Theory of Biquadratic Residues
First Treatise

Carl F. Gauss

*Commentationes soc. reg. sc. Gotting. recentiores. Vol. VI. Gottingae 1828**

1.

The theory of quadratic residues can be traced back to a few fundamental theorems counted among the most magnificent treasures of higher arithmetic, which, as is known, were first discovered easily by induction, and thereafter have been verified in such manifold ways that nothing more remains to be desired.

Much more difficult, however, is the theory of cubic and biquadratic residues. As we began to investigate this from 1805 on, besides the elements that first presented themselves, some special theorems arose that are of the utmost prominence due to their simplicity as well as the difficulty of their proofs. However, we soon came to the recognition that the hitherto employed principles of arithmetic would in no way suffice for the establishment of a general theory, and that, rather, this necessarily demands *the domain of higher arithmetic to be more or less infinitely more enlarged*; the way in which this is to be understood will become most clear through the course of this investigation. As soon as we enter upon this new field, a door is opened to knowledge of the simplest theorems which exhaust, inductively, the entire theory; in contrast, the proofs of the same lie so deeply enshrouded, that they can finally be brought to light only after many futile attempts.

Now, as we set out upon the presentation of these studies, we begin with the theory of biquadratic residues, and indeed *we will show, in this first treatise, those investigations that can be completely carried out without such an expansion of the field of arithmetic*, which to a certain degree, however, prepare the road to the former and at the same time provide an expansion to the theory of the division of the circle.

2.

We have introduced the concept of the **biquadratic residue** in Article 115 of the "*Disquisitiones Arithmeticae*." Namely, the whole, positive or negative number a will be taken as a biquadratic residue of the whole number p, if a can be congruent to a biquadrate relative to modulus p, or, conversely, as a **biquadratic nonresidue** if such a congruence does not exist. *In all following investigations*, where the contrary is not expressly emphasized, *we will assume the modulus* p *as an (odd positive)* prime number *and that* a *cannot be divided by* p, since all the remaining cases can be easily reduced to this.

3.

Obviously, every biquadratic residue of the number p will also be a quadratic residue of the same, and consequently, every quadratic nonresidue of p will be a biquadratic nonresidue of the same. This theorem can also be inverted whenever p is a prime number of the form $4n+3$. Then in this case, if a is a quadratic residue of p, then $a \equiv b^2$, where b will either be a quadratic residue or nonresidue of p. In the first case, we set $b \equiv c^2$, so that $a \equiv c^4$, i.e. a will be a biquadratic residue of p; in the latter case, $-b$ will be a quadratic residue of p (since -1 is a nonresidue of every prime number of the form $4n+3$), and if $-b \equiv c^2$, then $a \equiv c^4$ as before and a is a biquadratic residue of p. At the same time it is easily seen that

*Translated by Peter Martinson, Merv Fansler, Liona Fan-Chiang, Michael Kirsch, Sky Shields, and Tarrajna Dorsey. 2007

there are no other solutions of the congruence $x^4 \equiv a \pmod{p}$ in this case, other than the two $x = c$ and $x = -c$.

Since the extant theorems exhaust the entire theory of biquadratic residues for *prime number moduli of the form* 4n+3*, we will completely exclude such moduli from our investigation*, or, [in other words] we will limit ourselves to the prime number moduli of the form $4n + 1$.

4.

Thus, if p *is a prime number of the form* 4n+1, then the theorem of the previous article cannot be inverted; for quadratic residues could exist that are not at the same time biquadratic residues, and indeed this is the case whenever a quadratic residue is congruent to the square of a quadratic nonresidue. For [dann] if one sets $a \equiv b^2$, where b is a quadratic nonresidue of p, then, if the congruence $x^4 \equiv a$ can be satisfied by a value $x \equiv c$, $c^4 \equiv b^2$ or the product $(c^2 - b)(c^2 + b)$ would be divisible by p, whereby p must divide either the factor $c^2 - b$ or $c^2 + b$, i.e. either $+b$ or $-b$ is a quadratic residue of p and, accordingly, both must be quadratic residues of p (since -1 is a quadratic residue), which stands contrary to our assumption.

All of the whole numbers not divisible by p can be divided into three classes, of which the first contains the biquadratic residues, the second, those biquadratic nonresidues which are also quadratic residues, and the third, quadratic nonresidues. Evidently it is sufficient to subject only the numbers $1, 2, 3, \ldots, p - 1$ to such a division into classes, half of which belong to the third class, while the other half will be divided into the first and second classes.

5.

However, it is better to establish **four** classes, whose natures consist of the following:

Let A be the complex of all biquadratic residues situated between 1 and $p - 1$ (inclusively) and let e be an arbitrarily chosen quadratic nonresidue of p. Furthermore, let B be the complex of all least positive residues of the products eA relative to modulus p, and likewise let C, D be the complexes of the least positive residues of the products e^2A, e^3A, respectively, relative to modulus p. For it is easily seen that the several numbers B are different from one another, likewise the several numbers C as well as the several numbers D, while zero can not appear among any of them. Furthermore, it is clear that all numbers contained in A and C are quadratic residues of p, while all contained in B and D are quadratic nonresidues, and thus it is certain that the complexes A, C can have no number in common with complexes B or D. However, neither can A have a number in common with C, nor can B have a number in common with D. For, if we assume,

I. that some number from A, e.g. a, appears also in C, where it can have resulted from the products congruent to e^2a', in which a' is a number from the complex A; if we set further $a \equiv \alpha^4, a' \equiv \alpha'^4$ and assume a whole number θ, such that $\theta\alpha' \equiv 1$, then $e^2\alpha'^4 \equiv \alpha^4$ and therefore, if one multiplies by θ^4:

$$e^2 \equiv \alpha^4\theta^4$$

i.e. e^2 is a biquadratic residue, and hence, e is a quadratic residue, which contradicts the assumption.

