OBSERVATIONS
REGARDING THE DIVISION OF SQUARES
BY PRIME NUMBERS

Opuscula analytica 1, 1783, p. 64-84 [E552]

HYPOTHESIS

1. *If the squares a^2, b^2, c^2, d^2 etc. of the numbers a, b, c, d etc. may be divided by some prime number P, we will indicate the remainders [or residues] left in the division by the synonymous Greek letters α, β, γ, δ etc.*

COROLLARY 1

2. Therefore since the square *aa* divided by the number *P* may leave the remainder *α,* with the quotient put $= A$ there will be $aa = AP + \alpha$ and thus $aa - \alpha$ will be divisible by *P;* and in a similar manner these expressions $bb - \beta$, $cc - \gamma$, $dd - \delta$ etc. will be divisible by the same divisor *P*.

COROLLARY 2

3. The squares $(a+P)^2$, $(a+2P)^2$, $(a+3P)^2$ and in general $(a+nP)^2$ will leave the same remainder α, if they may be divided by the proposed number *P*. From which it is apparent the same remainders of greater numbers to be provided from the divisor *P*, which are generated from the squares of smaller numbers by the divisor *P*.

COROLLARY 3

4. Then since the squares $(P-a)^2$ divided by *P* must provide the same remainder, as the square *a^2,* it is evident to become $P - a < \frac{1}{2}P$, if $a > \frac{1}{2}P$. From which it is evident all the different remainders to emerge from the squares of numbers, shall be less than half the divisors *P*.

COROLLARY 4

5. Whereby if all the remainders may be desired, which emerge from the division of the squares divided by the given divisor *P*, it will be sufficient that only the squares to be considered, of which the roots may not exceed half of *P*.

COROLLARY 5

6. Hence if the divisor shall be $P = 2p+1$, if all the square numbers 1, 4, 9, 16, 25 etc. may be divided by that, then no more different remainders are able to be produced, than the units contained in the number *p*, and these result from the squares of the numbers 1, 2, 3, 4, ... *p;* indeed the squares of the following numbers $p+1$, $p+2$, $p+3$ etc. reproduce the same remainders, in the reverse order.

SCHOLIUM

7. Thence it is evident here, because these two squares p^2 and $(p+1)^2$ divided by the same number $2p+1$ provide the same remainder, if indeed the difference of these is divisible by $2p+1$. For generally, it is necessary the difference $M-N$ of any two numbers is divisible by $2p+1$, each of *M* and *N* themselves divided may leave the same remainder. Hence also, since there shall be

$$(p+2)^2-(p-1)^2=3(2p+1),$$

and each square separately, $(p+2)^2$ and $(p-1)^2$, likewise must produce the same remainder and in general the square $(p+n+1)^2$ likewise will give the same remainder, as the square $(p-n)^2$. Therefore with this shown it is evident more remainders are unable to arise, than the number of units contained in the number *p* ; but whether all these remainders shall be different or some may be equal to each other, is not defined from this ; and thus, if any divisors may be allowed, each is allowed to happen. But if the divisor $2p+1$ were a prime number, all the remainders will be different from each other, which I show in the following manner.

THEOREM 1

8. *If the divisor* $P = 2p+1$ *were a prime number and each and every square* 1, 4, 9, 16, *... as far as to* p^2 *may be divided by that, all the remainders hence resulting will be different amongst themselves and thus the amount of these will be p.*

DEMONSTRATION

If *a* and *b* shall be any two numbers with these either less or perhaps not greater than *p* and it is required to be shown, if the squares of these a^2 and b^2 may be divided by the prime number $2p+1$, the remainders produces certainly will be different. For if the same remainder were produced, the difference of these $aa-bb$ would be divisible by $2p+1$ and thus on account of the prime number $2p+1$ and $aa-bb=(a+b)(a-b)$ either of these factors must be divisible by $2p+1$. But since there shall be both $a<p$ as well as

$b < p$, certainly there shall not $a > p$, the sum $a+b$, and much more the difference $a-b$ is smaller than $2p+1$; and thence neither can be divisible by $2p+1$. From which evidently all the squares, the roots of which shall not be greater than p itself, certainly different remainders are going to be left behind when divided by the prime number $2p+1$.

COROLLARY 1

9. But if therefore all the squares 1, 4, 9, 16 etc. may be divided by the prime number $2p+1$ and all the remainders may be observed to be different, the number of these will neither be greater or less than *p,* but precisely equal to this number *p*.

COROLLARY 2

10. Truly all these diverse remainders arise from the number p from just as many squares occurring first in the natural series, evidently 1, 4, 9, 16, ... *pp,* and neither from any greater ones following are any new remainders elicited.

COROLLARY 3

11. Therefore not all the smaller numbers occur between the remainders for the divisor $2p+1$, but only just as many of these, as the number of ones contained in the smaller half of the divisor *p.* Whereby, since the number of smaller numbers for the divisor $2p+1$ shall be $=2p$, only the one half of these will be found in the order of the remainders, truly the other half is excluded completely.

SCHOLIUM

12. These smaller numbers for the prime number $2p+1$, which are excluded from the order of the remainders, I will indicate by the name *non-remainders* [or *non-residues*], the number of which therefore is equal always to the number of the remainders. It will help to distinguish properly with due care between the remainders and the non-remainders, whereby I will show here the smaller remainders as well as the non-remainders for some prime numbers with

Divisor 3, $p=1$	Divisor 5, $p=2$	Divisor 7, $p=3$
Squares 1	Squares 1, 4	Squares 1, 4, 9
Remainders 1	Remainders 1, 4	Remainders 1, 4, 2
Non-remainders 2	Non-remainders 2, 3	Non-remainders 3, 5,6

Divisor 11, $p=5$	Divisor 13, $p=6$
Squares 1, 4, 9, 16, 25	Squares 1, 4, 9, 16, 25, 36
Remainders 1, 4, 9, 5, 3	Remainders 1, 4, 9, 3, 12, 10
Non-remainders 2, 6, 7, 8, 10	Non-remainders 2, 5, 6, 7, 8, 11

Divisor 17, $p=8$
Squares 1, 4, 9, 16, 25, 36, 49, 64

Remainders 1, 4, 9, 16, 8, 2, 15, 13
Non-remainders 3, 5, 6, 7, 10, 11, 12, 14

Divisor 19, $p = 9$

Squares 1, 4, 9, 16, 25, 36, 49, 64, 81
Remainders 1, 4, 9, 16, 6, 17, 11, 7, 5
Non-remainders 2, 3, 8, 10, 12, 13, 14, 15, 18

Concerning these remainders and non-remainders for any prime divisor the more memorable properties may be observed, which therefore is worth the effort of a greater careful study, which thence would seem to inundate advances in the theory of numbers with innumerable theorems.

THEOREM 2

13. *If the numbers α and β arise in the order of the remainders from the divisor P , in that place also the product of these $\alpha\beta$ occurs, if indeed it were less than the divisor P; but if it shall be greater, in place of this it may be agreed to take $\alpha\beta - P$ or $\alpha\beta - 2P$, generally $\alpha\beta - nP$, as long as it may be expressed less than P.*

DEMONSTRATION

The remainders α and β may arise from the division of the squares *aa* and *bb* made by the divisor *P*, thus so that there shall become

$$aa = AP + \alpha \text{ and } bb = BP + \beta.$$

Hence there will be

$$aabb = ABP^2 + (A\beta + B\alpha)P + \alpha\beta.$$

Whereby if the square *aabb* may be divided by the divisor *P* , the remainder will be left $\alpha\beta$, or if $\alpha\beta$ may be greater than the divisor *P,* in its place the remainder must be taken, which is left from the division of $\alpha\beta$ made by *P*, which therefore will be either $\alpha\beta - P$, $\alpha\beta - 2P$, $\alpha\beta - 3P$ or generally $\alpha\beta - nP$, thus so that there shall be $\alpha\beta - nP < P$.

