (4(k-m)+1)^2 + 4(l-i)^2$$

Therefore, setting

$$4(k-m) + 1 = a, \quad 2l - 2i = b$$

we find that

$$p = aa + bb$$

However, it is clear that there is a unique way to decompose p as a sum of two squares, if one of them must be odd and denoted by aa, and the other is required to be even and denoted by bb, so that aa and bb are uniquely determined. Also, a itself will be a completely determined number; for the square root must be taken as positive or negative, depending on whether the positive root is of the form $4M+1$ or $4M+3$. We will soon discuss the determination of the sign of b.

Now combining these new equations with the last three from article 16, the five numbers h, i, k, l, m are completely determined by a, b, and n in the following way:

$$8h = 4n - 3a - 5$$
$$8i = 4n + a - 2b - 1$$
$$8k = 4n + a - 1$$
$$8l = 4n + a + 2b - 1$$
$$8m = 4n - a + 1$$

If these are expressed in terms of the modulus p rather than n, then the diagram S, with each term multiplied by 16 to avoid fractions, is as follows:

$p-6a-11$	$p+2a-4b-3$	$p+2a-3$	$p+2a+4b-3$
$p+2a-4b-3$	$p+2a+4b-3$	$p-2a+1$	$p-2a+1$
$p+2a-3$	$p-2a+1$	$p+2a-3$	$p-2a+1$
$p+2a+4b-3$	$p-2a+1$	$p-2a+1$	$p+2a-4b-3$

19.

It remains for us to explain how to assign the correct sign to b. Already in article 10 above we have pointed out that the distinction between the sets B and D is not essential in itself, but rather depends on the choice of a number f, for which one of the roots of the congruence $xx \equiv -1$ must be taken, and they are interchanged with each other if one of the roots is adopted instead of the other. Now, since an inspection of the diagram just presented shows that changing the sign of b results in a similar permutation, it may be foreseen that there must be a connection between the sign of b and the number f. In order to understand this, we first of all observe that if μ is a non-negative integer, and z runs through all the values 1, 2, $3 \ldots p-1$, then either $\Sigma z^\mu \equiv -1$ modulo p (if μ is not divisible by $p-1$) or $\Sigma z^\mu \equiv 0$ (if μ is divisible by $p-1$). The latter part of the theorem is clear from the fact that if μ is divisible by $p-1$, then we have $z^\mu \equiv 1$. The former part can be demonstrated as follows. Letting g be a primitive root, all the values of z agree with the minimal residues of all g^y, where we take for y all the numbers 0, 1, 2, $3 \ldots p-2$ as y. Therefore $\Sigma z^\mu \equiv \Sigma g^{\mu y}$. But

$$\Sigma g^{\mu y} = \tfrac{g^{\mu(p-1)}-1}{g^\mu - 1}, \text{ hence } (g^\mu - 1)\Sigma z^\mu \equiv g^{\mu(p-1)} - 1 \equiv 0$$

Since g^μ cannot be congruent to 1 for values of μ not divisible by $p-1$, i.e. $g^\mu - 1$ cannot be divisible by p, it follows that $\Sigma z^\mu \equiv 0$. Q. E. D.

Now, if the power $(z^4+1)^{\frac{1}{4}(p-1)}$ is expanded using the binomial theorem, then by the preceding lemma, we will have

$$\Sigma(z^4+1)^{\frac{1}{4}(p-1)} \equiv -2 \,(\text{mod. } p)$$

But the minimal residues of all z^4 exhibit all the numbers A, with each occurring four times. Therefore, among the minimal residues of z^4+1,

$$4(00) \text{ belong to } A$$
$$4(01) \text{ belong to } B$$
$$4(02) \text{ belong to } C$$
$$4(03) \text{ belong to } D$$

and four will be $=0$ (in the cases where $z^4 \equiv p-1$). Hence, considering how the complexes A, B, C, D were defined, we deduce

$$\Sigma(z^4+1)^{\frac{1}{4}(p-1)} \equiv 4(00)+4f(01)-4(02)-4f(03)$$

and therefore

$$-2 \equiv 4(00)+4f(01)-4(02)-4f(03)$$

or, substituting for for (00), (01) etc. the values found in the previous section,

$$-2 \equiv -2a-2-2bf$$

Hence we conclude that $a+bf \equiv 0$ must always be satisfied, or, multiplying by f,

$$b \equiv af$$

This congruence serves to determine the sign of b, if the number f has already been chosen, or to determine the number f, if the sign of b is prescribed elsewhere.

20.

Having completely solved our problem for moduli of the form $8n+1$, we proceed to the other case, in which p is of the form $8n+5$: we will be able to complete this more briefly because the reasoning differs little from the previous case.

Whereas for such a modulus, -1 belongs to the class C, the complements with respect to p of the number in the complexes A, B, C, D will be in classes C, D, A, B respectively. Hence it is easily found that

the symbol	denotes the multitude of solutions of the congruence
(00)	$1+\alpha+\gamma\equiv 0$
(01)	$1+\alpha+\delta\equiv 0$
(02)	$1+\alpha+\alpha'\equiv 0$
(03)	$1+\alpha+\beta\equiv 0$
(10)	$1+\beta+\gamma\equiv 0$
(11)	$1+\beta+\delta\equiv 0$
(12)	$1+\beta+\alpha\equiv 0$
(13)	$1+\beta+\beta'\equiv 0$
(20)	$1+\gamma+\gamma'\equiv 0$
(21)	$1+\gamma+\delta\equiv 0$
(22)	$1+\gamma+\alpha\equiv 0$
(23)	$1+\gamma+\beta\equiv 0$
(30)	$1+\delta+\gamma\equiv 0$
(31)	$1+\delta+\delta'\equiv 0$
(32)	$1+\delta+\alpha\equiv 0$
(33)	$1+\delta+\beta\equiv 0$

from which we immediately we have six equations:

$$(00)=(22),\quad (01)=(32),\quad (03)=(12),\quad (10)=(23),\quad (11)=(33),\quad (21)=(30)$$

Multiplying the congruence $1+\alpha+\gamma\equiv 0$ by the number γ' from the complex C such that $\gamma\gamma'\equiv 1$, and taking for γ'' the minimal residue of the product $\alpha\gamma'$, which will evidently also be from the complex C, we obtain $\gamma'+\gamma''+1\equiv 0$, from which we conclude that $(00)=(20)$.

Equations $(01)=(13)$, $(03)=(31)$, $(10)=(11)=(21)$ can be obtained in a completely similar manner.

With the help of these eleven equations, we can reduce our sixteen unknowns to five, and present the diagram S as follows:

$$\begin{array}{cccc} h, & i, & k, & l \\ m, & m, & l, & i \\ h, & m, & h, & m \\ m, & l, & i, & m \end{array}$$

Furthermore, we have the equations

$$(00)+(01)+(02)+(03)=2n+1$$
$$(10)+(11)+(12)+(13)=2n+1$$
$$(20)+(21)+(22)+(23)=2n$$
$$(30)+(31)+(32)+(33)=2n+1$$

or, using the symbols we have just introduced, these three (I):

$$h+i+k+l=2n+1$$
$$2m+i+l=2n+1$$
$$h+m=n$$

with the help of which we may now reduce our unknowns to two.

We will derive the remaining equations by considering the multitude of solutions of the congruence $1+\alpha+\beta+\gamma\equiv 0$,where A, B, C denote indefinite numbers from the complexes A, B, C respectively. Namely, by considering *firstly* $1+\alpha$, we obtain h, i, k, l numbers from A, B, C, D respectively, and for any given value of α we have, in these four cases, m, l, i, m solution respectively. Thus the total number of solutions will be

$$=hm+il+ik+lm$$

Secondly, since $1+\beta$ yields m, m, l, i numbers from the complexes A, B, C, D, and for any *given* value of β, there are h, m, h, m solutions in these four cases, the total number of solutions will be

$$=hm+mm+hl+im$$

from which we derive the equation

$$0=mm+hl+im-il-ik-lm$$

which, with the help of the equation $k=2m-h$ from (I), transforms into this:

$$0=mm+hl+hi-il-im-lm$$

Now, from the equations from (I), we also have $l+i=1+2h$, hence

$$2i=1+2h+(i-l)$$
$$2l=1+2h-(i-l)$$

Substituting these values into the preceding equation, we get:

$$0 = 4mm - 4m - 1 - 8hm + 4hh + (i-l)^2$$

Finally, if we substitute $2(h+m) - 2(h-m)$ for $4m$, or, due to the last equation in (I), $2n - 2(h-m)$, we obtain:

$$0 = 4(h-m)^2 - 2n + 2(h-m) - 1 + (i-l)^2$$

and therefore

$$8n + 5 = (4(h-m)+1)^2 + 4(i-l)^2$$

Setting

$$4(h-m)+1 = a, \quad 2i - 2l = b$$

this becomes

$$p = aa + bb$$

Since in this case too, p can be decomposed into two squares in only one way, with one even and the other odd, aa and bb will be completely determined numbers; for it is evident that a must be the square of an odd number, and b of an even number. Moreover, the *sign* of a must be chosen in such a way that $a \equiv 1 \pmod 4$, and the sign of b must be chosen in such a way that $b \equiv af \pmod p$, as can be proved easily using reasoning similar to that which we employed in the previous article.

The numbers h, i, k, l, m can then be determined from a, b, and n:

$$\begin{aligned} h &= \tfrac{1}{8}(4n + a - 1) \\ i &= \tfrac{1}{8}(4n + a + 2b + 3) \\ k &= \tfrac{1}{8}(4n - 3a + 3) \\ l &= \tfrac{1}{8}(4n + a - 2b + 3) \\ m &= \tfrac{1}{8}(4n - a + 1) \end{aligned}$$

or if we prefer expressions in terms of p, the diagram S, with each term multiplied by 16, will be as follows:

$p+2a-7$	$p+2a+4b+1$	$p-6a+1$	$p+2a-4b+1$
$p-2a-3$	$p-2a-3$	$p+2a-4b+1$	$p+2a+4b+1$
$p+2a-7$	$p-2a-3$	$p+2a-7$	$p-2a-3$
$p-2a-3$	$p+2a-4b+1$	$p+2a+4b+1$	$p-2a-3$

21

Having solved our problem, we return to the main discussion. We will now completely determine the complex to which the number 2 belongs.

I. Whenever p is of the form $8n+1$, it is already established that the number 2 either belongs to the complex A or to the complex C. In the former case, it is easily seen that the numbers $\frac{1}{2}(p-1)$ and $\frac{1}{2}(p+1)$ also belong to A, and in the latter case, they belong to C. Now consider that if α and $\alpha+1$ are consecutive numbers in the complex A, then $p-\alpha-1$ and $p-\alpha$ are also two such numbers, or, which is the same, numbers of the complex A that are followed by a number from the same complex, always come in associated pairs, (α and $p-1-\alpha$). Therefore, the multitude of such numbers, (00), will always be even, unless a number exists which is associated with itself, i.e. unless $\frac{1}{2}(p-1)$ belongs to A, in which case (00) will be odd. Hence we conclude that (00) is odd whenever 2 belongs to the complex A, and even whenever 2 belongs to C. But we have

$$16(00) = aa + bb - 6a - 11$$

or setting $a = 4q+1$, $b = 4r$ (see article 14),

$$(00) = qq - q + rr - 1$$

Therefore, since $qq-q$ is clearly always even, (00) will be odd or even, according as r is even or odd. Therefore, 2 will belong to A or C depending on whether b is of the form $8m$ or $8m+4$, which is the very theorem that was found by induction in article 14.

II. We may also complete the other case, where p is of the form $8n+5$. The number 2 here belongs to either B or D, and it is easily seen that in the former case $\frac{1}{2}(p-1)$ belongs to B and $\frac{1}{2}(p+1)$ belongs to D, and in the latter case $\frac{1}{2}(p-1)$ belongs to D and $\frac{1}{2}(p+1)$ belongs to B. Now consider that if β is a number in B that is followed by a number in D, then the number $p-\beta-1$ will also be in B and $p-\beta$ will be in D, i.e. numbers with this property are always present in associated pairs. Their multitude, (13), will therefore be even, except in the case when a number is associated with itself, i.e. when $\frac{1}{2}(p-1)$ belongs to B and $\frac{1}{2}(p+1)$ to D; then of course (13) will be odd. Hence we conclude that (13) is even whenever 2 belongs to D, and odd whenever 2 belongs to B. But we have

$$16(13) = aa + bb + 2a + 4b + 1$$

or, setting $a = 4q+1$, $b = 4r+2$,

$$(13) = qq + q + rr + 2r + 1$$

Therefore, (13) will be odd whenever r is even; and on the other hand, (13) will be even whenever r is odd. From this we conclude that 2 belongs to B whenever b is of the form $8m+2$, and to D whenever b is of the form $8m+6$.

The conclusion of these investigations can be stated as follows:

The number 2 belongs to the set A, B, C, or D, according to whether the number $\frac{1}{2}b$ is of the form $4m$, $4m+1$, $4m+2$, or $4m+3$.

22.

In *Disquisitiones Arithmeticae* we explained the general theory of the division of the circle, and the solution of the equation $x^p - 1 = 0$, and among other things, we showed that if μ is a divisor of the number $p-1$, then the function $\frac{x^p-1}{x-1}$ can be resolved into μ factors of order $\frac{p-1}{\mu}$, with the help of an auxiliary equation of order μ. In addition to the general theory of this resolution, we separately considered special cases where $\mu = 2$ or $\mu = 3$ in articles 356-358 of that work, and we showed how to assign the auxiliary equation a priori, i.e. without finding the minimal residue of a primitive root modulo p. Now, even without a reminder, attentive readers will easily perceive a close connection between the next simplest case of this theory, namely $\mu = 4$, with the investigations explained here in articles 15-20. Indeed, with the help of the former, the latter can also be completed without much difficulty. But we reserve this treatment for another occasion, and therefore in the present commentary, we preferred to complete the discussion using purely arithmetic methods, without mixing in the theory of the equation $x^p - 1 = 0$. Rather, in the conclusion of this work, we will add some new and purely arithmetic theorems, closely connected the subject which has been treated so far.

23.