II. Likewise, assuming that there were some number in common [between] B, D and that also arises from the products ea, e^3a', where a, a' are numbers from the complex A, then from the congruence $ea \equiv e^3a'$ would follow: $a \equiv e^2a'$, and consequently one would have a number which, resulting from the product e^2a', would belong to C at the same time as A, which we just now proved is impossible.

Furthermore it is easily proven that all quadratic residues of p lying between 1 and $p - 1$, inclusively, must necessarily appear in A or C, and all quadratic nonresidues of p between these limits necessarily appear in B or D. For

I. every quadratic residue which is a biquadratic residue of p at the same time, finds itself in A, according to the requirement.

II. The quadratic residue h (which is smaller than p), which is at the same time a biquadratic nonresidue, is set $\equiv g^2$, where g is a quadratic nonresidue. If such a whole number γ is assumed in such a way that $e\gamma \equiv g$, then γ will be a quadratic residue of p, which we will set $\equiv k^2$. Then:

$$h \equiv g^2 \equiv e^2\gamma^2 \equiv e^2k^4$$

Now, since the least residue of k^4 appears in A, then h, which is formed from the product of that number and e^2, must necessarily be contained in C.

III. If h denotes a quadratic nonresidue of p lying between 1 and $p-1$, and a whole number g is contained between the same limits, such that $eg \equiv h$, then g will be a quadratic residue, and is, consequently, contained in either A or in C; in the first case h is evidently found among the numbers B, in the latter case, however, among the numbers D.

From all this, it follows that all the numbers 1, 2, 3, ..., p-1 *divide themselves into the four series* A, B, C, D*, such that each of them appears in only one of these, so that each individual series must contain* $\frac{1}{4}(p-1)$ *numbers.* By this classification, the numbers appearing in the classes A and C are intrinsic to them, while the distinction between the classes B and D is arbitrary, insofar as they depend on the choice of e, which, itself, is always contained within the class B; consequently, the classes B and D will be exchanged with one another if, for e, another number from the class D is chosen instead.

6.

Since -1 is a quadratic residue of p, set $-1 \equiv f^2 \pmod{p}$, such that the four roots of the congruence $x^4 \equiv 1$ will be: $1, f, -1, -f$. Therefore, if a is a biquadratic residue of p, let us say $a \equiv \alpha^4$, then the four roots of the congruence $x^4 \equiv a$ will be: $\alpha, f\alpha, -\alpha, -f\alpha$, and it is easily seen that these are noncongruent with each other. It results from this that, if the least positive residues of the biquadrates $1, 16, 81, 256, \ldots, (p-1)^4$ are collected, they will always be equal in fours, so that one has $\frac{1}{4}(p-1)$ different biquadratic residues that form the complex A. If the least residues of the biquadrates are collected only up to $(\frac{1}{2}p - \frac{1}{2})$, then each one will only appear twice.

7.

The product of two biquadratic residues is evidently a biquadratic residue, or, multiplication of two numbers of the class A always results in a product whose least positive residue belongs to the same class. Likewise, the product of a number from B and a number from D or a number from C and [another, perhaps the same] number from C will have its least positive residue in A.

However, the residues of the products $A \cdot B$ and $C \cdot D$ belong to class B, the residues of the products $A \cdot C, B \cdot B$ and $D \cdot D$ belong to class C, and, finally, the residues of the products $A \cdot D$ and $B \cdot C$ belong to the class D.

The proofs are so clear that it is enough to mention [only] one. Let, eg. c and d be numbers from C and D, and let $c \equiv e^2 a, d \equiv e^3 a'$,where a, a' denote numbers from A. Then $e^4 aa'$ is a biquadratic residue, i.e. the least positive residue of this number belongs to A; consequently, since the product $cd \equiv e \cdot e^4 aa'$, the least residue of the same will be contained in B.

At the same time, *it can easily be decided with which class a product of multiple factors is grouped.* Namely, if the classes A, B, C, D are given the **characters** $0, 1, 2, 3$, respectively, then the character of the product will either be equal to the aggregate [sum] of the characters of the individual factors or equal to the least residue of the same relative to modulus 4.

8.

It appeared worth the effort to develop these elementary theorems without the aid of the theory of residues of powers; however, if this [theory] is used, then everything can be proven much more easily.

Let g be a primitive root for the modulus p, i.e. a number of such a type that in the series of powers $g, g^2, g^3, \ldots$ no power before g^{p-1} will be congruent to unity relative to modulus p. Then the least positive residues for the numbers $1, g, g^2, g^3, \ldots, g^{p-2}$ will correspond to the numbers $1, 2, 3, \ldots, p-1$, without regard for order, and divide themselves into four classes in the following manner:

Complex	*Members of complex*
A	$1, \quad g^4, \quad g^8, \quad g^{12}, \quad \ldots, \quad g^{p-5}$
B	$g, \quad g^5, \quad g^9, \quad g^{13}, \quad \ldots, \quad g^{p-4}$
C	$g^2, \quad g^6, \quad g^{10}, \quad g^{14}, \quad \ldots, \quad g^{p-3}$
D	$g^3, \quad g^7, \quad g^{11}, \quad g^{15}, \quad \ldots, \quad g^{p-2}$

Hence, the entirety of the preceding theorems result without further effort.