COROLLARY 1

14. Therefore if the number α may occur between the remainders, in the same place also $\alpha\alpha$ will occur, and likewise α^3, α^4 etc., and thus all of its powers, if indeed some particular multiple of this kind may be subtracted from the divisor *P*, so that the remainder may become less than the divisor *P*.

COROLLARY 2

15. Therefore with the divisor *P* arising from the prime number $2p+1$ the number of remainders shall be $=p$, if all the powers α^0, α^1, α^2, β^3, α^4 etc. of some one radius *a* may be divided by the same divisor *P*, thence not more than p different remainders can result.

COROLLARY 3

16. Hence it follows the power α^p divided by $P=2p+1$ presents the same remainder, because $\alpha^0=1$, or the remainder to become unity, as I have shown elsewhere [E134], if indeed the divisor $2p+1$ were a prime number.

SCHOLIUM

17. From these remarkable properties, which hence are able to be deduced, I will not tarry to establish here further, since this now shall have been made by me formerly. Those to be put in place here to repeat only the principles more briefly, from which I need to be explaining the properties of some new remainders, from which it may be allowed to demonstrate much more readily the outstanding properties of some numbers. To this end by considering, how indeed it can be seen by itself, how the numbers equivalent to $\alpha\beta-P$, $\alpha\beta-2P$ and in general $\alpha\beta-nP$ with *P* being the with the residue $\alpha\beta$, thus also all the numbers divided by *P* leaving the same remainder in this matter as this can be considered as the remainder itself. Thus in the order of the remainders for some divisor *P* clearly all the square numbers themselves are agreed to occur, since any *aa* of this kind with the form $AP+\alpha$ must be able to be shown and thus truly with the remainder α being estimated to be equivalent. Hence also between the remainders negative numbers will be able to be admitted, since the remainder α may be equivalent to $\alpha-P$, and with this agreed on all the remainders for the numbers smaller than half the divisor *P* will be allowed to be recalled.

18. *If in the order of the remainders arising from the divisor P the two remainders* α *and* β *occur*, *in that also the remainder* $\frac{\alpha+nP}{\beta}$ *will occur with the number n thus assumed, so that* $\frac{\alpha+nP}{\beta}$ *becomes a whole number, since that can always be allowed to happen.*

DEMONSTRATION

Let *aa* and *bb* be these squares, which divided by *P* leave the remainders α and β, so that there shall be

$$aa=AP+\alpha \text{ and } bb=BP+\beta.$$

Now c may be sought*,* so that $c = \frac{a+mP}{b}$ shall be a whole number, and there will be

$$cc = \frac{aa+2amP+mmPP}{bb} = \frac{\alpha+(A+2am+mm)P}{\beta+BP} = \text{a whole number.}$$

Now since the numerator may be considered as the remainder α itself*,* and truly the denominator as the remainder β, it is apparent, if cc may be divided by P, the remainder will go to the reduced form proposed. On putting for the sake of brevity, $A + 2am + mmP = D$*,* so that there shall be $cc = \frac{\alpha+DP}{\beta+BP}$, then truly $\frac{\alpha+nP}{\beta} = \gamma$*,* it is required to be shown $cc = CP + \gamma$*,* so that the remainder from the division of the square cc by the number P arising may produce $= \gamma$. But since there shall be $\alpha = \beta\gamma - nP$*,* certainly there will be able to become :

$$cc = \frac{\beta\gamma+(D-n)P}{\beta+BP} = CP + \gamma,$$

because then there follows:

$$(D-n)P = (\beta C + \gamma B + BCP)P \text{ or } D - n = \beta C + \gamma B + BCP,$$

a relation of this kind between the coefficients of P is completely necessary, so that whole numbers may be produced.

OTHERWISE

In place of the residue α another may be taken being equivalent $\alpha + nP$*,* so that there shall be $\alpha + nP = \beta\gamma$; and since all the squares of this form $(a + mP)^2$ may produce the same remainder α*,* which is assumed to arise from the square aa, m may be assumed thus, so that there becomes $a + mP = bc$; and since the square $bbcc$ divided by P leaves the remainder α or $\beta\gamma$*,* truly the square bb of the remainder is by necessity β*,* so that the square cc may leave the remainder $\gamma = \frac{\alpha+nP}{\beta}$. Indeed there shall become $bbcc = EP + \beta\gamma$ and $bb = BP + \beta$*;* then truly if you deny the square cc is going to give rise to the remainder γ*,* it may provide a different x*,* so that there shall be $cc = CP + x$*;* therefore there will be:

$$bbcc = EP + \beta\gamma = (BP + \beta)(CP + x) = \beta x + (\beta C + Bx + BCP)P.$$

Now with the multiples of the divisor P omitted from both sides, as is accustomed to happen in the estimation of the remainders, if indeed they may be desired in the smallest forms, there will be had $\beta x = \beta\gamma$ and thus $x = \gamma$.

COROLLARY 1

19. Therefore since unity shall be a remainder always, if for the divisor *P* there were some remainder α, then also $\frac{1+nP}{\alpha}$ will occur between the remainders; which if it may be called β, there will be $a\beta = 1+nP$, or the product $\alpha\beta$ between the remainders will be equivalent to unity.

COROLLARY 2

20. Therefore for any remainder α another can be assigned as its reciprocal β, so that $\alpha\beta$ may be equivalent to unity, evidently by taking $\beta = \frac{1+nP}{\alpha}$; and these two will be different reciprocal remainders α and β between each other, unless both were either $+1$ or -1. If indeed there shall be $\beta = \alpha$ and

$$\alpha\alpha = 1+nP = 1+2mP+mmPP,$$

there will become

$$\alpha = \pm(1+mP)$$

and with the multiple of the divisor mP being omitted, $\alpha = \pm 1$.

COROLLARY 3

21. Therefore provided that in the order of the remainders for any remainder its reciprocal is adjoined, in this manner both will be joined together ; but always a single unity will be remaining, then truly also the remainder -1 or $P-1$ occurs just as often between the remainders.

SCHOLIUM

22. This idea of the two reciprocal remainders is of the greatest importance and it will guide us to an easy demonstration of the prettiest theorem, which I have previously shown well enough by many other roundabout ways [E228 & E241], clearly because a prime number of the form $4q+1$ shall be always the sum of two squares. Here it will help to remember the following, if for some divisor *P* the remainders shall be $\alpha,\ \beta,\ \gamma,\ \delta$ etc., the non-remainders truly $\mathfrak{A},\ \mathfrak{B},\ \mathfrak{C},\ \mathfrak{D}$ etc., then all the mutual products of the remainders $\alpha\beta,\ \alpha\gamma$ etc. also to be found [§ 13] between the remainders, but the products of these by some non-remainder, such as $\alpha\mathfrak{A}$, to be found among the non-remainders. But a products from two non-remainders, such as $\mathfrak{A}\mathfrak{B}$, may pass into the order of the remainders.

THEOREM 4

23. *If the divisor P were a prime number of the form* $4q+3$, *then* -1 *or* $P-1$ *certainly is found in the order of non-remainders.*

Since on putting the divisor $P=2p+1$ here there shall be $p=2q+1$ and thus an odd number, the number of all the remainders will be odd. But if -1 may occur in the order of the remainders, for any remainder α there will correspond another remainder $-\alpha$, from which the order of the remainders themselves thus may soon be found :

$$+1,\ +\alpha,\ +\beta,\ +\gamma,\ +\delta \text{ etc.}$$
$$-1,\ -\alpha,\ -\beta,\ -\gamma,\ -\delta \text{ etc.}$$

and therefore there will become an even number of remainders. Therefore since the number of remainders certainly shall be odd, it cannot happen, so that in the order of remainders there may occur -1 or $P-1$; consequently by necessity it must be found in the order of the non-remainders.

