REGARDING THE CRITERIA OF THE EQUATION $fxx + gyy = hzz$, WHETHER OR NOT THAT MAY ADMIT A RESOLUTION

[E556]
Opuscula analytica 1, 1783, p. 211-241

1. It is required to know whether or not it is possible for an equation of this kind, $fxx + gyy = hzz$, according to the relation which exists between the numbers *f, g* and *h*, to be varied to accept rational numbers, and thus integers for *x, y* and *z,* as fractions may be changed easily into integers. Thus it is known this equation : $xx + yy = 2zz$ to be possible, but truly this one : $xx + yy = 3zz$ to be impossible. But when the letters *f, g* and *h* hold greater values, the judgement is put in place with difficulty, whether or not the equation may be possible ; truly with large numbers it scarcely appears able to be undertaken. Therefore here I have decided to inquire into certain criteria, from which it may be allowed to judge, whether or not this equation shall be possible, however great the numbers *f, g* and *h* will have become.

2. But first of all it will help to have observed the following :

I. Not only do I assume the numbers *f,* g and *h* to be integers, but also they are not squares, nor also are they divisible by squares; for if the number *f* had a square factor, this would be able to be involved with the square *xx*, which reasoning also is required to be extended to the rest.

II. Besides it is allowed to assume both negative and positive numbers equally ; and since the equation thus can always be set out, so that the members *fxx* and *hzz* may obtain positive values always, only the member *gyy* is left, which will be able to have positive or negative values.

III. The numbers *f* and *g* may be considered as prime between themselves; if indeed they may have a common divisor *d,* or the same number *h* must be had , in which case that will be removed by division, or the quantity *z* may be divisible by *d* . From which if in place of *z* we may write *dv,* our equation may be reduced to this form : $fxx + gyy = dhvv$, thus so that now *f* and *g* shall become prime between themselves.

IV. And finally the cases arising are to be noted especially, in which our equation shall be possible. Clearly in the first place this comes about, if there were either $h = f$ or $h = g$; truly in the first case there would become $y = 0$ and $z = x$, truly in the latter $x = 0$ and $z = y$. Then truly also the case will be clear enough, if there were $h = f + g$, because for that requiring to be satisfied, $z = x = y$. But the cases will be less obvious, in which $h = faa + gbb$; for then there may become $x = a$, $y = b$ and $z = 1$.

3. But first I will investigate, with the numbers *f* and *g* given, what kind of numbers *k* may be able to be put in place , so that the equation may become possible. Whereby since here we may regard *h* as an unknown number, we may refer our equation to this form : $fxx + gyy = szz$, so that now it may be required for suitable values for the letter *s* to be investigated, from which the equation may become possible, and indeed everything for this which may be outstanding ; which I add at the end of the following theorem.

THEOREM 1

If the equation $fxx + gyy = hzz$ *were possible for the case* $s = h$, *thus so that the letters x, y, z may now be known , truly if in addition this equation* $pp + fgqq = krr$ *may be had, then our equation will be possible also in the case* $s = hk$.

DEMONSTRATION

For these two equations may be multiplied together, and this new equation will be produced :

$$hkrrzz = (fxx + gyy)(pp + fgqq) = f(px \pm gqy)^2 + g(py \mp fqx)^2.$$

Whereby if we may put:

$$rz = Z,\ px \pm gqy = X \text{ et } py \mp fqx = Y,$$

this equation entirely similar to the proposed arises:

$$fX^2 + gY^2 = hkZ^2$$

COROLLARY 1

4. But if therefore the letters *p* and *q* may be allowed to be assumed thus, so that *k* may contain the factor *h*, evidently $k = hl$, then on account of $s = hhl$, a suitable new value will be $s = l$, since the square *hh* can be omitted.

COROLLARY 2

5. Therefore just as from that suitable value $s = h$ another has been elicited $s = hk$ or $s = l$, thus from this in a like manner another new value, for example $s = m$, and hence again a new value $s = n$ will be able to have arisen; and this determination will be allowed to continue indefinitely. Thus, from some known case, innumerable others will be able to be derived.

COROLLARY 3

6. If it may arise that the numbers h and k may have a common divisor d, then the new value hk will have the factor dd, which therefore will be able to be removed. In this manner it will be allowed continually to come upon smaller suitable numbers s , then finally we may be led to an obvious case.

COROLLARY 4

7. Hence if at this stage we may have been unsure, whether h shall be a suitable value of s, however by preceding in this manner we may finally arrive at the case in point, with care we will be able to conclude also the case $s = h$ to be possible. But if this may not succeed in any way, or finally a case of this kind may arrive at in smaller numbers, of which the impossibility may be apparent, also the value $s = h$ itself will be required to be considered impossible.

THEOREM 2

8. *If three possible cases* $s = h$, $s = h'$ and $s = h''$ *may be known for our equation, then also a suitable value will be* $s = hh'h''$.

DEMONSTRATION

Therefore since we may have three equations of this kind, which shall be

$$\text{I. } faa + gbb = hcc,$$
$$\text{II. } fAA + gBB = h'CC,$$
$$\text{III. } f\alpha\alpha + g\beta\beta = h''\gamma\gamma;$$

the first may be multiplied into the second, and the product will be :

$$hh'ccCC = (faa + gbb)(fAA + gBB) = (faA \pm gbB)^2 + fg(aB \mp bA)^2.$$

Now we may make

$$cC = r, \quad faA \pm gbB = p, \text{ and } aB \mp bA = q,$$

so that this product may become

$$pp + fgqq = hh'rr,$$

which multiplied anew into the third equation will give such a product :

$$hh'h''rr\gamma\gamma = (f\alpha\alpha + g\beta\beta)(pp + fgqq) = f(p\alpha \pm gq\beta)^2 + g(p\gamma \mp fq\alpha)^2;$$

since which form plainly shall agree with the proposed, the truth of the theorem is evident, and the case $s = hh'h''$ will be possible.

COROLLARY 1

9. Therefore from the three suitable values $h,\ h',\ h''$ a fourth can be found easily. And if perhaps these three may have common divisors, in this way it will be allowed to pertain continually to new smaller values.

COROLLARY 2

10. Therefore if we may indicate this new value by the letter h''', then suitable values will be also $s = hh'h''',\ s = hh''h''',\ s = h'h''h'''$; from which again in a similar manner more others are able to be deduced.

COROLLARY 3

11. But when these new values may be deprived of squares, as we have indicated before, they return continually to the same known values. Indeed since there shall be $h''' = hh'h''$, the form $hh'h'''$ is reduced to h'', truly this one $hh''h'''$ to h' and $h'h''h'''$ to h, thus so that actually only one new case may be found in this manner.

THEOREM 3

12. *If our equation* $fxx + gyy = szz$ *may satisfy the case* $s = h$, *then also all these values will be satisfied :*

$$s = 4fg + h,\ s = 8fg + h,\ s = 12fg + h,\ s = 16fg + h \text{ etc.},$$

and indeed these also, if h *were a large enough number,*

$$s = h - 4fg,\ s = h - 8fg,\ s = h - 12fg \text{ etc.},$$

and in general, $s = h \pm 4nfg$, *provided these numbers were prime.*

The demonstration of this most elegant theorem is still desired, after it has been investigated previously in vain several times now; the difficulty of this matter clearly is concerned with this, because all these numbers then finally must satisfy the question, when they are prime numbers. Indeed when they are composite, it can happen that they may not be satisfying the condition, even if they may not always be eliminated from the search. But since here only prime numbers must prevail, it is proper to consider negative numbers, which can result from the formula $s = h - 4fg$, not requiring to be prime numbers. Whereupon this will be the most outstanding matter to be considered at first, upon which the demonstration of this theorem to be found will succeed.

COROLLARY 1

13. Since in this manner perhaps it may be allowed to progress by increasing to infinity, also a multitude of suitable values for *s*, as far there as it will be able to be added, where it will be able to be constructed, as far as the table of prime numbers [Euler had shown how to construct such a table in E467].

COROLLARY 2

14. Thus since this equation $xx + yy = zz$ shall be possible, where there is $f = 1$, $g = 1$ and $s = h = 1$, this form $4n + 1$, evidently as far as it gives rise to prime numbers, also will give supply just as many suitable values for *s*, which numbers are :

1, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc.

But all these numbers themselves are equal to the sum of two squares, which now has been demonstrated by me most rigorously some time ago [E241], from which one is less bound to be driven to despair by demonstrating the rest of the cases. Therefore for all these cases it will be allowed to assume $z = 1$. Yet meanwhile hence also it will be allowed to find composite numbers for *s*, while by the first theorem the products from two or more of these numbers themselves will prevail also for *s*, because in this case the two formulas $fxx + gyy$ and $pp + fgqq$ agree.

COROLLARY 3

15. Because in the case $s = 341$ it will be possible for the equation $2xx + 3yy = szz$ to be satisfied, likewise the formula $341 \pm 24n$ will give the other outstanding cases, evidently as often as they will give rise to prime numbers. Hence therefore by decreasing, the following values arise

341, 317, 293, 269, 197, 173, 149, 101, 53, 29, 5.

But all these numbers themselves now are contained in the form $2xx + 3yy$, thus so that there shall be able to be $z = 1$.

SCHOLION

16. With this theorem, as if it may have been demonstrated, in the first place, for some cases of the numbers *f* and *g* plainly all the values of s suitable letter *s* will be able to be found easily. But towards showing this, it will be required to treat two separate cases: the former, where $f = 1$ and on that account the first terms of the first theorem agree between themselves ; truly the latter, where *f* is not unity. From which at first we may set out the equation $xx + gyy = szz$.

PROBLEM I

I7. *For the proposed equation* $xx + gyy = szz$*, to find all the suitable values for s, from which this equation is possible to emerge.*

SOLUTION

Here it is evident a suitable value to be $s = g$; while indeed there becomes $x = 0$ and $y = z$. For even if 4*g*, 9*g*, 16*g* etc. may be equally satisfactory, yet by reducing the square all may be returned to *g*. Truly on assuming $y = 0$, all the square numbers for *s* will be produced, which therefore all will be allowed to be reduced to unity. But besides these themselves also they are satisfied by the same numbers 4*ng* either increased or diminished, evidently as far as so that they will produce prime numbers, here it is not allowed to neglect these squares. But from these we need only these squares, which were prime to the number 4*g*, because otherwise no prime numbers thence will emerge; on account of which, at once all the even squares hence are excluded, and only with these odd primes is the place conceded, the roots of which were prime to the number *g*. Therefore here unity occurs always, while truly nine also, unless *g* shall be divisible by 3, again also 25, unless *g* may have the divisor 5, etc. But when these squares exceed the number 4*g*, in place of these the remainders left may be written from the division by 4*g*. Hence therefore we may put in place the formulas :

$$4ng + 1,\ 4ng + a,\ 4ng + b,\ 4ng + c,\ 4ng + d \text{ etc.,}$$

where clearly *a, b, c, d* etc. are these remainders, which result with the squares divided by 4*g*. Truly besides these cases another obviously is $s = 1 + g$, if indeed *g* were an even number; but if it were odd, there may be taken $s = 4 + g$, so that evidently a number may be had prime to the number 4*g*. Then truly because by the first theorem the products from the two satisfying numbers also are satisfying, in addition we will have these formulas themselves by writing *h* in place or $1 + g$ or $4 + g$

$$s = 4ng + h,\ 4ng + ah,\ 4ng + bh,\ 4ng + ch,\ 4ng + dh \text{ etc.,}$$

all which values we may set out thus to be seen taken together :

$$s = 4ng + \begin{pmatrix} 1, & a, & b, & c, & d \text{ etc.} \\ h, & ah, & bh, & ch, & dh \text{ etc.} \end{pmatrix}.$$

All the formulas prevail so far, in as much as they produce prime numbers, and in this manner plainly all the suitable prime numbers will be found; moreover placed together clearly they work with no difficulty, since they arise from two or more suitable prime numbers. Indeed also it will be required to enumerate the number *g* itself and the products by the numbers now found.

