Proof of a theorem of Fermat that every number whether whole or fraction is the sum of four or fewer squares *

Leonhard Euler

Theorem 1

1. From the series of squares

$$1, 4, 9, 16, 25, \text{etc.},$$

no numbers are divisible by the prime number p, unless their roots are divisible by the same number p.

Proof

For example, if some square number aa were divisible by the prime number p, because it consists of the factors a and a, it would be necessary for one or the other factor to be divisible by p. Therefore, the square number aa cannot be divisible by the prime number p unless its root a is divisible by p.

Corollary 1

2. Thus, the square numbers arising from the roots $p, 2p, 3p, 4p$, etc., namely, $pp, 4pp, 9pp, 16pp$, etc., are divisible by the prime number p, and all other square numbers will not be divisible by the prime number p.

Corollary 2

* Originally published as *Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum*, Novi Commentarii academiae scientiarum Petropolitanae **5** (1754/5), 1760, pp. 13–58. E242 in the Eneström index. Translated from the Latin by Paul R. Bialek, Department of Mathematics, Trinity International University, Deerfield, Illinois, email: pbialek@tiu.edu.

3. Therefore, if the square numbers whose roots are not contained in the arithmetic progression $p, 2p, 3p, 4p$, etc. are divided by the prime number p, after the division there will always be a residue left over which will be less than the number p.

Scholium

4. In this dissertation, I have resolved to investigate diligently in whatever way there may be residues which arise from division of individual squares by any prime number p. Indeed here these most remarkable phenomena will occur; through consideration of these, the nature of the numbers is not ordinarily made clear. Until now such extraordinary mysteries in the science of numbers have lain hidden; in them is disclosed a work which does not seem to have been done in vain.

Theorem 2

5. If a series of squares continued to infinity is separated into parts consisting of p terms, that is, $1, 4, ..., pp \mid (p+1)^2, ..., 4pp \mid (2p+1)^2, ..., 9pp \mid (3p+1)^2, ..., 16pp$ etc., then if the individual terms of each one of the parts are divided by the prime number p, the residues will repeat the same sequence.

Proof

For example, the first terms of each part, $1, (p+1)^2, (2p+1)^2, (3p+1)^2$, etc., if they are divided by p, will give the same residue, 1. And in the same way, the second terms, $4, (p+2)^2, (2p+2)^2, (3p+2)^2$, etc., divided by p, will produce the same residue, 4, if we let $p > 4$. And in the same way, it is evident that the third terms produce the same residues, and similarly, the fourth, the fifth, etc. And in general, if the number of terms in the first part is nn, the analogous terms of the remaining parts will be $(p+n)^2, (2p+n)^2, (3p+n)^2$, etc. which all divided by p produce the same residue, up to the nn term. Therefore, in each of the parts, the same residues occur and in the same order.

Corollary 1

6. Therefore, if we know the residues which arise from the terms of the first part, we will immediately have the residues produced by division of all the remaining parts by the number p.

Corollary 2

7. Because the last term of each part is divisible by the number p, the residue will be 0, just as the residue of the first term of each part is 1. Indeed, the residue of the second terms of each part will be 4 if $p > 4$, of the third terms will be 9 if $p > 9$, of the fourth terms will be 16 if $p > 16$, etc.

Corollary 3

8. That is, as long as the square numbers 1, 4, 9, 16, etc. are less than the number p, they themselves constitute the residues. From the sequence of squares greater than the number p, other residues less than the number p emerge.

Scholium

9. By the nature of division, it is evident that the residues will always be less than the divisor p, and if inadvertently by chance a residue is left that is greater than the divisor p, by subtracting p however often one can, it will be reduced to a number which is itself less than p. Thus, the residue $p + a$ and in general $np + a$ will be equivalent to the residue a, because by chance they will emerge from division by p. And when residues arise from division of numbers by p, all the residues of $a, p + a, 2p + a$, and $np + a$ have the same value, namely, all reduce to the minimum a. Because this reduction is available, we can safely ignore it or assume it already done. So if the square numbers 1, 4, 9, 16, 25, etc. are divided by the number p, nothing will prevent us from deisgnating the residues which arise to be 1, 4, 9, 16, 25, etc., even if here numbers greater than the divisor p itself occur. Another thing to be noted is that this theorem retains its validity whether the divisor p is a prime number or not.

Corollary 4

10. Because the last term of the first part pp generates no residue, all residues which can in fact arise from the entire series of squares originate from the terms $1, 4, 9, 16, ..., (p-1)^2$, of which the number of terms is $p - 1$.

Corollary 5

11. Thus, more than $p - 1$ different residues cannot arise; indeed it is clear in itself. That is, because all residues are less than the divisor p itself, and furthermore the number of all numbers less than p itself is $p - 1$, consequently the number of different residues cannot be a greater number.

Theorem 3

12. If all the terms of the series of squares 1, 4, 9, 16, etc. are divided by any number p and the residues are noted, not all numbers less than p occur among these residues.

Proof

That is, all residues which in fact arise from division of all squares by the number p—from these terms result $1, 4, 9, 16, ..., (p-4)^2, (p-3)^2, (p-2)^2, (p-1)^2$, of which the number of terms is $p-1$; and thus from these come the same number of residues. Truly these residues are not all different; for example, the last term $(p-1)^2 = pp - 2p + 1$ when divided by p leaves a residue equal to 1, which is the same as the first term, 1. In the same way, the penultimate term $(p-2)^2 = pp - 4p + 4$ produces the same residue as the second term, 4; and the term before this, $(p-3)^2$, gives the same residue as the third term, 9. And in general the nth term, which is nn, gives the same residue as term number $(p-n)$, which is $(p-n)^2$. Since therefore all residues arise from the terms $1, 4, 9, ..., (p-1)^2$ and the number of them is $p-1$, they are not all different from each other; among them, not all numbers less than p itself, of which the number of terms is $p-1$, can occur.

Corollary 1

13. Since therefore two residues are always equal, the number of different residues is reduced to half, $\frac{p-1}{2}$, because the number $p-1$ is even; and if $p-1$ is an odd number, i.e., p is even, then the number of different residues will be $\frac{p}{2}$; in this case a middle residue will be given, because it does not have its own counterpart.

Corollary 2

14. Since therefore the number of all numbers less than p itself is equal to $p-1$, it is evident that half of these numbers occur in residues; and therefore there will be numbers which never leave just one remainder from division of square numbers by the number p, except in the case when $p = 2$, because $p - 1 = \frac{p}{2} = 1$.

Corollary 3

15. Moreover, therefore, whatever may be the number p by which square numbers are divided, from numbers less than p itself there will always be at

least $\frac{p-1}{2}$ or $\frac{p-2}{2}$, numbers which are not found among the residues.[1] The first case is valid when p is an odd number; the second, when it is even.