COROLLARY 1

24. But if therefore for the prime divisor $P=4q+3$ the number α may occur among the remainders, then the number $-\alpha$ or $P-\alpha$ will be found among the non-remainders ; and in a similar manner, if $-\beta$ were a remainder, then $+\beta$ will be a non-remainder.

COROLLARY 2

25. If the square *aa* divided by the divisor $P=4q+3$ may leave the remainder α, because no squares xx may be given, which provide the remainder $-\alpha$, generally it will be impossible to happen, that any sum of two squares $aa+xx$ may exist divisible by that number $4q+3$.

COROLLARY 3

26. Besides the remainder β may arise from the square *bb,* and because the form βaa gives the remainder $\beta\alpha$, the form αbb truly the remainder $\alpha\beta$, this form $\beta aa-\alpha bb$ will be divisible by the divisor $P=4q+3$.

COROLLARY 4

27. But since no square xx may be given, which gives rise to the remainder $-\beta$, no form of the remainder αxx presents $-\alpha\beta$; therefore no form of this kind $\beta aa+\alpha xx$ will be

divisible by the number $P=4q+3$, if indeed α and β shall be remainders, and α the remainder corresponding to the square *aa*.

COROLLARY 5

28. But since neither this form $\beta aacc+\alpha ccxx$ shall be divisible by $P=4q+3$, unless the square *cc* may admit to being divided, which case can be excluded at will, since *aacc* can correspond to some other remainder besides α; from which by writing *dd* and *yy* in place of *aacc* and *ccxx,* no form of this kind $\beta dd+\alpha yy$ can be shown to be divisible by the number $P=4q+3$, while α and β shall be remainders.

SCHOLIUM

29. So that this may be seen more clearly, we may run through some prime numbers of the form $4q+3$ and thence we may represent the negative remainders by subtracting $4q+3$ from the greater half, so that the lower half remainders may be found and thence it may be apparent no remainder α and likewise the negative $-\alpha$ may occur in the order of the remainders [see the table in § 12, to which this table is a continuation]:

Divisor	Remainder
3	1
7	$1, -3, +2$
11	$1, \ +4, \ -2, \ +5, \ +3$
19	$1, +4, +9, \ -3, +6, \ -2, \ -8, +7, +5$
23	$1, \ +4, \ +9, \ -7, \ +2, \ -10, \ +3, \ -5, \ -11, \ +8, \ +6$
31	$1, \ +4, \ +9, \ -15, \ -6, \ +5, \ -13, \ +2, \ -12, \ +7, \ -3, \ -11, \ +14, \ +10, \ +8.$

Here it is evident among the remainders all the numbers not greater than the half the divisor occur affected either by a + or − sign, but none occur affected by both the signs. Hence if the signs may be changed of these individual remainders, it will be added to the order of the non-remainders. Hence for the divisor 31 the following forms can be shown never divisible by 31:

$$aa+bb,\ aa-15bb,\ aa-6bb,\ aa+5bb,\ aa-13bb,\ aa+2bb,\ aa+7bb,$$
$$aa-3bb,\ aa-11bb,\ aa+14bb,\ aa+10bb.$$

And in general, if α and β shall be any two remainders, no form of this kind

$$\alpha aa+\beta bb$$

admits to division by 31 .

THEOREM 5

30. *If the divisor P were a prime number of the form* $4q+1$, *then the number* -1 *or* $P-1$ *certainly will be found in the order of the remainders.*

DEMONSTRATION

The remainder shall be some α, and also its reciprocal will be $\frac{1}{\alpha}$ or $\frac{1+nP}{\alpha}$ (§ 19), so that, unless it shall be either $\alpha=+1$ or $\alpha=-1$, it will be different from α, thus so that with these two cases excepted, for any remainder α there may respond its reciprocal, which shall be α', different from α; where it may be observed of α' its reciprocal will be in turn α. Whereby if -1 may not be found among the remainders, all the remainders thus may be represented by two reciprocal remainders taken together

$$\begin{array}{l} 1,\ \alpha,\ \beta,\ \gamma,\ \delta \text{ etc.} \\ \quad \alpha',\beta',\ \gamma',\ \delta' \text{ etc.} \end{array}$$

and thus, since all shall be different, the number of all the remainders shall be odd. But since the divisor shall be a prime of the form $4q+1$, the number of all the remainders is $2q$ and thus is even; from which by necessity it follows among all the remainders also, the number -1 or $P-1$ occurs, because otherwise the number of remainders would be odd.

COROLLARY 1

31. Therefore since for the prime divisor $P=4q+1$ the number -1 certainly may be found among the remainders, if some other remainder were α, among the remainders $-\alpha$ will occur also.

COROLLARY 2

32. If therefore the square *aa* divided by the prime divisor $4q+1$ may leave the remainder α, another will give the square *bb,* because the remainder $-\alpha$ will be produced, from which the sum $aa+bb$ of these squares certainly will be divisible by the prime number $4q+1$.

COROLLARY 3

33. Because all the remainders arise from the squares, of which the roots do not surpass half the divisor, for any proposed square *aa* always another *bb* can be shown not greater than *4qq*, so that the sum $aa+bb$ may be produced divisible by $4q+1$.

COROLLARY 4

34. If $1+aa$ may admit a division by $4q+1$, then also $bb+aabb$ and hence $bb+(ab-(4q+1)n)^2$ will grant a division ; and thus with the other square *bb* assumed as it pleases, the other $(ab-(4q+1)n)^2$ is found easily.

COROLLARY 5

35. If the sum of these two squares $aa+bb$ were divisible by $4q+1$, then also $aaxx+bbxx$ and hence also this form

$$(ax-(4q+1)m)^2+(bx-(4q+1)n)^2$$

will admit division. But *x* is allowed always to be assumed thus, so that the other root $ax-(4q+1)m$ may be equal to the given number *c* by assuming $x=\frac{c+(4q+1)m}{a}$, which can be found always in integers .

SCHOLIUM 1

36. For any prime divisor, whither it be of the form $4q+1$ or $4q+3$, a consideration of the number of reciprocals merits all attention, since thence as we have elucidated this significant truth easily, because for some proposed prime number of the form $4q+1$, it may be able to show that the sum of two squares always to be divisible by that. Therefore since besides it shall be able to demonstrate the sum of two squares cannot admit divisors, unless they themselves shall be the sums of two squares, in the manner of Fermat's Theorem, so that all prime numbers of the form $4q+1$ shall be the sum of two squares, the demonstration is resolved much more expediently, as indeed has been established by me at one time [E228]. But just as the reciprocal numbers may themselves be had for some divisor *P*, while the reciprocal α of some number is $\frac{1+nP}{\alpha}$, that may be understood more clearly from the examples added below :

Divisor	Pairs of Reciprocal Remainders
3	
5	2 3 [$=\frac{5+1}{2}$, or $3\times 2=6\equiv 1(\bmod 5)$]
7	2, 3 4, 5 [$4\times 2=8\equiv 1(\bmod 7); 5\times 3=15\equiv 1(\bmod 7), \text{etc.}$]
11	2, 3, 5, 7 6, 4, 9, 8
13	2, 3, 4, 5, 6 7, 9, 10, 8, 11
17	2, 3, 4, 5, 8, 10, 11

	9, 6, 13, 7, 15, 12, 14
19	2, 3, 4, 6, 7, 8, 9, 14 10, 13, 5, 16, 11, 12, 17, 15
23	2, 3, 4, 5, 7, 9, 11, 13, 15, 17 12, 8, 6, 14, 10, 18, 21, 16, 20, 19
29	2, 3, 4, 5, 7, 8, 9, 12, 14, 16, 18, 19, 23 15, 10, 22, 6, 25, 11, 13, 17, 27, 20, 21, 26, 24

These individual reciprocal pairs thus are connected together, so that any single number may receive only a single reciprocal, evidently by division smaller, just as we have assumed in the theorem.