COROLLARY 1

18. Because the truth of this solution clearly has not yet been established, we will consider some obvious cases, which we will understand always to be contained in some of the above formulas. Thus the case $s = 1 + 4g$ will be contained in the formula $4ng + 1$ and $s = 1 + 9g$ will be contained in the formula $4ng + h$, if there were $h = 1 + g$; but if $h = 4 + g$, in that there will be contained $s = 4 + 9g$. And in a similar manner the property itself is found in the formulas
$1 + 16g,\ 1 + 25g,\ 1 + 36g$ or $4 + g,\ 4 + 9g,\ 4 + 25g$ etc., where we exclude these cases, which are unable to produce prime numbers.

COROLLARY 2

19. This solution equally has a place, whether g shall be a positive or negative number. But because in this latter case in the formulas found the letter h obtains a negative value, in place of the terms *h, ah, bh, ch* etc. the complements of these may be written for the number $4g$.

COROLLARY 3

20. In the case, where g is a negative number, if now it were found from the formulas above, which prevail for the formula $xx - gyy$, if the signs may be changed there, or if in place of the numbers 1, *a, b, c, d* etc. their complements to $4g$ may be written, then these may be used for this equation $gyy - xx = szz$.

SCHOLIUM

21. But these will be illustrated especially and will be able to be called into use more easily, if we may adjoin several examples, from which also the nature of the numbers and other more abstruse properties will be seen more clearly.

EXAMPLE 1

Let $g = 1$ and the proposed equation shall be $xx + yy = szz$, and here a single formula $4n + 1$ is had for the values of s. But in the case $1 + g = 2$, because it is not prime to $4g$, it cannot be connected to the general formula ; yet meanwhile by itself it presents the suitable number $= 2$. Therefore for the satisfying prime numbers besides 2 we will have the greater series :

$$1,\ 5,\ 13,\ 17,\ 29,\ 37,\ 41 \text{ etc.},$$

and the products from any of these will produce all the satisfying composite numbers.

But for the case $g = -1$ or from the equation $xx - yy = szz$ besides the form $4n + 1$ arising from the square the formula $4 + g = 3$ will give this in addition $4n + 3$. And thus all the prime numbers will be contained in either of these two formulas $4n+1$ and $4n+3$, and thus plainly in this case all the prime numbers are suitable, certainly all which may be allowed to be resolved into the difference of two squares. Hence indeed 2 is excluded, since it cannot be the difference of two squares ; but still a value can be given for *s*, if indeed an even number may be assumed for *z*. For certainly $2\cdot 4$ is $9-1$.

EXAMPLE 2

22. Now let $g=2$ and this proposed form $xx+2yy=szz$, where since there shall be $4g=8$, the odd squares 1, 9, 25 etc. all are reduced to the same form $8n+1$; but the case $1+g=k=3$ gives this form $8n+3$ in addition, and thus all the prime numbers may be referred to this kind : $8n+(1,3)$, to which in addition there is added $s=g=2$, and thus all these prime numbers are :

1, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97 etc.

But if there shall become $g=-2$, for the formula $xx-2yy=szz$ there is found $s=8n+(1,7)$, for which -2 must be taken into account, and hence in turn for the equation $2yy-xx=szz$ there will be $s=8n+(7,1)$. Therefore the same numbers prevail for the two latter cases.

EXAMPLE 3

23. For the formula $xx+3yy=szz$ the following given precept produces $s=12n+(1,7)$, and in addition the solitary number 3. But for the formula $xx-3yy=szz$ there is found $s=12n+(1)$.

EXAMPLE 4

For the formula $xx+5yy=szz$ there is found $s=20n+(1,9)$, with the number 5; but for the formula $xx-5yy=szz$ there is found $s=20n+(1,19)$, with the number -5.

EXAMPLE 5

For the formula $xx+6yy=szz$ there is found $s=24n+(1,7)$, together with the number 6; but for the formula $xx-6yy=szz$ there is deduced $s=24+(1,19)$, together with the number -6, where the numbers ± 6 are to be regarded as prime, even if between themselves they shall be composite.

SCHOLIUM

24. We will not set out more examples of this kind, since the calculation shall be clear enough, but rather we add the following table, in which for any formula $xx+gyy=szz$

we will show at first the form of the prime numbers for *s*, then truly the prime numbers themselves as far as to one hundred ; with which known all the products satisfied, both from two or more prime numbers, for the value of the letter *s*:

$xx + yy = szz$	$s = 4n + 1$ with 2
Prime nos.	1, 2, 5, 13, 17, 29, 37, 41 etc.
$xx - yy = szz$	$s = 4n + (1,3)$
Prime nos.	1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 etc.
$xx + 2yy = szz$	$s = 8n + (1,3)$ with 2
Prime nos.	2; 1, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97
$xx - 2yy = szz$	$s = 8n + (1,7)$ with -2
Prime nos.	− 2; 1, 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97
$xx + 3yy = szz$	$s = 12n + (1,7)$ with 3
Prime nos.	3; 1, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97
$xx - 3yy = szz$	$s = 12n + 1$ with the solitary -3
Prime nos.	−3; 1, 13, 37, 61, 73, 97
$xx + 5yy = szz$	$s = 20n + (1,9)$ with the number 5
Prime nos.	5; 1, 29, 41, 61, 89
$xx - 5yy = szz$	$s = 20n + (1,9,11,19)$ with the number -5
Prime nos.	−5; 1, 11, 19, 29, 31, 41, 59, 61, 71, 79, 89
$xx + 6yy = szz$	$s = 24n + (1,7)$ with the number 6
Prime nos.	6; 1, 7, 31, 73, 79, 97
$xx - 6yy = szz$	$s = 24n + (1,19)$ with -6
Prime nos.	−6; 1, 19, 43, 67, 73, 97
$xx + 7yy = szz$	$s = 28n + (1, 11, 23, 9, 25, 15)$ with the number 7
Prime nos.	7; 1, 11, 23, 29, 37, 43, 53, 67, 71, 79
$xx - 7yy = szz$	$s = 28n + (1, 9, 25)$ with -7
Prime nos.	−7; 1, 29, 37, 53
$xx + 10yy = szz$	$s = 40n + (1, 9, 11, 19)$ with 10
Prime nos.	10; 1, 11, 19, 41, 59, 89
$xx - 10yy = szz$	$s = 40n + (1, 9, 31, 39)$ with -10
Prime nos.	−10; 1, 31, 41, 71, 79, 89
$xx + 11yy = szz$	$s = 44n + \begin{pmatrix} 1, 9, 25, 5, 37, \\ 15, 3, 23, 31, 27 \end{pmatrix}$ with 11
Prime nos.	1, 3, 5, 23, 31, 37, 47, 53, 59, 67, 71, 89, 97
$xx - 11yy = szz$	$s = 44n + (1, 9, 25, 5, 37)$ with -11
Prime nos.	−11; 1, 5, 37, 53, 89, 97

PROBLEM 2

25. *For the proposed equation* $fxx + gyy = szz$ *, to find all the prime numbers, which produce suitable values for s, from which this possible equation emerges.*

SOLUTION

Let *h* be some suitable value for *s* and by the theorem while not yet shown it is apparent all the prime numbers contained in this formula $4nfg + h$, prevail equally for *s*; from which it is evident that same value *h* must be prime to 4*fg*. But such a value is readily found. If indeed both the numbers *f* and *g* were odd, there can be taken $h = 4f + g$ or $h = f + 4g$ *;* but if either of the numbers *f* and *g* were even, the other odd, a suitable value will be found $h = f + g$. But when in addition all the prime numbers, and thus everything may be obtained for *s*, the formula $pp + fgqq = krr$ may be considered, and thus in the preceding problem we may now assign primes prevailing for *k*, which shall become $4nfg + (1,\ a,\ b,\ c,\ d \text{ etc.})$; now these two equations may be multiplied by each other and now we have shown to produce a form of this kind *hkrrzz* or $hkZ^2 = fX^2 + g\mathrm{Y}^2$, on account of which the product *hk* also will give a suitable value for *s;* from which it is understood all the prime numbers suitable for *s* to be contained in this general form

$$s = 4nfg + (h,\ ah,\ bh,\ ch,\ dh \text{ etc.}).$$

But with the prime numbers known prevailing *s*, which satisfy our equation $fxx + gyy = szz$, if in addition all the prime numbers being used for *k* may be known, which shall be *A, B, C, D* etc., then the products of the former found for *s* into the individual terms, whether the second or third etc of these latter terms, will produce also suitable values for *s,* and therefore in this way an infinitude of values of the letter *x* to be shown.

COROLLARY 1

26. If it may happen, that the first value found for *h* shall be a square, then, since this may be present in the order of the numbers 1, *a, b, c, d* etc., the same values for *s* are found, which have been assigned for *k*.

COROLLARY 2

27. But if the number *h* may not be present in the order 1, *a, b, c, d* etc., then in no way can it happen, that the values for *s* and *k* may agree with each other, but all in turn will differ from each other.

EXAMPLE 1

28. The equation shall be proposed $2xx+3yy=szz$, where $f=2$ and $g=3$, but first the value $h=5$. Therefore the equation $pp+6qq=krr$ then may be considered, and we see the prime values for k to be contained in this formula $24n+(1,7)$. Therefore with these numbers 1, 7 multiplied by $h=5$ all the prime numbers for s may be found in this formula $24n+(5,11)$, which are 5, 11, 29, 53, 59, 83 etc.

For the equation $2xx-3yy=szz$, where $f=2$ and $g=-3$, the known value is found $h=-1$ or $h=23$; but for the equation $pp-6qq=krr$, for k this formula is found $24n+(1,19)$, from which all the prime numbers for s become : $24n+(5,23)$, which formula presents these prime numbers: 5, 23, 29, 47, 53, 71 etc.

Truly of this equation $3xx-2yy=szz$, where for $f=3$ and $g=-2$, the value h becomes $=1$; and because the formula $pp-6qq=krr$ is the same as before, also the same prime numbers are held in the for s in formula $24n+(1,19)$ and hence the prime numbers themselves $24n+(1,19)$, which therefore become : 19, 43, 67, 73 etc.

EXAMPLE 2

29. For the proposed equation $2xx+5yy=szz$, where $f=2$ and $g=5$, the first value h becomes $=7$, and since for the equation $pp+10qq=krr$ the formula arises :

$$40n+(1,\ 9,\ 11,\ 19)\ ,$$

and for the prime values of s we will have :

$$s=40n+(7,\ 23,\ 37,\ 13),$$

therefore these prime numbers will be 7, 13, 23, 37, 47, 53 etc.

But for the proposed equation $2xx-5yy=szz$ at once there becomes $h=-3$; and because for the equation $pp-10qq=krr$ we find the formula $40n+(1,\ 9,\ 31,\ 39)$, the prime numbers sought will be contained in this formula

$$40n+(37,\ 13,\ 27,\ 3)\ ;$$

therefore the prime numbers themselves will be 3, 13, 37, 43, 53, 67, 83 etc.