Moreover, as we here divided the numbers $1, 2, 3, \ldots, p-1$ into four classes, whose complexes we denote with A, B, C, D, one can likewise place any whole number whatsoever, not divisible by p, into any one of these classes according to its least residue relative to modulus p.

9.

We denote by f the residue of the power $g^{\frac{1}{4}(p-1)}$ relative to modulus p, and, since $f^2 \equiv g^{\frac{1}{2}(p-1)} \equiv -1$, then f will evidently have the same meaning as in article 6 (*Disquis. Arithm.* article 62). The power $g^{\frac{1}{4}\lambda(p-1)}$, in which λ denotes a positive whole number, will thus be congruent to the numbers $1, f, -1, -f$ relative to modulus p, according as λ is of the form $4m, 4m+1, 4m+2, 4m+3$, respectively, or according as the least residue of g^λ appears in A, B, C, D, respectively. Hence, we obtain a very simple criterion in order to decide to which class a given number h, not divisible by p, belongs; namely, h will belong to A, B, C, or D, according as the power $h^{\frac{1}{4}(p-1)}$ is congruent to the numbers $1, f, -1, -f$ relative to modulus p.

It follows as a corollary that -1 *always belongs to the class* A *whenever* p *is of the form* 8n+1*, on the contrary to the class* C *whenever* p *is of the form* 8n+3 [*sic*][1]. A proof of this theorem, independent of the theory of residues of powers, easily leads to that which we have presented in article 115, III of the "*Disquisitiones Arithmeticae.*"

10.

Since all the primitive roots for modulus p are given by the residues of the powers g^λ, if all the prime numbers up to $p-1$ are taken for λ, it is easily seen that these will be divided equally between the complexes B and D if the base g is always contained in B. If we now take another primitive root from the complex B in place of the number g, then the classification will remain the same; however, if a primitive root from the complex D is taken as the base, then the classes B and D will be exchanged.

If the division into classes is undertaken according to the criterion given in the foregoing article, then the distinction between the classes B *and* D *will depend upon which root of the congruence* $x^2 \equiv -1 \pmod{p}$ *we take as the characteristic number* f.

11.

In order to illustrate the subtile investigations to which we now apply ourselves, [which becomes] so much the easier through examples, we append here a table of the classes for all moduli under 100. For each one, we have chosen the smallest primitive root.

$p = 5$

$g = 2, f = 2$

A	1
B	2
C	4
D	3

$p = 13$

$g = 2, f = 8$

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

[1] This should be $8n + 5$. – *trans.*

$p = 17$

$g = 3, f = 13$

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

$p = 29$

$g = 2, f = 12$

A	1, 7, 16, 20, 23, 24, 25
B	2, 3, 11, 14, 17, 19, 21
C	4, 5, 6, 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 of all prime numbers of the form $8n+1$ and, on the contrary, a quadratic nonresidue of all prime numbers of the form $8n+5$, then for prime numbers of the first form, 2 will appear in class A or C, but for prime number moduli of the second form, in class B or D. Since the difference between B and D is trivial, as it only depends on the choice of the number f, we leave aside the moduli of the form $8n+5$ for the moment. However, if we subject the moduli of the form $8n+1$ to an inductive investigation, we find that 2 belongs to A for $p = 73, 89, 113, 233, 257, 281, 337, 353, \ldots$, and on the contrary, that 2 belongs to C for $p = 17, 41, 97, 137, 193, 241, 313, 401, 409, 433, 449, 457, \ldots$.

Furthermore, since the number -1 is a biquadratic residue of a prime number modulus of the form $8n+1$, *evidently* -2 *must simultaneously belong to the same class as* $+2$.

13.

If the examples of the previous articles are compared with each other, it appears that no simple criterion presents itself, at least at first glance, according to which the modulus of the former type could differ from that of the latter type. Nevertheless, *there are two criteria of that type which stand out because of their elegance and simplicity*, one of which will be developed in the following considerations.

The modulus p, if taken as a prime number of the form $8n+1$, can be brought to the form a^2+2b^2, and indeed only in one single way (*Disquisitiones Arithmeticae*, Article 182, II); here we assume that the roots a, b are taken as positive. Obviously, a will be odd, but b will be even; however, we set $b = 2^\lambda c$, so that c is odd. We now remark,

I. that, if $p \equiv a^2 \pmod{c}$, then p is a quadratic residue of c and also, accordingly, of the individual prime factors into which c decomposes; thus conversely, as a result of the fundamental theorem[2], these individual prime factors will be quadratic residues of p, and hence their product, c, is also a quadratic residue of p and, consequently, b^2 as well as $-b^2$ will be biquadratic residues.

II. consequently $-2b^2$ must belong to the same class as the one in which the number 2 appears; therefore, it is evident that since $a^2 \equiv -2b^2$, 2 appears either in class A or class C depending on whether a is a quadratic residue or a quadratic nonresidue of p.