SCHOLIUM 2

37. So that if therefore the first divisor were of the form $4q+1$, we may see, how the remaining second remainders according to this law of the reciprocals are themselves going to be disposed :

Divisor	Remainders [or residues]
5	$\underline{1,\ 4}$ $1,-1$
13	$\underline{1,\ 4,\ 9,\ \ 3,\ 12,\ 10}\left[i.e. 16\equiv 3(\bmod 13); 25\equiv 12(\bmod 13),\text{etc.}\right]$ 1, 4, 9, 12 10, 3, (-1) $\left[i.e. 4\times 10=40\equiv 1(\bmod 13),\text{etc.}\right]$
17	$\underline{1,\ 4,\ 9,\ 16,\ \ 8,\ 2,\ 15,\ 13}$ 1, 4, 9, 8, 16 13, 2, 15, (-1)
29	$\underline{1,\ 4,\ 9,\ 16,\ 25,\ 7,\ 20, 6,\ 23,\ 13,\ 5,\ 28,\ 24,\ 22}$ 1, 4, 9, 16, 25, 6, 23, 28 22,13, 20, 7, 5, 24, (-1)
37	$\underline{1,\ 4,\ 9,\ 16,\ 25,\ 36,\ 12,\ 27,\ 7,\ 26,\ 10,\ 33,\ 21,\ 11,\ 3,\ 34,\ 30,\ 28}$ 1, 4, 9, 16, 25, 12, 27, 26, 21, 36 28, 33, 7, 3, 34, 11, 10, 30, (-1)

It is seen from these examples, since the number one shall be alone and each of the remaining remainders may have its reciprocal adjoined, the number of remainders is going to be odd, unless besides unity another remainder of one may added, which itself will be the same reciprocal. Therefore since in these cases in which the divisor is a prime number of the form $4q+1$, the number of remainders certainly is $=2q$, it is necessary that besides unity the remainder $4q$ or -1 shall occur, certainly the reciprocal of which itself is equal. From which the truth of this significant theorem, of which the demonstration otherwise was with the greatest difficulty, certainly it becomes evident, which is evident, as often as the divisor shall be a prime number of the form $4q+1$, the number $4q$ or -1 may occur always among the remainders.

SCHOLIUM 3

38. Hence just as it is apparent the number -1 is to be found among the remainders, whenever the divisor were a prime number of the form $4q+1$, thus for some other prime number s the form of the prime divisors are to be assigned, but cannot yet be demonstrated, so that the same number s may be found in the remainders. This theorem is of this kind :

If a prime divisor were of the form $4ns+(2x+1)^2$ with s being some prime number, then the numbers $+s$ and $-s$ occur in the remainders;

and another theorem similar to this :
If a prime divisor were of the form $4ns-(2x+1)^2$ with s being some prime number, then the numbers $+s$ occurs in the remainders, $-s$ in the non-remainders.

But when in turn $-s$ may occur in the remainders, but $+s$ in the non-remainders, thus it cannot be defined in general. But for the particular cases the matter thus is understood to be had thus:

So that there shall be	the prime divisor must be
$\begin{Bmatrix} -2 \text{ remainder} \\ +2 \text{ non}-\text{remainder} \end{Bmatrix}$	$P=8n+3$
$\begin{Bmatrix} -3 \text{ remainder} \\ +3 \text{ non}-\text{remainder} \end{Bmatrix}$	$P=12n+7$
$\begin{Bmatrix} -5 \text{ remainder} \\ +5 \text{ non}-\text{remainder} \end{Bmatrix}$	$P=20n+3,7$
$\begin{Bmatrix} -7 \text{ remainder} \\ +7 \text{ non}-\text{remainder} \end{Bmatrix}$	$P=28n+11,\ 15,\ 23$
$\begin{Bmatrix} -11 \text{ remainder} \\ +11 \text{ non}-\text{remainder} \end{Bmatrix}$	$P=52n+7,\ 11,\ 19, 25,\ 31, 47$
$\begin{Bmatrix} -13 \text{ remainder} \\ +13 \text{ non}-\text{remainder} \end{Bmatrix}$	$P=52n+7,\ 11,\ 19,\ 25, 31, 47$
$\begin{Bmatrix} -17 \text{ remainder} \\ +17 \text{ non}-\text{remainder} \end{Bmatrix}$	$P=68n+3,\ 7,\ 11,\ 23,\ 27,\ 31,\ 39,\ 63$

$\left\{\begin{matrix}-19 \text{ remainder}\\ +19 \text{ non}-\text{remainder}\end{matrix}\right\}$	$P = 76n + 7,\ 11,\ 19,\ 23,\ 35,\ 39,\ 43,\ 47,\ 55,\ 63$
$\left\{\begin{matrix}-23 \text{ remainder}\\ +23 \text{ non}-\text{remainder}\end{matrix}\right\}$	$p = 92n + 3,\ 23,\ 27,\ 31,\ 35,\ 39,\ 47,\ 55,\ 59,\ 71,\ 75,\ 87$

The consideration of which cases gives rise to this theorem :

If a prime divisor were of the form $4ns - 4z - 1$ *with all the values excluded contained in the form* $4ns - (2x+1)^2$ *, with s being a prime number, then* $-s$ *will occur in the residues, but* $+s$ *will be a non-residue.*

To which theorems above this can be added on:

If the first divisor were of the form $4ns + 4z + 1$ *with all the values contained in the form* $4ns + (2x+1)^2$ *being excluded, with s a prime number, then both* $+s$ *as well as* $-s$ *occur in the non-residues.*

Therefore I attach these theorems, so that those who take delight in speculations of this kind, who may inquire into the demonstration of these, since there shall be no doubt, why the theory of numbers thence may not be going to gain a significant advance.

CONCLUSION

39. These four latter theorems, the demonstration of which is desired still, can be shown in the following concise form:

With some prime number s present only the odd squares 1, 9, 25, 49 *etc. may be divided by the divisor 4s and the residues may be noted, which all will be of the form* $4q+1$, *any of which may be indicated by the letter a, but of the remaining numbers of the form* $4q+1$, *which do not occur among the residues, any of which may be indicated by the letter* $\mathfrak{A}$ *; with which done there shall become :*

prime number divisor of the form	*while there is*
$4ns + \alpha$	$+s$ *residue and* $-s$ *residue*
$4ns - \alpha$	$+s$ *residue and* $-s$ *non-residue*
$4ns + \mathfrak{A}$	$+s$ *non-residue and* $-s$ *non-residue*
$4ns - \mathfrak{A}$	$+s$ *non-residue and* $-s$ *non-residue.*

OBSERVATIONES
CIRCA DIVISIONEM QUADRATORUM
PER NUMEROS PRIMOS

Opuscula analytica 1, 1783, p. 64-84 [E552]

HYPOTHESIS

1. *Si numerorum a, b, c, d etc. quadrata* a^2, b^2, c^2, d^2 *etc. per numerum quempiam primum P dividantur, residua in divisione relicta litteris cognominibus graecis* α, β, γ, δ *etc. indicemus.*

COROLLARIUM 1

2. Cum ergo quadratum *aa* per numerum *P* divisum relinquat residuum *α,* posito quoto $= A$ erit $aa = AP + \alpha$ ideoque $aa - \alpha$ divisibile erit per *P;* similique modo hae expressiones $bb - \beta$, $cc - \gamma$, $dd - \delta$ etc. divisibiles erunt per eundem divisorem *P.*

COROLLARIUM 2

3. Quadrata $(a+P)^2$, $(a+2P)^2$, $(a+3P)^2$ et in genere $(a+nP)^2$ idem residuum α relinquent, si per numerum propositum *P* dividantur. Unde patet numerorum divisore *P* maiorum quadrata eadem praebere residua, quae ex quadratis numerorum divisore *P* minorum nascuntur.