Finally for the formula $5xx-2yy=szz$ on account of $h=3$ from the same numbers k the values for s are :

$$40n+(37,\ 13,\ 27,\ 3).$$

SCHOLIUM 1

30. Up to this point, all the prime numbers being satisfied for *s*, which now have been treated, and from which examples have been shown, which multiplied into each other in turn, as we have presented, give equally satisfying composite numbers. Hence truly plainly neither always may all the suitable composite numbers be obtained for *s,* but cases may be given, for which in addition other prime numbers may be introduced into composite values of *s*. The cause of this situation consists in that, since we have excluded even numbers at once in the above investigation, which yet are able to be satisfactory taken together with other prime numbers sought. Therefore we may put at once for these requiring to be elicited $s=2h$, so that there shall be

$$\frac{fxx+gyy}{2}=hzz.$$

So that if now this formula $\frac{fxx+gyy}{2}$ may produce an odd number or the product from an odd into an even square, from that at once it is allowed to elicit infinitely many other values for *h*. Indeed let α be an odd number of this kind, and since for the form $xx+fgyy=szz$ all the prime values of *s* may be held in the form $4fg+(1,\ a,\ b,\ c,\ d\ \text{etc.})$, all the suitable prime numbers for our letter *h* will be held in this form :

$$4fg+(\alpha,\ \alpha a,\ \alpha b,\ \alpha c,\ \alpha d\ \text{etc.}),$$

which if they were different from these, which we have pursued before, also will have infinitely many other prime numbers, which are able to enter into the composition of the number *s*. Indeed these individual numbers, which we may designate by the letters *A, B, C, D* etc., multiplied by 2, will produce suitable values for *s,* which therefore will be 2*A,* 2*B,* 2*C,* 2 *D* etc. and because the products from two of those also may be satisfied , the odd prime numbers *AB, AC, AD, BC, BD, CD* etc. thus may arise. Thus in the example $xx-3yy=szz$ the formula $\frac{xx-3yy}{2}$ gives at once -1. Therefore since in the case found the formula shall be $s=12n+1$, for the values of h we will have the formula $12n-1$ or $12n+11$, which provides these prime numbers

11, 23, 47, 59, 71, 83,

which doubled also are satisfactory, and also the products from two of those, then truly also the products from these by the individual terms of these, which we have now assigned before ; and with this agreed on a multitude of composite values may be increased vigorously. This arises especially from these cases used, where the formulas found above will be constructed from fewer members. Moreover, for the formula $xx+7yy=szz$ its half $\frac{xx+7yy}{2}$ produces 4, or if $1=\alpha$, which value since now it may be present in the above given formula, hence new values do not arise. But truly the formula $\frac{xx-7yy}{2}$ presents $\alpha=-3$ and thus the values for *h* will be $28n+(1,\ 9,\ 25)$, which numbers now occur before. Therefore it is required for anyone to observe this properly, who would wish to investigate also all the composite numbers satisfying s, from which it would be superfluous for me to tarry over this matter.

SCHOLIUM 2

31. But however great these may seem to be outstanding, certainly this will be painful, because they have not yet been provided with firm demonstrations, an account of this matter chiefly may be considered in that place, because the formulas found for s so far only prevail, in as much as prime numbers are supposed. Though all the labours undertaken by me have dashed my hopes, yet I hope all my trials for those, who delight in speculations of this kind, may not be thankless, especially since now I have raised that difficulty publically, concerned with prime numbers, so that now without doubt the approach to this mystery of numbers may be seen to be rendered somewhat easier.

PROPOSITION 1

32. *If there were* $fxx+gyy=szz$, *with s being some prime number, then if all the squares may be divided by this number s and the remainders arising from the individual terms may be noted, among these* $-fg$ *will occur always, or if with the negative removed,* $s-fg$.

DEMONSTRATION

These remainders shall arise from the division by s : 1, a, b, c, d etc. and the square xx may give the remainder a, truly the square yy the remainder b, and it is evident the number $fa+gb$ to become divisible by s. Therefore there shall become $fa+gb=\lambda s$, and there will become $gb=\lambda s-fa$ and thus $bg^2=\lambda gs-fga$. Now since all of the remainders multiplied by a square, may again occur among the remainders, indeed they may be decreased to be below s, and thence the remainder c may be produced, thus so that there shall be $c=\lambda gs-fga$, and with the multiple of s itself removed, $c=-fga$ or $c=s-fga$, and because this prevails equally with all the remainders, assuming unity in place of a we will have $c=-fg$ or $c=s-fg$.

COROLLARY I

33. If therefore the value $s=h$ may be satisfactory, because the formula $4nfg+h$, if it were a prime number, also may be satisfactory for s, if all the squares may be divided by this number, $-fg$ certainly may occur among the remainders.

COROLLARY 2

34. Let that divisor $=D$, and because the square is given, which shall be *pp,* from which the remainder $-fg$ is generated, it is evident the formula $pp+fg$ to become divisible by *D.*

COROLLARY 3

35. But now here that condition of the prime number clearly involves a difficulty, because the order of the remainders mentioned here is not given, unless *D* shall be a prime number. For certainly it may be able, so that $-fg$ may not occur among the remainders, if the divisor may not be a prime.

PROPOSITION 2

36. *If, by dividing squares by some prime number* $D=2P+1$, *if the number r occurs among the remainders, then its power* r^P *divided by D will leave unity; and in turn, if* r^P-1 *may have the divisor D, by necessity the number r is to be found among the remainders.*

DEMONSTRATION

Since the divisor *D* may be put $=2P+1$, the number of divisors smaller than itself is 2*P;* because only half of these approach as remainders, the number of remainders shall be *P.* Then also it is certain, if the number *r* may occur among the remainders, then also all its powers must occur in that place, just as the simplest $r^0=1$ belongs there : On account of which the power r^P by necessity cannot produce a new remainder. And hence it is duly concluded the first remainder to be produced thence ought to be 1, and thus it is agreed the power proposed r^P, divided by the prime number *D*, to leave a remainder $=1$.

So that pertaining to the converse of the proposition, we may consider the formula $r^{2P}-1$ always to be divisible by $2P+1$, from which it follows either the formula r^P-1 or r^P+1 must be divisible. Therefore all the numbers taken for *r*, for which the latter formula r^P+1 becomes divisible, are excluded from the order of the remainders, and only those, which produce r^P-1 remaining divisible formulas ; since the number of these shall be *P,* it follows all the numbers *r* to become remainders.

COROLLARY 1

37. Since the prime divisor will become $=h$, we may put $h=2p+1$, and because $r=-fg$, it follows the formula $(-fg)^P-1$ to be divisible by $h=2p+1$, or there becomes

$r^P=1+m(2p+1)$. Then since also the divisor may be able to be $h+4nfg$, as long as it was a prime number, on account of $h=2p+1$, we may make

$$D=2p+1+4nfg=2P+1 \ ,$$

thus so that there shall be $P=p+2nfg$, and also this power

$$(-fg)^P=(-fg)^{p+2nfg}$$

becomes divisible by the divisor $2p+1+4nfg$ diminished by one.

COROLLARY 2

38. On account of which the whole matter is reduced to this, so that by putting for the sake of brevity $-fg=r$ there may be shown, if the formula r^p-1 were divisible by $2p+1$, then also this formula $r^{p+2nr}-1$ to become divisible by $2p+1+4nr$, if indeed the number $2p+1+4nr$ were a prime number.

COROLLARY 3

39. If we may put $r=-1$, it is clear the formula $(-1)^p-1$ cannot be divided by $2p+1$, unless p shall be an even number. Therefore there shall be $p=2q$ and $4q+1$ shall be a prime number, then certainly $4q$ will be found among the remainders. Let the square, from which this remainder arises, be $=vv$, and $vv+1$ will be divisible by $4q+1$. Thus from these reckonings it will appear most easily always to give the sum of two squares divisible by the number $4q+1$, that which is accustomed to be shown at last by other more round about ways.

40. Moreover with these put in place, which depend on principles not yet established well enough, we may enquire more precisely by certain principles into the nature of equations of this kind $fxx+gyy=szz$. And indeed in the first place we have shown more rigorously now, if this equation were possible in the case $s=h$, then by taking the number k, thus so that there shall be $pp+fgqq=krr$, a suitable value for s also becomes $s=hk$. Therefore on this premise we may progress to the following.

THEOREM 4

41. *If the equation* $fxx+gyy=hzz$ *were possible, then such a formula* $tt+fg$ *can be assigned always, divisible by* h, *thus so that the number t shall be less than* $\frac{1}{2}h$.

DEMONSTRATION

Since that formula $fxx+gyy$ shall be divisible by h, if that may be multiplied by the formula $fpp+gqq$, the product also will be divisible by h. Therefore the numbers p and q may be taken always, so that there shall be $py-qx=1$, that which always can happen, unless x and y may have a common divisor, but which case hence is excluded at once ; but then, from that $(fpx+gqy)^2+fg$ will be produced,

$$[\text{recall : } (fxx+gyy)(fpp+gqq)=(fpx+gqy)^2+fg(py-qx)^2.]$$

from which on taking $t=fpx+gqy$ the formula $tt+fg$ will be had divisible by h. But here we may put $t=t'\pm\lambda h$, and then this formula $t't'+fg$ even now will be divisible by h. Truly in this manner t' may become less than half the number h ; consequently it will give for sure the formula $tt+fg$ divisible by h, in which t may not exceed half of h itself.

COROLLARY 1

42. This same property of the number h, which depends only on the product fg, and extends equally to the equation $xx+fgyy=hzz$. Indeed, if the product fg may be able to be resolved into two factors ζ and η, the same condition is established, so that the equation $\zeta xx+\eta yy=hzz$ shall be possible.

COROLLARY 2

43. Therefore as often as the number h were a divisor of the formula $tt+fg$,thence it cannot be concluded always that the equation $fxx+gyy=hzz$ to be possible, but further it cannot be inferred thence, as to give the nearby formula $\zeta xx+\eta yy$ equal to hzz, provided there were $\zeta\eta=fg$.

COROLLARY 3

44. Because $t<\frac{1}{2}h$, the formula $tt+fg$ will be less than $\frac{1}{4}hh+fg$, which therefore if it may be divided by h, the quotient will be less than $\frac{1}{4}h+\frac{fg}{h}$.

COROLLARY 4

45. Therefore in turn it is apparent also, if no formula of this kind may be given divisible by *h*, then also neither this equation $fxx + gyy = hzz$ nor any other similar equation $\zeta xx + \eta yy = hzz$ to be possible, if indeed there were $\xi\eta = fg$. According therefore to this, it suffices to be examining only those cases established, for which $t < \frac{1}{2}h$.

THEOREM 5

46. *If the equation* $fxx + gyy = hzz$ *were possible, then always a number h' can be shown, smaller than h, thus so that this equation* $fxx + gyy = h'zz$ *shall be possible.*

DEMONSTRATION

If we may consider the formula $tt + fg = k$, we have shown above now this form $fxx + gyy = hkzz$ also to be possible. But thus we have seen only for *t* given a value less than $\frac{1}{2}h$, where the formula $tt + fg$ may have a factor *h*. Therefore let there be another factor *h'* and thus $k = hh'$ and $hk = h'h^2$, and with the square *hh* deleted, as can be done in the square involving *zz*, this possible equation also may arise :

$$fxx + gyy = h'zz, \text{ where } h' < \tfrac{1}{4}h + \tfrac{fg}{h}.$$

[see §'s 52, 53 below, Ex. 1 & 2, etc.]

COROLLARY 1

47. However great were the number *h'*, it will be possible continually to come upon smaller values *h', h''* etc., while finally numbers may be produced so small, which do not admit further diminution. For since $h' < \frac{1}{4}h + \frac{fg}{h}$, certainly h' will be able to exceed $\frac{fg}{h}$; from which it is evident, where a smaller number were returned *h*, further diminution to be slowed down and thus stopped at the lowest level.

COROLLARY 2

48. If, while smaller values for *h* are elicited continually, it may come finally to a value of *f* or *g,* hence certainly we will be able to conclude the proposed equation to be possible, since that case obviously involves the case $fxx + gyy = fzz$ especially, evidently where $y = 0$ et $z = x$. But if in no way may we be led either to *f* or *g,* but to another number ζ, a divisor of *fg,* that will not be the same proposed equation, but another related, evidently $\zeta xx + \eta yy = hzz$ to be possible; from which if finally it may arrive at unity, then the equation $xx + \eta gyy = hzz$ may be possible.