Corollary 4

16. For this reason, therefore, the numbers less than the divisor p itself, the quantity of which is $p-1$, separate themselves one by one into two classes, of which one contains numbers occurring in residues while the other has those which do not occur in the class of residues. Here I will call these numbers *nonresidues.*

Scholium

17. In order that these things may be perceived more clearly, it is helpful to look at some examples in which residues and nonresidues are separated.

Let	$p=3$	$p=4$	$p=5$	$p=6$
	1, 4	1, 4, 9	1, 4, 9, 16	1, 4, 9, 16, 25
residues	1, 1	1, 0, 1	1, 4, 4, 1	1, 4, 3, 4, 1
nonresidues	2	2, 3	2, 3	2, 5

Let	$p=7$	$p=8$
	1, 4, 9, 16, 25, 36	1, 4, 9, 16, 25, 36, 49
residues	1, 4, 2, 2, 4, 1	1, 4, 1, 0, 1, 4, 1
nonresidues	3, 5, 6	2, 3, 5, 6, 7

Let	$p=9$	$p=10$
	1, 4, 9, 16, 25, 36, 49, 64	1, 4, 9, 16, 25, 36, 49, 64, 81
residues	1, 4, 0, 7, 7, 0, 4, 1	1, 4, 9, 6, 5, 6, 9, 4, 1
nonresidues	2, 3, 5, 6, 8	2, 3, 7, 8

[1] Translator: In the *Opera Omnia*, Ferdinand Rudio points out that the first edition and the *Commentationes arithmeticae collectae* have *or* $\frac{p}{2}$, which is a mistake. Rudio corrects this to *or* $\frac{p-2}{2}$.

Let	$p = 11$
	1, 4, 9, 16, 25, 36, 49, 64, 81, 100
residues	1, 4, 9, 5, 3, 3, 5, 9, 4, 1
nonresidues	2, 6, 7, 8, 10

Let	$p = 12$
	1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121
residues	1, 4, 9, 4, 1, 0, 1, 4, 9, 4, 1
nonresidues	2, 3, 5, 6, 7, 8, 10, 11

From this it is seen that the number of nonresidues is sometimes either $\frac{p-1}{2}$ or $\frac{p-2}{2}$, depending on whether p is an odd number or an even number. Sometimes it is even greater, but certainly never less, so that a proof of the theorem is needed.

Theorem 4

18. To find all residues which can result from division of squares by any number p, the only task is to divide by p the squares from one to the term $\frac{p-1}{2}$ or $\frac{p}{2}$, depending on whether p is an odd number or an even number.

Proof

We have already proved beforehand that all residues arise from division of the terms $1, 4, 9, 16, ..., (p-1)^2$; then we have certainly seen that the series of residues produced from this goes forwards and backwards; that is, it stays the same but is written in reverse order. Therefore, all residues, as far as they are distinct among themselves, will be obtained if only the terms up to half of this series are taken, so that if p is an odd number and thus $p-1$ is even, all numbers which occur among the residues will arise from the terms $1, 4, 9, 16, ..., \left(\frac{p-1}{2}\right)^2$. But if p is an even number, because the progression above has a middle term which responds by going backwards on itself, all residues arise from the terms $1, 4, 9, 16, ..., \left(\frac{p}{2}\right)^2$.

Corollary 1

19. Therefore, if p is an odd number, say $p = 2q+1$, all residues are known from only the squares $1, 4, 9, 16, ..., qq$. But if p is an even number, say $p = 2q$, the squares $1, 4, 9, 16, ..., qq$ produce all residues.

Corollary 2

20. Suppose all these residues are different from each other. Because the number of them is q, in the first case, in which $p = 2q + 1$ and $p - 1 = 2q$, the number of nonresidues will be q; in the second case, in which $p = 2q$ and $p - 1 = 2q - 1$, the number of nonresidues will be $q - 1$.

Corollary 3

21. If a is any number not greater than $\frac{p-1}{2}$ or $\frac{p}{2}$ and is known to be a residue because it results from the division of a square mm, all squares contained in the general form $(np \pm a)^2$ will produce the same residue.[2] But all numbers in the form $np \pm a$ are included, so that a does not exceed $\frac{p-1}{2}$ or $\frac{p}{2}$.

Scholium

22. Therefore, in order that we may more easily explore the class of numbers which are residues, we will represent the series of residues with the letters $1, \alpha, \beta, \gamma, \delta, \epsilon, \zeta$, etc. according to the divisor p, so that the number of these terms is either $\frac{p-1}{2}$ or $\frac{p}{2}$, depending on whether p is an odd number or an even number. First, it is evident that in the series $1, \alpha, \beta, \gamma, \delta, \epsilon$, etc. occur in order all the square numbers $1, 4, 9, 16$, etc. which are of course less than the number p itself, but as residues are left over after division of the greater squares by the same number p. We will track down the remaining properties of residues in the theorems that follow.

Theorem 5

23. If any number r occurs in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc., also found there are all powers r^2, r^3, r^4, r^5, etc., that is, residues which arise from division of these powers by the given number p.

Proof

[2] Translator: All previous editions have aa instead of mm, but it is not always possible for a to be a residue arising from division of the square aa by p, because this would imply $aa = kp + a$ for some integer k. Thus, $aa - a = kp$, so that $a(a-1) = kp$. The number p need not be prime, but if if is prime, then it must divide a or $a - 1$, which is impossible because a is not greater than $\frac{p-1}{2}$ or $\frac{p}{2}$. Euler may have intended aa to represent a general square.

Let the residue r emerge from the square aa so that $aa = mp + r$; and the square $a^4 = (mp+r)^2$ divided by p will give the same residue, because it arises from rr; and from the square $a^6 = (mp + r)^3$ arises the same residue,[3] because it is from r^3; and in the same way, the residues of the squares a^8, a^{10}, a^{12}, etc. agree with the residues of the terms r^4, r^5, r^6, etc. But the residues arising from all squares, however large, already come from the smaller squares $1, 4, 9, 16, ..., \left(\frac{p-1}{2}\right)^2$ or $\left(\frac{p}{2}\right)^2$ and therefore are contained in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc. Thus, if the number r occurs in this series, also occurring there are the terms r^2, r^3, r^4, r^5, etc., that is, residues which remain after division of these by the given divisor p.

Corollary 1

24. Therefore, any of the powers r^2, r^3, r^4, r^5, etc., which are less than p will themselves be found in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc., But higher powers introduce here their own residues which remain after division by p.

Corollary 2

25. If $r = 1$, because all its powers are 1, from them arises no term except 1 in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc. Therefore, in this case a new term is not found in the series of residues.