COROLLARIUM 3

4. Cum deinde quadratum $\left(P-a\right)^2$ per *P* divisum idem praebeat residuum, quod quadratum a^2, patet, si fuerit $a > \frac{1}{2}P$, fore $P - a < \frac{1}{2}P$. Unde manifestum est omnia residua diversa ex quadratis numerorum, qui semisse divisoris *P* sint minores, resultare.

COROLLARIUM 4

5. Quare si omnia residua desiderentur, quae ex divisione quadratorum per datum divisorem *P* proveniunt, sufficiet ea tantum quadrata considerasse, quorum radices semissem ipsius *P* non superent.

COROLLARIUM 5

6. Hinc si divisor sit $P = 2p + 1$, si per eum omnes numeri quadrati 1, 4, 9, 16, 25 etc. dividantur, plura residua diversa inde prodire nequeunt, quam unitates in numero *p* continentur, eaque resultant ex quadratis numerorum 1, 2, 3, 4, ... *p;* sequentium enim

numerorum $p+1$, $p+2$, $p+3$ etc. quadrata eadem residua ordine retrogrado reproducunt.

SCHOLION

7. Manifestum hoc inde est, quod haec duo quadrata p^2 et $(p+1)^2$ per numerum $2p+1$ divisa idem praebent residuum, siquidem eorum differentia per $2p+1$ est divisibilis. Generatim enim, quorumcumque numerorum differentia $M-N$ per $2p+1$ est divisibilis, necesse est, ut uterque *M* et *N* seorsim divisus idem residuum relinquat. Hinc etiam, cum sit

$$(p+2)^2-(p-1)^2=3(2p+1),$$

utrumque quadratum seorsim, $(p+2)^2$ et $(p-1)^2$, idem residuum praebere debet et in genere quadratum $(p+n+1)^2$ idem residuum dabit, quod quadratum $(p-n)^2$. Hoc igitur ostenso perspicuum est plura residua resultare non posse, quam in numero *p* unitates continentur; utrum autem haec residua omnia sint diversa an quaepiam inter se conveniant, hinc non definitur; atque adeo, si divisores quicumque admittantur, utrumque evenire potest. Sin autem divisor $2p+1$ fuerit numerus primus, omnia illa residua erunt inter se diversa, quod sequenti modo demonstro.

THEOREMA 1

8. *Si divisor* $P=2p+1$ *fuerit numerus primus per eumque omnia quadrata* 1, 4, 9, 16, ... *usque ad* p^2 *dividantur, omnia residua hinc resultantia inter se erunt diversa eorumque adeo multitudo p.*

DEMONSTRATIO

Sint *a* et *b* duo numeri quicumque ipso *p* minores vel saltem non maiores ac demonstrandum est, si eorum quadrata a^2 et b^2 per numerum primum $2p+1$ dividantur, residua certe diversa esse proditura. Si enim idem praeberent residuum, eorum differentia $aa-bb$ per $2p+1$ foret divisibilis ideoque ob $2p+1$ numerum primum et $aa-bb=(a+b)(a-b)$ alter horum factorum per $2p+1$ divisibilis esse deberet. Cum autmn sit tam $a<p$ quam $b<p$, saltem non $a>p$, summa $a+b$ multoque magis differentia $a-b$ divisore $2p+1$ est minor; indeque neutra per $2p+1$ divisibilis esse potest. Ex quo manifesto sequitur omnia quadrata, quorum radices non sint ipso *p* maiores, per numerum primum $2p+1$ divisa certe diversa residua esse relictura.

COROLLARIUM 1

9. Quodsi ergo omnia quadrata 1, 4, 9, 16 etc. per numerum primum $2p+1$ dividantur omniaque residua diversa notentur, eorum numerus neque maior erit neque minor quam *p,* sed huic numero *p* praecise aequalis.

COROLLARIUM 2

10. Omnia vero haec residua diversa numero p oriuntur ex totidem quadratis in serie naturali primum occurrentibus, scilicet 1, 4, 9, 16, ... *pp,* neque ex sequentibus maioribus ulla nova residua eliciuntur.

COROLLARIUM 3

11. Non omnes ergo numeri ipso divisore $2p+1$ minores inter residua occurrent, sed tantum tot eorum, quot unitates continentur in divisoris minori semisse $p.$ Quare, cum numerorum divisore $2p+1$ minorum multitudo sit $=2p$, horum alter semissis tantum in ordine residuorum reperietur, alter vero inde penitus excluditur.

SCHOLION

12. Numeros hos divisore primo $2p+1$ minores, qui ex ordine residuorum excluduntur, nomine *non-residuorum* indicabo, quorum ergo multitudo semper numero residuorum est aequalis. Hoc discrimen inter residua et non-residua probe perpendisse iuvabit, quare pro divisoribus aliquot primis minoribus tam residua quam non-residua hic exhibebo.

Divisor 3, $p=1$	Divisor 5, $p=2$	Divisor 7, $p=3$
Quadratum 1	Quadrata 1, 4	Quadrata 1, 4, 9
Residuum 1	Residua 1, 4	Residua 1, 4, 2
Non-residuum 2	Non-residua 2, 3	Non-residua 3, 5,6

Divisor 11, $p=5$	Divisor 13, $p=6$
Quadrata 1, 4, 9, 16, 25	Quadrata 1, 4, 9, 16, 25, 36
Residua 1, 4, 9, 5, 3	Residua 1, 4, 9, 3, 12, 10
Non-residua 2, 6, 7, 8, 10	Non-residua 2, 5, 6, 7, 8, 11

Divisor 17, $p=8$
Quadrata 1, 4, 9, 16, 25, 36, 49, 64
Residua 1, 4, 9, 16, 8, 2, 15, 13
Non-residua 3, 5, 6, 7, 10, 11, 12, 14

Divisor 19, $p=9$
Quadrata 1, 4, 9, 16, 25, 36, 49, 64, 81
Residua 1, 4, 9, 16, 6, 17, 11, 7, 5
Non-residua 2, 3, 8, 10, 12, 13, 14, 15, 18

Circa haec residua et non-residua pro quovis divisore primo tam memorabiles proprietates observantur, quas eo maiori studio perpendisse operae est pretium, quod inde non contemnenda incrementa in numerorum Theoriam redundare videntur.

THEOREMA 2

13. *Si in ordine residuorum ex divisore P ortorum occurrant numeri α et β, ibidem quoque occurret eorum productum $\alpha\beta$ siquidem minus fuerit divisore P;sin autem sit maius, eius loco capi convenit $\alpha\beta - P$ vel $\alpha\beta - 2P$ vel generatim $\alpha\beta - nP$, donec infra P deprimatur.*

DEMONSTRATIO

Oriantur residua α et β ex divisione quadratorum *aa* et *bb* per divisorem *P* facta, ita ut sit

$$aa = AP + \alpha \text{ et } bb = BP + \beta.$$

Hinc erit

$$aabb = ABP^2 + (A\beta + B\alpha)P + \alpha\beta.$$

Quare si quadratum *aabb* per divisorem *P* dividatur, residuum relinquetur $\alpha\beta$, vel si $\alpha\beta$ superet divisorem *P,* eius loco sumi debet residuum, quod ex divisione ipsius $\alpha\beta$ per *P* facta relinquetur, quod proinde erit vel $\alpha\beta - P$ vel $\alpha\beta - 2P$ vel $\alpha\beta - 3P$ vel generatim $\alpha\beta - nP$, ita ut sit $\alpha\beta - nP < P$.