PROBLEM 3

49. *With the equation proposed* $fxx + gyy = hzz$ *, to investigate whether or not that shall be possible.*

SOLUTION

Since here three numbers are proposed, *f, g* and *h,* an equation thus may be shown, so that the number *h* shall be the maximum of these, since here likewise it is the case, whether the terms of the equation shall be positive or negative. Then the formula may be assumed $tt + fg$ and an examination may be put in place, whether or not, with numbers *t* assumed less than $\frac{1}{2}h$, this formula may become divisible by *h*. We will be able to announce at once the latter case not to be possible ; but in the first case in place of *h* we will obtain another smaller number h' requiring to be put under the same examination, then finally no further decrease may be found. And if among these values *f* or *g* may occur, that will be a sure indication the proposed equation to be possible ; but if we come upon another number ζ , a divisor of the product *fg*, then we may conclude the equation $\zeta xx + \eta yy = hzz$ to be possible with $\zeta\eta = fg$ present. But if by using neither it may arise, then we may agree with a smaller value succeeding in place of *h*, which shall be h', and thus now we may set aside the equation $fxx + gyy = h'zz$, so that of the letters *f* and *g* the greater, for example *g*, may be placed in this manner on the right : $h'zz - fxx = gyy$, and now in place of *g* in a similar manner g' may be sought, while it may either come to g' or to h' or equal to *f* itself, in which case our proposition likewise will prevail. But if indeed this may not unfold easily, in place of *g* we may introduce a small value thence g' arises, and now the equation $h'zz - g'yy = fxx$ may be treated in a similar manner ; and thus at last the equation may arrive at the three numbers f', g', h', so that the outcome will not have to labour with further difficulty.

COROLLARY 1

50. If *h* were very large, certainly there will be a need for a most tedious calculation before the all the cases of the formula $tt + fg$ as far as to $t = \frac{1}{2}h$ may be examined ; but scarcely any such labour will be undertaken. But with the above principle granted, the value for *h* will be decreased below 4*fg*.

COROLLARY 2

51. If that large number *h* may have factors, for example *m* and *n,* there the labour will be lightened considerably, while initially such a value for *t* may be investigated, so that the formula $tt + fg$ at least may be divisible either by *m* or by *n;* nor indeed subsequently will this case be difficult to elicit, when that same formula may be divisible by the

number h itself. Concerning the rest, this whole operation will be made clearer by examples.

EXAMPLE 1

52. This equation proposed is required to be examined $3xx + 5yy = 1007zz$. Therefore this formula may be taken $tt + 15$ on account of $f = 3$ and $g = 5$, and because $h = 1007 = 19 \cdot 53$, thus initially t may be sought [see § 46, Th. 5], so that $tt + 15$ may contain at least the divisor 19, which evidently shall be the case by accepting $t = 2$; for then there becomes $k = 19$ and thus producing $h' = 53$, with the square 19^2 removed. Now again t may be sought, so that the formula $tt + 15$ may contain the divisor 53, which happens, if $t = 12$, thus so that now we may have $k = 159 = 3 \cdot 53$ and thus $h'k = 3 \cdot 53^2$ and thus $h'' = 3$, which number since it shall be equal to f, indicates our formula to be possible.

EXAMPLE 2

53. This equation may be proposed : $2xx + 7yy = 23zz$. Here $f = 2$, $g = 7$ and $h = 23$. There may be taken $k = tt + 14$, which number becomes divisible by 23 by taking $t = 3$. Moreover there will be $k = 23 = h$ and thus $hk = 23^2$; from which it is understood this equation $xx + 14yy = zz$ to be possible; therefore nor hence does it follow the proposition to be impossible, since it may be able to happen, so that each likewise may have a place. Therefore we may see, or this form : $2xx + 7yy = 23zz$ shall be possible, which indeed is evident on taking $x = 1$, $y = 1$ and $z = 3$. But yet may we use our rule, and because there is $h' = 1$, by taking $t = 2$ there will be $k = 18 = 2 \cdot 3^2$, hence $h'k = 2 \cdot 3^2$ and thus $h'' = 2$, that is $h'' = f$; and thus also it is evident that same proposed equation to be possible.

COROLLARY

54. Therefore since in this case each form $fxx + gyy = hzz$ and $xx + fgyy = hzz$ shall be possible, there will be a need to inquire in these cases, by which each formula $fxx + gyy$ and $xx + fgyy$ may be able to be equal to the term hzz. But this evidently arises , when it can happen that $fxx + gyy = uu + fgvv$; because if it may be possible to happen, certainly an infinitude of cases can be shown, among which one will be given, where $v = 0$. That therefore arises , as often as $fxx + gyy = uu$ can prevail, which will be made clear by our example.

EXAMPLE 3

55. The equation may be proposed $xx + 6yy = 145zz = 5 \cdot 29zz$. Therefore in the formula $k = tt + 6$ we may take $t = 2$, so that there may become $k = 2 \cdot 5$ and thus $hk = 2 \cdot 5^2 \cdot 29$ and thus $h' = 2 \cdot 29$. Now t may be taken thus, so that k may be divisible by 29, which happens on taking $t = 9$; indeed there becomes $k = 87 = 3 \cdot 29$, therefore $h'k = 2 \cdot 3 \cdot 29^2$ and $h'' = 6 = g$; consequently our equation certainly is possible.

EXAMPLE 4

56. The equation $3xx + 7yy = 89zz$ may be proposed. Here there is $f = 3,\ g = 7$ and $h = 89$, and thus $k = tt + 21$. Therefore t is sought, so that formula may become divisible by 89. To this end we may put $tt + 84 = 89n$. Here indeed in place of 21 in general it will be allowed to write $21uu$, and here we have taken $u = 2$, so that we illustrate this case also. But since no square shall be of the form $3n + 2$, the values 1, 4, 7, 10 etc. are excluded for n and in general $3\alpha + 1$. Thereupon all the unequal even numbers 2, 6, 10, 14 etc. are excluded and, since all the squares are of the form either $5\alpha + 1$ or $5\alpha + 4$, for n these numbers are excluded also : 3, 4, 8, 9, 13, 14 and in general $5\alpha + 3$ and $5\alpha + 4$. With these excluded for n these numbers remain to be examined : 5, 11, 12, 15, 17, 20, 21, 27, 32, 35, 36, 41, which therefore will be required to be substituted in succession into the equation $tt = 89n - 84$ by being substituted in place of n. But truly the first value $n = 5$ provides a square at once, from which $k = 5 \cdot 89$ and $h' = 5$. But now k may become divisible by 5 by taking $t = 1$, from which there becomes $k = 5 \cdot 17$ and $h'' = 17$. Therefore since we neither come upon 3 nor 7, on taking $h' = 5$ we will examine the equation $5zz - 3xx = 7yy$ and now the whole business is required to be changed, while we have $f = 5,\ g = -3$ and $h = 7$; wherefore, on putting $k = tt - 15$, we may take $t = 1$, so that there may become $k = -2 \cdot 7$, from which there becomes $h' = -2$, thus so that now the equation to be examined shall be this $5zz - 3xx = -2yy$ or $3xx - 2yy = 5zz$, where $f = 3,\ g = -2$ and $h = 5$. Therefore on taking $k = tt - 6$, there becomes $t = 1$, there will become $k = -5$ and $h' = -1$, therefore we arrive at this equation: $3xx - 2yy = -zz$ sive $2yy - zz = 3xx$, where we have $f = 2,\ g = -1,\ h = 3$. Therefore there will be $k = tt - 2$; where since in no way may it be possible to happen, all these equations therefore and with the proposition itself are impossible.

EXAMPLE 5

57. The proposed equation shall be $3xx + 7yy = 178zz$, where as before $f = 3,\ g = 7$, but $h = 178 = 2 \cdot 89$ twice as great as in the preceding case. Therefore on putting $tt = 89n - 21$, the numbers are left behind for n:

5, 8, 9, 14, 18, 20, 24, 29, 30, 33, 38, 44.

But there is found $n = 14$, from which there becomes $t = 35$, and thus there will be $k = 14 \cdot 89$ and hence $h' = 2 \cdot 14 = 4 \cdot 7$ and thus $h' = 7$, which number, since it shall be equal to the number g, indicates our equation to be possible.

PROBLEM 4

58. *After the equation* $fxx + gyy = hzz$ *were found to be possible by the preceding method, while finally values will have been produced from found from* h *for* f *or for* g, *to determine the squares themselves* xx *and* yy, *from which a possible equation may arise.*

SOLUTION

Because the preceding solution has led to the following formulas

$$k = aa + fg = hh',\ k' = bb + fg = h'h'',\ k'' = cc + fg = h''h''' \text{etc.},$$

we will have $hk = h^2h' = h' \cdot \square$, and hence $hk^2 = h'k \cdot \square$. We will find in a similar manner :

$$h' \cdot \square = h''k',\ \text{likewise } h'' \cdot \square = h'''k'' \text{; etc.}$$

Now there shall become $h''' = f$; there will be $h'' \cdot \square = fk''$, hence $h' \cdot \square = fk''k'$ and finally $h \cdot \square = fkk''k'$; consequently we will have $h \cdot \square$, that is

$$hzz = f(aa + fg)(bb + fg)\left(cc + fg\right)(dd + fg) \text{ etc.},$$

which product clearly is reduced to $f(A^2 + fgB^2)$, thus so that hence there may become t $hzz = fA^2 + ffgB^2$, from which we come upon $x = A$ and $y = fB$, and thus the problem has been resolved.

DE CRITERIIS AEQUATIONIS $fxx+gyy=hzz$, UTRUM EA RESOLUTIONEM ADMITTAT NECNE

Commentatio 556 indicia ENESTROEMIANI
Opuscula analytica 1, 1783, p. 211-241
[Conventui exhibita die 7. decembris 1772]

1. Notum est huiusmodi aequationem pro varia relatione, quae inter numeros *f, g* et *h* intercedit, modo esse possibilem modo impossibilem, siquidem pro *x, y* et *z* numeros rationales accipi oportet, atque adeo integros, quia fracti facillime ad integros revocarentur. Ita notum est hanc aequationem: $xx+yy=2zz$ esse possibilem, hanc vero: $xx+yy=3zz$ impossibilem. Quando autem litterae *f, g* et *h* maiores tenent valores, iudicium, utrum aequatio sit possibilis necne, difficulter instituitur ; in maximis vero numeris vix suscipiendum videtur. Hic igitur constitui in certa criteria inquirere, ex quibus iudicare liceat, utrum haec aequatio sit possibilis necne, quantumvis magni fuerint numeri *f, g* et *h.*

2. Ante omnia autem sequentia notasse iuvabit:

I. Numeros *f,* g et *h* non solum integros assumo, sed etiam non-quadratos, neque etiam per quadratum divisibiles; si enim numerus f haberet factorem quadratum, is in quadrato *xx* involvi posset, quod etiam de reliquis tenendum.

II. Praeterea hos numeros aeque negativos ac positivos assumere licet; et quia aequatio ita semper disponi potest, ut membra *fxx* et *hzz* obtineant valores positivos, solum membrum *gyy* relinquitur, quod vel positivum vel negativum esse poterit.

III. Numeros *f* et *g* tamquam primos inter se spectamus; si enim haberent communem divisorem *d,* vel numerus *k* eundem habere deberet, quo casu ille per divisionem tolleretur, vel quantitas *z* per *d* esset divisibilis. Unde si loco *z* scribamus *dv,* nostra aequatio ad hanc formam reduceretur: $fxx+gyy=dhvv$, ita ut nunc *f et g* futuri sint primi inter se.

IV. Denique notandi sunt casus maxime obvii, quibus aequatio nostra sit possibilis. Primo scilicet hoc evenit, si fuerit vel $h=f$ vel $h=g$; illo enim casu foret $y=0$ et $z=x$, hoc vero $x=0$ et $z=y$. Tum vero etiam casus satis obvius erit, si fuerit $h=f+g$, quia ei satisfieret sumendo $z=x=y$ Minus obvii autem erunt casus, quibus $h=faa+gbb$; foret enim tum $x=a$, $y=b$ et $z=1$.