If the power $(x^4+1)^{\frac{1}{2}(p-1)}$ is expanded using the binomial theorem, there will be three terms in which the exponent of x is divisible by $p-1$, namely

$$x^{2(p-1)}, Px^{p-1} \text{ and } 1$$

where P denotes the middle coefficient

$$\frac{\frac{1}{2}(p-1)\cdot\frac{1}{2}(p-3)\cdot\frac{1}{2}(p-5)\ldots\frac{1}{2}(p+3)}{1\cdot 2\cdot 3\ldots\frac{1}{4}(p-1)}$$

Therefore, substituting the numbers 1, 2, $3 \ldots p-1$ in turn for x, we obtain by the lemma of article 19,

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv -2-P$$

But considering what we explained in article 19, namely that the numbers of the complexes A, B, C, D, when raised to the $\frac{1}{2}(p-1)^{th}$ power, are congruent modulo p to the numbers $+1$, -1, $+1$, -1 respectively, it is easy to see that

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv 4(00)-4(01)+4(02)-4(03)$$

and therefore, according to the diagrams given at the ends of articles 18 and 20, we have

$$\Sigma(x^4+1)^{\frac{1}{2}(p-1)} \equiv -2a-2$$

Comparing these two values yields a most elegant theorem: namely, we have

$$P \equiv 2a \pmod{p}$$

Denoting the four products

$$1\cdot 2\cdot 3\ldots\tfrac{1}{4}(p-1)$$
$$\tfrac{1}{4}(p+3)\cdot\tfrac{1}{4}(p+7)\cdot\tfrac{1}{4}(p+11)\ldots\tfrac{1}{2}(p-1)$$
$$\tfrac{1}{2}(p+1)\cdot\tfrac{1}{2}(p+3)\cdot\tfrac{1}{2}(p+5)\ldots\tfrac{3}{4}(p-1)$$
$$\tfrac{1}{4}(3p+1)\cdot\tfrac{1}{4}(3p+5)\cdot\tfrac{1}{4}(3p+9)\ldots(p-1)$$

by q, r, s, t respectively, the preceding theorem can be presented as follows:

$$2a \equiv \frac{r}{q} \pmod{p}$$

Since each factor of q has its complement with respect to p in t, we have $q \equiv t \pmod{p}$ whenever the multiplicity of factors is even, i.e. whenever p is of the form $8n+1$. On the other hand, $q \equiv -t \pmod{p}$ whenever the multiplicity of factors is odd, or p is of the form $8n+5$. Similarly, in the former case we will have $r \equiv s$, and in the latter case $r \equiv -s$. In both cases we will have, $qr \equiv st$, and because it is clear that $qrst \equiv -1$, we will also have $qqrr \equiv -1$, and consequently $qr \equiv \pm f \pmod{p}$.

Combining this congruence with the theorem just found, we obtain $rr \equiv \pm 2af$, and therefore, by articles 19 and 20,

$$2b \equiv \pm rr \text{ (mod. } p)^3$$

It is very remarkable that the decomposition of the number p into two squares can be found by completely direct operations; namely, the square root of the odd square will be the absolutely minimal residue of $\frac{r}{2q}$ modulo p, and the square root of the even square will be the absolutely minimal residue of $\frac{1}{2}rr$ modulo p. The expression $\frac{r}{2q}$, which becomes $= 1$ for $p = 5$, ican be presented for larger values of p as follows:

$$\frac{6 \cdot 10 \cdot 14 \cdot 18 \ldots (p-3)}{2 \cdot 3 \cdot 4 \cdot 5 \ldots \frac{1}{4}(p-1)}$$

But since we furthermore know by which sign this formula for the square root of an odd number is affected, namely, so that it always takes the form $4m+1$, it is highly noteworthy that a similar general criterion with respect to the sign of the square root of the even number has not yet been found. If anyone finds it and communicates it to us, they will do us a great favor. Meanwhile, it seems appropriate to include here the values of the numbers a, b, f, which produce the minimal residues of the expressions $\frac{r}{2q}$, $\frac{1}{2}rr$, qr, for all values of p less than 200.

[3] and $\{(a \mp b)q\}^2 \equiv a \equiv (\frac{r - qrr}{2})^2$

p	a	b	f
5	+1	+2	2
13	+3	−2	5
17	+1	−4	13
29	+5	+2	12
37	+1	−6	31
41	+5	+4	9
53	−7	−2	23
61	+5	−6	11
73	−3	−8	27
89	+5	−8	34
97	+9	+4	22
101	+1	−10	91
109	−3	+10	33
113	−7	+8	15
137	−11	+4	37
149	−7	−10	44
157	−11	−6	129
173	+13	+2	80
181	+9	+10	162
193	−7	+12	81
197	+1	−14	183

THE THEORY OF
BIQUADRATIC RESIDUES

SECOND COMMENTARY

A U T H O R

CARL FRIEDRICH GAUSS

DELIVERED TO THE ROYAL SOCIETY 1831, APR. 15.

Commentationes societatis regiae scientiarum Gottingensis recentiores. Vol. VII.
Göttingen 1832.

THE THEORY OF BIQUADRATIC RESIDUES.

SECOND COMMENTARY

24.

In the first commentary, that which is required for the biquadratic character of the number $+2$ was completely determined. Specifically, if we conceive of all numbers that are not divisible by the modulus p (which is assumed to be a prime number of the form $4n+1$) as being distributed amongst four complexes A, B, C, D according to whether they become congruent to $+1$, $+f$, -1, $-f$ modulo p when raised to the $\frac{1}{4}(p-1)^{th}$ power, where f denotes one of the roots of the congruence $ff \equiv -1 \pmod{p}$, then we find that the complex to which the number $+2$ should be assigned depends on the resolution of the number p into two squares. Namely, if $p = aa + bb$, with aa being an odd square, and bb being an even square, and assuming that the signs of a, b are taken in such a way that we have $a \equiv 1 \pmod{4}$, $b \equiv af \pmod{p}$, then the number $+2$ will belong to the complex A, B, C, D according to whether $\frac{1}{2}b$ is of the form $4n$, $4n+1$, $4n+2$, $4n+3$ resp.

The rule governing the classification of the number -2 also naturally arises in this way. Specifically, since -1 belongs to the class A for even values of $\frac{1}{2}b$, and to class C for odd values, it follows from the theorem of article 7 that the number -2 will belong to the complex A, B, C, D according to whether $\frac{1}{2}b$ is of the form $4n$, $4n+3$, $4n+2$, $4n+1$ resp.

The above theorems can also be expressed as follows:

The number	$+2$	-2
belongs to the complex	if b is congruent,	modulo 8, to
A	0	0
B	$2a$	$6a$
C	$4a$	$4a$
D	$6a$	$2a$

It is easily understood that the theorems thus stated no longer depend on the condition $a \equiv 1 \pmod 4$, but still hold if $a \equiv 3 \pmod 4$, provided that the other condition, $af \equiv b \pmod p$, is preserved.

It can be easily seen that all of these theorems can be elegantly condensed into a single formula, namely:

if a and b are assumed to be positive, then we always have

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

25.

Let us now see to what extent induction reveals the classification of the number 3. The table in article 11, continued further (and always adopting the minimum primitive root), shows that $+3$ belongs

to the complex

A, for			B, for			C, for			D, for		
p	a	b	p	a	b	p	a	b	p	a	b
13	-3	$+2$	17	$+1$	-4	37	$+1$	-6	5	$+1$	$+2$
109	-3	$+10$	29	$+5$	$+2$	61	$+5$	-6	41	$+5$	-4
181	$+9$	$+10$	53	-7	$+2$	73	-3	-8	149	-7	$+10$
193	-7	-12	89	$+5$	-8	97	$+9$	$+4$	173	$+13$	$+2$
229	-15	$+2$	101	$+1$	$+10$	157	-11	-6			
277	$+9$	$+14$	113	-7	-8	241	-15	-4			
			137	-11	-4						
			197	$+1$	-14						
			233	$+13$	$+8$						
			257	$+1$	-16						
			269	$+13$	$+10$						
			281	$+5$	$+16$						
			293	$+17$	$+2$						

At first glance, we do not observe a simple connection between the values of the numbers a, b that correspond to the same complex. However, if we consider that a similar question in the theory of quadratic residues can be resolved by a simpler rule for the number -3 than for the number $+3$, there is hope for an equally successful outcome in the theory of biquadratic residues. Indeed, 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	$+13$	$+10$
293	$+17$	$+2$

from which the inductive rule presents itself spontaneously. Namely, -3 belongs to the complex

A, whenever b is divisible by 3, or $b \equiv 0 \pmod 3$
B, whenever $a+b$ is divisible by 3, or $b \equiv 2a \pmod 3$
C, whenever a is divisible by 3, or $a \equiv 0 \pmod 3$
D, whenever $a-b$ is divisible by 3, or $b \equiv a \pmod 3$

26.

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 $p = 37,\ 53,\ 113,\ 137,\ 173,\ 257$

Upon consideration of the values of the numbers a, b corresponding to each p, the law here is just as easily grasped as it is for the classification of the number -3. Specifically, $+5$ belongs to the complex

A, whenever $b \equiv 0 \pmod 5$
B, whenever $b \equiv a$
C, whenever $a \equiv 0$
D, whenever $b \equiv 4a$

It is clear that these rules encompass all cases, since for $b \equiv 2a$ or $b \equiv 3a \pmod 5$, we would have $aa + bb \equiv 0$, Q.E.A., since by hypothesis p is a prime number different from 5.

27.

Applying induction in the same way to the numbers -7, -11, $+13$, $+17$, -19, -23 yields the following rules:

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 $b \equiv 3a$

For the number -11.

A	$b \equiv 0,\ 5a$, or $6a \pmod{11}$
B	$b \equiv a,\ 3a$ or $4a$
C	$a \equiv 0$, or $b \equiv 2a$ or $9a$
D	$b \equiv 7a,\ 8a$ or $10a$

For the number $+13$.

A	$b \equiv 0,\ 4a,\ 9a \pmod{13}$
B	$b \equiv 6a,\ 11a,\ 12a$
C	$a \equiv 0;\ b \equiv 3a,\ 10a$
D	$b \equiv a,\ 2a,\ 7a$

For the number $+17$.

A	$a \equiv 0;\ b \equiv 0,\ a,\ 16a \pmod{17}$
B	$b \equiv 2a,\ 6a,\ 8a,\ 14a$
C	$b \equiv 5a,\ 7a,\ 10a,\ 12a$
D	$b \equiv 3a,\ 9a,\ 11a,\ 15a$

For the number -19.

A	$b \equiv 0,\ 2a,\ 5a,\ 14a,\ 17a \pmod{19}$
B	$b \equiv 3a,\ 7a,\ 11a,\ 13a,\ 18a$
C	$a \equiv 0;\ b \equiv 4a,\ 9a,\ 10a,\ 15a$
D	$b \equiv a,\ 6a,\ 8a,\ 12a,\ 16a$

For the number -23.

A	$a \equiv 0;\ b \equiv 0,\ 7a,\ 10a,\ 13a,\ 16a \pmod{23}$
B	$b \equiv 2a,\ 3a,\ 4a,\ 11a,\ 15a,\ 17a$
C	$b \equiv a,\ 5a,\ 9a,\ 14a,\ 18a,\ 22a$
D	$b \equiv 6a,\ 8a,\ 12a,\ 19a,\ 20a,\ 21a$

28.

The special theorems found in this way are found confirmed, as long one continues, and they reveal criteria of the most beautiful form. If they are compared with each other, so that general conclusions may be derived from them, the following observations immediately present themselves at first sight.

The criteria for deciding to which complex number a given prime number $\pm q$ should be referred (where the sign is taken positively or negatively, depending on whether q is of the form $4n+1$ or $4n+3$), depend on the forms of the numbers a, b modulo q. Specifically,

I. When $a \equiv 0 \pmod{q}$, $\pm q$ belongs to a specific complex, which is A for $q = 7,\ 17,\ 23$, and C for $q = 3,\ 11,\ 13,\ 19$. From this arises the conjecture that the former case generally holds whenever q is of the form $8n \pm 1$, and the latter holds whenever q is of the form $8n \pm 3$. Moreover, the complexes B and D can already be excluded without induction when a is divisible by q, as we then have $p \equiv bb \pmod{q}$, i.e. p is a quadratic residue modulo q, and hence by the fundamental theorem, $\pm q$ must be a quadratic residue modulo p.

II. When a is not divisible by q, the criterion depends on the value of the expression $\frac{b}{a} \pmod{q}$. This expression indeed admits different values of q, namely $0,\ 1,\ 2,\ 3 \ldots q-1$, but whenever q is of the form $4n+1$, we must exclude the two values of the expression $\sqrt{-1} \pmod{q}$, which obviously cannot be values of the expression

$\frac{b}{a} \pmod{q}$, since $p = aa + bb$ is always assumed to be a prime number different from q. Therefore, the number of admissible values of the expression $\frac{b}{a} \pmod{q}$ is $= q-2$ for $q \equiv 1 \pmod{4}$, while it remains $= q$ for $q \equiv 3 \pmod{4}$.

We can now distribute these values into four classes, so that some, denoted indefinitely by α, correspond to the complex A; others, denoted by β, correspond to the complex B; others γ correspond to the complex C; and finally the remaining δ correspond to the complex D. We do this in such a way that $\pm q$ belongs to the complex A, B, C, or D depending on whether $b \equiv \alpha a$, $b \equiv \beta a$, $b \equiv \gamma a$, or $c \equiv \delta a \pmod{q}$.

The *law* of this distribution seems more abstruse than it actually is, although some general observations can be made promptly. Three of the classes have the same multitude, namely $\frac{1}{4}(q-1)$ or $\frac{1}{4}(q+1)$, while for the fourth (the one corresponding to the criterion $a \equiv 0$), the number is one less, so that the number of different criteria corresponding to each complex is the same, namely $\frac{1}{4}(q-1)$ or $\frac{1}{4}(q+1)$. Furthermore, we note that 0 is always found in the first class (among α), and that the complements of the numbers α, β, γ, δ to q, i.e. $q-\alpha$, $q-\beta$, $q-\gamma$, $q-\delta$ correspond to the first, fourth, third, second class, respectively. Finally, we see that the values of the expressions $\frac{1}{a}$, $\frac{1}{\beta}$, $\frac{1}{\gamma}$, $\frac{1}{\delta} \pmod{q}$ belong to the first, fourth, third, second class, whenever the criterion $a \equiv 0$ corresponds to the complex A; and to the third, second, first, fourth class, whenever the criterion $a \equiv 0$ is referred to the complex C. But these are almost all the observations that can be reached by induction, unless we presumptuously dare to anticipate those which will be derived below from genuine sources.

29.

Before we proceed further, it is worth noting that the criteria for prime numbers (taken positively if they are of the form $4n+1$, and negatively if they are of the form $4n+3$) suffice for the determination of all other numbers, provided that the theorem of article 7 and the criteria for -1 and ± 2 are called upon to assist. Thus, for example, if criteria for the number $+3$ is desired, then the criteria stated in article 25, which refer to -3, will still apply for $+3$ whenever $\frac{1}{2}b$ is an even number; on the other hand, the complexes A, B, C, D should be interchanged with the complexes C, D, A, B whenever $\frac{1}{2}b$ is odd. From this, the following criteria can be obtained:

	$+3$ belongs
to the complex	if
A	$b \equiv 0 \pmod{12}$; or simultaneously $a \equiv 0 \pmod{3}, b \equiv 2 \pmod{4}$
B	$b \equiv 8a$ or $10a \pmod{12}$
C	$b \equiv 6a \pmod{12}$; or simultaneously $a \equiv 0 \pmod{3}, b \equiv 0 \pmod{4}$
D	$b \equiv 2a$ or $4a \pmod{12}$

Similarly, the criteria for ± 6 can be found by combining the criteria for ∓ 2 and -3; specifically,

	$+6$ belongs
to the complex	if
A	$b \equiv 0, \quad 2a, 22a \pmod{24}$; or simultaneously $a \equiv 0 \pmod{3}, b \equiv 4a \pmod{8}$
B	$b \equiv 4a, \quad 6a, \ 8a \pmod{24}$; or simultaneously $a \equiv 0 \pmod{3}, b \equiv 2a \pmod{8}$
C	$b \equiv 10a, 12a, 14a \pmod{24}$; or simultaneously $a \equiv 0 \pmod{3}, b \equiv 0 \pmod{8}$
D	$b \equiv 16a, 18a, 20a \pmod{24}$; or simultaneously $a \equiv 0 \pmod{3}, b \equiv 6a \pmod{8}$

	-6 belongs
to the complex	if
A	$b \equiv 0, \ 10a, 14a \pmod{24}$; or simultaneously $a \equiv 0 \pmod{3}, b \equiv 4a \pmod{8}$
B	$b \equiv 4a, \ 8a, 18a \pmod{24}$; or simultaneously $a \equiv 0 \pmod{3}, b \equiv 6a \pmod{8}$
C	$b \equiv 2a, 12a, 22a \pmod{24}$; or simultaneously $a \equiv 0 \pmod{3}, b \equiv 0 \pmod{8}$
D	$b \equiv 6a, 16a, 20a \pmod{24}$; or simultaneously $a \equiv 0 \pmod{3}, b \equiv 2a \pmod{8}$

In a similar way, the criteria for the number $+21$ can be put together from the criteria for -3 and -7; the criteria for -105 from the criteria for -1, -3, $+5$, -7, etc.