COROLLARIUM 1

14. Si ergo inter residua occurrat numerus *a,* ibidem quoque occurret *aa* item a^3, a^4 etc. omnesque adeo eius potestates, siquidem a singulis eiusmodi multiplum divisoris *P* subtrahatur, ut residuum minus fiat divisore *P.*

COROLLARIUM 2

15. Cum igitur existente divisore *P* numero primo $2p+1$ residuorum numerus sit $= p$, si unius cuiuspiam residui *a* omnes potestates α^0, α^1, α^2,β^3, α^4 etc. per eundem divisorem *P* dividantur, inde non plura quam *p* residua diversa resultare possunt.

COROLLARIUM 3

16. Hinc sequitur potestatem α^p per $P = 2p+1$ divisam idem praebere residuum, quod $\alpha^0 = 1$, seu residuum fore unitatem, uti alibi ostendi, siquidem divisor $2p+1$ fuerit numerus primus.

SCHOLION

17. Eximiis proprietatibus, quae hinc deduci possunt, hic uberius evolvendis non immoror, cum hoc iam olim a me sit factum. Ea hic tantum principia breviter repetere constitui, quibus indigeo ad novas quasdam residuorum affectiones explicandas, unde insignes nonnullas numerorum proprietates multo expeditius demonstrare liceat. Hunc in

finem animadverto, quod quidem per se est perspicuum, quemadmodum residuo $\alpha\beta$ aequivalent numeri $\alpha\beta - P,\ \alpha\beta - 2P$ et in genere $\alpha\beta - nP$ existente *P* divisore, ita etiam omnes numeros per *P* divisos idem residuum relinquentes in hoc negotio tamquam hoc ipsum residuum spectari posse. Ita in ordine residuorum pro quocumque divisore *P* omnes plane numeri quadrati ipsi occurrere sunt censendi, cum quilibet *aa* huiusmodi forma $AP + \alpha$ exhiberi queat ideoque vero residuo α aequivalere sit existimandus. Hinc etiam inter residua numeri negativi admitti poterunt, cum residuo α aequivaleat $\alpha - P$, hocque pacto omnia residua ad numeros semisse divisoris *P* minores revocare licebit.

18. *Si in ordine residuorum ex divisore P ortorum occurrant bina residua* α *et* β, *in eo quoque occurret residuum* $\frac{\alpha+nP}{\beta}$ *numero n ita assumto, ut* $\frac{\alpha+nP}{\beta}$ *fiat numerus integer, id quod semper fieri licet.*

DEMONSTRATIO

Sint *aa* et *bb* ea quadrata, quae per *P* divisa relinquunt residua α et β, ut sit $aa = AP + \alpha$ et $bb = BP + \beta$.
Iam quaeratur *c,* ut sit $c = \frac{a+mP}{b}$ numerus integer, eritque

$$cc = \frac{aa+2amP+mmPP}{bb} = \frac{\alpha+(A+2am+mm)P}{\beta+BP} = \text{numero integro.}$$

Cum nunc numerator tamquam ipsum residuum α, denominator vero tamquam residuum β spectari possit, patet, si *cc* per *P* dividatur, residuum ad formam propositam reductum iri. Posito enim brevitatis gratia $A + 2am + mmP = D$, ut sit $cc = \frac{\alpha+DP}{\beta+BP}$, tum vero $\frac{\alpha+nP}{\beta} = \gamma$, ostendi oportet fore $cc = CP + \gamma$, ut residuum ex divisione quadrati *cc* per numerum *P* natum prodeat $= \gamma$. Cum autem sit $\alpha = \beta\gamma - nP$, utique fieri poterit

$$cc = \frac{\beta\gamma+(D-n)P}{\beta+BP} = CP + \gamma,$$

quoniam inde sequitur

$$(D-n)P = (\beta C + \gamma B + BCP)P \text{ seu } D - n = \beta C + \gamma B + BCP,$$

cuiusmodi relatio inter coefficientes ipsius *P* omnino necessaria est, ut numeri integri prodeant.

ALITER

Loco residui α aliud aequivalens accipiatur $\alpha + nP$, ut sit $\alpha + nP = \beta\gamma$; et cum omnia quadrata huius formae $(a + mP)^2$ idem praebeant residuum α, quod ex quadrato *aa* nasci assumitur, sumatur *m* ita, ut fiat $a + mP = bc$; et quia quadratum *bbcc* per *P* divisum relinquit residuum α vel $\beta\gamma$, quadratum vero *bb* residuum β, necesse est, ut quadratum *cc* relinquat residuum $\gamma = \frac{\alpha+nP}{\beta}$. Sit enim $bbcc = EP + \beta\gamma$ et $bb = BP + \beta$ *;* tum vero si neges quadratum *cc* praebiturum esse residuum *γ,* praebeat diversum *x,* ut sit $cc = CP + x$ *;* erit ergo

$$bbcc = EP + \beta\gamma = (BP + \beta)(CP + x) = \beta x + (\beta C + Bx + BCP)P.$$

Iam multiplis divisoris *P* utrimque omissis, quemadmodum in aestimatione residuorum fieri solet, siquidem in minima forma desiderentur, habebitur $\beta x = \beta\gamma$ ideoque $x = \gamma$.

COROLLARIUM 1

19. Cum igitur unitas semper sit residuum, si pro divisore *P* fuerit aliquod residuum *α,* tum etiam $\frac{1+nP}{\alpha}$ inter residua occurret; quod si vocetur *β,* erit $a\beta = 1 + nP$*,* seu inter residua productum $\alpha\beta$ unitati aequivalebit.

COROLLARIUM 2

20. Pro quolibet ergo residuo α aliud quasi eius reciprocum β assignari potest, ut $\alpha\beta$ unitati aequivaleat, sumendo scilicet $\beta = \frac{1+nP}{\alpha}$; atque haec duo residua reciproca α et β inter se erunt diversa, nisi ambo fuerint vel + 1 vel −1. Si enim sit $\beta = \alpha$ et

$$\alpha\alpha = 1 + nP = 1 + 2mP + mmPP,$$

erit

$$\alpha = \pm(1 + mP)$$

et multiplum divisoris *mP* omittendo $\alpha = \pm 1$.

COROLLARIUM 3

21. Dum igitur in ordine residuorum cuilibet residuo suum reciprocum adiungitur, hoc modo bina copulabuntur; semper autem unitas solitaria relinquetur, tum vero etiam residuum −1 seu $P - 1$, quoties quidem inter residua occurrit.

SCHOLION

22. Idea haec binorum residuorum reciprocorum maximi est momenti et ad demonstrationem facilem Theorematis pulcerrimi nos manuducet, quod alias per satis multas ambages demonstraveram, scilicet quod numerus primus formae $4q + 1$ semper sit summa duorum quadratorum. Ceterum hic meminisse iuvabit, si pro quopiam divisore *P* residua sint $\alpha,\ \beta,\ \gamma,\ \delta$ etc., nonresidua vero $\mathfrak{A},\ \mathfrak{B},\ \mathfrak{C},\ \mathfrak{D}$ etc., tum residuorum omnia producta mutua $\alpha\beta,\ \alpha\gamma$ etc. etiam inter residua reperiri [§ 13], eorum autem producta per quodpiam non-residuum, veluti $\alpha\mathfrak{A}$, inter non-residua esse referenda. At producta ex binis non-residuis, uti $\mathfrak{A}\mathfrak{B}$, in ordinem residuorum transeunt.