3. Primum autem investigabo, datis numeris *f* et *g,* cuiusmodi numeri pro *k* locum habere queant, ut aequatio fiat possibilis. Quare quum hic *h* ut numerum incognitum spectemus, aequationem nostram hac forma referamus: $fxx+gyy=szz$, ut iam idoneos

valores pro littera *s* investigari oporteat, quibus aequatio fiat possibilis, et quidem omnes, qui hoc praestent; quem in finem sequentia Theoremata adiungo.

THEOREMA 1

Si casu $s = h$ *possibilis fuerit aequatio* $fxx + gyy = hzz$, *ita ut litterae x, y, z iam sint cognitae, si vero insuper habeatur haec aequatio* $pp + fgqq = krr$, *tum nostra aequatio quoque erit possibilis casu* $s = hk$.

DEMONSTRATIO

Multiplicentur enim hae duae aequationes in se et prodibit haec nova aequatio

$$hkrrzz = (fxx + gyy)(pp + fgqq) = f(px \pm gqy)^2 + g(py \mp fqx)^2.$$

Quare si statuamus

$$rz = Z,\ px \pm gqy = X \text{ et } py \mp fqx = Y,$$

nascitur haec aequatio propositae omnino similis

$$fX^2 + gY^2 = hkZ^2$$

COROLLARIUM 1

4. Quodsi ergo litterae *p* et *q* ita assumere liceat, ut *k* obtineat factorem *h,* scilicet $k = hl$, tum ob $s = hhl$ novus valor idoneus erit $s = l$, quoniam quadratum *hh* omittere licet.

COROLLARIUM 2

5. Quemadmodum igitur ex illo valore idoneo $s = h$ erutus est alius $s = hk$ sive $s = l$, ita ex hoc simili modo alius novus valor, puta $s = m$, hincque denuo novus $s = n$ erui poterit; atque hanc determinationem in infinitum continuare licebit. Ita ex casu quocunque cognito innumerabiles alii derivari poterunt.

COROLLARIUM 3

6. Si eveniat, ut numeri *h* et *k* communem habeant divisorem *d,* tum novus valor *hk* factorem habebit *dd,* qui ergo expungi poterit. Hoc modo continuo ad minores numeros idoneos pro *s* pervenire licebit, donec tandem ad casum obvium perducamur.

COROLLARIUM 4

7. Hinc si adhuc fuerimus incerti, utrum *h* sit valor idoneus ipsius *s*, hoc autem modo procedendo perveniamus tandem ad casum obvium, tuto concludere poterimus etiam casum $s = h$ esse possibilem. Sin autem hoc nullo modo succedat, vel tandem in minoribus numeris ad eiusmodi casum perveniatur, cuius impossibilitas patescat, etiam valor ipse $s = h$ pro impossibili erit habendus.

THEOREMA 2

8. *Si pro nostra aequatione tres innotescant casus possibiles* $s = h$, $s = h'$ et $s = h''$, *tum etiam valor idoneus erit* $s = hh'h''$.

DEMONSTRATIO

Quum igitur habeantur tres huiusmodi aequationes, quae sint

$$\text{I. } faa + gbb = hcc,$$
$$\text{II. } fAA + gBB = h'CC,$$
$$\text{III. } f\alpha\alpha + g\beta\beta = h''\gamma\gamma;$$

ducatur prima in secundam et productum erit

$$hh'ccCC = (faa + gbb)(fAA + gBB) = (faA \pm gbB)^2 + fg(aB \mp bA)^2.$$

Faciamus nunc

$$cC = r \text{ et } faA \pm gbB = p \text{ et } aB \mp bA = q,$$

ut hoc productum fiat

$$pp + fgqq = hh'rr,$$

quod denuo multiplicatum in tertiam aequationem dabit tale productum

$$hh'h''rr\gamma\gamma = (f\alpha\alpha + g\beta\beta)(pp + fgqq) = f(p\alpha \pm gq\beta)^2 + g(p\gamma \mp fq\alpha)^2;$$

quae forma cum plane conveniat cum proposita, veritas Theorematis est manifesta et casus $s = hh'h''$ erit possibilis.

COROLLARIUM 1

9. Ex cognitis ergo tribus valoribus idoneis $h,\ h',\ h''$ quartus facile invenitur. Ac si forte illi terni habeant divisores communes, hoc modo ad novos valores continuo minores pertingere licebit.

COROLLARIUM 2

10. Si ergo hunc novum valorem indicemus littera h''', tum etiam valores idonei erunt $s=hh'h''',\ s=hh''h''',\ s=h'h''h'''$; ex quibus porro simili modo plures alii deduci possunt.

COROLLARIUM 3

11. Quando autem hi novi valores per quadrata, uti praecepimus, deprimuntur, continuo iidem casus cogniti recurrent. Quum enim sit $h'''=hh'h''$, forma $hh'h'''$ reducitur ad h'', haec vero $hh''h'''$ad h' et $h'h''h'''$ ad h, ita ut revera unus tantum casus novus hoc modo reperiatur.

THEOREMA 3

12. *Si aequationi nostrae* $fxx+gyy=szz$ *satisfaciat casus* $s=h$, *tum quoque omnes isti valores satisfacient*

$$s=4fg+h,\ s=8fg+h,\ s=12fg+h,\ s=16fg+h \text{ etc.},$$

quin etiam, si h fuerit numerus satis magnus, isti

$$s=h-4fg,\ s=h-8fg,\ s=h-12fg \text{ etc.},$$

et in genere $s=h\pm 4nfg$, *dummodo hi numeri fuerint primi.*

Huius elegantissimi Theorematis demonstratio adhuc desideratur, postquam a pluribus iam dudum frustra est investigata; cuius rei difficultas manifesto in hoc est sita, quod omnes hi numeri tum demum quaesito satisfaciant, quando sunt numeri primi. Quando enim sunt compositi, evenire potest, ut non satisfaciant, etiamsi non semper a scopo aberrent. Quum autem hic tantum valeant numeri primi, probe notandum est numeros negativos, qui ex formula $s=h-4fg$ resultare possunt, non pro primis esse habendos. Quocirca plurimum is praestitisse erit censendus, cui successerit demonstrationem huius Theorematis invenire.

COROLLARIUM 1

13. Quum hoc modo saltem ascendendo in infinitum progredi liceat, etiam multitudo valorum idoneorum pro s eo usque augeri poterit, quo usque Tabula numerorum primorum fuerit constructa.

COROLLARIUM 2

14. Ita quum haec aequatio $xx + yy = zz$ sit possibilis, ubi est $f = 1$, $g = 1$ et $s = h = 1$, haec forma $4n + 1$, quatenus scilicet praebet numeros primos, etiam totidem valores idoneos pro *s* suppeditabit, qui numeri sunt

1, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc.

Hos autem numeros omnes ipsos aequari summae duorum quadratorum iam dudum rigorosissime a me est demonstratum, unde eo minus de demonstratione reliquorum casuum desperare fas est. His igitur omnibus casibus licebit sumere $z = 1$. Interim tamen hinc etiam numeros compositos pro *s* invenire licet, dum per Theorema primum producta ex binis vel pluribus horum ipsorum numerorum etiam pro *s* valebunt, quoniam binae illae formulae $fxx + gyy$ et $pp + fgqq$ hoc casu congruunt.

COROLLARIUM 3

15. Quia aequationi $2xx + 3yy = szz$ satisfieri potest casu $s = 341$, alios casus idem praestantes dabit formula $341 \pm 24n$, quoties scilicet prodierint numeri primi. Hinc ergo descendendo oriuntur sequentes valores

341, 317, 293, 269, 197, 173, 149, 101, 53, 29, 5.

Hi autem omnes numeri ipsi iam in forma $2xx + 3yy$ continentur, ita ut possit esse $z = 1$.

SCHOLION

16. Hoc Theoremate, quasi demonstratum esset, praemisso, pro quovis casu numerorum *f* et *g* omnes plane valores idonei litterae *s* facile inveniri poterunt. Ad hoc autem ostendendum, duos casus separatim tractari oportet: priorem, quo $f = 1$ atque idcirco primi termini primi Theorematis inter se conveniunt; alterum vero, quo *f* non est unitas. Unde primo aequationem $xx + gyy = szz$ evolvemus.

PROBLEMA I

I7. *Proposita aequatione* $xx + gyy = szz$ *, invenire omnes valores idoneos pro s, quibus haec aequatio evadit possibilis.*

SOLUTIO

Hic statim evidens est valorem idoneum fore $s = g$; tum enim fit $x = 0$ et $y = z$. Etsi enim 4*g*, 9g, 16g etc. aeque satisfaciant, tamen omnes per quadratum depressi redeunt ad *g*. Verum sumto $y = 0$, omnes numeri quadrati pro *s* prodeunt, quos igitur omnes ad unitatem reducere liceret. Sed quia praeter hos ipsos numeros etiam iidem numeris $4ng$ sive aucti sive minuti satisfaciunt, quatenus scilicet prodeunt numeri primi, haec quadrata hic negligere non licet. Iis autem tantum quadratis indigemus, quae ad numerum $4g$ fuerint primi, quia aliter nulli numeri primi inde emergerent; quamobrem statim omnia quadrata paria hinc excluduntur et iis tantum imparibus locus conceditur, quorum radices ad numerum g fuerint primi. Semper ergo hic occurrit unitas, tum vero etiam novem, nisi g sit per 3 divisibilis, porro etiam 25, nisi g divisorem habeat 5, etc. Quando autem haec quadrata excedunt numerum $4g$, eorum loco scribantur residua ex divisione per $4g$ remanentia. Ponamus ergo hinc prodire formulas:

$$4ng+1, 4ng+a,\ 4ng+b,\ 4ng+c,\ 4ng+d \text{ etc.},$$

ubi scilicet *a, b, c, d* etc. sunt ea residua, quae ex quadratis per $4g$ divisis resultant. Verum praeter hos casus alius est obvius $s=1+g$, siquidem g fuerit numerus par; sin autem fuerit impar, sumatur $s=4+g$, ut scilicet habeatur numerus ad $4g$ primus. Tum vero quia per Theorema primum producta ex binis numeris satisfacientibus etiam satisfaciunt, habebimus insuper istas formulas loco $1+g$ vel $4+g$ scribendo h

$$s=4ng+h, 4ng+ah,\ 4ng+bh,\ 4ng+ch,\ 4ng+dh \text{ etc.},$$

quos omnes valores coniunctim ita ob oculos constituamus:

$$s=4ng+\begin{pmatrix} 1, & a, & b, & c, & d \text{ etc.} \\ h, & ah, & bh, & ch, & dh \text{ etc.} \end{pmatrix}.$$

Quae omnes formulae eatenus valent, quatenus numeros primos producunt, hocque modo omnes plane numeri primi idonei reperientur; compositi autem nulla plane laborant difficultate, quum nascantur ex duobus pluribusve numeris primis idoneis. Quin etiam ipsum numerum g eiusque producta per numeros iam inventos annumerari oportet.

COROLLARIUM 1

18. Quia veritas huius solutionis nondum plane est evicta, casus aliquos obvios consideremus, quos semper in aliqua superiorum formularum contineri deprehendemus. Ita casus $s=1+4g$ continetur in formula $4ng+1$ et $s=1+9g$ continetur in formula $4ng+h$, si fuerit $h=1+g$; at si $h=4+g$, in ea continebitur $s=4+9g$. Similique modo res se habet in formulis $1+16g,\ 1+25g, 1+36g$ vel $4+g, 4+9g, 4+25g$ etc., ubi eos casus, qui numeros primos producere nequeunt, excludimus.

COROLLARIUM 2

19. Haec solutio aeque locum habet, sive g sit numerus positivus, sive negativus. At quia hoc posteriori casu in formulis inventis littera h obtinet valorem negativum, loco terminorum *h, ah, bh, ch etc*. eorum complementa ad numerum 4g scribantur.

