Theory of Biquadratic Residues

First Commentary

Art. 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.

But the theory of cubic and biquadratic residues is a far deeper undertaking. When we began to examine it 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 difficult of their demonstrations. We soon found out that the principles of Arithmetic hitherto used are by no means sufficient to establish a general theory, but 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 investigations. 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. But the demonstrations were so deeply concealed, that only after many fruitless attempts could they finally be brought to light.

Now that we are ready to put forward these lucubrations, we will begin with the theory of biquadratic residues, and indeed in this first commentary we will explain those investigations which we have already been permitted to complete in the expanded field of Arithmetic, which paved the way, as it were, and at the same time add some new developments to the theory of the division of circles.

Art. 2

We have already introduced the notion of biquadratic residue *Disquisitiones Arithmeticae* Art. 115. Namely, an integer a, positive or negative, is said to be a biquadratic residue of an integer p, if a is congruent to a biquadratic modulo p, and likewise a biquadratic non-residue, if no such congruence exists. In all the following discussions, where the contrary is not expressly indicated, we will assume that the modulus p is a prime number (odd positive), and that a is not divisible by p, since all the remaining cases can be easily reduced to this.

Art. 3

It is clear that every biquadratic residue of the number 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 if in this case a is a quadratic residue modulo p, we set $a \equiv bb \pmod{p}$, and b will either be a quadratic residue or non-residue modulo p. In the former case we set $b \equiv cc$, and hence $a \equiv c^4$, i.e. a is a biquadratic residue modulo p. In the latter case, $-b$ will be a quadratic residue modulo p (since -1 is a non-residue of any prime number of the form $4n+3$), and setting $-b = cc$ we will have as before $a \equiv c^4$, and a is a biquadratic residue modulo p. At the same time, it can be seen easily that solutions of the congruence $x^4 \equiv a \pmod{p}$ other than $x \equiv c$ and $x \equiv -c$ cannot be found in this case. Since these propositions seem to exhaust the entire theory of biquadratic residues for prime moduli of the form $4n+3$, we shall exclude such moduli from our discussion altogether, or in other words we will limit ourselves to prime moduli of the form $4n+1$.

Art. 4

Given a prime number p of the form $4n+1$, the converse of the proposition in the previous article is invalid: namely, there may exist quadratic residues which are not at the same time biquadratic residues, and 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 $x^4 \equiv c$ could be satisfied, with the 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 either the factor $cc - b$ or $cc + b$, i.e. either b or $-b$ would be a quadratic residue modulo p, and therefore both (since -1 is a quadratic residue), contrary to hypothesis.

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

Art. 5

We will establish four classes, whose character should be as follows.

Let A be the complex of all biquadratic residues of p, located between 1 and $p-1$ (inclusive), and let e be an arbitrary quadratic non-residue modulo p. Furthermore, let B be the complex of minimal positive residues obtained from the products eA modulo p, and likewise C, D respectively the complex of minimal positive resiudes from the products e^2A, e^3A modulo p. Having done things in this way, it is easy to see that each of the numbers B will be distinct from one another, and likewise each of C, and even each of D. Furthermore, it is clear that all the numbers contained in A and C are quadratic residues modulo p, but all those in B and D are quadratic non-residues, so that certainly the complexes A and C cannot have any number in common with the complex B or D. But neither A and C nor B and D can have any number in common:

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

$$ee = \alpha^4\theta^4$$

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

II. Likewise, supposing that some number were common to the complexes B, D, and that this came from products ea, e^3a' with numbers a, a' from the complex A, the congruence $ea \equiv e^3a'$ would imply $a \equiv eea'$, and thus we would have a number, which being a product eea' would originate from C, but also at the same time would belong to A, which we have just shown to be impossible.

Furthermore, it is easily demonstrated that all the quadratic residues modulo p, between 1 and $p-1$ inclusively, are necessarily located either in A or C, and all quadratic non-residues modulo p between the same limits must necessarily occur in either B or in D. For

I. Every such quadratic residue, which is at the same time a biquadratic residue, is found in A by hypothesis.

II. A quadratic residue h (less than p), which is at the same time a biquadratic non-residue, can be written as gg, where g is a quadratic non-residue. Let an integer γ be found such that $e\gamma \equiv g$, and γ will be a quadratic residue modulo p, which we will set $\equiv kk$. Hence

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

Therefore, since the minimal remainder of k^4 is found in A, the number h, which arises from the product of it with ee, will necessarily be contained in C.