30.

Induction therefore opens up a very abundant harvest of special theorems, similar for the theorem for the number 2. However, a common link and rigorous demonstrations are desired, since the method by which we classified the number 2 in the first commentary does not allow further application. Now, there are various methods by which it would be possible to obtain demonstrations for particular cases, especially those which concern the distribution of quadratic residues among the complex A, C. However, we do not linger with these, since the theory should encompass *all* cases in general. When we started dedicating our thoughts to this

matter in 1805, we soon became aware that the genuine source of the general theory was to be sought in the field of arithmetic, as we already mentioned in article 1.

Whereas higher arithmetic, in the questions hitherto treated, concerns only real integral numbers, so the theorems about biquadratic residues shine forth in the highest simplicity and genuine beauty only when the field of arithmetic is extended to imaginary quantities, so that, without restriction, the object of study consists of numbers of the form $a+bi$, where i denotes the usual imaginary quantity $\sqrt{-1}$, and a, b indefinitely denote all real integral numbers between $-\infty$ and $+\infty$. We shall call such numbers *complex integral numbers*, so that they are not opposed to real complex numbers, but are rather considered to be contained among these as a species. The present essay will present both the elementary doctrine of complex numbers and the initial elements of the theory of biquadratic residues, which we will undertake to render perfect in every respect in the subsequent continuation[4].

31.

In the interest of brevity and clarity, we first introduce some notation.

The field of complex numbers $a+bi$ contains

I. real numbers, where $b=0$, and, among these, depending on the nature of a,

1) zero

2) positive numbers

3) negative numbers

II. imaginary numbers, where b is a non-zero number. Here again we distinguish

1) purely imaginary numbers, i.e. those for which $a=0$

2) imaginary numbers with a real part, for which neither b nor a equals 0.

If you like, the former can be called pure imaginary numbers, the latter can be called mixed imaginary numbers.

[4]It is appropriate to note here that the field defined in this manner is adapted primarily to the theory of biquadratic residues. The theory of cubic residues can be built in a similar way by considering numbers of the form $a+bh$, where h is an imaginary root of the equation $h^3-1=0$, for instance $h=-\frac{1}{2}+\sqrt{\frac{3}{4}}\cdot i$. Similarly, the theory of residues of higher powers will require the introduction of other imaginary quantities.

We use four units in this theory, $+1$, -1, $+i$, $-i$, which are positive, negative, positive imaginary, and negative imaginary.

We will call the products of any complex number by -1, $+i$, $-i$ its *associates* or *numbers associated with it.* Except for the number zero (which is its own associate), there are always four *unequal* associates of any number.

On the other hand, we call a complex number *conjugate* if it arises from a permutation of i with $-i$. Therefore, among imaginary numbers, any two unequal numbers are always conjugate, while real numbers are conjugate to themselves, if it is pleasing to extend the denomination to them.

The product of a complex number with its conjugate is called the *norm* of that number. So, the norm of a real number is the same as its square.

In general, we have eight related numbers,

$$\begin{array}{r|l} a+bi & a-bi \\ -b+ai & -b-ai \\ -a-bi & -a+bi \\ b-ai & b+ai \end{array}$$

in which we see two quartets of associated numbers, four pairs of conjugates, and the common norm of all is $aa+bb$. However, these eight numbers are reduced to four unequal numbers when $a=\pm b$, or when one of the numbers a, $b=0$.

The following are immediate consequences of the given definitions:

The conjugate of a product of two complex numbers is the product of the conjugates of those numbers.

The same holds for products with several factors, as well as for quotients.

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

This theorem also extends to products with any number of factors and to quotients.

The norm of any complex number (except for zero, which is usually tacitly understood from now on) is a *positive* number.

There is nothing preventing our definitions from extending to fractional or even irrational values of a, b; but $a+bi$ is only called an integer complex number when *both* a, b are integers, and it is only rational when *both* a, b are rational.

32.

The algorithms for arithmetic operations on complex numbers are commonly known: division, through the introduction of the norm, is reduced to multiplication, since we have

$$\frac{a+bi}{c+di} = (a+bi)\cdot\frac{c-di}{cc+dd} = \frac{ac+bd}{cc+dd} + \frac{bc-ad}{cc+dd}\cdot i$$

Extraction of square roots is accomplished with the help of the formula

$$\sqrt{(a+bi)} = \pm(\sqrt{\frac{\sqrt{(aa+bb)}+a}{2}} + i\sqrt{\frac{\sqrt{(aa+bb)}-a}{2}})$$

if b is a positive number, or with this

$$\sqrt{(a+bi)} = \pm(\sqrt{\frac{\sqrt{(aa+bb)}+a}{2}} - i\sqrt{\frac{\sqrt{(aa+bb)}-a}{2}})$$

if b is a negative number. It is not necessary to dwell here on the use of the transformation of the complex quantity $a+bi$ into $r(\cos\varphi + i\sin\varphi)$ for the purpose of facilitating calculations.

33.

We call a complex integer which can be resolved into two factors which are not units[5], a composite complex number; conversely, a complex number is said to be prime if it admits no such resolution. From this it immediately follows that any composite real number also is a composite complex number. But a prime real number could be a composite complex number, and indeed this holds for the number 2 and for all positive real prime numbers of the form $4n+1$ (except for the number 1), since it is known that they can be decomposed into two positive squares; namely, $2 = (1+i)(1-i)$, $5 = (1+2i)(1-2i)$, $13 = (3+2i)(3-2i)$, $17 = (1+4i)(1-4i)$, etc.

On the other hand, positive real prime numbers of the form $4n+3$ are always prime complex numbers. For if such a number q were $= (a+bi)(\alpha+\beta i)$, it would also be $= (a-bi)(\alpha-\beta i)$, and therefore $qq = (aa+bb)(\alpha\alpha+\beta\beta)$. But qq can only be resolved into positive factors greater than unity in a single way, namely as $q\times q$, from which it would follow that $q = aa+bb = \alpha\alpha+\beta\beta$, Q.E.D.; since a sum of two squares cannot be of the form $4n+3$.

[5]or equivalently, whose norms are greater than unity.

Real negative numbers are classified as prime or composite in the same way as positive numbers, and the same holds for pure imaginary numbers.

Thus it remains for us to explain how to distinguish between prime and composite mixed imaginary numbers, as can be done by the following

THEOREM. *A mixed imaginary integer $a+bi$ is either a complex prime number or a composite number, depending on whether its norm is a prime or a composite real number.*

Proof. I. Since the norm of composite complex numbers is always a composite number, it is clear that a complex number whose norm is a prime real number must necessarily be a complex prime number. Q. E. P.

II. If the norm $aa+bb$ is a composite number, let p be a positive real prime number that divides it. There are now two distinct cases to consider.

1) If p is of the form $4n+3$, it is clear that $aa+bb$ cannot be divisible by p unless p also divides a and b, so $a+bi$ will be a composite number.

2) If p is not of the form $4n+3$, it can definitely be decomposed into two squares: so let us assume that $p=\alpha\alpha+\beta\beta$. Since we have

$$(a\alpha+b\beta)(a\alpha-b\beta)=aa(\alpha\alpha+\beta\beta)-\beta\beta(aa+bb)$$

it is divisible by p, and thus it must divide either the factor $a\alpha+b\beta$ or the factor $a\alpha-b\beta$. In addition, since

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

and so is divisible by pp, it is clear that in the first case $b\alpha-a\beta$ must also be divisible by p, while in the latter case $b\alpha+a\beta$ must also be divisible by p. Therefore, in the first case

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

will be a complex integer, and in the latter case

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

will be an integer. Therefore, since the given number is divisible either by $\alpha+\beta i$ or by $\alpha-\beta i$, and since the norm of the quotient $=\frac{aa+bb}{p}$ is different from unity by the hypothesis, it is clear that $a+bi$ is a composite complex number in both cases. Q. E. S.

34.

Therefore, the entire set of prime numbers can be exhausted by the following four species:

1) the four units, 1, $+i$, -1, $-i$, which, however, we will usually understand to be excluded when discussing prime numbers.

2) the number $1+i$ with its three associates $-1+i$, $-1-i$, $1-i$.

3) positive real prime numbers of the form $4n+3$ along with their three associates.

4) complex numbers, the norms of which are real prime numbers of the form $4n+1$ greater than unity, and indeed for any given norm there will always be exactly eight such prime complex numbers, since a norm of this kind can be decomposed into only two squares in a unique way.

35.

Just as the integers are distributed into evens and odds, and the evens are further divided into evenly even and oddly even, so too does an equally essential distinction present itself among complex numbers: namely,

either they are not divisible by $1+i$, which is the case for numbers $a+bi$ such that one of a, b is odd and the other is even;

or they are divisible by $1+i$ but not by 2, whenever both a, b are odd;

or they are divisible by 2, whenever both a, b are even.

For convenience, the numbers of the first class can be called odd complex numbers, those of the second semi-even, and those of the third even.

The product of multiple complex factors will always be odd, provided all factors are odd; semi-even, whenever one factor is semi-even and the rest are odd; and even, whenever among the factors, either two are semi-even, or at least one is even.

The norm of any odd complex number is of the form $4n+1$; the norm of a semi-even number is of the form $8n+2$; and finally, the norm of an even number is the product of a number of the form $4n+1$ and a power of two which is greater than or equal to 4.

36.

Since the connection between four associated complex numbers is analogous to the connection between two opposite real numbers (i.e. they are absolutely equally and affected by opposite signs), and among these, the positive number is usually considered as the primary one, the question arises whether a similar distinction

can be established for four associated complex numbers, and whether it should be considered useful. In order to decide this, we must consider that the principle of distinction should be such that the product of two numbers, which are considered as primary among their associates, always becomes a primary number among their associates. But we are soon assured that such a principle does not exist at all unless the distinction is restricted to integers: so much so that the only *useful* distinction should be limited to odd numbers. For these purposes, the proposed goal can be achieved in two ways. Namely,

I. Given two numbers $a+bi$, $a'+b'i$ such that a, a' are of the form $4n+1$, and b, b' are even, their product will enjoy the same property, that the real part is $\equiv 1 \pmod 4$, and the imaginary part is even. And it can be easily seen that among four odd associates, only one is of that form.

II. Given a number $a+bi$ such that $a-1$ and b are either both even or both odd, then its product with a complex number of the same form will be of the same form, and it is easily seen that among four odd associates, only one is of this form.

From these two almost equally suitable principles, we will adopt the latter, namely that among four odd associated complex numbers, the one which is congruent to the positive unit modulo $2+2i$ will be considered to be primary. In this way, it will be possible to state several important theorems with greater concision. Thus, the primary complex prime numbers are $-1+2i$, $-1-2i$, $+3+2i$, $+3-2i$, $+1+4i$, $+1-4i$, etc., and also the real numbers -3, -7, -11, -19, etc., which are always explicitly marked with a negative sign. The conjugate of a primary odd complex number will always be primary.

For semi-even and even numbers in general, a similar distinction would be too arbitrary and of little use. From the associated prime numbers $1+i$, $1-i$, $-1+i$, $-1-i$, we can indeed choose one as primary over the others, but we will not extend such a distinction to composite numbers.

37.

If among the factors of a complex composite number, numbers are found which are themselves composite, and these again are resolved into their factors, it is clear that we will eventually descend to prime factors, i.e., any composite number is resolvable into prime factors. If any non-primary numbers are found, substitute in

place of each of them the product of the primary associate by i, -1 or $-i$. In this way, it is clear that any composite complex number M can be reduced to the form

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

such that A, B, C etc. are distinct primary complex prime numbers, and $\mu = 0$, 1, 2 or 3. Concerning such resolutions, a theorem presents itself, that it can only be done in one way. This theorem might appear obvious in passing, but it certainly requires a demonstration. To which the following lays out a path

THEOREM. *A product $M = A^{\alpha} B^{\beta} C^{\gamma} \dots$, where A, B, C are distinct primary complex prime numbers, cannot be divisible by any primary complex prime number, which is not found among A, B, C, etc.*

Proof. Let P be a primary complex prime number not contained among A, B, C, etc., and let p, a, b, c, etc. be the norms of the numbers P, A, B, C, etc. It is easily seen that the norm of the number M is $= a^{\alpha} b^{\beta} c^{\gamma}$ etc., from which it follows that if M were divisible by P, then its norm would be divisible by p. Since the norms are either real prime numbers (from the sequence 2, 5, 13, 17 etc.), or squares of real prime numbers (from the sequence 9, 49, 121 etc.), it is clear that this cannot occur, unless p is identical to some norm a, b, c, etc.: we thus suppose $p = a$. But since P and A are assumed to be distinct primary complex prime numbers, it is easy to see that these cannot simultaneously hold, unless P and A are imaginary complex numbers, and therefore $p = a$ is an odd real prime number (not the square of a prime number). We therefore set $A = k + li$, $P = k - li$. It follows (by extending the concept and sign of congruence to complex integers) that we have $A \equiv 2k \pmod{P}$, from which it is easily deduced that

$$M \equiv 2^{\alpha} k^{\alpha} B^{\beta} C^{\gamma} \dots \pmod{P}$$

Therefore, while M is supposed to be divisible by P,

$$2^{\alpha} k^{\alpha} B^{\beta} C^{\gamma} \dots$$

will also be divisible by P, and hence the norm of this number,

$$= 2^{2\alpha} k^{2\alpha} b^{\beta} c^{\gamma} \dots$$

will be divisible by p. But since 2 and k are not divisible by p, it follows that p

must be identical to some of the numbers b, c, etc.: let's say $p = b$. From this, we conclude that either $B = k + li$, or $B = k - li$, i.e. either $B = A$, or $B = P$, both of which contradict the hypothesis.

From this theorem, another one is easily derived, namely that the resolution into prime factors can only be accomplished in a single way. This follows using reasoning entirely analogous to that which we used for real numbers in *Disquisitiones Arithmeticae* (art. 16); it would therefore be superfluous to dwell on it here.

38.

We now proceed to congruences of numbers with respect to complex moduli. But at the outset of this discussion, it is convenient to indicate how the domain of complex quantities can be visualized intuitively.

Just as every real quantity can be expressed in terms of a segment originating from an arbitrary starting point on a doubly infinite line, by comparing it to another arbitrary segment which is taken as a unit, and can thus also be represented by another point, so that points on one side of the starting point represent positive quantities and on the other side represent negative quantities, so can any complex quantity be represented by a point in an infinite plane, in which a line is fixed for real quantities, so that a complex quantity $x + iy$ is represented by a point whose abscissa is $= x$ and whose ordinate (taken positively on one side of the line of abscissas, and negative on the other) is $= y$. In this way, it can be said that an arbitrary complex quantity can be measured by the distance between the position of the referred point and the position of the initial point, with a positive unit denoting a determined arbitrary deflection towards a determined arbitrary direction; a negative unit denoting an equally large deflection towards the opposite direction; and finally imaginary units denoting equally large deflections towards two perpendicular directions.