Corollary 3

26. Because in the series of residues, not more than $\frac{p-1}{2}$ or $\frac{p}{2}$ terms occur, neither can there be found more distinct residues from the powers r^2, r^3, r^4, r^5, etc., even if continued to infinity. Thus, infinitely many of these powers divided by p will produce equal residues.

Corollary 4

27. Therefore, let the powers r^m and r^n produce the same residue; their difference $r^m - r^n$, that is, $r^n(r^{m-n} - 1)$, will be divisible by the number p. Thus, if the factor r^n is coprime to p, which will happen if the residue r is coprime to p, then the other factor $r^{m-n} - 1$ will be divisible by p, and therefore the power r^{m-n} divided by p will leave a remainder of 1.

Corollary 5

[3] Translator: The same residue as that of r^3.

28. Therefore, suppose a power r^λ which leaves a remainder of 1 when divided by p is given; it is certainly contained in the series of residues, since r is a number coprime to p. But then the power $r^{\lambda+1}$ will give the residue r, the power $r^{\lambda+2}$ will give the residue r^2, $r^{\lambda+3}$ will give the residue r^3, etc., and thus the higher powers produce the same residues as the lower powers r, r^2, r^3, etc.

Corollary 6

29. Since therefore more than $\frac{p-1}{2}$ or $\frac{p}{2}$ different residues cannot arise, what remains is to produce a number λ not greater than $\frac{p-1}{2}$ or $\frac{p}{2}$ so that the power r^λ leaves a remainder of 1 when divided by p.

Scholium

30. Hence it is understood that, for example, although one can make powers r^2, r^3, r^4, r^5, etc. progress to infinity, nevertheless from them arise a finite number of residues if they are divided by the divisor p. Indeed, I have proven in a previous paper that if r is a number coprime to p, then a power of the form r^λ, where $\lambda < p.$ can always be given which leaves a remainder of 1 when divided by p. But we have already seen that if r is contained in the series of residues arising from squares, then the exponent λ can be made less than even $\frac{p}{2}$.

Theorem 6

31. If the numbers r and s appear in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc. which arise from division of squares by the number p, the product of those numbers rs also appears there, that is, the residue which comes from division of it by the number p.

Proof

Suppose the residue r comes from the square aa and the residue s from the square bb; $aa = mp + r$ and $bb = np + s$; now let the square $aabb = mnpp + msp + nrp + rs$ be formed, which therefore gives the same residue as rs when divided by p, or, if $rs > p$, gives the same residue as that which arises from rs. Therefore, since the residue arising from the square $aabb$ is contained in the series of residues, here also rs or the residue arising from it is found.

Corollary 1

32. Therefore, if the two numbers r and s appear in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc., then there occur not only the powers r, r^2, r^3, r^4, etc. and s, s^2, s^3, s^4, etc., but also products from the two terms in any way: rs, r^2s, rs^2, r^3s, r^3s^2, rs^3, etc.

Corollary 2

33. For this reason, therefore, it is evident[4] that if the formula $\frac{1}{(1-r)(1-s)}$ is broken up into a series $1 + r + s + rr + rs + ss + r^3 + rrs + rss + s^3 +$ etc., individual terms of this series occur in the series of residues or else residues from the terms arising from division by p.

Corollary 3

34. But even if the number of these terms is infinite, still it is known that from these cannot be produced more than $\frac{p-1}{2}$ or $\frac{p}{2}$ different residues, depending on whether p is an odd number or an even number.

Scholium

35. Therefore, it is more clearly apparent that, from these terms infinite in number, the number of different residues is nonetheless finite, and certainly not more than $\frac{p-1}{2}$ or $\frac{p}{2}$ arise; let us roll out a particular example and let $p = 19$; then $\frac{p-1}{2} = 9$, so that from the squares

$$1, 4, 9, 16, 25, 36, 49, 64, 81$$

arise the residues $1, 4, 9, 16, 6, 17, 11, 7, 5$. From this series of residues, let us consider the two numbers 5 and 6, from which we first form the series of powers

$$5, 25, 125, 625, 3125, 15625, 78125, \text{etc.},$$

$$6, 36, 216, 1296, 7776, 46656, 279936, \text{etc.}$$

From the former series divided by 19, these residues appear: 5, 6, 11, 17, 9, 7, 16, 4, 1; namely, the sequence of residues is always obtained if the preceding term is multiplied by 5, and if the product is greater than 19, it is reduced to less than 19. In the same way, from the powers of the number 6 will appear these residues: 6, 17, 7, 4, 5, 11, 9, 16, 1.

[4] Translator: The *Commentationes arithmeticae collectae* has $(r - s)$ in the denominator, which is a mistake. In the *Opera Omnia*, Ferdinand Rudio corrects this to $(1 - s)$.

Moreover, if each individual residue is multiplied by the above terms and the products are reduced to less than 19, the same numbers appear; that is, the latter series is first multiplied by 5, then by 6, 11, 17, etc., so that what follows is

by 5:	11,	9,	16,	1,	6,	17,	7,	4,	5,
by 6:	17,	7,	4,	5,	11,	9,	16,	1,	6,
by 11:	9,	16,	1,	6,	17,	7,	4,	5,	11,
by 17:	7,	4,	5,	11,	9,	16,	1,	6,	17,
by 9:	16,	1,	6,	17,	7,	4,	5,	11,	9,
by 7:	4,	5,	11,	9,	16,	1,	6,	17,	7,
by 16:	1,	6,	17,	7,	4,	5,	11,	9,	16,
by 4:	5,	11,	9,	16,	1,	6,	17,	7,	4.

Therefore, it is observed that however the numbers 1, 4, 9, 16, 6, 17, 11, 7, 5 are combined by multiplication among themselves to create a series of residues, since division done by 19 reduces to less than 19, they always return the same numbers, and no number of those which are not residues ever appears, that is, 2, 3, 8, 10, 12, 13, 14, 15, 18.

Corollary 4

36. Therefore, if $1, \alpha, \beta, \gamma, \delta$, etc., is the series of all residues which result from division of squares by the number p, in that same series also occur all products of two or more of the numbers $\alpha, \beta, \gamma, \delta$, etc. Therefore, if the expression $\dfrac{1}{(1-\alpha)(1-\beta)(1-\gamma)(1-\delta)\text{ etc.}}$ is broken up into a series, all of its terms occur in the series of residues.

Theorem 7

37. If in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc. which come from division of squares by the number p are found the numbers r and rs which are coprime to p, then the number s, which is a factor of it, will also be contained in the same series of residues.