COROLLARIUM 3

20. Casu, quo g est numerus negativus, si iam fuerint inventae formulae superiores, quae valent pro formula $xx-gyy$, si ibi signa mutentur, sive loco numerorum 1, *a, b, c, d* etc. scribantur eorum complementa ad 4g, tum illae inservient huic aequationi $gyy-xx=szz$.

SCHOLION

21. Haec autem maxime illustrabuntur et facilius in usum vocari poterunt, si plura exempla adiungamus, quibus etiam natura numerorum aliaeque abstrusae proprietates clarius perspicientur.

EXEMPLUM 1

Sit $g=1$ et aequatio proposita $xx+yy=szz$, atque hic pro valoribus ipsius s unica habetur formula $4n+1$. Casus autem $1+g=2$, quia ad 4g non est primus, generali formulae innecti nequit; interim tamen seorsim praebet numerum idoneum $=2$. Pro numeris igitur primis satisfacientibus praeter 2 habemus superiorem seriem

1, 5, 13, 17, 29, 37, 41 etc.

et producta ex quocunque horum praebebunt omnes numeros compositos satisfacientes.

At pro casu $g=-1$ seu aequatione $xx-yy=szz$ praeter formam $4n+1$ ex quadratis ortam formula $4+g=3$ dabit insuper hanc $4n+3$. Sicque omnes numeri primi in alterutra harum duarum formularum $4n+1$ et $4n+3$ erunt contenti, ideoque omnes plane numeri primi hoc casu sunt idonei, quippe quos omnes in differentiam duorum quadratorum resolvere licet. Hinc quidem 2 excluditur, quoniam differentia duorum quadratorum esse nequit; attamen valorem pro s dari potest, siquidem pro z sumatur numerus par. Nam $2\cdot 4$ utique est $9-1$.

EXEMPLUM 2

22. Sit nunc $g=2$ et proposita haec forma $xx+2yy=szz$, ubi quum sit $4g=8$, quadrata imparia 1, 9, 25 etc. omnia reducuntur ad eandem formam $8n+1$; at casus $1+g=k=3$ insuper dat hanc formam $8n+3$, sicque omnes numeri primi hac specie referentur: $8n+(1,3)$, quibus accedit insuper $s=g=2$, sicque omnes hi numeri primi sunt

1, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97 etc.

At si sit $g=-2$, pro formula $xx-2yy=szz$ reperitur $s=8n+(1,7)$, quibus annumerari debet -2, atque hinc vicissem pro aequatione $2yy-xx=szz$ erit $s=8n+(7,1)$. Iidem ergo numeri pro his duobus posterioribus casibus valent.

EXEMPLUM 3

23. Pro formula $xx+3yy=szz$ secundum praecepta data prodit $s=12n+(1,7)$, et insuper numerus solitarius 3. Pro formula autem $xx-3yy=szz$ reperitur $s=12n+(1)$.

EXEMPLUM 4

Pro formula $xx+5yy=szz$ reperitur $s=20n+(1,9)$, cum numero 5; at pro formula $xx-5yy=szz$ reperitur $s=20n+(1,19)$, cum numero -5.

EXEMPLUM 5

Pro formula $xx+6yy=szz$ reperitur $s=24n+(1,7)$, una cum numero 6; pro formula autem $xx-6yy=szz$ colligitur, una cum numero -6, ubi numeri ± 6 tamquam primi sunt spectandi, etiamsi in se sint compositi.

SCHOLION

24. Plura huiusmodi exempla non evolvimus, quum calculus satis sit perspicuus, sed potius Tabulam sequentem adiungimus, in qua pro quavis formula $xx+gyy=szz$ primo formam numerorum primorum pro *s* exhibebimus, deinde vero ipsos numeros primos usque ad centum; quibus cognitis omnia producta, tam ex binis quam pluribus numeris primis, pro valore litterae *s* satisfaciunt:

$xx+yy=szz$	$s=4n+1$ cum 2
Num. primi	1, 2, 5, 13, 17, 29, 37, 41 etc.
$xx-yy=szz$	$s=4n+(1,3)$
Num. primi	1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 etc.
$xx+2yy=szz$	$s=8n+(1,3)$ cum 2
Num. primi	2; 1, 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97
$xx-2yy=szz$	$s=8n+(1,7)$ cum -2
Num. primi	− 2; 1, 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97
$xx+3yy=szz$	$s=12n+(1,7)$ cum 3
Num. primi	3; 1, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97
$xx-3yy=szz$	$s=12n+1$ cum solitario -3
Num. primi	−3; 1, 13, 37, 61, 73, 97
$xx+5yy=szz$	$s=20n+(1,9)$ cum numero 5
Num. primi	5; 1, 29, 41, 61, 89
$xx-5yy=szz$	$s=20n+(1,9,11,19)$ cum numero -5

Num. primi	-5; 1, 11, 19, 29, 31, 41, 59, 61, 71, 79, 89
$xx+6yy=szz$	$s=24n+(1,7)$ cum numero 6
Num. primi	6; 1, 7, 31, 73, 79, 97
$xx-6yy=szz$	$s=24n+(1,19)$ cum -6
Num. primi	-6; 1, 19, 43, 67, 73, 97
$xx+7yy=szz$	$s=28n+(1,\ 11,\ 23,\ 9,\ 25,\ 15)$ cum numero 7
Num. primi	7; I, 11, 23, 29, 37, 43, 53, 67, 71, 79
$xx-7yy=szz$	$s=28n+(1,\ 9,\ 25)$ cum -7
Num. primi	-7; 1, 29, 37, 53
$xx+10yy=szz$	$s=40n+(1,\ 9,\ 11,\ 19)$ cum 10
Num. primi	10; 1, 11, 19, 41, 59, 89
$xx-10yy=szz$	$s=40n+(1,\ 9,\ 31,\ 39)$ cum -10
Num. primi	-10; 1, 31, 41, 71, 79, 89
$xx+11yy=szz$	$s=44n+\begin{pmatrix}1,\ 9,\ 25,\ 5,\ 37,\\ 15,\ 3,\ 23,\ 31,\ 27\end{pmatrix}$ cum11
Num. primi	1, 3, 5, 23, 31, 37, 47, 53, 59, 67, 71, 89, 97
$xx-11yy=szz$	$s=44n+(1,\ 9,\ 25,\ 5,\ 37)$ cum -11
Num. primi	-11; 1, 5, 37, 53, 89, 97

PROBLEMA 2

25. *Proposita aequatione* $fxx+gyy=szz$*, invenire omnes numeros primos, qui pro s valores idoneos praebent, quibus haec aequatio evadit possibilis.*

SOLUTIO

Sit *h* valor quicunque idoneus pro *s* et per Theorema nondum demonstratum patet omnes numeros primos in hac formula contentos $4nfg+h$, pariter pro *s* valere; ex quo manifestum est istum valorem *h* ad 4*fg* primum esse debere. Talis autem valor facile invenitur. Si enim ambo numeri *f* et *g* fuerint impares, capi poterit $h=4f+g$ sive $h=f+4g$*;* sin autem numerorum *f* et *g* alter fuerit par, alter impar, valor idoneus habetur $h=f+g$. Quo autem alii insuper numeri primi, atque adeo omnes, pro *s* obtineantur, consideretur formula $pp+fgqq=krr$ atque in Problemate praecedente iam assignavimus omnes primos pro *k* valentes, qui sint $4nfg+(1,\ a,\ b,\ c,\ d\ \text{etc.})$; nunc hae duae aequationes ducantur in se et iam ostendimus prodire huiusmodi formam *hkrrzz* sive $hkZ^2=fX^2+gY^2$, quocirca productum *hk* etiam dabit valorem idoneum pro *s;* unde perspicuum est omnes numeros primos pro *s* idoneos contineri debere in hac forma generali

$$s=4nfg+(h,\ ah,\ bh,\ ch,\ dh\ \text{etc.}).$$

Cognitis autem numeris primis pro *s* valentibus, qui nostrae aequationi $fxx+gyy=szz$ satisfaciunt, si insuper omnes numeri primi pro *k* adhibendi innotescant, qui sint *A, B, C, D* etc., tum producta priorum pro *s* inventorum in singulos vel binos vel ternos etc. horum posteriorum praebebunt etiam valores idoneos pro *s,* hocque adeo modo facile erit infinitos valores litterae *x* exhibere.

COROLLARIUM 1

26. Si eveniat, ut primus valor pro *h* inventus sit quadratus, tum, quia is iam in ordine numerorum 1, *a, b, c, d* etc. continetur, iidem valores pro *s* locum habebunt, qui pro *k* sunt assignati.

COROLLARIUM 2

27. Sin autem numerus *h* in ordine 1, *a, b, c, d* etc. non contineatur, tum nullo modo fieri poterit, ut valores pro *s* et *k* inter se conveniant, sed omnes a se invicem discrepabunt.

EXEMPLUM 1

28. Proposita sit aequatio $2xx+3yy=szz$, ubi $f=2$ et $g=3$, primus autem valor $h=5$. Tum ergo consideretur aequatio $pp+6qq=krr$, et vidimus valores primos pro *k* contineri in hac formula $24n+(1,7)$. His igitur numeris 1, 7 in $h=5$ ductis omnes numeri primi pro *s* in hac formula continentur $24n+(5,11)$, qui sunt 5, 11, 29, 53, 59, 83 etc.

Pro aequatione $2xx-3yy=szz$, ubi $f=2$ et $g=-3$, valor cognitus habetur $h=-1$ sive $h=23$; at aequationi $pp-6qq=krr$ pro *k* inventa est formula $24n+(1,19)$, unde omnes numeri primi pro *s* fiunt: $24n+(5,23)$, quae formula praebet hos numeros primos: 5, 23, 29, 47, 53, 71 etc.

Verum pro hac aequatione $3xx-2yy=szz$, ubi $f=3$ et $g=-2$, valor *h* fit $=1$; et quia formula $pp-6qq=krr$ eadem est quae ante, iidem etiam numeri primi pro *s* in formula $24n+(1,19)$ continentur hincque ipsi numeri primi $24n+(1,19)$, qui igitur fient: 19, 43, 67, 73 etc.

EXEMPLUM 2

29. Proposita aequatione $2xx+5yy=szz$, ubi $f=2$ et $g=5$, primus valor *h* fit $=7$, et quia aequationi $pp+10qq=krr$ convenit formula

$$40n+(1,\ 9,\ 11,\ 19)\ ,$$

pro valoribus primis ipsius s habebimus

$$s=40n+(7,\ 23,\ 37,\ 13),$$

ergo ipsi numeri primi erunt 7, 13, 23, 37, 47, 53 etc.

At proposita aequatione $2xx-5yy=szz$ fit statim $h=-3$; et quia pro aequatione $pp-10qq=krr$ invenimus formulam $40n+(1,\ 9,\ 31,\ 39)$, numeri primi quaesiti continebuntur in hac formula

$$40n+(37,\ 13,\ 27,\ 3)\ ;$$

ergo ipsi numeri primi erunt 3, 13, 37, 43, 53, 67, 83 etc.