In this way the metaphysics of so-called imaginary quantities is remarkably elucidated. If the initial point is denoted by (0), and two complex quantities m, m' are referred to the points M, M', which express their relative position to (0), the difference $m - m'$ will be nothing but the position of the point M relative to the point M'; likewise, by representing the product mm' as the position of the point N relative to (0), you will easily see that this position is determined just as much by the position of the point M to (0), as the position of the point M' is determined by the position of the point corresponding to the positive unit, so that it is not inappropriate to say that the positions of the points corresponding to the complex quantities mm', m, m', 1 form a *proportion.* But we reserve a

more extensive treatment of this matter for another occasion. The difficulties which are supposedly involved in the theory of imaginary quantities largely derive from unsuitable nomenclature (indeed, some have inappropriately referred to them as impossible quantities). If, starting from the concept of variations in two dimensions (which are understood most purely through spatial intuition), we had called positive quantities direct, negative quantities inverse, and imaginary quantities lateral, then clarity would succeeded over obscurity.

39.

The things that were brought forth in the preceding article referred to continuous complex quantities: in arithmetic, which deals only with integers, the schema of complex numbers will be a system of equidistant points and lines arranged in such a way that the infinite plane is divided into infinitely many equal squares. All numbers divisible by a given complex number $a+bi=m$ will also form infinitely many squares, whose sides $=\sqrt{aa+bb}$ and areas $=aa+bb$; the latter squares will be inclined to the former whenever neither of the numbers a, b is $=0$. To every number not divisible by the modulus m, there will be a corresponding point, either situated inside such a square, or in a side adjacent to two squares; however, the latter cannot occur unless a, b have a common divisor. Furthermore, it is clear that numbers congruent modulo m will occupy congruent positions in their squares. Hence it is easily concluded that if we collect all numbers situated within a determined square, togther with all those which may lie on two of its non-opposite sides, and finally one number divisible by m, then we will have a complete system of incongruent residues modulo m, i.e. any integer will be congruent to precisely one of them. It would not be hard to show that the number of these residues is equal to the norm of the modulus, $aa+bb$. But it seems advisable to demonstrate this weighty theorem in a purely arithmetic way.

40.

THEOREM. *Let $m=a+bi$ be a given complex modulus, with norm $aa+bb=p$, and assume that a, b are relatively prime numbers. Then any complex integer will be congruent, modulo m, to at least one residue from the series $0,\ 1,\ 2,\ 3\ldots p-1$, and not to more than one.*

Proof. I. Let α, β be integers such that $\alpha a + \beta b = 1$. Then we have

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

Therefore, given an integral complex number $A + Bi$, we have

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

Hence, denoting by h the smallest positive residue of the number $A + (\alpha b - \beta a)B$ modulo p, and setting

$$A + (\alpha b - \beta a)B = h + kp = h + m(ak - bki)$$

we get

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

or

$$A + Bi \equiv h \,(\text{mod. } m). \quad \text{Q. E. P.}$$

II. If a given complex number is congruent to two real numbers h, h' modulo m, then these will also be congruent to each other. Therefore, letting $h - h' = m(c + di)$, we have

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

and hence

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

Moreover, since $a\alpha + b\beta = 1$,

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

Therefore, since h and h' are not equal, they cannot both be included in the complex of numbers 0, 1, 2, $3 \ldots p - 1$. Q. E. S.

41.

THEOREM. *Let $m = a + bi$ be a complex modulus, whose norm is $aa + bb = p$, and assume that a, b are not relatively prime, but instead have a greatest common divisor λ (which we assume to be positive). Then any complex number will be congruent to one and only one residue $x + yi$ such that x is one of the numbers $0, 1, 2, 3 \ldots \frac{p}{\lambda} - 1$, and y is one of the numbers 0, 1, 2, $3 \ldots \lambda - 1$.*

Proof. I. By taking integers α, β such that $\alpha a + \beta b = \lambda$, we have $\lambda i = \alpha b - \beta a + m(\beta + \alpha i)$. Now let $A + Bi$ be the given complex number, let y the minimal positive residue of B modulo λ, let x be the minimal positive residue of $A + (\alpha b - \beta a) \cdot \frac{B-y}{\lambda}$ modulo $\frac{p}{\lambda}$, and set

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

Then

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

which is divisible by m, i.e. $A + Bi \equiv x + yi \,(\text{mod. } m)$ Q. E. P.

II. Let us suppose that two complex numbers $x + yi$, $x' + y'i$ are congruent to the same complex number modulo m, so that they will also be congruent to each other modulo m. Then they will also be congruent modulo λ, and thus $y \equiv y' \,(\text{mod. } \lambda)$. Therefore, if both y, y' are assumed to be among the numbers $0, 1, 2, 3 \ldots \lambda - 1$, then we must necessarily have $y = y'$. Likewise, we must also have $x \equiv x' \,(\text{mod. } m)$, i.e. $x - x'$ is divisible by m, and therefore $\frac{x-x'}{\lambda}$ is an integer divisible by $\frac{a}{\lambda} + \frac{b}{\lambda} \cdot i$, i.e.

$$\tfrac{x-x'}{\lambda} \equiv 0 \,(\text{mod. } \tfrac{a}{\lambda} + \tfrac{b}{\lambda} \cdot i)$$

From this, since $\frac{a}{\lambda}$, $\frac{b}{\lambda}$ are relatively prime, it is concluded by the second part of the theorem of the previous article that $\frac{x-x'}{\lambda}$ is also divisible by the norm of the number $\frac{a}{\lambda} + \frac{b}{\lambda} \cdot i$, i.e. by the number $\frac{p}{\lambda\lambda}$, and therefore $x - x'$ is divisible by $\frac{p}{\lambda}$. Therefore, if both x, x' are assumed to be in the complex of numbers $0, 1, 2, 3 \ldots \frac{p}{\lambda} - 1$, then we must necessarily have $x = x'$, i.e. the residues $x + yi$, $x' + y'i$ are identical. Q. E. S.

It is clearly also necessary to refer to the case where the modulus is a real number, in which case $b = 0$ and $\lambda = \pm a$, and also where it is a pure imaginary number, in which case $a = 0$ and $\lambda = \pm b$. In both cases, we have $\frac{p}{\lambda} = \lambda$.

42.

Therefore, if we sort all complex numbers into classes in such a way that numbers which are congruent with respect to a given modulus are in the same class, and incongruent numbers are assigned to different classes, then there will be exactly p classes exhaustively covering the entire domain of complex integers, where p denotes the norm of the modulus. If we form a complex of p numbers by choosing one number from each class as in articles 40, 41, then we will have a complete system of incongruent residues. In this system, the choice of a representative from each class was based on the principle, that for any class, a residue $x+yi$ should be adopted, such that y has the minimum possible non-negative value, and such that x has the minimum possible non-negative value among all residues with the same minimum value of y. But for other purposes, it will be suitable to use different principles. Of particular note is the method where residues are adopted which, when divided by the modulus, yield the simplest possible quotients. Clearly, if $\alpha+\beta i$, $\alpha'+\beta' i$, $\alpha''+\beta'' i$ etc. are quotients resulting from the division of congruent numbers by the modulus, then the differences between the quantities α, α', α'' etc. will be whole numbers, as will be the differences between the quantities β, β', β'' etc., so it is clear that there will always be one residue for which both α and β lie between the limits 0 and 1, with the former being included and the latter excluded: we will simply call such a residue the minimal residue. If preferable, the limits $-\frac{1}{2}$ and $+\frac{1}{2}$ may be adopted instead (with one included and the other excluded): we will call the residue which satisfies these conditions the *absolute minimum*.

Regarding these minimal residues, the following problems present themselves.

43.

The minimum residue of a given complex number $A+Bi$ with respect to the modulus $a+bi$, whose norm is $=p$, can found in the following way. If $x+yi$ is the minimal residue to be found, then $(x+yi)(a-bi)$ will be the minimal residue of the product $(A+Bi)(a-bi)$ with respect to the modulus $(a+bi)(a-bi)$, i.e. with respect to the modulus p. Therefore, assuming

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

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

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

or

$$x = \tfrac{af-bg}{p} = A - aF + bG$$
$$y = \tfrac{ag+bf}{p} = B - aG - bF$$

Clearly, the minimum residues f, g should be taken either within the limits 0 and $p-1$, or within $-\frac{1}{2}p$ and $\frac{1}{2}p$, depending on whether the simply minimal or the absolutely minimal residue is desired.

44.

The construction of a complete system of minimal residues for a given modulus can be accomplished in several ways. The first method proceeds by first determining the limits within which the real parts must lie, and then assigning limits for the imaginary parts for each value within these limits. The general criterion for a minimal residue $x+yi$ modulo $a+bi$ consists in the conditions that both $ax+by=\xi$ and $ay-bx=\eta$ must lie within the limits 0 and $aa+bb$, whenever we deal with simply minimal residues, or lie within the limits $-\frac{1}{2}(aa+bb)$ and $\frac{1}{2}(aa+bb)$ whenever absolutely minimal residues are desired, with one of the limits excluded. Specific rules are required to distinguishing cases that are brought about by the variety of signs of the numbers a, b, but since the the solution of this presents no difficulty, it has been deferred and we shall refrain from lingering on it here: a single example will suffice to explain the nature of the method.

For the modulus $5+2i$, the simply minimal residues $x+yi$ must be prepared in such a way that both $5x+2y=\xi$ and $5y-2x=\eta$ are among the numbers $0, 1, 2, 3, \ldots, 28$. The equation $29x = 5\xi - 2\eta$ shows that the positive values of x cannot exceed $\frac{5\cdot 28}{29}$, and by considering the sign, the negative values cannot exceed $\frac{2\cdot 28}{29}$. Therefore, the admissible values of x are -1, 0, 1, 2, 3, 4. For $x=-1$, $2y$ must be among the numbers 5, 6, 7 ... 33, and $5y$ must be among -2, -1, 0, 1 ... 26. Hence, the minimum value of y is $+3$, and the maximum is $+5$. Treating the remaining values of x similarly, the following schema for all minimal 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, for the absolutely minimal residues, ξ and η must be among the numbers $-14,\ -13,\ -12 \ldots +14$; hence $29x$ cannot be outside the limits -7.14 and $+7.14$, and therefore x must be among the numbers $-3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3$. For $x = -3,\ 2y = \xi - 5x = \xi + 15$ will be among the numbers $1,\ 2,\ 3 \ldots 29$, however $5y = \eta + 2x = \eta - 6$ will be among $-20,\ -19,\ -18 \ldots +8$: hence it follows that for y only the value $+1$ is possible. Proceeding in the same way for the other values of x, we have the following schema for all absolutely minimal 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.

In applications of the second method, it is convenient to distinguish two cases.

In the first case, where a and b do not have a common divisor, let $\alpha a + \beta b = 1$, and let k be the minimal positive residue of $\beta a - \alpha b$ modulo p. Then the identities

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

show that $ak \equiv -b,\ bk \equiv a \pmod{p}$. Therefore, if we assume that $ax + by = \xi$, $ay - bx = \eta$ as above, then we have $\eta \equiv k\xi,\ \xi \equiv -k\eta \pmod{p}$. So all numbers $\xi + \eta i$

corresponding to simply minimal residues $x+yi$ are obtained when the values 0, 1, 2, $3 \ldots p-1$ are successively taken for ξ, and the minimal positive residues of the products $k\xi$ modulo p are taken for η. Likewise the simply minimal residues will be obtained, but in a different order, if the values 0, 1, 2, $3 \ldots p-1$ are taken for η and the minimum residues of the products $-k\eta$ are taken for ξ. From each $\xi+\eta i$, the corresponding $x+yi$ are given by the formula

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

Now, it is clear that when η increases by unity, ξ will undergo an increase of k or a decrease of $p-k$, and thus $x+yi$

$$\text{will become } \tfrac{a-kb}{p} + \tfrac{ak+b}{p} \cdot i \text{ or } \tfrac{a-kb}{p} + b + (\tfrac{ak+b}{p} - a) \cdot i$$

an observation which serves to facilitate the construction.

Finally, it is clear that if the absolutely minimal residues of $x+yi$ are desired, these instructions are only to be changed in such a way that the values of ξ are subsequently assigned to be between the limits $-\frac{1}{2}p$ and $+\frac{1}{2}p$, while for η one should obtain the absolutely minimal residues of the products $k\xi$. Here is a table of the absolutely minimal residues for the modulus $5+2i$ arranged in this way:

Simply minimal residues.

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

Absolutely minimal residues.

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

In the second case, where a, b are not coprime, it is easy to reduce to the previous case. Let λ be the greatest common divisor of the numbers a, b, and let $a=\lambda a'$, $b=\lambda b'$. Let F denote an indefinite minimal residue for the modulus λ, insofar as it is considered as a complex number, i.e., it represents an indefinite number $x+yi$ such that x, y are either between 0 and λ or between $-\frac{1}{2}\lambda$ and $\frac{1}{2}\lambda$ (depending on whether simply or absolutely minimal residues are in question). Let F' denote an indefinite minimal residue for the modulus $a'+b'i$. Then $(a'+b'i)F+F'$ will be an indefinite minimal residue for the modulus $a+bi$, and the complete system of these residues will emerge as all F are combined with all F'.

46.

Two complex numbers are said to be prime to each other if they do not admit any common divisors other than units. But whenever such common divisors are present, the one with the maximum norm is called the greatest common divisor.

If the resolution of two numbers into prime factors is given, the determination of the greatest common divisor is carried out entirely in the same way as for real numbers (*Disquiss. Ar.* art. 18). At the same time it becomes clear from this that all the common divisors of the two given numbers must be divisible by the greatest common divisor found in this way. Since it is already evident that the three associated numbers are also common divisors, it follows that there will always be four greatest common divisors, and no more, and their norm will be a multiple of

the norm of any other common divisor.

If the factorization of two given numbers into prime factors is not known, the greatest common divisor can be found using a similar algorithm as for real numbers. Let m, m' be the two given numbers, and form a repeated division series m'', m''', etc., such that m'' is the absolutely minimal residue of m with respect to the modulus m', m''' is the absolutely minimal residue of m' with respect to the modulus m'', and so on. Denoting the norms of the numbers m, m', m'', m''', etc., by p, p', p'', p''', etc., we have $\frac{p''}{p'}$ as the norm of the quotient $\frac{m''}{m'}$, and therefore, by the definition of absolutely minimal residue, it is certainly not greater than $\frac{1}{2}$; the same holds for $\frac{p'''}{p''}$ etc. Therefore, the positive real integers p', p'', p''', etc., will form a continuously decreasing series, which necessarily reaches 0 at some point, or, equivalently, in the series m, m', m'', m''', etc., we will eventually reach a term that measures the preceding without residue. Let this term be $m^{(n+1)}$, and suppose that

$$m = km' + m''$$
$$m' = k'm'' + m'''$$
$$m'' = k''m''' + m''''$$

etc., up to

$$m^{(n)} = k^{(n)}m^{(n+1)}$$

By going through these equations in reverse order, it is clear that $m^{(n+1)}$ divides each preceding term $m^{(n)} \dots m''$, m', m; going through the same equations in direct order, it is clear that any common divisor of the numbers m, m' also divides each subsequent term. The former conclusion shows that $m^{(n+1)}$ is a common divisor of the numbers m, m'; the latter shows that this divisor is the greatest.