Proof

Suppose the residue r comes from the square aa, and rs from bb; then $aa = mp + r$ and $bb = np + rs$; from this, $bb - aas = np - mps$, and thus $bb - aas$ will be divisible by p. And since r and rs are numbers coprime to p, the squares aa and bb will also be coprime to p; thus, if the squares aa and bb are not coprime, they can be reduced to coprime by a common square divisor so that $bb - aas$ is still divisible by p. Therefore, let b and a be coprime numbers; since the form $(mp \pm b)^2 - aas$ is divisible by p, such a number m can always be chosen so that it makes $mp \pm b$ a multiple of a itself. Thus, let $mp \pm b = ac$; $aacc - aas$ will be divisible by p; because this equals $aa(cc - s)$ and one factor aa is coprime to p, it is necessary that the other factor $cc - s$ is divisible by p, so that the square cc divided by p leaves a remainder of s; thus, the number s is found in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc., since the numbers r and rs appear here and they are coprime to p.

Corollary 1

38. Therefore, so that the truth of the theorem is preserved, it is necessary that the numbers r and rs, or equivalently, r and s, be relatively prime to the divisor p. For exanple, earlier we saw that if $p = 12$, the numbers 4 and 0, or 4 and 12, are found among the residues. but having set $r = 4$ and $rs = 12$, it does not follow that the number $s = 3$ is found among the residues, because r and s are not numbers relatively prime to p; and, in fact, the number 3 is contained among the nonresidues.

Corollary 2

39. If, however, the divisor p is a prime number, so that all residues $\alpha, \beta, \gamma, \delta$, etc. are thus coprime to it, and among these occur the numbers r and rs, then the number s certainly also occurs among them.[5]

Corollary 3

40. If among the residues appear the numbers r and s relatviely prime to p, then because the residues $p + r$, $2p + r$, and, in general, $np + r$ are regarded as equivalent to the residue r, and $np + r = ts$, then the number t is also found among the residues.

Scholium

41. We are not obliged to consider exceptions, when residues are numbers not relatively prime to p: in the following we always suppose the divisor p to be a prime number; and since the residues arising from the number 2 are obvious, let the divisor p be an odd number, that is, $p = 2q + 1$; now then a series of residues will be formed from the terms

$$1, 4, 9, 16, ..., qq,$$

[5] Translator: The *Commentationes arithmeticae collectae* has 5, which is a mistake. In the *Opera Omnia*, Ferdinand Rudio corrects this to s.

so that the number of them, since they are different from each other, cannot be greater than q. If therefore the residues from this prime divisor $p = 2q + 1$ are $1, \alpha, \beta, \gamma, \delta$, etc., then in this series occur not only the products from two or more terms $\alpha, \beta, \gamma, \delta$, etc., but, because all these residues are coprime to p, if r and rs appear among them so that one is divisible by the other, then also the quotient s arising from these will be contained in the same series of residues.

Theorem 8

42. If from the prime divisor $p = 2q + 1$ by which all square numbers are divided there arises a series of residues $1, \alpha, \beta, \gamma, \delta, \epsilon$, etc., then the number of them is q, and all these residues will be different from each other.

Proof

First, it is evident that no residue in this series can be 0; since they arise from squares not greater than qq itself, none of these squares is divisible by the prime number $p = 2q + 1$; therefore 0 certainly occurs less than twice among the residues. Now let us set equal two residues which arise from the squares aa and bb; the difference $aa - bb$ of these squares will be divisible by the divisor $p = 2q + 1$. But since the residues $1, \alpha, \beta, \gamma, \delta$, etc. arise from the smallest squares, which do not exceed qq, those squares aa and bb are not greater than qq; for this reason, a will not be greater than q, nor will b be greater than q, and consequently $a + b$ will not be greater than $2q$, so that certainly $a + b < p$. Therefore, since the difference of the squares $aa - bb$ was divisible by p because the residues were equal and p is a prime number, either the sum $a + b$ or the difference $a - b$ will be divisible by p; but neither is possible, because $a - b < p$ and $a + b < p$. Therefore, all residues which result from division of the squares $1, 4, 9, 16, ..., qq$ by the prime number $p = 2q + 1$ are unequal to each other.

Corollary 1

43. Therefore, the number of all different residues which arise from division of squares by the prime number $p = 2q + 1$ is certainly q; indeed, before it was shown that it is not greater than q, but here we have proven irrefutably that it is not less than q.

Corollary 2

44. Since the number of all numbers less than the divisor $p = 2q + 1$ itself is $p - 1 = 2q$, it is evident that only half of these numbers occur in the series of residues $1, \alpha, \beta, \gamma$, etc. and they constitute it, but the other half constitute the series of nonresidues, so that if p is a prime number, the series of nonresidues also consists of q numbers.

Corollary 3

45. Therefore, if x is any number from the series of nonresidues corresponding to p, we can certainly affirm, whatever n may be, that no number in the form $np + x$ can be a square.

Scholium

46. Because we now direct our investigations only to prime divisors, the divisor will produce both residues and nonresidues, which correspond to the smaller prime numbers, as shown here. That is, in general, if p is a divisor, we represent the series of residues by $1, \alpha, \beta, \gamma, \delta$, etc. and the series of nonresidues by a, b, c, d, e, etc.; and so that we may more easily refer to the residues and the nonresidues, we will present them in this way:

$$p\left\{\begin{matrix} 1, & \alpha, & \beta,. & \gamma, & \delta, & \epsilon, & \zeta, & \text{etc.} \\ a, & b, & c, & d, & e, & f, & g, & \text{etc.} \end{matrix}\right\}$$

Surely we will write two series of numbers in any case, of which the upper contains residues and the lower contains nonresidues, and we will prefix both of them with the divisor p, to which they belong. Residues and nonresidues result from single prime divisors, so that they will be indicated in this way:

$$3\left\{\begin{matrix} 1 \\ 2 \end{matrix}\right\}, 5\left\{\begin{matrix} 1, & 4 \\ 2, & 3 \end{matrix}\right\}, 7\left\{\begin{matrix} 1, & 4, & 2 \\ 3, & 5, & 6 \end{matrix}\right\}, 11\left\{\begin{matrix} 1, & 4, & 9, & 5, & 3 \\ 2, & 6, & 7, & 8, & 10 \end{matrix}\right\},$$

$$13\left\{\begin{matrix} 1, & 4, & 9, & 3, & 12, & 10 \\ 2, & 5, & 6, & 7, & 8, & 11 \end{matrix}\right\}, 17\left\{\begin{matrix} 1, & 4, & 9, & 16, & 8, & 2, & 15, & 13 \\ 3, & 5, & 6, & 7, & 10, & 11, & 12, & 14 \end{matrix}\right\},$$

$$19\left\{\begin{matrix} 1, & 4, & 9, & 16, & 6, & 17, & 11, & 7, & 5 \\ 2, & 3, & 8, & 10, & 12, & 13, & 14, & 15, & 18 \end{matrix}\right\},$$

$$23\left\{\begin{matrix} 1, & 4, & 9, & 16, & 2, & 13, & 3, & 18, & 12, & 8, & 6 \\ 5, & 7, & 10, & 11, & 14, & 15, & 17, & 19, & 20, & 21, & 22 \end{matrix}\right\},$$

$$29\left\{\begin{matrix} 1, & 4, & 9, & 16, & 25, & 7, & 20, & 6, & 23, & 13, & 5, & 28, & 24, & 22 \\ 2, & 3, & 8, & 10, & 11, & 12, & 14, & 15, & 17, & 18, & 19, & 21, & 26, & 27 \end{matrix}\right\}.$$