III. We now assume that a is decomposed into its prime factors, of which those [factors] of the form $8m+1$ or the form $8m+7$ may be denoted by $\alpha, \alpha', \alpha'', \ldots$, however those [factors] of the form $8m+3$ or $8m+5$ may be denoted by $\beta, \beta', \beta'', \ldots$; let the number of the latter be equal to μ. Since now $p \equiv 2b^2 \pmod{a}$, p will be a quadratic residue of the same prime factors of a which have 2 as a quadratic residue, i.e. of the factors $\alpha, \alpha', \alpha'', \ldots$; on the contrary, p will be a quadratic nonresidue of those factors which do not have 2 as a quadratic residue i.e. $\beta, \beta', \beta'', \ldots$; conversely, as a consequence of the fundamental theorem, each $\alpha, \alpha', \alpha'', \ldots$ is a quadratic residue of p, however each $\beta, \beta', \beta'', \ldots$ is a quadratic nonresidue of p. Hence we conclude that the product a is or is not a quadratic residue of p depending on whether μ is even or odd.

IV. However it is easily verified that the product of all $\alpha, \alpha', \alpha'', \ldots$ will be of the form $8m+1$ or $8m+7$ and that the same applies with the product of all $\beta, \beta', \beta'', \ldots$ if the number of these is even, so that in this case, the product a must necessarily be of the form $8m+1$ or $8m+7$. On the contrary, the product of all $\beta, \beta', \beta'', \ldots$, whenever the number of these is odd, will be of the form $8m+3$ or $8m+5$, and hence, in this case, the same applies to the product a.

All of this yields the elegant theorem:

Whenever a *is of the form* 8m+1 *or* 8m+7 *the number 2 is contained in the complex* A*; on the contrary, whenever* a *is of the form* 8m+3 *or* 8m+5*, 2 will be in the complex* C.

[2]Gauss held this theorem in the highest regard, referring to it as the "Golden Theorem." The entirety of Section IV of his *Disquisitiones Arithmeticae* is devoted to the first publication of its proof.

This is confimed via the examples which were enumerated in the foregoing article. That is to say, the first type of modulus is decomposed in the following ways:

$$\begin{array}{llll} 73= & 1+2\cdot 36, & 89=81+2\cdot 4, & 113=81+2\cdot 16, \quad 233=225+2\cdot 4, \\ 257=225+2\cdot 16, & 281=81+2\cdot 100, & 337=49+2\cdot 144, & 353=225+2\cdot 64; \end{array}$$

the second type however in this way:

$$\begin{array}{llll} 17= & 9+2\cdot 4, & 41= & 9+2\cdot 16, \quad 97= 25+2\cdot 36, \quad 137= 9+2\cdot 64, \\ 193=121+2\cdot 36, & 241=169+2\cdot 36, & 313= & 25+2\cdot 144, \quad 401= 9+2\cdot 196, \\ 409=121+2\cdot 144, & 433=361+2\cdot 36, & 449=441+2\cdot 4, & 457=169+2\cdot 144. \end{array}$$

14.

Since the decomposition of the number p into [the sum of] a single and a double square reveals such an outstanding connection with the classification of the number 2, it may well be worth the effort to investigate if the decomposition into 2 squares, which, as is known, can likewise be carried out for the number p, perhaps promises a similar result. Hence, [we present] here the decompositions of the numbers p for which 2 belongs to the classes

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

At the outset we note that, of the two squares into which p is decomposed, the one which we will set equal to a^2 must be odd, the other which we set equal to b^2 must be even. Since a^2 will be of the form $8n+1$, a value of p of the form $8n+5$ will evidently correspond to unevenly even values of b, which are presently excluded from our investigation, since for them the number 2 would be included in classes B or D. However for values of p that are of the form $8n+1$, b must be evenly even, and if our inductive conclusion, which the given schema places before our eyes, is to be believed, *then the number 2 must be included in class A for all moduli in which* b *is of the form* 8n*, and on the contrary, to the class* C *for all moduli in which* b *is of the form* 8n+4. *However this theorem demands a much deeper investigation than the one which we found in the foregoing chapter*, and its proof must be prefaced with many preliminary discussions, which are related to the sequence in which the numbers of the complex A, B, C, D follow one another.

15.

We denote the quantity of numbers from the complex A, which are immediately succeeded by a number from the complex A, B, C, D, by (00), (01), (02), (03), respectively; similarly, the quantity of numbers from the complex B which are immediately succeeded by a number from the complex A, B, C, D with (10), (11), (12), (13), respectively; and analogously there are (20), (21), (22), (23) numbers in complex C, (30), (31), (32), (33) numbers in complex D, which are succeeded by a number from the complex A, B, C, D, respectively. *We are presented with the problem of determining these sixteen quantities a priori.* In order that the reader might compare the general conclusions with the examples more

conveniently, we consider it worthwhile to lay out here the numerical values of the terms of the schema (S)

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

for those individual moduli whose classes we have assigned above 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, we must treat each separately; we begin with the first.

16.