Moreover, whenever the final residue $m^{(n+1)}$ turns out to be equal to one of the four units 1, -1, i, $-i$, this will indicate that m and m' are relatively prime.

47.

If the equations of the foregoing article, except for the last one, are combined in such a way that m'', m''', $m'''' \dots m^{(n)}$ are eliminated, there arises an equation of the form

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

where h, h' will be integers. Indeed, if we use the notation introduced in *Disquiss.*

Ar. art. 27 then

$$h = \pm\left[k', k'', k''' \dots k^{(n-1)}\right] = \pm\left[k^{(n-1)}, k^{(n-2)} \dots k'', k'\right]$$
$$h' = \mp\left[k, k', k'', k''' \dots k^{(n-1)}\right] = \mp\left[k^{(n-1)}, k^{n-2)} \dots k'', k', k\right]$$

where the upper or lower signs hold, depending on whether n is even or odd. We state this theorem as follows:

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

This is clearly valid not only for the greatest common divisor to which the algorithm in the previous article led, but also for the three associated divisors, for which one should replace the coefficients h, h' with either hi, $h'i$ or $-h$, $-h'$, or $-hi$, $-h'i$.

Therefore, whenever the numbers m, m' are relatively prime, the equation

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

can be satisfied.

Let us consider e.g. the numbers $31 + 6i = m$ and $11 - 20i = m'$. 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 thus

$$\left[k', k'', k'''\right] = -6 - 5i$$
$$\left[k, k', k'', k'''\right] = +4 - 10i$$

and therefore

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

as well as

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

which is confirmed by calculation.

48.

By all of the above, everything required for the theory of congruences of the first degree in the arithmetic of complex numbers has been prepared; but since it does not essentially differ from that which holds for the arithmetic of real numbers,

and which is copiously set out in the *Disquisitiones Arithmeticae*, it will suffice to set down the principal points here.

I. The congruence $mt \equiv 1 \pmod{m'}$ is equivalent to the indeterminate equation $mt + m'u = 1$, and if this is satisfied by the values $t = h, u = h'$, then its general solution is exhibited by $t \equiv h \pmod{m'}$; the condition for solvability is that the modulus m' does not have a common divisor with the coefficient m.

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

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

and if this is satisfied by $t = h$, the general solution is given in the formula

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

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

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

Therefore, when the greatest common divisor of the numbers a, M is adopted for λ, the solution of the proposed congruence is reduced to the preceding case, and for this to be solvable it is clearly necessary and sufficient that λ also divides the difference $c - b$.

49.

So far we have only touched on elementary matters, yet it was not permissible to omit the logical connections. In more advanced investigations, the arithmetic of complex numbers is similar to the arithmetic of real numbers, in that more elegant and simpler theorems emerge, if we only consider such moduli which are prime numbers: in fact, the extension to composite moduli is usually more lengthy than difficult, and involves more labor than skill. Therefore, in the following, we will primarily deal with prime moduli.

50.

Let X denote a function of the variable x of the form

$$Ax^n + Bx^{n-1} + Cx^{n-2} + \text{etc.} + Mx + N$$

where n is a positive real integer, A, B, C, etc. are real or imaginary integers, and

m is a complex integer. Any integer that, when substituted for x, yields a value of X which is divisible by m, we will call a *root* of the congruence $X \equiv 0 \,(\text{mod. } m)$. Roots which are congruent with respect to the modulus will not be considered distinct.

When the modulus is a prime number, such a congruence of order n cannot admit more than n distinct solutions. Letting α be an arbitrary integer (complex), X can be divided by $x-\alpha$ and thereby reduced to the indefinite form $X = (x-\alpha)X' + h$, where h is an integer and X' is a function of degree $n-1$ with integer coefficients. Now, whenever α is a root of the congruence $X \equiv 0 \,(\text{mod. } m)$, it is clear that h will be divisible by m, and therefore we obtain indefinitely $X \equiv (x-\alpha)X' \,(\text{mod. } m)$.

Now, if β is a given integer, and X' is reduced to the form $(x-\beta)X'' + h'$, then X'' will be a function of degree $n-2$ with integral coefficients. However, if β is assumed to be a root of congruence $X \equiv 0$, it must also satisfy $(\beta-\alpha)X' \equiv 0$ and $X' \equiv 0$, since the roots α, β are incongruent. Hence, it follows that h' must be divisible by m, or indefinitely, $X \equiv (x-\alpha)(x-\beta)X'' \,(\text{mod. } m)$.

Similarly, with the introduction of a third root γ incongruent to the previous ones, we will have indefinitely $X \equiv (x-\alpha)(x-\beta)(x-\gamma)X'''$, such that X''' is a function of order $n-3$ with integral coefficients. This process can be further extended, and it is evident that the coefficient of the highest term in each function is $= A$, which is assumed to be indivisible by m. Otherwise, the congruence $X \equiv 0$ would essentially have a lower degree. Therefore, whenever there are n incongruent roots, say $\alpha, \beta, \gamma \ldots \nu$, we will have indefinitely

$$X \equiv A(x-\alpha)(x-\beta)(x-\gamma)\ldots(x-\nu) \,(\text{mod. } m)$$

Hence, the substitution of new values which are not congruent to one of $\alpha, \beta, \gamma \ldots \nu$ will produce a value of X which is not divisible by m, and the truth of the theorem follows naturally.

Moreover, this demonstration essentially agrees with that which we presented in *Disq. Ar.* art. 43, with every step being equally valid for complex numbers as for real numbers.

51.

For the most part, the results presented in the third section of the *Disquisitiones Arithmeticae* concerning residues of powers also hold true, with slight modifications, in the arithmetic of complex numbers. Indeed, the proofs of the theorems can often be retained. Nevertheless, in order to provide a complete account, we will present the main theorems and establish them with concise proofs, in which it should always be understood that the modulus is a prime number.

THEOREM. *Let k denote an integer not divisible by the modulus m. If the norm of m is $= p$, then $k^{p-1} \equiv 1 \,(mod.\, m)$.*

Proof. Let a, b, c, etc. be a complete system of incongruent residues for the modulus m. Remove the residue divisible by m, and denote the resulting complex by C, so that the multitude of C is $= p-1$. Let C' be the complex of products ka, kb, kc, etc. By hypothesis, none of these products will be divisible by m, so each of them will be congruent to a residue in the complex C. Set $ak \equiv a'$, $bk \equiv b'$, $ck \equiv c'$, etc. $(\mathrm{mod.}\, m)$, where the numbers a', b', c', etc. are found in the complex C: let us denote the complex of numbers a', b', c', etc. by C''. Let P, P', P'' be the products of individual numbers of the complexes C, C', C'', respectively, that is,

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

Since the numbers of the complex C'' are congruent to the numbers of the complex C', $P'' \equiv P'$ or $P'' \equiv k^{p-1}P$. But since it is easy to see that any two numbers of the complex C'' are incongruent with each other, and thus all of them are distinct, the complex of numbers C'' must agree completely with the complex of numbers C, with only the order changed, whence $P'' = P$. Thus, $(k^{p-1}-1)P$ will be divisible by m, and thus, since m is a prime number that does not divide any of the factors of P, $k^{p-1}-1$ will necessarily have to be divisible by m. Q. E. D.

52.

THEOREM. *If k denotes, as in the preceding article, an integer not divisible by the modulus m, and t denotes the smallest exponent (other than 0) for which $k^t \equiv 1 \,(mod.\, m)$, then t will be a divisor of any other exponent u for which $k^u \equiv 1 \,(mod.\, m)$.*

Proof. Suppose t is not a divisor of u, and let gt be the multiple of u that is just greater than u, so that $gt-u$ is a positive integer less than t. From $k^t \equiv 1$, $k^u \equiv 1$, it follows that $0 \equiv k^{gt} - k^u \equiv k^u(k^{gt-u} - 1)$, so $k^{gt-u} \equiv 1$, that is, a power of k with exponent less than t is equivalent to 1, contrary to the hypothesis.

As a corollary, it follows that t must divide the number $p-1$.

We will call numbers k for which $t = p-1$, *primitive roots* for the modulus m: we will show that they in fact exist.

53.

Let the number $p-1$ be resolved into its prime factors, so that we have

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

where a, b, c, etc. are distinct real positive prime numbers. Let A, B, C, etc. be integers (complex) not divisible by m, which *do not* satisfy the respective congruences

$$x^{\frac{p-1}{a}} \equiv 1, x^{\frac{p-1}{b}} \equiv 1, x^{\frac{p-1}{c}} \equiv 1 \text{ etc.}$$

modulo m. The existence of A, B, C, etc. is clearly guaranteed by the theorem of article 50. Finally, let h be congruent, modulo m, to the product

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

Then I claim that h will be a primitive root.

Proof. Let t denote the exponent of the lowest power h^t which is congruent to unity. If h were not a primitive root, then t would be a proper divisor of $p-1$, or equivalently $\frac{p-1}{t}$ would be an integer greater than unity. Evidently, this integer will have its real prime factors among a, b, c, etc.: let us therefore suppose (which is allowed), that $\frac{p-1}{t}$ is divisible by a, and set $p-1 = atu$. Then, since $h^t \equiv 1$, we also have $h^{tu} \equiv 1$ or

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

But evidently $\frac{p-1}{ab^\beta}$ is an integer, so

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

similarly,

$$C^{\frac{p-1}{c^\gamma}\cdot\frac{p-1}{a}} \equiv 1, \text{ and so on; hence we must have } A^{\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \equiv 1$$

Next, let a positive integer λ be determined so that

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

which can be done, since the prime number a does not divide $b^\beta c^\gamma \ldots$, and set $\lambda b^\beta c^\gamma \ldots = 1 + a\mu$. Then it is clear that

$$A^{\lambda\cdot\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a}} \equiv 1, \text{ or, since } \lambda\cdot\frac{p-1}{a^\alpha}\cdot\frac{p-1}{a} = (1+a\mu)\frac{p-1}{a} = (p-1)\mu + \frac{p-1}{a}$$

we have $A^{(p-1)\mu}\cdot A^{\frac{p-1}{a}} \equiv 1$, and hence, since we automatically have $A^{(p-1)\mu} \equiv 1$, we also have $A^{\frac{p-1}{a}} \equiv 1$, contrary to the hypothesis. Therefore, the assumption that t is a proper divisor of $p-1$ is inconsistent, and so h must necessarily be a primitive root.

54.

Let h denote a primitive root modulo m, with norm $= p$. Then the terms of the sequence

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

will be incongruent to each other. Hence we easily conclude that any integer not divisible by the modulus must be congruent to one of these, or in other words, it must exhibit a complete system of incongruent residues excluding zero. The exponent of the power to which a given number is congruent can be called its *index*, while h can be called the *base*. Here are some examples in which we have given the absolutely minimal residue for each index.

First Example.

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

Ind.	Residue	Ind.	Residue	Ind.	Residue	Ind.	Residue	Ind.	Residue
0	$+1$	8	-4	1	$-2+2i$	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	$-1-3i$

Example 2.

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

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

55.

We add some observations about primitive roots and indices, omitting the proofs for the sake of simplicity.

I. Indices which are congruent modulo $p-1$ correspond to residues which are congruent modulo m and vice versa.

II. The residues corresponding to the indices which are relatively prime to $p-1$ are primitive roots and vice versa.

III. If a primitive root h is accepted as the base, and the index of another primitive root h' is t, and t' is the index of h when h' is taken as the base, then $tt' \equiv 1 \pmod{p-1}$; and if the indices of any other number in these two systems are u, u' respectively, then $tu' \equiv u$, $t'u \equiv u' \pmod{p-1}$.

IV. While the numbers 1, $1+i$ and their three associates (being too meager) are excluded from the moduli we consider, the remaining prime numbers are those which we referred to as the third and fourth species in article 34. The norms of the latter will be prime numbers of the form $4n+1$; the norms of the former will be the squares of real prime numbers: in both cases, therefore, $p-1$ will be divisible by 4.

V. Denoting the index of the number -1 by u, we will have $2u \equiv 0 \pmod{p-1}$, and therefore either $u \equiv 0$ or $u \equiv \frac{1}{2}(p-1)$: but 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, denoting the index of the number i by u, we will have $2u \equiv \frac{1}{2}(p-1) \pmod{p-1}$, and therefore either $u \equiv \frac{1}{4}(p-1)$ or $u \equiv \frac{3}{4}(p-1)$. But this ambiguity depends on our choice of a primitive root. Specifically, if the primitive root h is taken as the base and the index of the number i is $\frac{1}{4}(p-1)$, then the

index will become $\frac{3}{4}(p-1)$ when h^μ is taken as the base, where μ denotes a positive integer of the form $4n+3$ which is relatively prime to $p-1$, e.g. the number $p-2$, and vice versa. Therefore, with different choices of primitive root, the number i will have the index $\frac{1}{4}(p-1)$ for one base, and the index $\frac{3}{4}(p-1)$ for the other, and for the latter base, $-i$ will clearly have the index $\frac{3}{4}(p-1)$, and for the former, it will have the index $\frac{1}{4}(p-1)$.

VII. When the modulus is a positive real prime of the form $4n+3$, say $=q$, and thus $p=qq$, the indices of all real numbers will be divisible by $q+1$; for denoting the index of the real number k by t, we will have, since $k^{q-1} \equiv 1 \pmod{q}$, $(q-1)t \equiv 0 \pmod{qq-1}$, and therefore $\frac{t}{q+1}$ will be an integer. Likewise, the indices of purely imaginary numbers like ki will be divisible by $\frac{1}{2}(q+1)$. It is therefore clear that only mixed numbers can be primitive roots for such moduli.

VIII. On the contrary, for a modulus m which is a prime complex mixed number (whose norm p is a prime real number of the form $4n+1$), all primitive roots can be chosen from among the real numbers, among which a complete system of incongruent residues can be demonstrated (article 40). It is clear that any real number which is a primitive root for the complex modulus m will at the same time be a primitive root modulo p in the arithmetic of the real numbers, and vice versa.

56.

The theory of quadratic residues and non-residues in the arithmetic of complex numbers is contained within the theory of biquadratic residues, but before we discuss this, we will separately present its remarkable theorems here. For the sake of brevity, however, we will speak here only about the principal case, in which the modulus is a complex prime number (odd).

Let m be such a modulus, and let p be its norm. It is clear that any given integer (which is always understood to be indivisible by m) will either be congruent to a quadratic residue modulo m or not, depending on whether its index, taken with respect to some primitive root as a base, is even or odd. In the former case, that integer is said to be a quadratic residue modulo m, and in the latter case, it is said to be a non-residue. It is concluded from this that among the $p-1$ numbers that constitute a complete system of incongruent residues (indivisible by m), half are quadratic residues and the other half are quadratic non-residues. For any other number outside this system, the same character is attributed to it as to the number

which is congruent to it and belongs to the system.

It follows from this that the product of two quadratic residues, as well as the product of two quadratic non-residues, is a quadratic residue. On the other hand, the product of a quadratic residue with a quadratic non-residue results in a quadratic non-residue. Generally, the product of any number of factors is a quadratic residue or a non-residue, depending on whether the number of quadratic non-residues among the factors is even or odd.