Here the residues are put in order according to the squares from which they arise, but we have assembled nonresidues progressing from least to greatest because they are not connected to any order. These examples can also serve this end: through them, the properties of residues can be investigated before they are proved.

Theorem 9

47. If from the division of squares by the prime number $p = 2q + 1$ arise the series of residues $1, \alpha, \beta, \gamma, \delta$, etc. and the series of nonresidues a, b, c, d, e, etc., and the number r occurs in this series of nonresidues, then in it also occur all the numbers $\alpha r, \beta r, \gamma r, \delta r$, etc. or their residues left over after division by p.

Proof

Any of the numbers, say, αr, is contained in either the series of residues or the series of nonresidues. But since α is contained in the series of residues, if αr were also contained there, then r would necessarily appear in the series of residues as well. Therefore, since by hypothesis r is a number from the series of nonresidues, the number αr will not be in the series of residues; αr will thus appear in the series of nonresidues, like the numbers $\beta r, \gamma r, \delta r$, etc. However, just as we have proved about the products $\beta r, \gamma r, \delta r$, etc. which are greater than p, it needs to be understood that this concerns the residues which the product leaves when divided by p.

Corollary 1

48. Because all the numbers $1, \alpha, \beta, \gamma, \delta$, etc., of which the number is q, are different from each other, it also follows that the numbers $r, \alpha r, \beta r, \gamma r, \delta r$, etc. are different from each other; thus, if all residues are obtained, from one known nonresidue all the remaining nonresidues can be specified.

Corollary 2

49. Therefore, the series $r, \alpha r, \beta r, \gamma r, \delta r$, etc. will clearly give all nonresidues; it thus contains as many as q different numbers, and no more nonresidues exist, if indeed the divisor p is a prime number.

Corollary 3

50. Therefore, if from the series of nonresidues any other number s is taken, the products $\alpha s, \beta s, \gamma s$, etc. do not produce other numbers which are nonresidues,[6] nor are they found in this way from any other r.

[6] Translator: In the *Opera Omnia*, Ferdinand Rudio points out that the first edition and the *Commentationes arithmeticae collectae* have *residues*, which is a mistake. Rudio corrects this to *nonresidues.*

Theorem 10

51. The products of two numbers from the series of nonresidues are contained in the series of residues, since these residues arise from division of square numbers by some prime number.

Proof

Therefore, let $p = 2q + 1$ be a prime divisor, and let the series of residues be $1, \alpha, \beta, \gamma, \delta$, etc., and let the series of nonresidues be a, b, c, d, e, etc. But we have seen that if r is any nonresidue, the series of nonresidues can be presented in this way:

$$r, \alpha r, \beta r, \gamma r, \delta r, \text{etc.}$$

Now the product of any two of these terms $\alpha\beta r^2$ consists of the two factors $\alpha\beta$ and rr, and both of them are contained in the series of residues, because all squares, and therefore also rr, appear here. Thus, it is evident that the product of any two nonresidues is contained in the series of residues.

Corollary 1

52. Thus, just as the product of two residues gives a residue, so also the product of two nonresidues will give a residue. But the product of a residue and a nonresidue always produces a nonresidue.

Corollary 2

53. Therefore, it also follows that just as a residue divided by a residue yields a residue, so also a nonresidue divided by a nonresidue yields a residue. Certainly a residue divided by a nonresidue or, conversely, a nonresidue divided by a residue produces a nonresidue.

Corollary 3

54. Just as two nonresidues multiplied together produce a residue, so also three nonresidues multiplied together will produce a nonresidue; certainly four nonresidues again produce a residue, while five, a nonresidue, and so on.

Definition

55. The *complement* of a residue is its difference from the divisor from which it arose; thus if the divisor is p and the residue is r, the complement of the residue will be $p - r$.

Corollary 1

56. Because, on account of the residues, all the numbers $r, p + r, 2p + r$, and in general $np + r$ are considered the same, regardless of what number is chosen for n, the complement will be $p - np - r$; so if $n = 1$ is chosen, the complement of the residue will be $-r$.

Corollary 2

57. If n is chosen to be -1, the residue r can also be expressed as $r - p$ so that it is negative. In division, for example, if the obtained quotient is too large, it can be shifted to a negative residue. Thus, the positive residue r will be equivalent to the negative residue $r - p$.

Corollary 3

58. If $r > \frac{1}{2}p$, then the negative residue can be expressed as $r - p$, which will be less[7] than $\frac{1}{2}p$. So if the use of negative expressions is called for, all residues can be expressed by numbers not greater than $\frac{1}{2}p$, half the divisor. Thus, for the divisor $p = 23$, these residues expressed by numbers not greater than $\frac{23}{2}$ will be obtained:

$$1, 4, 9, -7, 2, -10, 3, -5, -11, 8, 6.$$

Corollary 4

59. And in the same way, nonresidues can also be expressed by numbers less than $\frac{1}{2}p$ itself, and the nonresidues for the divisor $p = 23$ will be

$$5, 7, 10, 11, -9, -8, -6, -4, -3, -2, -1.$$

Thus, if $p = 2q + 1$, the number of residues and the number of nonresidues will be q, and numbers greater than q cannot occur in either series.

[7] Translator: In absolute value, that is (here and throughout the paper).

Corollary 5

60. If residues are expressed in this way, it is immediately evident that either the complement of some residue is contained in the same series of residues, or it is not. Of course, if r is a residue, $-r$ will be its complement, and conversely if $-r$ is a residue, then $+r$ will be its complement. Therefore unless the same number occurs twice in the series of residues, namely positively and negatively, its complement is not contained in the series of residues.

Theorem 11

61. If, in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc. which are generated by division of squares by the prime number $p = 2q + 1$, the complement of one term occurs, then the complements of all terms also occur in the same series.