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

From all this it is deduced that the whole 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 one of these, hence each series must contain $\frac{!}{4}(p-1)$ numbers. In this classification, classes A and C do indeed possess their numbers naturally, but the distinction between the classes B and D is at this point arbitrary, insofar as it depends on the choice of a number e, which itself must always be referred to B. Therefore, if another from class D adopts its place, classes B and D will be interchanged.

Art. 6

Since -1 is a quadratic residue modulo p, let us establish that $-1 \equiv ff$ (mod. p), so that the four roots of the congruence $x^4 \equiv 1$ will be 1, f, -1, $-f$. If therefore a is a biquadratic residue modulo p, say $\equiv \alpha^4$, the four roots of the congruence $x^4 \equiv a$ will be $\alpha, f\alpha, -\alpha, -f\alpha$, which are easily seen to be incompatible with each other. Hence it is clear that if the minimal positive residues of the biquadratics $1, 16, 81, 256, \ldots (p-1)^4$ are collected, each will be present four times, so that there will be $\frac{1}{4}(p-1)$ different biquadratic residues forming the complex A. If only the minimal biquadratic residues up to $(\frac{1}{2}p - \frac{1}{2})^4$ are collected, then each will be present twice.

Art. 7

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

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

The demonstrations are so obvious that it is sufficient to have indicated just one. Let e.g. c and d be numbers from C and D, with $c \equiv eea$, $d \equiv e^3 a$, where a and a' are numbers from A. Then $e^4 aa'$ will be a biquadratic residue, i.e. its minimal residue will lie in A; therefore since the product cd is $\equiv e.e^4 aa'$, its minimal residue will be contained in B.

At the same time, it is now easy to decide to which class the product belongs based on several factors. Of course, assigning class A, B, C, D the respective characters $0, 1, 2, 3$, the character of a product will be equal to the sum of the characters of the individual factors, or rather its minimal residue modulo 4.

Art. 8

It has been thought worthwhile to develop these elementary propositions without the support of the theory of powers of residues, with whose help it is far easier still to demonstrate everything.

Let g be a primitive root modulo p, i.e. a number such that in the series of powers $g, gg, g^3, \ldots$ there is none before g^{p-1} which 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 will be distributed in four classes in the following manner:

ad	residua minima numerorum
A	$1, \quad g^4, \quad g^8, \quad g^{12}, \ldots, g^{p-5}$
B	$g, \quad g^5, \quad g^9, \quad g^{13}, \ldots, g^{p-4}$
C	$g^2, \quad g^6, \quad g^{10}, \quad g^{14}, \ldots, g^{p-3}$
D	$g^3, \quad g^7, \quad g^{11}, \quad g^{15}, \ldots, g^{p-2}$

Hence all the previous propositions follow automatically.

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

Art. 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 the character f signifies the same thing as in Art. 6. Therefore, the power $g^{\frac{1}{4}\lambda(p-1)}$, where λ is an arbitrary integer, will be congruent to 1, f, -1, $-f$ modulo p according as λ is of the form $4m, 4m+1, 4m+2, 4m+3$ resp., or as the minimum residue of g^{λ} is found in A, B, C, D respectively. 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 according as 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 ifollows 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 $8n+5$. The demonstration of this theorem independent of the theory of residual powers can be easily gleaned from that which we taught in *Disquisitiones Arithmeticae* Art. 115, III.

Art. 10

Since *all* the primitive roots modulo p come from the residues of the powers g^{λ}, taking for λ all number relatively prime to $p-1$, it is easy to see that they will be equally dispersed between the complexes B and D, the base g always being contained in B. If, instead of the number g another primitive root is taken from the complex B, then the classification will be the same. If, on the other hand, a primitive root from the complex D is adopted as a base, then the classes B and D will be interchanged.