The following general criterion for distinguishing quadratic residues from quadratic non-residues immediately presents itself:

A number k, which is not divisible by the modulus, is a quadratic residue or non-residue depending on whether $k^{\frac{1}{2}(p-1)} \equiv 1$ or $k^{\frac{1}{2}(p-1)} \equiv -1 \pmod{m}$.

The truth of this theorem immediately follows from the fact that, no matter which primitive root is taken for the base, the index of the power $k^{\frac{1}{2}(p-1)}$ will be either $\equiv 0$ or $\equiv \frac{1}{2}(p-1)$, depending on whether the index of the number k is even or odd.

57.

It is indeed easy, given a modulus, to divide the system of incongruent residues into two classes, namely quadratic residues and non-residues, by which means at the same time all other numbers are automatically assigned to these classes. However, a much more profound inquiry is required to develop criteria that distinguish the moduli for which a given number is a quadratic residue from those for which it is a non-residue.

As regards the real units $+1$ and -1, these are actually squares in the arithmetic of complex numbers, and therefore they are also quadratic residues for *any* modulus. From the criterion in the preceding article, it follows equally easily that the number i (and similarly $-i$) is a quadratic residue for any modulus whose norm is of the form $8n+1$, and a quadratic non-residue for any modulus whose norm is of the form $8n+5$. Since clearly it makes no difference whether the number m or any of the associated numbers im, $-m$, $-im$ is adopted as the modulus, it may be assumed, according to article 36, II, that the modulus is a primary associate, and hence by stipulating that the modulus $= a+bi$, that a is odd and b is even. Thus, since it is always the case that $aa \equiv 1 \pmod{8}$, and bb is either $\equiv 0$ or $\equiv 4 \pmod{8}$, depending on whether b is also even or is odd, it is clear that the numbers $+i$ and $-i$ are quadratic residues of the modulus in the former case, and non-residues in the latter.

58.

Since the character of a composite number (whether it is a quadratic residue or non-residue), depends on the characters of the factors, it will be sufficient to limit the development of criteria for distinguishing the moduli for which a given number k is a quadratic residue or non-residue, to values of k which are prime numbers, and moreover to those among them which are primary associates. In this investigation, *induction* immediately provides particularly elegant theorems.

Let us begin with the number $1+i$, which is found to be a quadratic residue modulo

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

and a quadratic non-residue modulo

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

If we carefully examine the above lists, in which we have always recorded the primary associate, we straightforwardly observe that the moduli $a+bi$ for which $a+b \equiv +1 \pmod 8$ are all in the former class, and the moduli for which $a+b \equiv -3 \pmod 8$ are all in the latter class. If we had chosen $-m$ as the modulus instead of the primary associate m, the criteria would need to be modified, so that moduli for which $a+b \equiv -1 \pmod 8$ would be in the former class, and moduli for which $a+b \equiv +3 \pmod 8$ would be in the latter class. Therefore, if the induction has not failed, in general, denoting the primary number by $a+bi$, where a is odd and b is even, $1+i$ will be a quadratic residue or quadratic non-residue, depending on whether $a+b \equiv \pm 1$ or $\equiv \pm 3 \pmod 8$.

The same rule applies to the number $-1-i$ as for the number $1+i$. Conversely, considering $1-i$ as the product of $-i$ and $1+i$, it is evident that the number $1-i$ has the same character as $1+i$ when b is even, and the opposite character when b is odd. Hence, it can be easily inferred that $1-i$ is a quadratic residue modulo the primary number $a+bi$ whenever $a-b \equiv \pm 1$, and it is a quadratic non-residue when $a-b \equiv \pm 3 \pmod 8$, assuming as always that a is odd and b is even.

Moreover, this second proposition can also be deduced from the previous one, with the help of the following more general theorem, which we state as follows:

In the theory of quadratic residues, the character of the number $\alpha+\beta i$ with respect to the modulus $a+bi$ is the same as that of the number $\alpha-\beta i$ with respect to the modulus $a-bi$.

The proof of this theorem is found in the fact that each modulus has the same norm p, and that as many times as $(\alpha+\beta i)^{\frac{1}{2}(p-1)}-1$ is divisible by $a+bi$, $(\alpha-\beta i)^{\frac{1}{2}(p-1)}-1$ must also be divisible by $a-bi$; and as many times as $(\alpha+\beta i)^{\frac{1}{2}(p-1)}+1$ is divisible by $a+bi$, $(\alpha-\beta i)^{\frac{1}{2}(p-1)}+1$ must also be divisible by $a-bi$.

59.

Let us proceed to odd prime numbers.

We find that the number $-1+2i$ is a quadratic residue modulo $+3+2i$, $+1-4i$, $-5+2i$, $-5-2i$, $-1-6i$, $+7-2i$, $-3+8i$, $+5+8i$, $+5-8i$, $+9+4i$, etc.

and it is a non-residue modulo $-1-2i$, -3, $+3-2i$, $+1+4i$, $-1+6i$, $+5+4i$, $+5-4i$, -7, $+7+2i$, $-5+6i$, $-5-6i$, $-3-8i$, $+9-4i$, etc.

When we reduce the moduli of the former class to their absolutely minimal residues modulo $-1+2i$, we obtain only $+1$ and -1. Namely, $+3+2i \equiv -1$, $+1-4i \equiv -1$, $-5+2i \equiv +1$, $-5-2i \equiv -1$, etc.

On the other hand, all moduli of the latter class are found to be congruent to $+i$ or $-i$ with respect to the modulus $-1+2i$.

Now, the numbers $+1$ and -1 are quadratic residues modulo $-1+2i$, whereas $+i$ and $-i$ are non-residues. Hence, as far as induction is concerned, the theorem is as follows: The number $-1+2i$ is a quadratic residue or non-residue modulo the prime number $a+bi$, depending on whether $a+bi$ is a quadratic residue or non-residue modulo $-1+2i$, provided that $a+bi$ is the primary number among its four associates, that is, if a is odd and b is even.

Furthermore, from this theorem, analogous theorems naturally follow concerning the numbers $+1-2i$, $-1-2i$, $+1+2i$.

60.

By performing a similar induction for the numbers -3 and $+3$, we find that each of them is a quadratic residue modulo $+3+2i$, $+3-2i$, $-1+6i$, $-1-6i$, -7,

$-5+6i,\ -5-6i,\ -3+8i,\ -3-8i,\ +9+4i,\ +9-4i$ etc.

and each is a quadratic non-residue modulo $-1+2i,\ -1-2i,\ +1+4i,\ +1-4i,$ $-5+2i,\ -5-2i,\ +5+4i,\ +5-4i,\ +7+2i,\ +7-2i,\ +5+8i,\ +5-8i$ etc.

The former are all congruent to one of the four numbers $+1,\ -1,\ +i,\ -i$ modulo 3; whereas the latter are all congruent to one of $+1+i,\ +1-i,\ -1+i,$ $-1-i$. The former are precisely the quadratic residues modulo 3, whereas the latter are the quadratic non-residues.

Therefore, this induction shows us that the primary number $a+bi$, assuming a is odd and b is even, has the same relation with the number -3 (and also with $+3$) as -3 does with $a+bi$, with regard to whether each is a quadratic residue or non-residue modulo the other.

Extending a similar induction to other primary numbers, we find that this most elegant law of reciprocity is confirmed everywhere, and we are brought to the following fundamental theorem concerning quadratic residues in the arithmetic of complex numbers.

Let $a+bi$, $A+Bi$ be primary numbers, so that a, A are odd and b, B are even. Then either both of them are quadratic residues of the other, or both of them are quadratic non-residues of the other.

Despite the great simplicity of the theorem, its proof is pressed by great difficulties, which, however, we do not dwell on here, since the theorem itself is only a special case of a more general theorem, which almost exhausts the theory of biquadratic residues. Let us now move on to this.

61.

The concepts expounded in article 2 of the previous treatise regarding biquadratic residues and nonresidues can be extended to the arithmetic of complex numbers, and similarly, here as there, our examination is limited to moduli that are prime numbers; furthermore, it will generally be understood tacitly that the modulus should be taken such that it is the primary number among its associates, namely $\equiv 1$ modulo $2+2i$, and also that the numbers whose character is in question (regarding whether they are biquadratic residues or non-residues), are not divisible by the modulus.

Thus, given a modulus, the numbers not divisible by it can be divided into three classes, with the first containing the biquadratic residues, the second containing the biquadratic non-residues which are quadratic residues, and the third containing the quadratic non-residues.

But here too it is better to establish two classes in place of the third, so that in total there are four.

Whichever primitive root is taken as the base, the biquadratic residues will have indices divisible by 4, or of the form $4n$; the biquadratic non-residues which are quadratic residues will have indices of the form $4n+2$; finally, the indices of quadratic non-residues will be partly of the form $4n+1$, and partly of the form $4n+3$. In this way, four classes indeed arise, but the distinction between the latter two classes are not absolute, and rather depend on the choice of primitive root; for it is easy to see that, given a quadratic non-residue, its index will have the form $4n+1$ for half of the primitive roots, and for the other half the index will be of the form $4n+3$. In order to remove this ambiguity, we will always suppose that a primitive root is adopted for which the index $\frac{1}{4}(p-1)$ corresponds to the number $+i$ (cf. article 55, VI). In this way, a classification arises, which we can describe more concisely in a way that does not involve primitive roots.

The *first* class contains the numbers k for which $k^{\frac{1}{4}(p-1)} \equiv 1$; these numbers are the biquadratic residues.

The *second* class contains those for which $k^{\frac{1}{4}(p-1)} \equiv i$.

The *third* class contains those for which $k^{\frac{1}{4}(p-1)} \equiv -1$.

Lastly, the *fourth* class contains those for which $k^{\frac{1}{4}(p-1)} \equiv -i$.

The third class will include biquadratic non-residues which are quadratic residues; the quadratic non-residues will be distributed between the second and fourth.

We assign the respective numbers of these classes as *biquadratic characters* 0, 1, 2, 3. If the character λ of the number k modulo m is defined to be the exponent of the power of i to which the number $k^{\frac{1}{2}(p-1)}$ is congruent, then it is clear that characters which are equivalent modulo 4 are to be considered equivalent. However, this notion is limited for the time being to moduli which are prime numbers: in the continuation of these discussions, we will show how it can also be adapted to composite moduli.

62.

To make it easier to construct a comprehensive induction for the characters of numbers, we attach a concise table here, by the help of which the character of any given number with respect to a modulus whose norm does not exceed the value 157 can be easily obtained, provided that attention is paid to the following observations.

Since the character of a composite number is equal (or rather, congruent modulo 4) to the sum of the characters of its individual factors, it suffices to compute the characters of all prime numbers for the given modulus. Moreover, since the characters of the units -1, i, $-i$ are clearly congruent to the numbers $\frac{1}{2}(p-1)$, $\frac{1}{4}(p-1)$, $\frac{3}{4}(p-1)$ modulo 4, it is also sufficient to have exhibited the characters of numbers which are primary among their associates. Furthermore, since numbers which are congruent modulo m have the same character, it suffices to include in the table the characters of those numbers which are contained in the system of absolutely minimal residues modulo m. Finally, by reasoning similar to that of article 58, if the character of a number $A+Bi$ is λ for the modulus $a+bi$, and the character of the number $A-Bi$ is λ' for the modulus $a-bi$, then we always have $\lambda \equiv -\lambda' \pmod 4$, or equivalently, $\lambda+\lambda'$ is divisible by 4. Therefore, it suffices to include moduli for which b is either 0 or positive in the table.

Thus if we seek e.g. the character of the number $11-6i$ with respect to the modulus $-5-6i$, we substitute $11+6i$, $-5+6i$ for the given numbers; then we determine (article 43) the absolutely minimal residue of the number $11+6i$ modulo $-5+6i$, which is $-1-4i = -1 \times (1+4i)$; therefore, since the character of -1 with respect to the modulus $-5+6i$ is 30, and the character of the number $1+4i$, from the table, is 2, it follows that the character of the number $11+6i$ with respect to the modulus $-5+6i$ will be 32 or 0, and consequently, by the final observation, the character of the number $11-6i$ with respect to the modulus $-5-6i$ will also be 0. Similarly, if we seek the character of the number $-5+6i$ with respect to the modulus $11+6i$, its absolutely minimal residue $1-5i$ is resolved into the factors $-i$, $1+i$, $3-2i$, which correspond to characters 117, 0, 1, whence the sought character will be 118 or 2; the number $-5-6i$ will have the same character 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	$1+i,\ -1+2i$

Modulus.	Character.	Numeri.
$-1+6i$	2	$-1-2i$
$+5+4i$	0	$1+i$
	1	-3
	3	$-1+2i,\ -1-2i$
-7	0	-3
	1	$-1+2i,\ -3-2i$
	2	$1+i$
	3	$-1-2i$
$+7+2i$	0	$1+i,\ 3+2i,\ 3-2i,\ 1-4i$
	1	-3
	2	$-1-2i,\ 1+4i$
	3	$-1+2i$
$-5+6i$	0	$1+i,\ -3,\ 3+2i,\ 3-2i$
	1	$1-4i$
	2	$1+4i$
	3	$-1+2i,\ -1-2i$
$-3+8i$	0	$-1+2i,\ 3-2i,\ 1-4i$
	1	$1+i,\ 3+2i$
	2	-3
	3	$-1-2i,\ 1+4i,\ -5+2i$
$+5+8i$	0	$-1-2i$
	1	$-5-2i,\ -1+6i$
	2	$-1+2i,\ 3-2i$
	3	$1+i,\ -3,\ 3+2i,\ 1+4i,\ 1-4i$
$+9+4i$	0	$-1+2i,\ 3+2i$
	1	$1+i,\ -1-2i,\ 3-2i$
	2	$-3,\ 1+4i$
	3	$1-4i,\ -5+2i$
$-1+10i$	0	$1+i,\ -1+2i,\ -1-2i,\ 3+2i$
	1	-3
	2	$3-2i,\ -5+2i,\ 5-4i$
	3	$1+4i,\ 1-4i$

Modulus.	Character.	Numeri.
$+3+10i$	1	$1+i,\ -1-2i,\ 1-4i$
	2	$-3,\ 3+2i,\ 1+4i,\ -5-2i$
	3	$-1+2i,\ 3-2i$
$-7+8i$	0	$1+i,\ -7$
	1	$3+2i,\ 3-2i,\ 1-4i,\ -5-2i$
	2	$-1-2i,\ 1+4i,\ -5+2i,\ -1-6i$
	3	$-1+2i,\ -3,\ -1+6i$
-11	0	-3
	1	$1+i,\ 3-2i,\ 1+4i,\ -5+2i,\ 5+4i$
	2	$-1+2i,\ -1-2i$
	3	$3+2i,\ 1-4i,\ -5-2i,\ 5-4i$
$-11+4i$	0	$1+i,\ -1+2i,\ 3+2i,\ 5+4i$
	1	$-1-2i,\ -1+6i$
	2	$-5+2i$
	3	$-3,\ 3-2i,\ 1+4i,\ 1-4i,\ -5-2i$
$+7+10i$	0	$1+4i,\ 1-4i,\ -1+6i,\ -1-6i$
	1	$-1+2i,\ 3+2i,\ -5+2i$
	2	$1+i,\ 3-2i$
	3	$-1-2i,\ -3,\ -5-2i$
$+11+6i$	0	$1+i,\ -1+2i,\ -3,\ 1+4i,\ 1-4i,\ -7$
	1	$-1-2i,\ 3+2i,\ 3-2i$
	2	$-5-2i,\ -1+6i,\ -5-4i$
	3	$-5+2i,\ 5+4i,\ 7-2i$

63.