Solution

Let r be a residue whose complement $-r$ also occurs in the series $1, \alpha, \beta, \gamma, \delta$, etc. Therefore, since $-r$ divided by r yields -1, the number -1 also occurs in the same series; that is, the value of one of the letters $\alpha, \beta, \gamma, \delta$, etc. will be -1. Therefore, since products of two terms are also found in the same series, the terms $-\alpha, -\beta, -\gamma, -\delta$, etc. appear here. Thus, the complement of any residue is also found in the series of residues, since the complement of one term appears in it.

Corollary 1

62. Therefore, if the complement $-r$ of one term r is contained in the series of residues, then any number of this series occurs twice, namely, first positively and then certainly also negatively. For example, in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc., the terms $-1, -\alpha, -\beta, -\gamma, -\delta$, etc. will also be contained.

Corollary 2

63. Therefore, in the case in which every term occurs twice in the series of residues, the number of all terms will necessarily be even. But the number of all terms is q; therefore, unless q is an even number, it cannot be done, namely, that the complements of residues would also be contained in the series of residues.

Corollary 3

64. Therefore, if q is an odd number, say $q = 2n+1$, so that $p = 4n+3$, clearly in the series of residues no number occurs whose complement is also contained in the same series. Therefore, in this case, all complements go into the series of nonresidues, and in both[8] the number of terms will be odd, $q = 2n + 1$.

Scholium

65. Therefore, this is recognized as the most important distinction: $p = 2q+1$ appears among the prime numbers, and all depends on whether q is an even number or an odd number, because in the latter case we certainly know that the complement of no residue is contained in the series of residues. But if we set $q = 2n$ in the former case and $q = 2n-1$ in the latter case, the prime number will be $p = 4n + 1$ in the former case, certainly $p = 4n - 1$ in the latter; from this it is evident that all prime numbers, except 2, are either one more than a multiple of 4 or one less than it, and thus we obtain two classes of numbers, of which one is contained in the form $4n + 1$, and the other in the form $4n - 1$. Therefore, the prime numbers 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc. are of the first class $4n + 1$, and certainly 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, etc. are of the second class $4n - 1$. About the first class of prime numbers, Fermat once pronounced that each one is the sum of two squares, of which theorem I have finally established the truth not long ago after many attempts. But about the numbers of the latter class, it is easily shown that none of them is a sum of two squares; rather, I will also soon prove that there cannot be a sum of two squares $aa + bb$ which is divisible by a prime number of the type $p = 4n - 1$, unless each square aa or bb is individually divisible by it. Nevertheless, about these numbers Fermat affirmed that individual ones were the sum of three or four squares; for example, we see that $3 = 1 + 1 + 1$, $7 = 1 + 1 + 1 + 4$, $11 = 1 + 1 + 9$, $19 = 1 + 9 + 9$, $23 = 1 + 4 + 9 + 9$, $31 = 4 + 9 + 9 + 9 = 1 + 1 + 4 + 25$, etc., but no number of this kind exists which cannot be broken up into at least four squares. Even if it is claimed that Fermat found a proof for himself, he has not published it anywhere, so that since it seems to have died out completely and nothing has been developed subsequently, this proof, which can be found in the analysis of Diophantus and the universal knowledge of numbers, is of greatest importance. Indeed, here I will prove that any given prime number $4n - 1$ is always the sum of four squares, and moreover can show that a sum of three squares is divisible by it. Therefore, since it can also be proved that the product of two numbers, both of which are a sum of four squares, is also a sum of four squares, the desired proof we appear to lack is not far off. That is, it remains only to be proved that if the sum of four squares is divisible by a number which is also a sum of four squares, the quotient will also certainly be a sum of four squares.

Theorem 12

[8] Translator: Both the residues and their complements, the nonresidues.

66.[9] If all squares are divided by the prime number $4n-1$ and from these arise a series of residues $1, \alpha, \beta, \gamma, \delta$, etc., the complement of no residue will be contained in this series of residues.

Proof

All the residues

$$1, \alpha, \beta, \gamma, \delta, \ldots, \nu$$

result from division of the squares

$$1, 4, 9, 16, 25, \ldots, (2n-1)^2;$$

thus the number of these residues is $2n-1$ and is therefore odd. But if the complement $p-\alpha$ (or $-\alpha$) of one residue α were also in the series, then the complements of all residues should occur there as well, and thus since each residue appears twice, namely with the $+$ sign present and with the $-$ sign present, the number of residues would be even. Therefore, since it is odd, it cannot be that the complement of one residue is contained in the series of residues as well.

Corollary 1

67. If the last term of a series of residues is set equal to ν, because it arises from the square $(2n-1)^2 = 4nn - 4n + 1$ divided by $4n-1$, the residue will be $\nu = -3n - 1$, that is, n, with $n-1$ obtained as the quotient. Therefore, its complement $-n$, which is $3n-1$, is not found in the series of residues. Thus, the number $-n$, which is $3n-1$, will surely be in the series of nonresidues.

Corollary 2

68. Since $mp - n$, that is, $m(4n-1) - n$, is included among all numbers which when divided by $4n-1$ give a residue of $-n$, it is evident that none of the numbers $m(4n-1) - n$, that is, $4mn - m - n$, can ever be a square.

Corollary 3

69. Because the square numbers 1, 4, 9, 16, 25, etc. appear in the series of residues, the complements of them, $-1, -4, -9, -16, -25$, etc., certainly do not appear in it. Thus, the square numbers with the $-$ sign included go into the series of nonresidues.

[9] Translator: In the *Commentationes arithmeticae collectae*, this section is mistakenly labeled as 67. In the *Opera Omnia*, Ferdinand Rudio corrects this to 66.

Theorem 13

70. A sum of two squares which is divisible by a prime number of the form $4n-1$ cannot be produced, unless each of the squares is individually divisible by it; that is, a sum of two coprime squares which is divisible by the prime number $4n-1$ cannot be produced.

Proof

Let us suppose, for example, that the sum of two squares $aa+bb$ is divisible by the prime number $4n-1$, where neither aa nor bb is individually divisible by $4n-1$. Therefore, let r be the residue which is left over after division of the square aa by $4n-1$, and let s be the residue arising from division of the square bb; and in particular, both r and s appear in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc. Now the sum of squares $aa+bb$ divided by $4n-1$ leaves the residue $r+s$; since by hypothesis this should equal[10] the divisor $4n-1$, $s = 4n-1-r$, that is, $s = -r$ and so s is a complement of the residue r. Therefore, if r is contained in the series of residues, its complement s certainly does not appear in it; thus, given the arbitrary square aa, there is no such square bb so that the sum $aa+bb$ is divisible by the prime number $4n-1$, unless the square aa itself is divisible by $4n-1$, in which case bb should also be divisible by $4n-1$. Therefore, no sum of two coprime squares can be produced which is divisible by the prime number $4n-1$.