The symbol (00) indicates in how many different ways the equation $\alpha + 1 = \alpha'$ can be satisfied, where α, α' denote undetermined numbers from the complex A. Since for a modulus of the form $8n+1$, as we assume here, α' and $p - \alpha'$ belong to the same complex, we can say more briefly, that (00) will express the number of different ways to satisfy the equation $1 + \alpha + \alpha' = p$. It is clear that the congruence $1 + \alpha + \alpha' \equiv 0 \pmod{p}$ can be used in place of this equation. Likewise:

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

etc.

if the undetermined numbers from complex B are indicated by β, β', those from complex C by γ, and those from complex D by δ. From this arise immediately the following six equations:

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

From every given solution of the congruence $1 + \alpha + \beta \equiv 0$ arises a solution of the congruence $1 + \delta + \delta' \equiv 0$, if for δ is chosen that number between the limits 1 and $p - 1$, for which $\beta\delta \equiv 1$ (which evidently, will be from the complex D), and for δ' the least positive residue of the product $\alpha\delta$ (which likewise will be from the complex D); likewise one evidently returns from the given solution of the congruence $1 + \delta + \delta' \equiv 0$ to the solution of the congruence $1 + \alpha + \beta \equiv 0$, if β is so chosen that $\beta\delta \equiv 1$ and at the same time sets $\alpha \equiv \beta\delta'$. From this we conclude that both congruences have an equal number of solutions, or that $(01) = (33)$.

In an analogous way we obtain from the congruence $1 + \alpha + \gamma \equiv 0$ the following: $1 + \gamma + \gamma' \equiv 0$, if we choose γ' from the complex C such that $\gamma\gamma' \equiv 1$ and γ'' from the same complex is congruent to

the product $\alpha\gamma'$. From here we easily conclude, that these two congruences have an equal number of solutions, or that $(02) = (22)$.

Likewise we derive from the congruence $1 + \alpha + \delta \equiv 0$ the following: $\beta + \beta' + 1 \equiv 0$, in which we take β, β' such that $\beta\delta \equiv 1$ and $\beta\alpha \equiv \beta'$, consequently, $(03) = (11)$.

Finally, we derive from the congruence $1+\beta+\gamma \equiv 0$ in an analogous way the congruence $\delta+1+\beta' \equiv 0$ as well as $\gamma' + \delta' + 1 \equiv 0$, and we conclude from this that $(12) = (13) = (23)$.

Hence, we have obtained eleven equations between our sixteen unknown magnitudes, which will thus be reduced to five, and the schema (S) can be represented in the following way:

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

However, three new equations of condition can be added. That is to say, since each number of complex A, excluding $p-1$, must be followed by a number from complex A, B, C, or D, we thus have:

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

and likewise:

$$\begin{array}{c} (10) + (11) + (12) + (13) = 2n \\ (20) + (21) + (22) + (23) = 2n \\ (30) + (31) + (32) + (33) = 2n \end{array}$$

In the symbols just introduced, the three first equations yield the folowing:

$$\begin{array}{c} h + i + k + l = 2n - 1 \\ i + l + 2m = 2n \\ k + m = n \end{array}$$

The fourth equation becomes identical to the second. With the help of these equations, three unknowns can be eliminated, whereby all sixteen unknowns are already reduced to two.

17.

In order to obtain the complete determination, we want to establish the quantity of the solutions of the congruence

$$1 + \alpha + \beta + \gamma \equiv 0 \pmod{p}$$

where α, β, γ denote undetermined numbers from the complexes A, B, C. Evidently, the value $\alpha = p-1$ is not permissible, since $\beta+\gamma$ cannot be $\equiv 0$; however, substituting the remaining values for α in succession will give h, i, k, l values for $1 + \alpha$, belonging to A, B, C, D respectively. However, for each given value of $1+\alpha$ belonging to A, e.g. for $1+\alpha = \alpha^\circ$, the congruence $\alpha^\circ + \beta + \gamma \equiv 0$ will have just as many solutions as the congruence $1 + \beta' + \gamma' \equiv 0$ (that is, by setting $\beta \equiv \alpha^\circ\beta'$, $\gamma \equiv \alpha^\circ\gamma'$), i.e. $(12) = m$. Likewise, for each given value $\alpha + 1$ belonging to B, say for $1 + \alpha = \beta^\circ$, the congruence $\beta^\circ + \beta + \gamma \equiv 0$ has just as many solutions as the congruence $1 + \alpha' + \beta' \equiv 0$ (that is to say, by setting $\beta \equiv \beta^\circ\alpha'$, $\gamma \equiv \beta^\circ\beta'$), i.e. $(01) = i$. Analogously, for each given value of $1 + \alpha$ belonging to C, say for $1 + \alpha \equiv \gamma^\circ$, the congruence $\gamma^\circ + \beta + \gamma \equiv 0$ can be solved in just as many ways as the congruence $1 + \delta + \alpha' \equiv 0$ (that is to say, by setting $\beta \equiv \gamma^\circ\delta'$, $\gamma \equiv \gamma^\circ\alpha'$), i.e. the number of solutions will be $(03) = l$. Finally, for each value of $\alpha+1$ belonging to D, e.g. for $1+\alpha \equiv \delta^\circ$, the congruence $\delta^\circ + \beta + \gamma \equiv 0$ will have just as many solutions as the congruence $1 + \gamma' + \delta' \equiv 0$ (that is to say, by setting $\beta \equiv \delta^\circ\gamma'$, $\gamma \equiv \delta^\circ\delta'$), i.e. $(23) = m$. Thus, collecting all these solutions has the result, that the congruence $1 + \alpha + \beta + \gamma \equiv 0$ has

$$hm + i^2 + kl + lm$$

different solutions.