If the classification criterion from the preceding article is used, the distinction between the classes B and D will instead depend on which root of the congruence $xx \equiv -1$ (mod. p) is adopted as the characteristic number f.

Art. 11

In order that the finer inquiries which we are now about to attack may be more easily illustrated by examples, we attach here the construction of the classes for all moduli less than 100. We adopted the smallest primitive root for each.

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

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

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

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														

Art. 12

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

Moreover, since -1 is a biquadratic reside modulo any prime of the form $8n + 1$, it is clear that -2 is always in the same class as 2.

Art. 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, of an elegant and simple form, to which the following considerations pave the way.

The modulus p, which is a prime number of the form $8n + 1$, can be reduced, and indeed in a unique way, to the form $aa + 2bb$ (*Disquiss. Arithm.* Art. 182, II); we will assume that the roots a, b are taken positively. Obviously, a will be odd, and b will be even. Let us set $b = 2^\lambda c$ where c is odd. We then observe

I. By assumption, $p \equiv aa \pmod{c}$, so p is a quadratic residue modulo c, and therefore also modulo each of the prime factors 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 applies to the number 2, it is clear that b is a quadratic residue modulo p, and therefore both bb and $-bb$ are biquadratic residues.

II. Hence $-2bb$ must be referred to the same class in which the number 2 is found. Therefore, since $aa \equiv -2bb$, it is clear that 2 must be found in class A or C, according as a is either a quadratic residue or non-residue modulo p.

III. Now let us suppose that a has been resolved into prime factors. Denote the factors of the form $8m+1$ or $8m+7$ by $\alpha, \alpha', \alpha''$ etc. and denote those of the form $8m+3$ or $8m+5$ by β, β', β'' etc. Let the multitude of the latter by $= \mu$. 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. of the factors $\alpha, \alpha', \alpha''$ etc., and it will be a quadratic non-residue modulo those factors for which 2 is a quadratic non-residue, i.e. β, β', β'' etc. Therefore, by the fundamental theorem, each $\alpha, \alpha', \alpha''$ etc. will be a quadratic residue modulo p, but each β, β', β'' etc. will be a quadratic non-residue. From this it is concluded that the product a will be a quadratic residue or non-residue modulo p, according as μ is even or odd.

IV. But it is easily confirmed that the product of all $\alpha, \alpha', \alpha''$ etc. is of the form $8m+1$ or $8m+7$, and the same applies to the product of all β, β', β''etc. if the multitude of these is even. So in this case also the product 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 applies in this case to the product a.

From all this, an elegant theorem can be concluded:

Whenever a is of the form $8m+1$ or $8m+7$, the number 2 will be found in the complex A. Whenever a is of the form $8m+3$ or $8m+5$, the number 2 will be found in the complex C.

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

Art. 14

Since the decomposition of 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 division into two squares, to which the number p is equally liable, may supply a similar success. Behold then, the divisions of the numbers p, for which 2 belongs to the class

A	C
$9+64$	$1+16$
$25+64$	$25+16$
$49+64$	$81+16$
$169+64$	$121+16$
$1+256$	$19+144$
$25+256$	$225+16$
$81+256$	$169+144$
$289+64$	$1+400$
	$9+400$
	$289+144$
	$49+400$
	$441+16$

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

Art. 15

Let us denote the set of numbers from the complex A, which are immediately followed by a number from the complex A, B, C, D by (00),(01),(02),(03) respectively. Likewise, denote the set of numbers from the complex B which are followed by a number from A, B, C, D by $(10), (11), (12), (13)$ respectively, and likewise in the complex C by $(20), (21), (22), (23)$ respectively and in complex D by $(30), (31), (32), (33)$. We propose to determine these sixteen multitudes a priori. In order that readers may more easily compare the general reasoning with the examples, it was thought to write here the numerical values of the terms in the diagram (S)

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

for each of the moduli 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	0,	1,	0,	1	2,	1,	2,	1
0,	0,	1,	0	1,	0,	1,	1	1,	0,	1,	1	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 $8n+5$ are different, we must treat both separately: we will start with the former.