Corollary 1

71. Therefore, a number of the form $aa+1$ which is divisible by the prime number $4n-1$ cannot be produced. In other words, it would be required that the residue arising from the square would be -1, but this will not appear in the series of residues.

Corollary 2

72. Because the sum of two squares $aa+bb$ is divisible by no prime number of the form $4n-1$, neither will it be divisible by any composite number p whose prime factors have the form $4n-1$; for if it were divisible by this number p, then it would also be divisible by its factor $4n-1$.

Theorem 14

[10] Translator: Here, Euler uses equality loosely; strictly speaking, this equality and the next equality are congruences modulo $4n-1$.

73. Whether the number $4n-1$ is prime or composite, there is no sum of two coprime squares which is divisible by the number $4n-1$.

Proof

Of course, if the number $4n-1$ is prime, the validity of the theorem has already been established. But if $4n-1$ is not a prime number, it will be a product of different prime numbers, certainly odd, because the number $4n-1$ is itself odd. However, all prime numbers are of the form $4m+1$ or $4m-1$; but not all factors of the number $4n-1$ can be of the form $4m+1$; for if any numbers of the form $4m+1$ are multiplied together, the product will always be a number of the form $4n+1$, one more than a multiple of four. Thus it is necessary that the number $4n-1$ have at least one prime factor of the form $4m-1$; and because no sum of two coprime squares is divisible by such a prime number, neither can one be divisible by the composite number $4n-1$.

Corollary 1

74. Since no sum of two coprime squares is divisible by the number $4n-1$, whether it is prime or composite, how much less will the number $4n-1$ itself be a sum of two squares. For if $4n-1 = aa+bb$, both of the squares aa and bb would have to be divisible by $4n-1$, which cannot be the case, because each is less than $4n-1$.

Scholium

75. That no number of the form $4n-1$ can be the sum of two squares is easily shown in this way as well. For if the number $4n-1$ were a sum of two squares, one of them would be even, and the other odd. But all even squares are numbers of the form $4f$ and all odd squares are of the form $4g+1$. Therefore, the sum of two squares, of which one is even and the other odd, will be a number of the form $4f+4g+1$, that is, $4n+1$; thus, a number of the form $4n-1$ cannot be a sum of two squares.

Corollary 2

76. Also, no number which has a factor of the form $4n-1$ can be a divisor of a sum of two coprime squares; for if it were a divisor, its factor $4n-1$ would also be a divisor, which cannot be.

Corollary 3

77. Thus, how much less can a number which has a factor $4n-1$ be a sum of two coprime squares. So it is impossible that $m(4n-1)=aa+bb$ if a and b are indeed coprime numbers.

Theorem 15

78. No number contained in the form $4mn-m-n$, where any numbers are chosen for m and n, can ever be a square.

Proof

Since no number which has a factor $4n-1$ can be a sum of two coprime squares, that is, which have no one common divisor, it follows that it cannot be that $(4m-1)(4n-1)=1+aa$. Thus, one will not have $16mn-4m-4n=aa$, so that one-fourth of it, $4mn-m-n$, can never be a square.

Theorem 16

79. In the series of residues $1, \alpha, \beta, \gamma, \delta$, etc. which result from division of squares by any number p, if the complement of some residue appears in the same series of residues, then there are two squares whose sum is divisible by the same number p, even if neither is individually divisible by p.

Proof

Suppose the square aa produces the residue r while the square bb produces the residue $-r$, that is, $p-r$, which is its complement, so that r is the residue whose complement is also contained in the series of residues. Now it is evident that the sum of these squares $aa+bb$ will be divisible by the number p.

Corollary 1

80. If p is a prime number and a complement of one residue appears in the series of residues, the complements of individual residues will also be there. Therefore, for any given square aa whose residue is r, there will be a different one xx whose residue will be $-r$, where x is not greater than $\frac{p}{2}$ and the sum $aa+xx$ is divisible by p.

Corollary 2

81. Thus, if there is a sum of two squares $aa + bb$ divisible by the prime number p, because of the residues arising from aa and bb, one being the complement of the other, the complement of a residue arising from any other square cc will also be found in the series of residues. Thus, there will be a sum of two squares $cc + xx$ divisible by the number p.

Corollary 3

82. However, from what is preceding, it is evident that this case cannot take place, neither if p is a prime number of the form $4n-1$ nor even if p has a factor of this form, because in either case there is a sum of two squares divisible by p, squares which are in fact coprime.

Corollary 4

83. Thus, no prime numbers remain to which the theorem can be applied, except those which are contained in the form $4n + 1$.

Scholium

84. But all prime numbers of the form $4n+1$ have this property, that in the series of residues arising from them, the complement of any term is also found here; this has not yet been proved, nor does it seem hopeless; in fact, a proof can be elicited from these same principles, even if I am not permitted to reach it. But the series of residues arising from simpler prime numbers of this form is presented in the following way, where the residues greater than half of the arbitrary number have been shown represented by negative numbers, in order that it may more readily appear which are the complements of others:

$$5\{1,-1\}; 13\{1,4,-4,3,-1,-3\}; 17\{1,4,-8,-1,8,2,-2,-4\};$$
$$29\{1,4,9,-13,-4,7,-9,6,-6,13,5,-1,-5,-7\}$$
$$37\{1,4,9,16,-12,-1,12,-10,7,-11,10,-4,-16,11,3,-3,-7,-9\}$$

Thus, in these series it is clear that the complement of any term also appears in them. A direct proof that it necessarily turns out like this if the divisor is a prime number of the form $4n + 1$ is still desired, that in this way it should be seen as established. From the prime number $4n+1$ appears the series of residues $1, \alpha, \beta, \gamma, \delta$, etc., of which the number of terms is $2n$; now if anyone denies that that complements of these terms are contained in the same series as well, he should say that all the complements $-1, -\alpha, -\beta, -\gamma, -\delta$, etc., constitute the series of nonresidues; since the number of these terms is $2n$, it would follow that there are no other nonresidues besides these; thus, if any number contained in the series of nonresidues could be formed which is not the complement of any term contained in the series of residues, it would also clearly follow that no complement of the series of residues appears in the series of nonresidues. Therefore, if this could be proved, one would have the desired proof, and indeed, a direct one. For there is now an indirect proof from all of this, because I have proved that every prime number of the form $4n+1$ is a sum of two squares; thus, if $4n+1 = aa+bb$, of the residues arising from the squares aa and bb one of the two will be a complement, and hence it is rightly concluded that the complement of any residue is also contained in the series of residues.