THEOREMA 4

23. *Si divisor P fuerit numerus primus formae* $4q+3$, *tum* -1 *seu* $P-1$ *certe in ordine non-residuorum reperitur.*

Cum posito divisore $P=2p+1$ hic sit $p=2q+1$ ideoque numerus impar, numerus omnium residuorum erit impar. At si -1 in ordine residuorum occurreret, cuilibet residuo α responderet aliud residuum $-\alpha$, unde ordo residuorum ita se esset habiturus

$$\begin{array}{l} +1,\ +\alpha,\ +\beta,\ +\gamma,\ +\delta \text{ etc.} \\ -1,\ -\alpha,\ -\beta,\ -\gamma,\ -\delta \text{ etc.} \end{array}$$

foretque ergo numerus residuorum par. Cum igitur numerus residuorum certo sit impar, fieri nequit, ut in ordine residuorum occurrat -1 seu $P-1$; consequenter in ordine non-residuorum necessario reperiri debet.

COROLLARIUM 1

24. Quodsi ergo pro divisore primo $P=4q+3$ inter residua occurrat numerus α, tum numerus $-\alpha$ seu $P-\alpha$ certe inter non-residua reperietur; similique modo, si $-\beta$ fuerit residuum, tum $+\beta$ erit non-residuum.

COROLLARIUM 2

25. Si quadratum *aa* per divisorem $P=4q+3$ divisum relinquat residuum α, quia nullum datur quadratum *xx,* quod praebeat residuum $-\alpha$, fieri omnino nequit, ut ulla summa duorum quadratorum $aa+xx$ per numerum illum $4q+3$ divisibilis existat.

COROLLARIUM 3

26. Oriatur praeterea residuum β ex quadrato *bb,* et quia forma βaa residuum dat $\beta\alpha$, forma vero αbb residuum $\alpha\beta$, haec forma $\beta aa-\alpha bb$ per divisorem $P=4q+3$ erit divisibilis.

COROLLARIUM 4

27. Cum autem nullum detur quadratum *xx,* quod residuum praebeat $-\beta$, nulla datur forma αxx residuum praebens $-\alpha\beta$; nulla [ergo] huiusmodi forma $\beta aa+\alpha xx$ per numerum $P=4q+3$ erit divisibilis, siquidem α et β sint residua et α residuum quadrato *aa* respondens.

COROLLARIUM 5

28. Cum autem neque haec forma $\beta aacc+\alpha ccxx$ per divisorem $P=4q+3$ sit divisibilis, nisi quadratum *cc* divisionem admittat, qui casus sponte excluditur, quadrato *aacc* quodcumque aliud residuum praeter α respondere potest; unde loco *aacc* et *ccxx* scribendo *dd* et *yy* nulla huiusmodi forma

$$\beta dd+\alpha yy$$

exhiberi potest per numerum $P=4q+3$ divisibilis, dum α et β sint residua.

SCHOLION

29. Quo haec clarius perspiciantur, percurramus quosdam numeros primos formae $4q+3$ ac residua eius semisse maiora subtrahendo inde $4q+3$ negative repraesentemus, ut infra semissem revocentur indeque pateat nullius residui α negativum $-\alpha$ simul in ordine residuorum occurrere:

Divisor	Residua
3	1
7	1,−3, +2
11	$1,\ +4,\ -2,\ +5,\ +3$
19	1, +4, +9, -3, +6, -2, -8, +7, +5
23	$1,\ +4,\ +9,\ -7,\ +2,\ -10,\ +3,\ -5,\ -11,\ +8,\ +6$
31	$1,\ +4,\ +9,\ -15,\ -6,\ +5,\ -13,\ +2,\ -12,\ +7,\ -3,\ -11,\ +14,\ +10,\ +8.$

Hic evidens est inter residua omnes numeros semisse divisoris non maiores occurrere vel signo + vel −affectos, nullum autem bis utroque signo affectum occurrere. Hinc si singulorum horum residuorum signa mutentur, ordo non-residuorum complebitur. Hinc pro divisore 31 sequentes formae exhiberi possunt numquam per 31 divisibiles:

$$aa+bb,\ aa-15bb,\ aa-6bb,\ aa+5bb,\ aa-13bb,\ aa+2bb,\ aa+7bb,$$
$$aa-3bb,\ aa-11bb,\ aa+14bb,\ aa+10bb.$$

Atque in genere, si α et β sint duo quaecumque residua, nulla huiusmodi forma

$$aaa+\beta bb$$

per numerum 31 divisionem admittet.

THEOREMA 5

30. *Si divisor P fuerit numerus primus formae* $4q+1$, *tum numerus* -1 *seu* $P-1$ *certe in ordine residuorum reperitur.*

DEMONSTRATIO

Sit *a* residuum quodcumque eritque etiam eius reciprocum $\frac{1}{\alpha}$ seu $\frac{1+nP}{\alpha}$ residuum

(§ 19), quod, nisi sit vel $\alpha = +1$ vel $\alpha = -1$, ab α erit diversum, ita ut exceptis his duobus casibus cuilibet residuo α respondeat suum reciprocum, quod sit α', ab α diversum; ubi notetur ipsius α' reciprocum vicissim esse α. Quare si -1 inter residua non reperiretur, omnia residua ita repraesentari possent binis reciprocis coniungendis

$$\begin{array}{l} 1,\ \alpha,\ \beta,\ \gamma,\ \delta \text{ etc.} \\ \ \ \alpha',\ \beta',\ \gamma',\ \delta' \text{ etc.} \end{array}$$

sicque, cum omnia sint diversa, numerus omnium residuorum foret impar. Cum autem divisor sit numerus primus formae $4q+1$, numerus omnium residuorum est $2q$ ideoque par; unde necessario sequitur inter residua quoque numerum -1 seu $P-1$ occurrere, quia alioquin numerus residuorum foret impar.

COROLLARIUM 1

31. Cum ergo pro divisore primo $P = 4q+1$ numerus -1 certe inter residua reperiatur, si aliud residuum quodcumque fuerit α, inter residua etiam occurret $-\alpha$.

COROLLARIUM 2

32. Si igitur quadratum *aa* per divisorem primum $4q+1$ divisum relinquat residuum α, aliud dabitur quadratum *bb,* quod residuum praebebit $-\alpha$, unde horum quadratorum summa *aa* + *bb* certe erit per numerum primum $4q+1$ divisibilis.

COROLLARIUM 3

33. Quoniam omnia residua ex quadratis; quorum radices semissem divisoris non superant, nascuntur, quadrato quocumque proposito *aa* aliud semper *bb* non maius quam *4qq* exhiberi potest, ut summa $aa+bb$ prodeat divisibilis per $4q+1$.

COROLLARIUM 4

34. Si $1+aa$ divisionem per $4q+1$ admittat, tum etiam $bb+aabb$ ac proinde quoque $bb+(ab-(4q+1)n)^2$ divisionem admittet; sicque altero quadrato *bb* pro lubitu assumto alterum $(ab-(4q+1)n)^2$ facile reperitur.

COROLLARIUM 5

35. Si haec duorum quadratorum summa $aa+bb$ per divisorem $4q+1$ fuerit divisibilis, tum etiam $aaxx+bbxx$ ac proinde quoque haec forma

$$(ax-(4q+1)m)^2+(bx-(4q+1)n)^2$$

divisionem admittet. Semper autem *x* ita assumere licet, ut alterius radix

$ax-(4q+1)m$ dato numero c aequetur sumendo $x=\frac{c+(4q+1)m}{a}$, quod semper in integris fieri potest.