Art. 16

The character (00) indicates how many different ways the equation $\alpha + 1 = \alpha'$ can be satisfies, where α, α' denote indefinite numbers from the complex A. Whereas for a modulus of the form $8n+1$, such as we mean here, α' and $p-\alpha'$ belong to the same complex, we shall say more properly that (00) expresses the multitude of different ways of satisfying the equation $1+\alpha+\alpha' = p$. Obviously, this equation can be replaced by the congruence $1+\alpha+\alpha' \equiv p$.

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)	indicates the multitude of solutions of the congruence	$1+\alpha+\delta \equiv 0$
(11)	indicates 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 is a number between the limits $1, \ldots, p-1$ such that $\beta\delta \equiv 1$ (which is manifestly 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 solution of the congruence $1+\delta+\delta' \equiv 0$ to a solution of the congruence $1+\alpha+\beta \equiv 0$, if β is taken so that $\beta\delta \equiv 1$, and we simultaneously let $\alpha \equiv \beta\delta$. Hence we conclude that both congruences enjoy an equal number of solutions, or that $(01) = (33)$.

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

LIkewise, from the congruence $1+\alpha+\delta \equiv 0$ we deduce $\beta+\beta'+1 \equiv 0$, where β, β' are taken so that $\beta\delta \equiv 1, \beta\alpha \equiv \beta'$, and thus $(03) = (11)$.

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

We have therefore obtained, among our sixteen unknowns, eleven equations, so that they can be reduced to five, and the diagram S can be presented as follows:

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

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

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

and so on,

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

In the parameters just introduced, the first three equations supply

$$h+i+k+\ell = 2n-1$$
$$i+\ell+2m = 2n$$
$$k+m = n$$

The fourth is identical to the second. With the aid of these equations it is possible to eliminate three of the unknowns, by which mean all sixteen are now reduced to two.

Art. 17

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

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

where α, β, γ are indefinite numbers from the complexes A, B, C. Obviously the value $\alpha = p-1$ is not admissible, since we cannot have $\beta+\gamma \equiv 0$. Therefore, by substituting the remaining values for α produces h, i, k, ℓ values of $1+\alpha$ from A, B, C, D respectively. For any *given* value of $1+\alpha$ from A, say $1+\alpha = \alpha^o$, the congruence $\alpha^o+\beta+\gamma \equiv 0$ will admit the same number of solutions as the congruence $1+\beta'+\gamma' \equiv 0$ (where we set $\beta \equiv \alpha^o\beta' 4, \gamma \equiv \alpha^o\gamma'$), i.e. the number of solutions is $(12) = m$. Similarly, for any given value of $1+\alpha^o$ from B, say $1+\alpha = \beta^o$, the congruence $\beta^o+\beta+\gamma \equiv 0$ will have as many solutions as $1+\alpha'+\beta' \equiv 0$ (where we set $\beta = \beta^o\alpha', \gamma \equiv \beta^0\gamma'$), i.e. the number of solutions is $(01) = i$. Similarly for any value of $1+\alpha$

from C, say $1+\alpha=\gamma^o$, the congruence $\gamma^o+\beta+\gamma\equiv 0$ has the same number of solutions as $1+\delta+\alpha'\equiv 0$ (where we set $\beta=\gamma^o\delta, \gamma=\gamma^o\alpha'$), i.e. the number of solutions is $(03)=\ell$. Finally, for every value of $1+\alpha$ from D, say $1+\alpha=\delta^o$, the congruence $\delta^o+\beta+\gamma\equiv 0$ will have as many solutions as $1+\gamma'+\delta'\equiv 0$ (where we set $\beta=\delta^o\gamma', \gamma=\delta^o\delta'$), i.e. the number of solutions is $(23)=m$. Putting all of this together, it is clear that the congruence $1+\alpha+\beta+\gamma\equiv 0$ admits

$$hm+ii+k\ell+\ell m$$

distinct solutions.

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

$$=ik+\ell m+km+mm$$

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

Art. 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 help of the equation $h=2m-k-1$,

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

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

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

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

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

or

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

Therefore, setting

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

we find that

$$p=aa+bb.$$

But it is clear that this is the unique way to decompose p as a sum of two squares, if aa is required to be odd and bb is is required to be even, so that aa and bb are uniquely determined. But even a itself will be a completely determined number, for the root of the square must be taken positively or negatively, according as the positive root is of the form $4M+1$ or $4M+3$. We shall speak shortly of the determination of the sign of b.