We shall now endeavor to discover, by induction, common properties of moduli for which a given prime number has the same character. We always assume that the moduli are primary among their associates, meaning that they are of the form $a+bi$, where either $a \equiv 1,\ b \equiv 0$, or $a \equiv 3,\ b \equiv 2 \pmod 4$.

With respect to the number $1+i$, from which we begin the induction, the law is more easily grasped if we separate the moduli of the former type (for which $a \equiv 1,\ b \equiv 0$) from the moduli of the latter type (for which $a \equiv 3,\ b \equiv 2$). With the help of the table in the previous article, we find the result

character	moduli of the first kind
0	$5+4i,\ -7+8i,\ -7-8i,\ -11+4i$
1	$1-4i,\ -3+8i,\ -3-8i,\ 9+4i,\ -11$
2	$5-4i,\ -7,\ -11-4i$
3	$-3,\ 1+4i,\ 5+8i,\ 5-8i,\ 9-4i$

If we consider these seventeen examples attentively, we find that for all of them the character is $\equiv \frac{1}{4}(a-b-1) \pmod 4$.

Likewise, we have the result

character	moduli of the second kind
0	$3-2i,\ -1-6i,\ 7+2i,\ -5+6i,\ -1+10i,\ 11+6i$
1	$-5+2i,\ -1+6i,\ 7-2i,\ -1-10i,\ 3+10i$
2	$-1+2i,\ -5-2i,\ 3-10i,\ 7+10i$
3	$-1-2i,\ 3+2i,\ -5-6i,\ 7-10i,\ 11-6i$

In all of these twenty examples, with a little attention, we find that the character is $\equiv \frac{1}{4}(a-b-5) \pmod 4$.

One can easily condense these two rules into one that can be applied to both types of moduli, by observing that $\frac{1}{4}bb$ is $\equiv 0 \pmod 4$ for moduli of the former type, and $\equiv 1 \pmod 4$ for moduli of the latter type. Thus the character of the number $1+i$ with respect to any prime modulus is $\equiv \frac{1}{4}(a-b-1-bb) \pmod 4$.

It is convenient to note here, that since $(b+1)^2$ is always of the form $8n+1$, or $\frac{1}{4}(2b+bb)$ is even, this character will be even or odd, depending on whether $\frac{1}{4}(a+b-1)$ is even or odd, which accords with the rule for the quadratic character stated in article 58.

Since $\frac{1}{4}(a-b-1)$, $\frac{1}{4}(a-b+3)$ are integers, of which one is even and the other odd, their product will be even, so $\frac{1}{8}(a-b-1)(a-b+3) \equiv 0 \pmod 4$. Hence, in place of the above expression for the biquadratic character, the following can also be adopted

$$\tfrac{1}{4}(a-b-1-bb) - \tfrac{1}{8}(a-b-1)(a-b+3) = \tfrac{1}{8}(-aa+2ab-3bb+1)$$

This formula also recommends itself by the fact that it is not restricted to primary moduli, but only assumes that a is odd and b is even. It is clear that under this assumption, either $a+bi$ or $-a-bi$ will be primary among its associates, and the value of this formula will be the same for both moduli.

64.

Departing from the last rule extracted in the previous article, we find

numbers	character $\equiv$
$-1+i$	$\frac{1}{8}(aa+2ab-bb-1)$
$-1-i$	$\frac{1}{8}(-aa+2ab+bb+1)$
$+1-i$	$\frac{1}{8}(aa+2ab+3bb-1)$

This immediately implies that the character of i is $\frac{1}{4}(aa+bb-1)$, and the character of -1 is $\frac{1}{2}(aa+bb-1) \equiv \frac{1}{2}bb$, since $aa-1$ is always of the form $8n$. Clearly these four rules, even if they have so far been borrowed from induction, are so interconnected that as soon as the demonstration of one is complete, the other three are demonstrated simultaneously. There is scarcely any need to mention that in these rules we only assume a to be odd and b to be even.

If you do not mind using formulas restricted to primary moduli, we can use them in the following way. It is

numbers	character $\equiv$
$-1+i$	$\frac{1}{4}(-a-b+1-bb)$
$-1-i$	$\frac{1}{4}(a-b-1+bb)$
$+1-i$	$\frac{1}{4}(-a-b+1+bb)$

The simplest formulas emerge if, as we did at the beginning of our induction, we distinguish between moduli of the first and second kind. That is, the character is

numbers	for moduli of the first kind	for moduli of the second kind
$-1+i$	$\frac{1}{4}(-a-b+1)$	$\frac{1}{4}(-a-b-3)$
$-1-i$	$\frac{1}{4}(a-b-1)$	$\frac{1}{4}(a-b+3)$
$+1-i$	$\frac{1}{4}(-a-b+1)$	$\frac{1}{4}(-a-b+5)$

65.

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

character	moduli of the first kind
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	$-3,\ +5+4i,\ +9-4i,\ -7+8i,\ -11-4i$

Reducing each of these moduli to their absolutely minimal residues modulo $-1+2i$, we observe that all those corresponding to character 0 are congruent to 1; those corresponding to character 1 are congruent to i; those with character 2 become congruent to -1; finally, all those with character 3 become congruent to $-i$. Now the characters of the numbers 1, i, -1, $-i$ with respect to the modulus $-1+2i$ are themselves 0, 1, 2, 3 respectively, thus in each of these 17 examples the character of the number $-1+2i$ with respect to the modulus of the first kind $a+bi$ is identical to the character of this number with respect to the modulus $-1+2i$.

Likewise, from the table, we have the result

character	moduli of the second kind
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	$-1-2i,\ +7+2i,\ -5+6i,\ +3+10i,\ +3-10i,\ +11-6i$

Reducing these moduli to their minimal residues modulo $-1+2i$, those corresponding to characters 0, 1, 2, 3 are found to be congruent to the numbers -1, $-i$, $+1$, $+i$ respectively; however, if $-1+2i$ is adopted as the modulus, these same numbers corresponding to the characters 2, 3, 0, 1 respectively. Therefore, in all these 19 examples, the character of $-1+2i$ with respect to a modulus of the second kind differs by two units from the character of this number with respect to $-1+2i$.

Moreover, it is easily understood that the situation will be completely similar with respect to the number $-1-2i$.

66.

We omit the distinction between moduli of the first and second kind for the number -3, since experience shows that it is superfluous here. The result is thus

character	modules
0	$-1+6i,\ -1-6i,\ -7,\ -5+6i,\ -5-6i,\ -11,\ 11+6i,\ 11-6i$
1	$-1-2i,\ 1-4i,\ -5+2i,\ 5+4i,\ 7+2i,\ 5-8i,\ -1+10i,\ -7-8i,$ $-11-4i,\ 7-10i$
2	$3+2i,\ 3-2i,\ -3+8i,\ -3-8i,\ 9+4i,\ 3+10i,\ 3-10i$
3	$-1+2i,\ 1+4i,\ -5-2i,\ 5-4i,\ 7-2i,\ 5+8i,\ -1-10i,\ -7+8i,$ $-11+4i,\ 7+10i$

Reducing these moduli to their minimal residues modulo 3, we see that those corresponding to the character 0 become either $\equiv 1$ or $\equiv -1$; those with character 1 become either $\equiv 1-i$ or $\equiv -1+i$; those with the character 2 become either $\equiv i$ or $\equiv -i$; and finally, those with character 3 become either $\equiv 1+i$ or $\equiv -1-i$. From this induction, we conclude that the character of the number -3 with respect to a prime modulus which is primary among its associates, is identical to the character of that number modulo 3, or equivalently modulo -3.

67.

By carrying out a similar induction with respect to other prime numbers, we find that the numbers $3\pm 2i$, $-1\pm 6i$, $7\pm 2i$, $-5\pm 6i$, etc., are subject to theorems similar to those which we found in article 65 for the number $-1+2i$; on the other hand, the numbers $1\pm 4i$, $5\pm 4i$, $-3\pm 8i$, $5\pm 8i$, $9\pm 4i$, etc., behave just like the number -3. Therefore, induction leads to a most elegant theorem, which, following the theory of quadratic residues in the arithmetic of real numbers, may be called the FUNDAMENTAL THEOREM of the theory of biquadratic residues, namely:

Let $a+bi$, $a'+b'i$ be distinct numbers which are primary among their associates, i.e., which are congruent to unity modulo $2+2i$. Then the biquadratic character of the number $a+bi$ with respect to the modulus $a'+b'i$ will be identical with the character of the number $a'+b'i$ with respect to the modulus $a+bi$, if one or both of the numbers $a+bi$, $a'+b'i$, is of the first kind i.e., is congruent to unity modulo 4: on the other hand, the characters will differ by two units if neither of the numbers $a+bi$, $a'+b'i$ is of the first kind, i.e., if both are congruent to the number $3+2i$ modulo 4.

Despite the simplicity of this theorem, its demonstration should be considered among the most hidden mysteries of the higher arithmetic, so that, at least for now, it can be unravelled only through the most subtle investigations, which would far exceed the limits of the present discussion. Therefore, we reserve the publication of this proof, as well as the development of the connection between this theorem and those which we began to establish by induction at the beginning of this discussion, for a third discussion. In the place of a conclusion, however, we will now present what is required for the proof of the theorems proposed in articles 63, 64.

68.

We begin with the prime numbers $a+bi$, for which $b=0$ (the third kind in article 34), where (so that the number will be primary among its associates) a must be a negative real prime number of the form $-(4n+3)$, for which we write $-q$, such as -3, -7, -11, -19 etc. Denoting by λ the character of the number $1+i$ with respect to this modulus, we must have

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

But it is known that 2 is a quadratic residue or non-residue modulo q, depending on whether q is of the form $8n+7$ or of the form $8n+3$, from which we infer, in general,

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

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

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

Therefore, the preceding equation takes the form

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

from which it follows that

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

or since we have $\frac{1}{4}(q+1)^2 \equiv 0 \pmod{4}$, $\lambda \equiv -\frac{1}{4}(q+1) \equiv \frac{1}{4}(a-1) \pmod{4}$. Which is the theorem of article 63, for the case $b=0$.

69.

Far more difficult are the moduli $a+bi$ for which b is not equal to 0 (numbers of the fourth kind in article 34), and various investigations need to be carried out before treating these cases. We will denote the norm $aa+bb$, which will be a prime number of the form $4n+1$, by p.

Let S be the complex of all simply minimal residues for the modulus $a+bi=m$, excluding 0, such that the multitude of numbers contained in S is $=p-1$. Let $x+yi$ denote an indefinite number of this system, and suppose that $ax+by=\xi$, $ay-bx=\eta$. Then ξ, η will be integers between the limits 0 and p *exclusive*: in the present case, where a, b are prime to one another, the formulas of article 45, namely $\eta \equiv k\xi$, $\xi \equiv -k\eta \pmod{p}$, show that neither of the numbers ξ, η can be $=0$ unless the other simultaneously vanishes, and thus $x=0$, $y=0$, a combination which we have already dismissed. Therefore, the criterion for the number $x+yi$ to be contained in S is that the four numbers ξ, η, $p-\xi$, $p-\eta$ are positive.

Furthermore, we observe that for no such numbers can $\xi=\eta$ hold; for it would then follow that $p(x+y)=a(\xi+\eta)+b(\xi-\eta)=2a\xi$, which is absurd, as none of the factors 2, a, ξ is divisible by p. By similar reasoning, 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 the numbers $\xi-\eta$, $p-\xi-\eta$ must be either positive or negative, we can subdivide the system S into four complexes C, C', C'', C''', as follows:

the complex	contains 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

Therefore, the criterion for a number to be in the complex C is properly sixfold, namely, six numbers ξ, η, $p-\xi$, $p-\eta$, $\xi-\eta$, $p-\xi-\eta$ must be positive; but clearly, conditions 2, 5, and 6 already imply the remaining ones. Similar considerations apply to 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'''	$\xi,$	$\eta-\xi,$	$p-\xi-\eta$

Moreover, even without our guidance, anyone will easily understand that, in the graphical representation of complex numbers (see article 39), the numbers of the system S are contained within a square, whose sides connect points representing the numbers $0,\ a+bi,\ (1+i)(a+bi),\ i(a+bi)$, and the subdivision of the system S corresponds to the partition of the square by diagonal lines. However, we prefer to use purely arithmetic reasoning here, leaving the illustration through figurative intuition to the knowledgeable reader for the sake of brevity.

70.

If four complex numbers $r=x+yi,\ r'=x'+y'i,\ r''=x''+y''i,\ r'''=x'''+y'''i$ are connected 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 r belongs to the complex C, then the remaining $r',\ r'',\ r'''$ respectively will belong to the complexes $C',\ C'',\ C'''$. For if we assume $\xi=ax+by,\ \eta=ay-bx,\ \xi'=ax'+by',\ \eta'=ay'-bx',\ \xi''=ax''+by'',\ \eta''=ay''-bx'',\ \xi'''=ax'''+by''',\ \eta'''=ay'''-bx'''$, we find

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

and hence, with the help of the criteria above, the truth of the theorem follows automatically. Moreover, if $r=m+ir'''$, then it is easy to see that, if r is assumed to belong to C', then numbers $r',\ r'',\ r'''$ respectively belong to $C'',\ C''',\ C$; if it belongs to C'', then they belong to $C''',\ C,\ C'$; and finally, if it belongs to C''', then they belong to $C,\ C',\ C''$.

It follows that in each of the complexes $C,\ C',\ C'',\ C'''$ an equal multitude of numbers is found, namely $\frac{1}{4}(p-1)$.

71.

THEOREM. *Let k be an integer not divisible by m. If each number in the complex C is multiplied by k, and the simply minimal residues of the products modulo*

m are distributed among the complexes C, C', C'', C''', and the multitudes of each of these complexes are denoted by c, c', c'', c''' respectively, then the character of the number k with respect to the modulus m will be $\equiv c' + 2c'' + 3c'''$ $(mod.\ 4)$.

Proof. Let c be the number of minimal residues α, β, γ, δ, etc. belonging to C; let c' be the number of minimal residues $m + i\alpha'$, $m + i\beta'$, $m + i\gamma'$, $m + i\delta'$, etc. belonging to C'; let c'' be the number of minimal residues $(1+i)m - \alpha''$, $(1+i)m - \beta''$, $(1+i)m - \gamma''$, $(1+i)m - \delta''$, etc. belonging to C''; and finally, let c''' be the number of minimal residues $im - i\alpha'''$, $im - i\beta'''$, $im - i\gamma'''$, $im - i\delta'''$, etc. belonging to C'''. Now let us consider four products, namely

1) the product of all $\frac{1}{4}(p-1)$ numbers from the complex C;
2) the product of all numbers obtained from these upon multiplying them by k;
3) the product of the minimal residues of these products, i.e., of numbers α, β, γ, δ, etc., $m + i\alpha'$, $m + i\beta'$ etc. etc.;
4) the product of all $c + c' + c'' + c'''$ numbers α, β, γ, δ etc., α', β', γ', δ' etc., α'', β'', γ'', δ'' etc., α''', β''', γ''', δ''' etc.