Denique pro formula $5xx-2yy=szz$ ob $h=3$ ex iisdem numeris k numeri quaesiti pro s sunt:

$$40n+(37,\ 13,\ 27,\ 3).$$

SCHOLION 1

30. Quae hactenus iam tradita hisque exemplis illustrata sunt, omnes numeros primos pro s satisfacientes suppeditant, qui in se invicem multiplicati, uti praecepimus, dant numeros compositos aeque satisfacientes. Neque vero hinc semper omnes plane numeri compositi pro s idonei obtinentur, sed dantur casus, quibus praeterea alii numeri primi in valores compositos ipsius s ingrediuntur. Caussa huius rei in eo consistit, quod in investigatione superiori numeros pares statim exclusimus, qui tamen cum aliis numeris primis iuncti quaesito satisfacere possunt. Ad hos ergo eruendos ponamus statim $s=2h$, ut sit

$$\frac{fxx+gyy}{2}=hzz.$$

Quodsi iam haec formula $\frac{fxx+gyy}{2}$ praebeat numerum imparem sive productum ex impari in quadratum par, ex eo statim infinitos alios valores pro h elicere licet. Sit enim α eiusmodi numerus impar, et quum pro forma $xx+fgyy=szz$ omnes valores primi ipsius s in hac forma contineantur $4fg+(1,\ a,\ b,\ c,\ d\ \text{etc.})$, omnes numeri primi idonei pro nostra littera h in hac forma continebuntur

$$4fg+(\alpha,\ \alpha a,\ \alpha b,\ \alpha c,\ \alpha d\ \text{etc.}),$$

qui si fuerint diversi ab iis, quos ante sumus assecuti, etiam infiniti alii habebuntur numeri primi, qui in compositionem numeri s ingredi possunt. Singuli enim isti numeri, quos litteris *A, B, C, D* etc. designemus, per 2 multiplicati, idoneos praebent valores pro s, qui ergo erunt 2*A*, 2*B*, 2*C*, 2 *D* etc. Et quia producta ex binis eorum etiam satisfaciunt, hinc nascentur numeri impares, *AB*, *AC*, *AD*, *BC*, *BD*, *CD* etc. Ita in exemplo $xx-3yy=szz$ formula $\frac{xx-3yy}{2}$ statim dat -1. Quum ergo pro hoc casu inventa sit formula $s=12n+1$, pro valoribus ipsius *h* habebimus formulam $12n-1$ sive $12n+11$, quae praebet hos numeros primos

11, 23, 47, 59, 71, 83,

qui duplicati omnes etiam satisfaciunt, atque etiam producta ex eorum binis, tum vero etiam producta ex his in singulos eorum, quos ante iam assignavimus; hocque pacto multitudo valorum compositorum vehementer augetur. Hoc praecipue iis casibus usu venit, ubi formulae supra inventae ex paucioribus membris constabant. Pro formula autem $xx+7yy=szz$ eius dimidium $\frac{xx+7yy}{2}$ praebet 4, sive $1=\alpha$, qui valor quum iam in formula supra data contineatur, hinc novi valores non oriuntur. At vero formula $\frac{xx-7yy}{2}$ praebet $\alpha=-3$ ideoque valores pro *h* erunt $28n+(1,\ 9,\ 25)$, qui numeri iam antea occurrunt. Hoc ergo probe observare oportet eum, qui etiam omnes numeros compositos pro *s* satisfacientes investigare voluerit, unde huic negotio immorari superfluum foret.

SCHOLION 2

31. Quamtumvis autem haec egregia videantur, utique hic erit dolendum, quod nondum firmis demonstrationibus sunt munita, cuius rei ratio potissimum in eo sita videtur, quod formulae pro *s* inventae eatenus tantum valent, quatenus numeros primos suppeditant. Quamquam autem omnes labores a me suscepti spem meam fefellerunt, tamen spero conatus meos iis, qui huiusmodi speculationibus delectantur, non fore ingratos, praecipue quia iam memoratam illam difficultatem circa numeros primos de medio sustuli, ita ut nunc sine dubio aditus ad ista numerorum mysteria non mediocriter facilior reddi videatur.

PROPOSITIO 1

32. *Si fuerit* $fxx+gyy=szz$, *existente s numero primo, tum si omnia quadrata per hunc numerum s dividantur et residua ex singulis enata notentur, inter ea semper occurret* $-fg$ *sive sublata negatione* $s-fg$.

DEMONSTRATIO

Sint residua illa ex divisione per *s* orta 1, *a*, *b*, *c*, *d* etc. ac praebeat quadratum *xx* residuum *a*, quadratum vero *yy* residuum *b*, atque evidens est numerum $fa+gb$ per *s* fore divisibilem. Sit ergo $fa+gb=\lambda s$ eritque $gb=\lambda s-fa$ ideoque $bg^2=\lambda gs-fga$. Quum iam omne residuum, in quadratum ductum, iterum inter residua occurrat, siquidem infra *s* deprimatur, prodeat inde residuum *c*, ita ut sit $c=\lambda gs-fga$, et multiplo ipsius *s* sublato $c=-fga$ sive $c=s-fga$, et quia hoc aeque valet de omnibus residuis, loco *a* sumentes unitatem habebimus $c=-fg$ sive $c=s-fg$.

COROLLARIUM I

33. Si ergo satisfaciat valor $s=h$, quia formula $4nfg+h$, si fuerit numerus primus, etiam satisfaciat pro *s*, si per hunc numerum omma quadrata dividantur, inter residua certo occurret $-fg$.

COROLLARIUM 2

34. Sit ille divisor $=D$, et quia datur quadratum, quod sit *pp*, unde nascitur residuum $-fg$, manifestum est formulam $pp+fg$ divisibilem fore per divisorem *D*.

COROLLARIUM 3

35. Hic autem iam manifesto involvitur difficilis illa conditio numeri primi, quia ordo residuorum hic memoratus locum non habet, nisi *D* sit numerus primus. Fieri enim utique posset, ut $-fg$ non inter residua occurreret, si divisor non esset primus.

PROPOSITIO 2

36. *Si quadrata dividendo per quemcunque numerum primum* $D=2P+1$ *inter residua occurrat numerus r, tunc eius potestas* r^P *per D divisa unitatem relinquet; et vicissim, si* r^P-1 *divisorem habeat D, numerum r inter residua reperiri necesse est.*

DEMONSTRATIO

Quum divisor *D* ponatur $2P+1$, omnium numerorum ipso minorum multitudo est 2*P;* quorum quia semissis tantum in residua ingreditur, multitudo residuorum erit *P.* Deinde etiam certum est, si inter residua occurrat numerus *r,* tum quoque omnes eius potestates ibidem occurrere debere, quemadmodum simplicissima $r^0=1$ inest: Quocirca potestas r^P necessario non novum residuum praebere potest. Atque hinc rite concluditur inde ipsum primum residuum 1 prodire debere, sicque constat propositam potestatem r^P, per numerum primum *D* divisam, residuum relinquere $=1$.

Quod ad inversionem propositionis attinet, perpendamus formulam $r^{2P}-1$ perpetuo divisibilem esse per $2P+1$, ex quo sequitur vel formulam r^P-1 vel r^P+1 divisibilem esse debere. Omnes ergo numeri pro *r* sumti, quibus formula posterior r^P+1 fit divisibilis, ex ordine residuorum excluduntur, atque illi tantum, qui formulam r^P-1 divisibilem producunt, relinquuntur; quorum numerus quum sit *P,* sequitur omnes numeros *r* fore residua.

COROLLARIUM 1

37. Quum primus divisor fuerit $=h$, ponamus $h=2p+1$, et quia $r=-fg$, sequitur formulam $(-fg)^P-1$ per $h=2p+1$ esse divisibilem seu fore $r^P=1+m(2p+1)$. Quum deinde etiam divisor esse possit $h+4nfg$, dummodo fuerit numerus primus, ob $h=2p+1$ faciamus

$$D=2p+1+4nfg=2P+1 \;,$$

ita ut sit $P=p+2nfg$, atque etiam haec potestas

$$(-fg)^P=(-fg)^{p+2nfg}$$

unitate minuta per divisorem $2p+1+4nfg$ evadet divisibilis.

COROLLARIUM 2

38. Quocirca totum negotium huc redit, ut ponendo brevitatis gratia $-fg=r$ ostendatur, si formula r^p-1 fuerit divisibilis per $2p+1$, tum etiam hanc formulam $r^{p+2nr}-1$ fore divisibilem per $2p+1+4nr$, siquidem numerus $2p+1+4nr$ fuerit numerus primus.

COROLLARIUM 3

39. Si ponamus $r=-1$, evidens est formulam $(-1)^p-1$ dividi non posse per $2p+1$, nisi p sit numerus par. Sit ergo $p=2q$ et $4q+1$ numerus primus, tum certe inter residua reperietur $4q$. Sit quadratum, unde hoc residuum nascitur, $=vv$, et $vv+1$ divisibile erit per $4q+1$. Ita ex his rationibus facillime patet semper dari summam duorum quadratorum divisibilem per numerum $4q+1$, id quod alias per multas demum ambages ostendi solet.

40. Missis autem his, quae principiis nondum satis corroboratis innituntur, per certa principia in indolem huiusmodi aequationum $fxx+gyy=szz$ accuratius inquiramus. Ac primo quidem iam rigorose monstravimus, si haec aequatio possibilis fuerit casu $s=h$, tum sumto numero *k*, ita ut sit $pp+fgqq=krr$, fore etiam $s=hk$ valorem idoneum pro *s*. Hoc igitur praemisso ad sequentia progrediamur.

THEOREMA 4

41. *Si aequatio* $fxx+gyy=hzz$ *fuerit possibilis, tum semper assignari potest talis formula* $tt+fg$, *per numerum h divisibilis, ita ut numerus t minor sit quam* $\frac{1}{2}h$.

DEMONSTRATIO

Quum formula illa $fxx + gyy$ divisibilis sit per *h,* si ea ducatur in formulam $fpp + gqq$, etiam productum per *h* erit divisibile. Sumantur ergo numeri *p* et *q* ita, ut sit $py - qx = 1$, id quod semper fieri potest, nisi *x* et *y* habeant communem divisorem, qui autem casus hinc sponte excluditur; tum autem productum illud erit $(fpx + gqy)^2 + fg$, unde sumto $t = fpx + gqy$ formula $tt + fg$ divisorem habebit *h.* Hic autem ponamus $t = t' \pm \lambda h$, acque tum haec formula $t't' + fg$ etiamnunc per *h* erit divisibilis. Hoc vero modo *t'* infra semissem numeri *h* deprimetur; consequenter certo dabitur formula $tt + fg$ divisibilis per *h,* in qua *t* non excedit semissem ipsius *h.*

COROLLARIUM 1

42. Haec eadem proprietas numeri *h,* quia tantum a producto *fg* pendet, aeque patet ad hanc aequationem $xx + fgyy = hzz$. Quin etiam, si productum *fg* in duos alios factores ζ et η resolvi queat, eadem conditio locum habet, ut aequatio $\zeta xx + \eta yy = hzz$ sit possibilis.

COROLLARIUM 2

43. Quoties ergo numerus *h* fuerit divisor formulae $tt + fg$, inde non semper concludi potest aequationem $fxx + gyy = hzz$ esse possibilem, sed plus inde inferri nequit, quam dari formulam affinem $\zeta xx + \eta yy$ aequalem *hzz,* dummodo fuerit $\zeta\eta = fg$.

COROLLARIUM 3

44. Quia $t < \frac{1}{2}h$, formula $tt + fg$ minor erit quam $\frac{1}{4}hh + fg$, quae ergo si dividatur per *h,* quotus minor erit quam $\frac{1}{4}h + \frac{fg}{h}$.

COROLLARIUM 4

45. Vicissim ergo etiam patet, si nulla detur huiusmodi formula per *h* divisibilis, tum etiam neque hanc aequationem: $fxx + gyy = hzz$ neque ullam aliam adfinem esse $\zeta xx + \eta yy = hzz$ possibilem, si scilicet fuerit $\xi\eta = fg$. Ad hoc ergo examinandum sufficit eos tantum casus evolvisse, quibus $t < \frac{1}{2}h$.