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

$$\begin{aligned}
8h&=4n-3a-5\\
8i&=4n+a-2b-1\\
8k&=4n+a-1\\
8\ell&=4n+a+2b-1\\
8m&=4n-a+1
\end{aligned}$$

If instead of n we introduce the modulus p, the scheme S, with each term multiplied by 16 to avoid fractions, looks like this:

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

Art. 19

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

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

and therefore

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

From this it follows, since for values of g not divisible by $p-1$, g^μ cannot be congruent to 1, or $g^\mu - 1$ cannot be divisible by p, hence $\sum z^\mu \equiv 0$. Q.E.D.

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

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

But the minimal residues of all z^4 encompass all the numbers A, each occurring four times. Therefore we shall have among the minimal residues of z^4+1

$$\begin{aligned} &4(00) \text{ from } A \\ &4(01) \text{ from } B \\ &4(02) \text{ from } C \\ &4(03) \text{ from } D, \end{aligned}$$

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

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

and therefore

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

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

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

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

$$b \equiv af.$$

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

Art. 20

Having completely solved our problem for moduli of the form $8n+1$, we proceed to the second case, in which p is of the form $8n+5$, which will be solved more briefly, because all the considerations differ little from the previous ones.

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

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 have six equations:

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

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

In a similar way we have equations $(01) = (13)$, $(03) = (31)$, $(10) = (11) = (21)$.

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

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

We have further 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 just introduced, these three (I):

$$\begin{aligned} h+i+k+\ell &= 2n+1 \\ 2m+i+\ell &= 2n+1 \\ h+m &= n \end{aligned}$$

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 α, β, γ denote indefinite numbers from the complexes A, B, C respectively). *First*, evaluating $1 + \alpha$ provides 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 solutions respectively, the total number of solutions will be

$$= hm + i\ell + ik + \ell m$$

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

$$= hm + mm + h\ell + im$$

from which we derive the equation

$$0 = mm + h\ell + hi - i\ell - im - \ell m$$

With the help of the equation $k = 2m - h$, obtained from (I), this becomes

$$0 = mm + h\ell + hi - i\ell - im - \ell m$$

Now from equatiosn (I) we also have $\ell + i = 1 + 2h$, hence

$$2i = 1 + 2h + (i - \ell)$$
$$2\ell = 1 + 2h - (i - \ell)$$

By substituting these values in the previous equation, we get:

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

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

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

and therefore

$$8n + 5 - (4(h - m) + 1)^2 + 4(i - \ell)^2$$

Setting

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

this becomes

$$p = aa + bb.$$

Since in this case too, p can only be divided into two squares, with one even and one odd, in a single way, aa and bb will be completely determined numbers. For it is evident that aa is an odd square, and bb must be an even square. Moreover, the sign of a must be established in such a way that $a \equiv 1$ (mod. 4), and the sign of b so that $b = af$ (mod. p), which is easily demonstrated using reasoning exactly similar to that of the previous article.

From these premises, the numbers h, i, k, ℓ, m are determined by a, b and n as follows:

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

or if we prefer to express this in terms of p, the terms of the diagram S multiplied by 16 will be thus:

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

Art. 21

Having solved our problem, we now return to the main discussion, the complete determination of the complex to which the number 2 belongs.

I. When p is of the form $8n+1$, it is already established that the number 2 is found either in the complex A or in the complex C. It is easy to see that in the former case the numbers $\frac{1}{2}(p-1)$, $\frac{1}{2}(p+1)$ 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 also $p-a-1$ and $p-a$ are such numbers, or what is the same, the numbers of the complex A that are followed by a number from the some complex always come in pairs (α and $p-1-\alpha$). Therefore, the multitude of such numbers, (00), will always be even, unless one exists which is associated with itself, in which case the multitude will be odd. From this we conclude that (00) is odd whenever 2 belongs to the complex A, but even whenever 2 belongs to C. But we have

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

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

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

Since $qq - q$ is evidently always even, (00) will be odd or even according as r is even or odd, and therefore 2 will belong to either A or C, according as b is of the form $8m$ or $8m+4$. Which is the very theorem that was found by induction in Art. 14.