In a completely analogous way, however, we derive that, if for β is set the individual numbers of complex B sequentially, the sum $1+\beta$ obtains the values, respectively, $(10), (11), (12), (13)$, or i, l, m, m,

belonging to A, B, C, D, and that for each given value of $1+\beta$ belonging to this complex, the congruence $1+\alpha+\beta+\gamma \equiv 0$ has, respectively, $(02), (31), (20), (13)$ or k, m, k, m different values, so that the number of solutions will be equal to

$$ik + lm + km + m^2.$$

We will be led to the same value, if we base the development on the consideration of the value of the sum $1+\gamma$.

18.

From this twofold expression for the same quantity, we obtain the equation:

$$0 = hm + i^2 + kl - ik - km - m^2,$$

and from here, by eliminating h with help from the equation $h = 2m - k - 1$:

$$0 = (k-m)^2 + i^2 + kl - ik - k^2 - m.$$

However, the two last equations of article 16 yield $k = \frac{1}{2}(l+i)$, and if this value is substituted, then $i^2 + kl - ik - k^2$ turns into $\frac{1}{4}(l-i)^2$, and hence the preceding equation, after being multiplied by 4, turns into the following:

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

From here results, since $4m = 2(k+m) - 2(k-m) = 2n - 2(k-m)$ is

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

or:

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

Hence, setting:

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

one obtains:

$$p = a^2 + b^2.$$

However, it is known that p can be decomposed into two squares in only one unique way; the odd one must be taken for a^2, the even one for b^2, such that a^2 and b^2 are completely determined numbers. However, a itself will also be a completely determined number; since the root of the square must be taken as positive or negative, depending on whether the positive root is of the form $4M+1$ or $4M+3$. We will discuss the determination of the positive or negative sign of b below.

Now, if these new equations are combined with the three last equations of article 16, then the five numbers h, i, k, l, m are completely determined by a, b, and n in the following manner:

$$\begin{array}{rl} 8h & = 4n - 3a - 5 \\ 8i & = 4n + a - 2b - 1 \\ 8k & = 4n + a - 1 \\ 8l & = 4n + a + 2b - 1 \\ 8m & = 4n - a + 1. \end{array}$$

If one prefers to introduce the modulus p in the place of n, then the schema (S) can be represented in the following way, after the individual terms are multiplied by 16 to avoid fractions:

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

19.

It still remains to be shown how the sign of b can be determined. We have already remarked above in article 10 that the difference between the complexes B and D is, in itself, trivial, because it depends on the choice of the number f, which must be taken as one or the other root of the congruence $x^2 \equiv -1$, and that one complex is exchanged with the other, if instead of the one root, the other root is taken. Now, since a glance at the just indicated schema teaches that a similar exchange is related to a change of sign of b, it can be anticipated that a relationship must exist between the sign of b and the number f. In order to discover this relationship, *we remark first of all that, if a non-negative whole number is denoted by* μ *and for* z *is taken all numbers* 1,2,3,...,p-1*, either* $\sum z^\mu \equiv 0$ *or* $\sum z^\mu \equiv -1$ *relative to modulus* p*, according as* μ *is not divisible or is divisble by* p-1. The latter part of the theorem arises from the fact that for every value of μ divisible by $p-1$, $z^\mu \equiv 1$; however, the former part we prove in the following way. If g denotes a primitive root, then all the z will agree with all the g^y if all the numbers $0, 1, 2, 3, \ldots, p-2$ are taken for y, and therefore $\sum z^\mu \equiv \sum g^{\mu y}$. However:

$$\sum g^{\mu y} = \frac{g^{\mu(p-1)} - 1}{g^\mu - 1}$$

and hence:

$$(g^\mu - 1) \sum z^\mu \equiv g^{\mu(p-1)} - 1 \equiv 0.$$

However, since for a value of μ not divisible by $p-1$, g^μ cannot be congruent with 1 or, in other words, $g^\mu - 1$ cannot be divisible by p, it follows that $\sum z^\mu \equiv 0$.

Now, if $(z^4+1)^{\frac{1}{4}(p-1)}$ is developed according to the binomial theorem, then by our stated lemma:

$$\sum (z^4+1)^{\frac{1}{4}(p-1)} \equiv -2 \pmod{p}.$$

However, the least residues of all z^4 represent all the numbers A, where each appears four times; hence we have for the least residues of z^4+1

4(00) belonging to A
4(01) belonging to B
4(02) belonging to C
4(03) belonging to D

and four of them will be equal to zero (namely for $z^4 \equiv p-1$). Hence, by consideraton of the criteria of complexes A, B, C, D, we derive the congruence:

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

and hence:

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

or, by substituting for $(00), (01), \ldots$ their values in the foregoing article:

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

From this, we conclude accordingly that $a + bf \equiv 0$, or, if we multiply by f,

$$b \equiv af$$

must hold, and the congruence serves for the determination of the sign of b, if the number f is already chosen, or alternatively, if the sign of b is given, for the determination of the number f.

20.

Since we have completely solved our problem for moduli of the form $8n+1$, we proceed to another case, where p is of the form $8n+5$; we will be able to carry this out much more quickly, since the conclusions only differ a little from those preceding.