THEOREMA 5

46. *Si aequatio* $fxx + gyy = hzz$ *fuerit possibilis, tum semper numerum h', minorem quam h, exhibere licet, ita ut haec aequatio* $fxx + gyy = h'zz$ *sit possibilis.*

DEMONSTRATIO

Si ponamus formulam $tt + fg = k$, supra iam demonstravimus etiam hanc formam $fxx + gyy = hkzz$ esse possibilem. Modo autem vidimus pro *t* dari valorem adeo minorem quam $\frac{1}{2}h$, quo formula $tt + fg$ habeat factorem *h*. Sit ergo alter factor *h'* ideoque $k = hh'$ et $hk = h'h^2$, et deleto quadrato *hh*, utpote in quadrato *zz* involvendo, orietur aequatio quoque possibilis:

$$fxx + gyy = h'zz, \text{ ubi } h' < \tfrac{1}{4}h + \tfrac{fg}{h}.$$

COROLLARIUM 1

47. Quantuscunque ergo fuerit numerus *h'*, hoc modo continuo ad minores valores *h'*, *h''* etc. pervenire licebit, donec tandem numeri prodeant tam parvi, qui ulteriorem diminutionem non admittunt. Quia enim $h' < \frac{1}{4}h + \frac{fg}{h}$, utique *h'* excedere debebit $\frac{fg}{h}$; unde manifestum est, quo minor numerus *h* fuerit redditus, ulteriorem diminutionem retardari atque adeo penitus sisti.

COROLLARIUM 2

48. Si, dum hoc modo pro *h* continuo minores valores eruuntur, tandem perveniatur ad valorem vel *f* vel *g*, hinc certo concludere poterimus aequationem propositam esse possibilem, quandoquidem ista: $fxx + gyy = fzz$ casum maxime obvium involvit, scilicet $y = 0$ et $z = x$. Sin autem nullo modo deducamur ad *f* vel *g*, sed ad alium numerum, ζ, divisorem ipsius *fg*, indicio id erit non ipsam aequationem propositam, sed aliam adfinem, scilicet $\zeta xx + \eta yy = hzz$, esse possibilem; unde si tandem adeo perveniretur ad unitatem, tum aequatio $xx + \eta gyy = hzz$ foret possibilis.

PROBLEMA 3

49. *Proposita aequatione* $fxx + gyy = hzz$, *investigare, utrum ea sit possibilis necne.*

SOLUTIO

Quia hic tres numeri proponuntur, *f*, *g* et *h*, aequatio ita exhibeatur, ut numerus *h* eorum sit maximus, quandoquidem hic perinde est, utrum termini aequationis sint positivi, an negativi. Tum sumatur formula $tt + fg$ et examen instituatur, utrum, pro *t* numeris minoribus quam $\frac{1}{2}h$ sumendis, haec formula fiat divisibilis per *h* necne. Casu posteriore statim pronunciare poterimus aequationem propositam non esse possibilem;

priore autem casu loco h nanciscemur alium numerum minorem h' simili modo examini subiiciendum, donec tandem ulterior diminutio non habeat locum. Et si inter hos valores occurrat f vel g, certum hoc erit indicium aequationem propositam esse possibilem; sin autem ad alium numerum ζ, divisorem producti fg, perveniamus, tum concludemus aequationem $\zeta xx + \eta yy = hzz$ esse possibilem existente $\zeta\eta = fg$. Quodsi autem neutrum usu veniat, tum in valore minimo in locum h succedente acquiescamus, qui sit h', et nunc aequationem $fxx + gyy = h'zz$ ita disponamus, ut litterarum f et g maior, puta g, ad dextram referatur hoc modo: $h'zz - fxx = gyy$, et nunc loco g simili modo quaerantur g', donec perveniatur ad g' sive ipsi h' sive ipsi f aequalem, quo casu propositum nostrum itidem erit evictum. At si ne hoc quidem facile patescat, loco g introducamus valorem exiguum inde ortum g', et nunc aequatio $h'zz - g'yy = fxx$ simili modo tractetur; sicque tandem ad ternos numeros f', g', h' pervenietur, ut iudicium nulla amplius difficultate laborare possit.

COROLLARIUM 1

50. Si numerus h fuerit praegrandis, utique taedioso calculo erit opus antequam formulae $tt + fg$ omnes casus usque ad $t = \frac{1}{2}h$ exigantur; vix autem talem laborem quisquam suscipiet. Admisso autem superiore principio statim valor iste h infra $4fg$ deprimetur.

COROLLARIUM 2

51. Si ingens ille numerus h habeat factores, puta m et n, hic labor non parum sublevabitur, dum primo talis valor pro t investigatur, ut formula $tt + fg$ saltem divisibilis fiat vel per m vel per n; neque enim deinceps difficile erit casum elicere, quo ista formula per ipsum numerum h fiat divisibilis. De caetero tota haec operatio exemplis clarius illustrabitur.

EXEMPLUM 1

52. Examinanda proponatur haec aequatio $3xx + 5yy = 1007zz$. Sumatur ergo formula $tt + 15$ ob $f = 3$ et $g = 5$, et quia $h = 1007 = 19 \cdot 53$, quaeratur t primo ita, ut $tt + 15$ saltem divisorem obtineat 19, quod manifesto fit sumendo $t = 2$; tum enim fit $k = 19$ et sic prodit $h' = 53$, sublato quadrato 19^2. Nunc porro quaeratur t, ut formula $tt + 15$ divisorem nanciscatur 53, quod fit, si $t = 12$, ita ut iam habeamus $k = 159 = 3 \cdot 53$ ideoque $h'k = 3 \cdot 53^2$ sicque $h'' = 3$, qui numerus, quum aequalis sit ipsi f, indicat nostram formulam esse possibilem.

EXEMPLUM 2

53. Proponatur haec aequatio: $2xx + 7yy = 23zz$. Hic $f = 2$, $g = 7$ et $h = 23$. Sumatur $k = tt + 14$, qui numerus fit divisibilis per 23 sumendo $t = 3$. Erit autem $k = 23 = h$

ideoque $hk=23^2$; unde intelligimus hanc aequationem $xx+14yy=zz$ esse possibilem; neque vero hinc sequitur propositam esse impossibilem, quum fieri possit, ut utraque simul locum habeat. Videamus ergo, an haec forma: $2xx+7yy=23zz$ sit possibilis, quod quidem manifestum est sumendo $x=1$, $y=1$ et $z=3$. Sed tamen regula nostra utamur, et quia est $h'=1$, sumendo $t=2$ erit $k=18=2\cdot3^2$, hinc $h'k=2\cdot3^2$ ideoque $h''=2$, hoc est $h''=f$; sicque patet etiam ipsam propositam aequationem esse possibilem.

COROLLARIUM

54. Quum ergo hoc casu utraque forma $fxx+gyy=hzz$ et $xx+fgyy=hzz$ sit possibilis, operae pretium erit in eos casus inquirere, quibus utraque formula $fxx+gyy$ et $xx+fgyy$ eidem termino hzz aequalis esse possit. Hoc autem manifesto eveniet, quando fieri poterit $fxx+gyy=uu+fgvv$; quod si evenire possit, infiniti certe exhiberi poterunt casus, inter quos dabitur unus, quo $v=0$. Illud igitur evenit, quoties evadere potest $fxx+gyy=uu$, id quod nostro exemplo manifesto fit.

EXEMPLUM 3

55. Proponatur aequatio $xx+6yy=145zz=5\cdot29zz$. In formula ergo $k=tt+6$ sumamus $t=2$, ut fiat $k=2\cdot5$ ideoque $hk=2\cdot5^2\cdot29$ sicque $h'=2\cdot29$. Nunc sumatur t ita, ut k fiat per 29 divisibile, quod evenit sumendo $t=9$; fiet enim $k=87=3\cdot29$, ergo $h'k=2\cdot3\cdot29^2$ et $h''=6=g$; consequenter nostra aequatio est utique possibilis.

EXEMPLUM 4

56. Proponatur aequatio $3xx+7yy=89zz$. Hic est $f=3$, $g=7$ et $h=89$ ideoque $k=tt+21$. Quaeratur ergo t, ut illa formula divisibilis fiat per 89. Ponamus in hunc finem $tt+84=89n$. Hic enim loco 21 scribere liceret $21uu$ in genere, atque hic sumpsimus $u=2$, ut etiam hunc casum illustramus. Quum autem nullum quadratum sit formae $3n+2$, pro numero n excluduntur valores 1, 4, 7, 10 etc. et in genere $3\alpha+1$. Deinde excluduntur omnes numeri impariter pares 2, 6, 10, 14 etc. et, quia omnia quadrata sunt formae vel $5\alpha+1$ vel $5\alpha+4$, pro n etiam excluduntur hi numeri: 3, 4, 8, 9, 13, 14 et in genere $5\alpha+3$ et $5\alpha+4$. His exclusis pro n remanent examinandi hi numeri: 5, 11, 12, 15, 17, 20, 21, 27, 32, 35, 36, 41, quos ergo successive in aequatione $tt=89n-84$ loco n substitui oportet. At vero primus valor $n=5$ statim praebet quadratum, unde $k=5\cdot89$ et $h'=5$. Nunc autem k per 5 fiet divisibile sumendo $t=1$, unde fit $k=5\cdot17$ et $h''=17$. Quia ergo neque ad 3 neque ad 7 pervenimus, sumto $h'=5$ examinemus aequationem $5zz-3xx=7yy$ atque iam tota operatio est mutanda, dum habemus $f=5$, $g=-3$ et $h=7$; quocirca, posito $k=tt-15$, sumamus $t=1$, ut fiat $k=-2\cdot7$, unde fit $h'=-2$, ita ut nunc aequatio examinanda sit haec $5zz-3xx=-2yy$ sive $3xx-2yy=5zz$, ubi $f=3$, $g=-2$ et $h=5$. Sumto ergo $k=tt-6$, fiat

$t = 1$, erit $k = -5$ et $h' = -1$, ergo pervenimus ad hanc aequationem: $3xx - 2yy = -zz$ sive $2yy - zz = 3xx$, ubi habemus $f = 2$, $g = -1$, $h = 3$. Erit ergo $k = tt - 2$; quod quum nullo modo fieri possit, omnes istae aequationes ideoque et ipsa proposita sunt impossibiles.

EXEMPLUM 5

57. Sit proposita aequatio $3xx + 7yy = 178zz$, ubi ut antea $f = 3$, $g = 7$, at $h = 178 = 2 \cdot 89$ duplo maior quam casu praecedente. Posito igitur $tt = 89n - 21$ pro *n* relinquuntur numeri

5, 8, 9, 14, 18, 20, 24, 29, 30, 33, 38, 44.

Reperitur autem $n = 14$, unde fit $t = 35$, sicque erit $k = 14 \cdot 89$ hincque $h' = 2 \cdot 14 = 4 \cdot 7$ ideoque $h' = 7$, qui numerus, quum ipsi numero *g* sit aequalis, indicat aequationem nostram esse possibilem.

PROBLEMA 4

58. *Postquam aequatio* $fxx + gyy = hzz$ *methodo praecedente possibilis fuerit inventa, dum tandem valores ex h inventi perducti fuerint ad f sive ad g, determinare ipsa quadrata xx et yy, quibus aequatio evadit possibilis.*

SOLUTIO

Quia solutio praecedens ad sequentes formulas est perducta

$$k = aa + fg = hh',\ k' = bb + fg = h'h'',\ k'' = cc + fg = h''h''' \text{etc.},$$

habebimus $hk = h^2h' = h' \cdot \square$, hincque $hk^2 = h'k \cdot \square$. Simili modo reperiemus

$$h' \cdot \square = h''k',\ \text{item}\ h'' \cdot \square = h'''k''\text{; etc.}$$

Sit nunc $h''' = f$; erit $h'' \cdot \square = fk''$, hinc $h' \cdot \square = fk''k'$ ac tandem $h \cdot \square = fkk''k'$; consequenter habebimus $h \cdot \square$, hoc est

$$hzz = f(aa + fg)(bb + fg)(cc + fg)(dd + fg) \text{ etc.},$$

quod productum manifesto reducitur ad $f(A^2 + fgB^2)$, ita ut hinc fiat $hzz = fA^2 + ffgB^2$, quocirca nanciscimur $x = A$ et $y = fB$, sicque Problema est resolutum.