II. But also the second case, in which p is of the form $8n+5$, may be solved just as completely. The number 2 here belongs either to B or to D. It is easy to see 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 from B that is followed by a number from D, there would also be a number $p-b-1$ from B with $p-b$ being from D, i.e. the numbers with this property are always present in associated pairs. Their multitude, (13), will therefore be even, except in the case in which one of them is associated with itself, i.e. where $\frac{1}{2}(p-1)$ belongs to B and $\frac{1}{2}(p+1)$ belongs to D, and then of course (13) will be odd. From this we conclude that (13) is even whenever 2 belongs to D, but 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 $8m+2$, but 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 complex A, B, C, or D, according as the number $4b$ is of the form $4m$, $4m+1$, $4m+2$, or $4m+3$.

Art. 22

In *Disquisitiones Arithmeticae* we explained the general theory of the division of the circle, and of 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 with the help of an auxiliary equation of order μ. In addition to the general theory, we separately considered the special cases of this resolution where $\mu = 2$ or $\mu = 3$, in articles 356-358, and we showed how to assign an auxiliary equations a priori, that is without finding the minimum residues of a primitive root modulo p. Already, even without being warned, attentive

readers will easily perceive a close connection between the simplest case of this theory, namely $m = 4$, and the investigations detailed here in articles 15-20, and indeed, with the help of the former, the latter can be solved without much difficulty. But we reserve this treatment for another occasion, and therefore, even in the present commentary, we prefer to complete the discussion in a purely arithmetical form, in no way mixed with the theory of the equation $x^p - 1 = 0$. In the conclusion of this work, we will rather add some new and purely arithmetical theorems, closely connected with the subject which has been treated so far.

Art. 23

If the power $(x^4+1)^{\frac{1}{2}(p-1)}$ is expanded according to 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 coefficeint

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

Therefore, subsituting for x all of the numbers $1, 2, 3, \ldots, p-1$, we will obtain by the lemma of Art. 19

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

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

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

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

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

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

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

Denoting the four products

$$\begin{aligned}
&1.2.3.\ldots.\tfrac{1}{4}(p-1)\\
&\tfrac{1}{4}(p+3).\tfrac{1}{4}(p+7).\tfrac{1}{4}(p+11).\ldots.\tfrac{1}{2}(p-1)\\
&\tfrac{1}{2}(p+1).\tfrac{1}{2}(p+3).\tfrac{1}{2}(p+5).\ldots.\tfrac{3}{4}(p-1)\\
&\tfrac{1}{4}(3p+1).\tfrac{1}{4}(3p+5).\tfrac{1}{4}(3p+9).\ldots.(p-1)
\end{aligned}$$

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

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

Since each of the factors of q has its complement with respect to p in t, we have $q \equiv t \pmod{p}$ whenever the multitude of factors is even, i.e. whenever p is of the form $8n+1$. On the other hand, $q \equiv -t$ whenever the multitude of factors is odd, or when 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 $qr = st$, and since we have $qrst \equiv -1$, we will also have $qqrr \equiv -1$, and therefore $qr \equiv \pm f \pmod{p}$. Combining this congruence with the theorem just found, we obtain $rr \equiv \pm 2af$, and thus by articles 19 and 20,

$$2b \equiv \pm rr \pmod{p}$$[1]

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

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

$$\frac{6.10.14.18.\ldots.(p-3)}{2.3.4.5.\ldots.\frac{1}{4}(p-1)}$$

But when we know, moreover, by what sign the root of an odd square is obtained from this formula, namely that it must always be of the form $4m + 1$, it is worthy of attention that a similar general criterion with regard to the sign of the square root of the even number has not hitherto been found. If anyone finds it, and shares it with us, it will be a great favor to us. In the meantime, it is advisable to add numerical values here for a, b, f, which will produce the minimal residues of the expressions $\frac{r}{2q}, \frac{1}{2}rr, qr$ for values of p below 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	+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