Since, for such a modulus, -1 belongs to the class C, the compliments of the numbers of the complexes A, B, C, D, with respect to the sum p, are contained in the complexes C, D, A, B, respectively. Therefore, it easily follows that,

that the symbol :	denotes the number of solutions to 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, six equations are immediately obtained:

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

If the congruence $1+\alpha+\gamma\equiv 0$ is multiplied with the number γ' from the complex C, which is chosen so that $\gamma\gamma'\equiv 1$, and for γ'' is taken the least residue of the products $\alpha\gamma'$, which is evidently also grouped in complex C, then the congruence $1+\gamma+\gamma'\equiv 0$ arises, wherefrom we conclude: $(00)=(20)$.

In an entirely analogous way are obtained the equations:

$$(01)=(13),\ (03)=(31),\ (10)=(11)=(21).$$

By aid of these eleven equations, we can reduce our sixteen unknown equations to five, and represent the schema (S) in the following form:

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

We further obtain these equations:

$$\begin{aligned} (00)+(01)+(02)+(03) &= 2n+1 \\ (10)+(11)+(12)+(13) &= 2n+1 \\ (20)+(21)+(22)+(23) &= 2n \\ (30)+(31)+(32)+(33) &= 2n+1, \end{aligned}$$

or, if we adopt the notation established above, the three following:

$$\text{(I)}\qquad \begin{aligned} h+\ i\ +\ k\ +l &= 2n+1 \\ 2m+\ i\ +\ l\ \ \ &= 2n+1 \\ h\ +\ m\ \ \ &= \ n\,, \end{aligned}$$

by whose aid our unknowns can already be reduced to two.

We derive the remaining equations from the consideration of the numbers of solutions of the congruence $1+\alpha+\beta+\gamma\equiv 0$ (where here we denote the undetermined numbers of the complexes A, B, C

α, β, γ, respectively). That is to say, if one first considers that $1+\alpha$ yields h, i, k, l numbers belonging to A, B, C, D, respectively, and that, in these four cases, m, l, i, m solutions are obtained, respectively, for each given value of α, then the number of all solutions equals

$$hm + il + ik + lm.$$

Secondly, since m, m, l, i represent the numbers of $1+\beta$ belonging to A, B, C, D, respectively, and for each given value of β in these four cases, there exist h, m, h, m solutions, respectively, the number of all solutions is equal to

$$hm + m^2 + hl + im$$

from which we obtain the equation:

$$0 = m^2 + hl + im - il - ik - lm,$$

which, with the aid of the equation $k = 2m - h$ derived from (1), turns into the following:

$$0 = m^2 + hl + hi - il - im - lm.$$

Now, from equations (I), we obtain $l + i = 1 + 2h$, hence:

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

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

Substituting these values into the previous equation produces:

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

Finally, if we now substitute for $4m$, $2(h+m) - 2(h-m)$ or, on account of the last equation in (I), $2n - 2(h-m)$, then we obtain:

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

and hence:

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

We set therefore:

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

then:

$$p = a^2 + b^2.$$

However, since now in this case p can be decomposed in only one unique way into two squares, one even and one odd, a^2 and b^2 will be completely determined numbers; then, evidently, a^2 must be set equal to the odd square, b^2 to the even. Otherwise, the sign of a is determined in such a way, that $a \equiv 1 \pmod 4$, and the sign of b such that $b \equiv af \pmod p$, as can be easily proven through conclusions which are completely analogous to those which were applied in the foregoing article.

With this established, the five numbers h, i, k, l, m will be determined through a, b and n as follows:

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

or, if one prefers to express these through p, then the terms of the schema (S), multiplied by 16, are as follows:

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

21.

Now that we have solved our problem, we turn back to our main investigation, by now tackling the *complete determination of the complex to which the number 2 belongs.*

I. *If* p *is of the form* 8n+1, then it is already determined that the number 2 will appear either in the complex A or in the complex C. In the former case, it is easily seen that the numbers $\frac{1}{2}(p-1)$, $\frac{1}{2}(p+1)$ also belong to A, while in the latter case, [they belong] to C. If we now consider that, if α and $\alpha+1$ are successive numbers of the complex A, and $p-\alpha-1$, $p-\alpha$ are also such numbers, or, what is the same, that if such numbers of complex A, from which a number of the same complex follows, are always are associated in pairs, α and $p-1-\alpha$, then the quantity of such numbers, i.e. (00), will always be even, unless a number thus associated with itself exists, i.e. unless $\frac{1}{2}(p-1)$ belongs to A, in which case that quantity is odd. We therefore conclude that (00) is odd whenever 2 belongs to the complex A, and, on the contrary, even when 2 belongs to the complex C. However, we have:

$$16(00) = a^2 + b^2 - 6a - 11,$$

or, if we set $a = 4q+1, b = r$ (cf. Article 14):

$$(00) = q^2 - q + r^2 - 1$$

Now, since $q^2 - q$ is evidently always even, (00) will be odd or even, depending on whether r is even or odd, and hence the number 2 will belong to the complex A or to the complex C, depending on whether b is of the form $8m$ or of the form $8m+4$. This is exactly the theorem which we had found in article 14 through induction.