Denoting these four products P, P', P'', P''' respectively, it is clear that

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

and thus

$$Pk^{\frac{1}{4}(p-1)} \equiv P''' i^{c' + 2c'' + 3c'''} \ (\mathrm{mod.}\ m)$$

But it is easy to see that the numbers α', β', γ', δ', etc., α'', β'', γ'', δ'', etc., α''', β''', γ''', δ''', etc. all belong to complex C, and are distinct from each other and from the numbers α, β, γ, δ etc., just as these very numbers are distinct from each other. Therefore, all these numbers taken together, and disregarding order, must be entirely identical with all of the numbers constituting C. From this we deduce that $P = P'''$, and therefore

$$Pk^{\frac{1}{4}(p-1)} \equiv P i^{c' + 2c'' + 3c'''} \ (\mathrm{mod.}\ m)$$

Finally, since each factor of the product P is not divisible by m, we may conclude

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

and thus $c' + 2c'' + 3c'''$ will be the character of the number k with respect to the modulus m. Q. E. D.

72.

To apply the general theorem of the preceding article to the number $1+i$, it is necessary to subdivide the complex C again into two smaller complexes G and G'. To the complex G we will assign all numbers $x+yi$ such that $ax+by=\xi$ is less than $\frac{1}{2}p$, and to the complex G' we will assign those for which ξ is greater than $\frac{1}{2}p$. We denote the multitude of numbers contained in the complexes G, G' respectively by g, g', so that $g+g'=\frac{1}{4}(p-1)$.

The complete criterion for a number to belong to G will therefore be that the three numbers η, $\xi-\eta$, $p-2\xi$ are positive: indeed, the third condition for the complex C, according to which $p-\xi-\eta$ must be positive, is implicitly contained in these, since $p-\xi-\eta=(\xi-\eta)+(p-2\xi)$. Similarly, the complete criterion for a number to belong to G' will consist in the positivity of the three numbers η, $p-\xi-\eta$, $2\xi-p$.

Hence it is easily concluded that the product of any number from the complex G with $1+i$ belongs to the complex C'''; for if we set

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

then we find

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

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

It can be shown in a completely similar way that the product of any number from the complex G' with $1+i$ belongs to the complex C''.

Therefore, if in the preceding article we assign the value $1+i$ to k, we will have $c=0$, $c'=0$, $c''=g'$, $c'''=g$, and therefore for the character of the number $1+i$ we will have $3g+2g'=\frac{1}{2}(p-1)+g$. And whereas the characters of the numbers i, -1, are $\frac{1}{4}(p-1)$, $\frac{1}{2}(p-1)$, the characters of the numbers $-1+i$, $-1-i$, $1-i$ respectively will be $\frac{3}{4}(p-1)+g$, g, $\frac{1}{4}(p-1)+g$. Therefore, the whole essence of the matter now turns on the investigation of the number g.

73.

What we have explained in articles 69-72 is completely independent of the assumption that m is a primary number: from now on, however, we will at least assume that a is odd and b is even, and further that a, b, and $a-b$ are positive numbers. First of all, it is necessary to establish the limits of the values of x in the complex G.

Setting $ay - bx = \eta,\ (a+b)x - (a-b)y = \zeta,\ p - 2ax - 2by = \theta$, the criterion for a number $x + yi$ to belong to the complex G consists of three conditions, that η, ζ, and θ are positive numbers. Since $px = (a-b)\eta + a\zeta,\ p(a-2x) = a\theta + 2b\eta$, it is clear that x and $2a - x$ must be positive numbers, i.e., x should be equal to one of the numbers $1,\ 2,\ 3 \ldots \frac{1}{2}(a-1)$. Furthermore, since $(a-b)\theta = 2b\zeta + p(a-b-2x)$, it is evident that as long as x is less than $\frac{1}{2}(a-b)$, the second condition (that ζ must be positive) already implies the third condition (that θ must be positive); conversely, whenever x is greater than $\frac{1}{2}(a-b)$, the second condition is already contained in the third condition. Therefore, if x is equal to one of the values $1,\ 2,\ 3 \ldots \frac{1}{2}(a-b-1)$, it is only necessary to require that η and ζ are positive, i.e., that y is greater than $\frac{bx}{a}$ and less than $\frac{(a+b)x}{a-b}$. Therefore, for a given value of x, there will be

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

values of $x + yi$, if we use brackets in the same sense that we have already used them elsewhere (compare *Theorematis arithm. dem. nova* art. 4 and *Theorematis fund. in doctr. de residuis quadr. etc. Algorithm. nov.* art. 3). On the other hand, for the values of x being $\frac{1}{2}(a-b+1),\ \frac{1}{2}(a-b+3) \ldots \frac{1}{2}(a-1)$, it will suffice to reconcile the positive values of η and θ, i.e., that y is greater than $\frac{bx}{a}$ and less than $\frac{p-2ax}{2b}$ or $\frac{1}{2}b + \frac{aa-2ax}{2b}$. Therefore, for such a given value of x, the numbers $x + yi$ will be present

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

Hence, we conclude that the multitude of numbers in the complex G is

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

where, in the first term, the summation should extend over all integral 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 symbol φ in the same sense as in loc. cit. (cf. *Theorematis fund.* etc. *Algor. nov.* art. 3), so that

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

where t, u denote arbitrary positive numbers, and t' is the number $\left[\frac{1}{2}t\right]$, then the first term is $= \varphi(a-b, a+b)$, the third $= -\varphi(a,b)$; but the second is

$$= \tfrac{1}{4}bb + \Sigma\left[\tfrac{aa-2ax}{2b}\right]$$

However, by writing the terms in reverse order, we have

$$\Sigma\left[\tfrac{aa-2ax}{2b}\right] = \left[\tfrac{a}{2b}\right] + \left[\tfrac{3a}{2b}\right] + \left[\tfrac{5a}{2b}\right] + \ldots + \left[\tfrac{(b-1)a}{2b}\right] = \varphi(2b,a) - \varphi(b,a)$$

Therefore, our formula takes the following form:

$$g = \varphi(a-b,a+b) + \varphi(2b.a) - \varphi(a,b) - \varphi(b,a) + \tfrac{1}{4}bb$$

Let us consider the first term $\varphi(a-b,a+b)$, which is immediately transformed into $\varphi(a-b,2b) + 1 + 2 + 3 + \text{etc.} + \frac{1}{2}(a-b-1)$ or into

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

Then, since by the general theorem we have $\varphi(t,u) + \varphi(u,t) = \left[\frac{1}{2}t\right] \cdot \left[\frac{1}{2}u\right]$ when t,u are positive relatively prime integers, we have

$$\varphi(a-b,2b) = \tfrac{1}{2}b(a-b-1) - \varphi(2b,a-b)$$

and thus

$$\varphi(a-b,a+b) = \tfrac{1}{8}(aa + 2ab - 3bb - 4b - 1) - \varphi(2b,a-b)$$

Let us arrange the parts of $\varphi(2b,a-b)$ in the following manner

$$\begin{aligned}&\left[\tfrac{a-b}{2b}\right] + \left[\tfrac{3(a-b)}{2b}\right] + \left[\tfrac{5(a-b)}{2b}\right] + \text{etc.} + \left[\tfrac{(b-1)(a-b)}{2b}\right]\\ &+\left[\tfrac{a-b}{b}\right] + \left[\tfrac{2(a-b)}{b}\right] + \left[\tfrac{3(a-b)}{b}\right] + \text{etc.} + \left[\tfrac{\frac{1}{2}b(a-b)}{b}\right]\end{aligned}$$

The second series is evidently

$$= \varphi(b,a-b) = \varphi(b,a) - 1 - 2 - 3 - \text{etc.} - \tfrac{1}{2}b = \varphi(b,a) - \tfrac{1}{8}(bb + 2b)d$$

We represent the first series in reverse order of terms as follows:

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

This expression, where t denotes an integer and u denotes a fraction, is transformed, since we generally have $[t-u] = t - 1 - [u]$, into the following

$$\begin{aligned}&\tfrac{1}{8}b(2a-4-b) - \left[\tfrac{a}{2b}\right] - \left[\tfrac{3a}{2b}\right] - \left[\tfrac{5a}{2b}\right] - \text{etc.} - \left[\tfrac{(b-1)a}{2b}\right]\\ =&\tfrac{1}{8}b(2a-4-b) - \varphi(2b,a) + \varphi(b,a)\end{aligned}$$

Hence,

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

and therefore,

$$\varphi(a-b, a+b) = \varphi(2b,a) - 2\varphi(b,a) + \tfrac{1}{8}(aa - bb + 2b - 1)$$

Substituting this value into the formula for g given above, and also using the fact that $\varphi(a,b) + \varphi(b,a) = \tfrac{1}{4}b(a-1)$, we obtain

$$g = 2\varphi(2b,a) - 2\varphi(b,a) + \tfrac{1}{8}(aa - 2ab + bb + 4b - 1)$$

74.

The case where a, b remain positive and $a-b$ is negative or $b-a$ is positive can be completely resolved by very similar reasoning. The equations $p(a-2x) = 2b\eta + a\theta$, $p(b-a+2x) = 2b\zeta + (b-a)\theta$ show that $\tfrac{1}{2}a - x$ and $x + \tfrac{1}{2}(b-a)$ are positive, and so x must be equal to one of the numbers $-\tfrac{1}{2}(b-a-1)$, $-\tfrac{1}{2}(b-a-3)$, $-\tfrac{1}{2}(b-a-5) \ldots + \tfrac{1}{2}(a-1)$. Furthermore, from the equation $px + (b-a)\eta = a\zeta$, it follows that for negative values of x, the condition for η to be positive, is already contained in the condition for ζ to be positive, but the contrary happens whenever a positive value is assigned to x. Hence, the values of y for a given negative value of x must lie between $\frac{(a+b)x}{a-b}$ and $\frac{p-2ax}{2b}$, while for a positive value of x, they must lie between $\frac{bx}{a}$ and $\frac{p-2ax}{2b}$. For $x = 0$ it is clear that these limits are 0 and $\frac{p-2ax}{2b}$, with the value $y = 0$ being excluded. Thus, we deduce

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

where in the first term, the summation extends over all negative values of x from -1 down to $-\tfrac{1}{2}(b-a-1)$; in the second term, over all values of x from $a - \tfrac{1}{2}(b-a-1)$ up to $\tfrac{1}{2}(a-1)$; and in the third, over all positive values of x from 1 up to $\tfrac{1}{2}(a-1)$. Thus, the first summation becomes $-\varphi(b-a, b+a)$, the second becomes $\tfrac{1}{4}bb + \varphi(2b,a) - \varphi(b,a)$ as in the preceding article, and finally the third becomes $-\varphi(a,b)$, giving us

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

In a similar manner as in the previous article, we find

$$\varphi(b-a,b+a) = \varphi(b-a,2b) - \tfrac{1}{8}\left((b-a)^2-1\right)$$
$$= \tfrac{1}{8}\left(3bb-2ab-aa-4b+1\right) - \varphi(2b,b-a)$$

and also

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

thus

$$\varphi(b-a,b+a) = 2\varphi(b,a) - \varphi(2b,a) + \tfrac{1}{8}\left(bb-aa-2b+1\right)$$

and finally

$$g = 2\varphi(2b,a) - 2\varphi(b,a) + \tfrac{1}{8}\left(aa-2ab+bb+4b-1\right)$$

It has therefore been shown that the same formula holds for g, whether $a-b$ is positive or negative, provided that a, b are positive.

75.

In order to obtain further a reduction, we set

$$L = \left[\tfrac{a}{2b}\right] + \left[\tfrac{2a}{2b}\right] + \left[\tfrac{3a}{2b}\right] + \text{etc.} + \left[\tfrac{\frac{1}{2}ba}{2b}\right]$$
$$M = \left[\tfrac{(\frac{1}{2}b+1)a}{2b}\right] + \left[\tfrac{(\frac{1}{2}b+2)a}{2b}\right] + \left[\tfrac{(\frac{1}{2}b+3)a}{2b}\right] + \text{etc.} + \left[\tfrac{ba}{2b}\right]$$
$$N = \left[\tfrac{a+b}{2b}\right] + \left[\tfrac{2a+b}{2b}\right] + \left[\tfrac{3a+b}{2b}\right] + \text{etc.} + \left[\tfrac{\frac{1}{2}ba+b}{2b}\right]$$

Since it is easily seen that in general, $[u] + \left[u+\frac{1}{2}\right] = [2u]$, for any arbitrary real quantity u, we have $L+N = \varphi(b,a)$, and since it is clear that $L+M = \varphi(2b,a)$, we obtain

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

Moreover, it is obvious that the sum of the first term of the series N with the penultimate term of the series M, for example $\left[\frac{a+b}{2b}\right] + \left[\frac{(b-1)a}{2b}\right]$ becomes $= \frac{1}{2}(a-1)$, and the same sum is produced by the second term of the series N with the antepenultimate series M, and so on. Therefore, since the ultimate term of the series M also becomes $= \frac{1}{2}(a-1)$, and the ultimate term of the series N will be $= \left[\frac{a+2}{4}\right] = \frac{1}{4}(a \mp 1)$, with the upper or lower sign depending on whether a is of the form $4n+1$ or $4n-1$. Thus we have

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

and therefore

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

Setting $a \mp 1 = 4n$, where n is an integer, the formula for g found in articles 73 and

74 becomes

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

But since we have $1 = 16nn - 8an + aa$ here, this formula can also be expressed in the following way:

$$g = \tfrac{1}{8}(-aa + 2ab + bb + 1) + 4(\tfrac{1}{2}(a+1)n - nn - N)$$

Therefore, since g is the character of the number $-1-i$ modulo $a+bi$, this character becomes $\equiv \frac{1}{8}(-aa + 2ab + bb + 1) \pmod 4$, which is the theorem obtained above by induction (article 64), and hence the theorems concerning the characters of the numbers $1+i$, $1-i$, $-1+i$ naturally follow. Therefore, these four theorems, for the case where a and b are positive, are now rigorously demonstrated.

76.

If a remains positive and b is negative, let $b = -b'$, so that b' is positive. Since it has already been proved that the character of the number $-1-i$ modulo $a+b'i$ is $\equiv \frac{1}{8}(-aa + 2ab' + b'b' + 1) \pmod 4$, by the theorem in article 62 the character of the number $-1+i$ for the modulus $a-b'i$ will be $\equiv \frac{1}{8}(aa - 2ab' - b'b' - 1)$, that is, the character of the number $-1+i$ for the modulus $a+bi$ becomes $\equiv \frac{1}{8}(aa + 2ab - bb - 1)$: but this is the same theorem as that mentioned in article 64, from which the three remaining characters $1+i$, $1-i$, $-1-i$ are automatically determined. Therefore, these theorems have also been proved for the case where b is negative, and thus for all cases where a is positive.

Finally, if a is negative, let $a = -a', b = -b'$. Then, by what has already been proved, the character of the number $1+i$ with respect to the modulus $a'+b'i$ is $\equiv \frac{1}{8}(-a'a' + 2a'b' - 3b'b' + 1) \pmod 4$, and it makes no difference as to whether we have the number $a'+b'i$ or its opposite $-a'-b'i$ in place of the modulus; it is clear that the character of the number $1+i$ with respect to the modulus $a+bi$ is $\equiv \frac{1}{8}(-aa + 2ab - 3bb + 1)$, and the same is valid for the characters of the numbers $1-i$, $-1+i$, $-1-i$.

From all this, it is clear that the demonstration of the theorems concerning the characters of the numbers $1+i$, $1-i$, $-1+i$, $-1-i$ (arts. 63. 64) is no longer subject to any limitation.