SCHOLION 1

36. Pro quovis divisore primo, sive sit formae $4q+1$ sive $4q+3$, numerorum reciprocorum consideratio omnem attentionem meretur, cum inde tam facile hanc insignem veritatem elicuerimus, quod proposito numero primo quocumque formae $4q+1$ semper summae binorum quadratorum exhiberi queant per illum divisibiles. Cum igitur demonstrari praeterea possit summam duorum quadratorum alios non admittere divisores, nisi qui ipsi sint summae duorum quadratorum, hoc modo Theorematis FERMATIANI, quod omnes numeri primi formae $4q+1$ sint duorum quadratorum, aggregata, demonstratio multo expeditius absolvitur, quam quidem olim a me est factum. Quemadmodum autem numeri reciproci pro quovis divisore P se habeant, dum cuiusvis numeri α reciprocus est $\frac{1+nP}{\alpha}$, ex subiunctis exemplis clarius intelligetur:

Divisor	Reciprocorum paria
3	
5	2 3
7	2, 3 4, 5
11	2, 3, 5, 7 6, 4, 9, 8
13	2, 3, 4, 5, 6 7, 9, 10, 8, 11
17	2, 3, 4, 5, 8, 10, 11 9, 6, 13, 7, 15, 12, 14
19	2, 3, 4, 6 ' 7, 8, 9, 14 10, 13, 5, 16, 11, 12, 17, 15
23	2, 3, 4, 5, 7, 9, 11, 13, 15, 17 12, 8, 6, 14, 10, 18, 21, 16, 20, 19
29	2, 3, 4, 5, 7, 8, 9, 12, 1'4, 16, 18, 19, 23 15, 10, 22, 6, 25, 11, 13, 17, 27, 20, 21, 26, 24

Singula haec paria reciproca ita inter se sunt connexa, ut quilibet numerus unicum tantum recipiat reciprocum, divisore scilicet minorem, prorsus uti in Theoremate assumsimus.

SCHOLION 2

37. Quodsi ergo divisor primus fuerit formae $4q+1$, videamus, quomodo residua secundum hanc legem reciprocorum disposita se sint habitura:

Divisor	Residua
5	1, 4
	1, (−1)
13	1, 4, 9, 3, 12, 10
	1, 4, 9, 12 10, 3, (−1)
17	1, 4, 9, 16, 8, 2, 15, 13
	1, 4, 9, 8, 16 13, 2, 15, (−1)
29	1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22
	1, 4, 9, 16, 25, 6, 23, 28 22, 13, 20, 7, (−1)
37	4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28
	4, 9, 16, 25, 12) 27, 26, 21, 36 28, 33, 7, 3, 34, 11, 10, 30, (−1)

Ex his exemplis perspicuum est, cum unitas sit solitaria et reliquorum residuorum quodque suum reciprocum habeat adiunctum, numerum residuorum futurum esse imparem, nisi praeter unitatem aliud residuum solitarium accederet, quod sibi ipsi esset reciprocum. Quoniam igitur his casibus, quibus divisor est numerus primus formae $4q+1$, numerus residuorum certo est par $=2q$, necesse est, ut praeter unitatem residuum $4q$ vel -1 occurrat, cuius quippe reciprocum ipsi est aequale. Unde veritas insignis istius Theorematis, cuius demonstratio alioquin maxime erat difficilis, admodum fit perspicua, quod scilicet, quoties divisor sit numerus primus formae $4q+1$, inter residua semper occurrat numerus $4q$ vel -1.

SCHOLION 3

38. Quemadmodum hinc patet numerum -1 inter residua reperi, quoties divisor fuerit numerus primus formae $4q+1$, ita pro quovis alio numero primo s divisorum primorum forma assignari, at nondum demonstrari potest, ut iste numerus s in residuis reperiatur. Cuiusmodi est hoc Theorema:

Si divisor primus fuerit formae $4ns+(2x+1)^2$ *existente s numero primo, tum in residuis occurrent numeri* $+s$ *et* $-s$ *;*
alterumque huic simile:
Si divisor primus fuerit $4ns-(2x+1)^2$ *existente s numero primo, tum in residuis occurret numerus + s, at* $-s$ *erit in* non-residuis.

Quando autem vicissim $-s$ occurrat in residuis, at $+s$ in non-residuis, ita in genere definiri nequit. Pro casibus autem particularibus res ita se habere deprehenditur:

Ut sit	divisor primus debet esse

$\left.\begin{cases} -2 \text{ residuum} \\ +2 \text{ non} - \text{residuum} \end{cases}\right\}$	$P = 8n + 3$
$\left.\begin{cases} -3 \text{ residuum} \\ +3 \text{ non} - \text{residuum} \end{cases}\right\}$	$P = 12n + 7$
$\left.\begin{cases} -5 \text{ residuum} \\ +5 \text{ non} - \text{residuum} \end{cases}\right\}$	$P = 20n + 3, 7$
$\left.\begin{cases} -7 \text{ residuum} \\ +7 \text{ non} - \text{residuum} \end{cases}\right\}$	$P = 28n + 11,\ 15,\ 23$
$\left.\begin{cases} -11 \text{ residuum} \\ +11 \text{ non} - \text{residuum} \end{cases}\right\}$	$P = 52n + 7,\ 11,\ 19, 25,\ 31, 47$
$\left.\begin{cases} -13 \text{ residuum} \\ +13 \text{ non} - \text{residuum} \end{cases}\right\}$	$P = 52n + 7,\ 11,\ 19,\ 25, 31, 47$
$\left.\begin{cases} -17 \text{ residuum} \\ +17 \text{ non} - \text{residuum} \end{cases}\right\}$	$P = 68n + 3,\ 7,\ 11,\ 23,\ 27,\ 31,\ 39,\ 63$
$\left.\begin{cases} -19 \text{ residuum} \\ +19 \text{ non} - \text{residuum} \end{cases}\right\}$	$P = 76n + 7,\ 11,\ 19,\ 23,\ 35,\ 39,\ 43,\ 47,\ 55,\ 63$
$\left.\begin{cases} -23 \text{ residuum} \\ +23 \text{ non} - \text{residuum} \end{cases}\right\}$	$p = 92n + 3,\ 23,\ 27,\ 31,\ 35,\ 39,\ 47,\ 55,\ 59,\ 71,\ 75,\ 87$

Quorum casuum contemplatio hoc suppeditat Theorema:

Si divisor primus fuerit formae $4ns - 4z - 1$ *excludendo omnes valores in forma* $4ns - (2x+1)^2$ *contentos, existente s numero primo, tum in residuis occurret* $-s$*, at* $+ s$ *erit non-residuum.*

Quibus Theorematibus insuper hoc adiungi potest:

Si divisor primus fuerit formae $4ns + 4z + 1$ *excludendo omnes valores in forma* $4ns + (2x+1)^2$ *contentos, existente s numero primo, tum tam* $+ s$ *quam* $-s$ *in non-residuis occurret.*

Theoremata haec ideo subiungo, ut, qui huiusmodi speculationibus delectantur, in eorum demonstrationem inquirant, cum nullum sit dubium, quin inde Theoria numerorum insignia incrementa sit adeptura.

CONCLUSIO

39. Quatuor haec Theoremata postrema, quorum demonstratio adhuc desideratur, sequenti modo concinnius exhiberi possunt:

Existente s numero quocumque primo dividantur tantum quadrata imparia 1, 9, 25, 49 *etc. per divisorem 4s notenturque residua, quae omnia erunt formae* $4q+1$, *quorum quodvis littera a indicetur, reliquorum autem numerorum formae* $4q+1$, *qui inter residua non occurrunt, quilibet littera* $\mathfrak{A}$ *indicetur; quo facto si fuerit*

divisor numerus	*tum est*
primus formae	
$4ns+\alpha$	$+s$ *residuum et* $-s$ *residuum*
$4ns-\alpha$	$+s$ *residuum et* $-s$ *non-residuum*
$4ns+\mathfrak{A}$	$+s$ *non-residuum et* $-s$ *non-residuum*
$4ns-\mathfrak{A}$	$+s$ *non-residuum et* $-s$ *non-residuum*