II. Also, however, we could similarly carry out the other case completely, where p is of the form $8n+5$. Here, the number 2 belongs either to B or to D, and it can easily be seen that, in the former case, $\frac{1}{2}(p-1)$ belongs to B, $\frac{1}{2}(p+1)$ belongs to D, in the latter case, $\frac{1}{2}(p-1)$ belongs to D, $\frac{1}{2}(p+1)$ belongs to B. Now, considering that, if β is such a number from B, that is followed by a number in D, the number $p-\beta-1$ will be from B and the number $p-\beta$ will be from D, i.e. that that property is always present in pairs of associated numbers. Hence, the quantity of those, i.e. (13), will be even, excluding the case in which one of them is associated with itself, i.e. where $\frac{1}{2}(p-1)$ belongs to B, $\frac{1}{2}(p+1)$ belongs to D; then, (13) will be odd. We therefore conclude that (13) is even whenever 2 belongs to D, and, on the contrary, odd whenever 2 belongs to B. However, we have:

$$16(13) = a^2 + b^2 + 2a + 4b + 1,$$

or, if we set $a = 4q+1, b = 4r+2$:

$$(13) = q^2 + q + r^2 + 2r + 1.$$

(13) will be odd if r is even; but, on the contrary, (13) will be even if r is odd. Therefore, we conclude that 2 belongs to B as long as b is of the form $8m+2$, but, on the contrary, to D as long as b is of the form $8m+6$.

The ***result*** *of these investigations* can be stated as follows:

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

22.

In the *Disquisitiones Arithmeticae*, we have presented the general theory of the division of the circle and the solution to the equation $x^p - 1 = 0$, and demonstrated, among other things, that if μ is a divisor of the number $p-1$, the function $\frac{x^p-1}{x-1}$ can be decomposed into μ factors of the order $\frac{p-1}{\mu}$, with the aid of an auxiliary equation of the order μ. Out of the general theory of these solutions, we have separately considered the special cases where $\mu = 2$ or $\mu = 3$, in articles 356-358 of that work, and have learned to establish the auxiliary equation *a priori*, i.e. without the development of the schema of the least residues of the powers of some primitive root of the modulus p. Now, without our having to refer to that, the

attentive reader will recognize the close dependence of the next case of that theory, i.e. the case $\mu = 4$, on the investigation here laid out in articles 15 through 20, with whose aid this case can be determined completely without difficulty. Yet, we hold off this discussion for another occasion, and instead, in the present treatise, we have preferred to develop the investigation in a purely arithmetic form without consideration of the theory of the equation $\frac{x^p-1}{x-1}$. Nevertheless, we will add to the conclusion yet another new theorem of pure arithmetic, which stands in close connection with the subject treated up to now.

23.

If $(x^4+1)^{\frac{1}{2}(p-1)}$ is developed by means of the binomial theorem, then three terms will appear in the development, 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

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

Thus, if the numbers $1, 2, 3, \ldots, p-1$ are substituted for x, then we obtain by use of the lemma in article 19:

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

However, considering what we have discussed in article 19, and further, that the numbers of the complexes A, B, C, D raised to the power $\frac{1}{2}(p-1)$ are congruent to the numbers $+1, -1, +1, -1$, respectively, relative to modulus p, it is easily seen that

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

and, consequently, according to the schemata given at the conclusions of articles 18 and 20

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

The comparison of these two values yeilds a very elegant theorem: namely we have:

$$P \equiv 2a \pmod p.$$

If we denote the four products by q, r, s, t, respectively,

$$\begin{array}{l}
1\cdot 2\cdot 3\cdots\cdots\cdots\cdots\cdots\cdots\frac{1}{4}(p-1)\\
\frac{1}{4}(p+3)\cdot\frac{1}{4}(p+7)\cdot\frac{1}{4}(p+11)\cdots\frac{1}{2}(p-1)\\
\frac{1}{2}(p+1)\cdot\frac{1}{2}(p+3)\cdot\frac{1}{2}(p+5)\cdots\frac{3}{4}(p-1)\\
\frac{1}{4}(3p+1)\cdot\frac{1}{4}(3p+5)\cdot\frac{1}{4}(3p+9)\cdots(p-1),
\end{array}$$

then the forementioned theorem is represented in the following way:

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

Since each of the factors of q has as its compliment t, relative to p, then $q \equiv t \pmod p$, whenever the number of factors is even, i.e. whenever p is of the form $8n+1$, on the other hand $q \equiv -t$ whenever the number of factors is odd, or p is of the form $8n+5$. Likewise, $r \equiv s$ in the former case, and $r \equiv -s$ in the latter. In both cases, $qr \equiv st$, and, since it is known that $qrst \equiv -1$, then $q^2r^2 \equiv -1$, and hence

$qr \equiv \pm f \pmod{p}$. If these congruences are combined with the just discovered theorem, then we obtain $r^2 \equiv \pm 2af$, and hence, by articles 19 and 20:[3]

$$2b \equiv \pm r^2 \pmod{p}$$

It is very noteworthy, that the decomposition of the number p can be discovered by means of entirely direct methods; that is to say, the root of the odd square is the absolute least residue of $\frac{r}{2q}$, however the root of the even square is the absolute least residue of $\frac{1}{2}r^2$ relative to modulus p. The expression $\frac{r}{2q}$, whose value will be equal to 1 for $p = 5$, can be represented in the following way for greater values of p:

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

However, since we know which sign the aforementioned root of the odd square bears, namely, that for which it will be of the form $4m + 1$, then is it worthy of note that a similar, general criterion with respect to the sign of the root of the even square could not be discovered up until now. Were someone to find such a criterion, and communicate it to us, we would thank him greatly. In the meantime, I consider it sufficient to append the values of the numbers a, b, f from the least residues of the expressions $\frac{r}{2q}, \frac{1}{2}r^2, qr$, as they arise for values of p under 200.

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	+ 5	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.

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