Theorem 17

85. If, in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc. which arise from division of squares by any number p, a term appears which is the complement of a sum of two other terms, then a sum of three squares can be produced which is divisible by the number p such that no root of a square is greater than $\frac{p}{2}$.

Proof

Let r and s be residues arising from the two squares aa and bb, of which the sum is $r+s$ whose complement is thus $p-r-s$, which is $-r-s$. Now if this complement is found in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc., there will be a square $cc < \frac{1}{4}pp$ which leaves a remainder of $-r-s$ when divided by p; and thus it will be clear that the sum of these three squares will be divisible by the number p, and not one of these squares is greater than $\frac{1}{4}pp$.

Corollary 1

86. Thus, if in the series of residues $1, \alpha, \beta, \gamma, \delta$, etc. appear some of the numbers $-2, -1-\alpha, -2\alpha, -1-\beta, -\alpha-\beta, -2\beta, -1-\gamma, -\alpha-\gamma, -\beta-\gamma, -2\gamma, -1-\delta, -\alpha-\delta$, etc., a sum of three squares can always be produced so that it is divisible by the number p.

Corollary 2

87. And if p is a prime number, because the roots a, b, c of the squares are each less than $\frac{p}{2}$, the numbers will be coprime to p and thus also the squares themselves; and if three squares are themselves not relatively prime to each other but instead have a common square divisor, because this is necessarily relatively

prime to p, those squares can de divided by it to produce smaller numbers which are relatively prime to each other; and their sum, taken together, will be divisible by p.

Corollary 3

88. If, in the series of residues, the complements of individual terms are also there, then furthermore a sum of two squares can be produced which is divisible by the number p. However, when there is a sum of two squares, there will moreover be a sum of three squares, since the form $aa + bb$ is contained in the form $aa + bb + cc$.

Scholium

89. It is proved in the same way that if in the series of residues there appears a number which is the complement of the sum of three residues, then a sum of four squares can be produced which is divisible by the number p. Truly, if sums of two or three residues are taken, so many different numbers are produced that it is seen clearly enough that the complements of all of them cannot be contained in the series of nonresidues.

Theorem 18

90. For any given prime number p, if it can be shown that no sum of two coprime squares is divisible by it, certainly a sum of three squares divisible by it can always be created, where none of the terms is individually divisible by p.

Proof

Let $1, \alpha, \beta, \gamma, \delta, \epsilon$, etc. be a series of residues arising from division of squares by a given prime number p. Now in this series, either -1 appears or it does not appear. If -1 appears here, the complements of individual residues also appear here, and thus there will be several ways a sum of two squares is divisible by p. If, however, -1 is not contained in the series of residues, it will be found in the series of nonresidues, where the complements of all residues also appear; therefore, in this case, there will be no sum of two squares divisible by the number p unless each individually has that divisor. But for these cases, I show there is a sum of three squares divisible by the prime number p.

First, let it be noted that if any number r appears in the series of residues, its complement $-r$ is certainly in the series of nonresidues. and conversely if r is a nonresidue, then $-r$ will certainly be a residue. Now let us suppose that there is no sum of three squares divisible by p; because in the series of residues the number 1 appears first, the number -2 will not appear there (for there would be elsewhere a sum of three squares divisible by p, contrary to the hypothesis). Therefore, -2 appears in the series of nonresidues and thus the number 2 in the series of residues. Now since the numbers 1 and 2 are contained in the series of residues, the complement of their sum -3 will be a nonresidue and therefore 3, a residue. In this same way, from the residues 1 and 3 it is concluded that -4 is a nonresidue, and so 4, a residue. And in general if any residue is r, $-r-1$ is bound to be a nonresidue, and therefore $1+r$ will be a residue. So from this hypothesis it follows that all whole numbers 1, 2, 3, 4, 5, 6, etc. are contained in the series of residues, and thus no whole numbers remain for the series of nonresidues; since this is absurd, we must conclude that there is a sum of either three or four squares divisible by the prime number p, none individually divisible by p. If by chance they are not relatively prime, they can be reduced by the greatest common divisor to relatively prime, because the greatest common divisor of squares is certainly a square.

Corollary 1

91. By similar reasoning, one is proved much more inconsistent if one will deny that the sum of four squares is divisible by a prime number. Thus, for any given prime number p, there will always be a sum of four squares divisible by it.

Corollary 2

92. If the prime number p is not a divisor of any sum of two squares, those three squares aa, bb, cc for which the sum is divisible by p, those terms will be less than $\frac{1}{4}pp$. Consequently, $aa + bb + cc < \frac{3}{4}pp$. so that the quotient which arises from division of the sum $aa + bb + cc$ by p will be less than $\frac{3}{4}p$.

Theorem 19

93. If a sum of four squares is divided by a sum of four squares, the quotient will also be a sum of four squares, at the very least, as fractions.

Proof

Let $aa + bb + cc + dd$ be a sum of four squares, which, divided by the sum of four squares $pp + qq + rr + ss$, will be the quotient

$$\frac{aa + bb + cc + dd}{pp + qq + rr + ss},$$

which, whether it is an integer or a fractional number, can always be broken up into four squares, at the very least, as fractions. For example, let us multiply the numerator and denominiator by $pp+qq+rr+ss$, so that the denominator is made a square; that quotient will be

$$\frac{(aa+bb+cc+dd)(pp+qq+rr+ss)}{(pp+qq+rr+ss)^2};$$

now if the numerator can be broken up into four squares, the fraction itself will be equal to the sum of four squares. But the numerator can be broken up into four squares in several ways; for instance, if we suppose

$$(aa+bb+cc+dd)(pp+qq+rr+ss) = xx+yy+zz+vv,$$

then

$$\begin{aligned} x &= ap+bq+cr+ds \\ y &= aq-bp\pm cs\mp dr \\ z &= ar\mp bs-cp\pm dq \\ v &= as\pm br\mp cq-dp, \end{aligned}$$

which four numbers, if each is divided by the common denominator $pp+qq+rr+ss$, will give the roots of four squares, the sum of which equals the given quotient. Therefore, unless the numbers x, y, z, and v are divisible by $pp+qq+rr+ss$, they can be expressed as four squares, at least as fractions, the sum of which is equal to the quotient $\dfrac{aa+bb+cc+dd}{pp+qq+rr+ss}$.

Corollary 1

94. Those things which are proved here about sums of four squares also extend to sums of three or of two, since nothing prevents one or two of the numbers a, b, c, d and p, q, r, s from being equal to zero.

Corollary 2

94.[11] Thus, if the sum of three squares is divided by a sum of three or four squares, the quotient will certainly be a sum of four squares.

Corollary 3

[11] Translator: In the *Commentationes arithmeticae collectae* and the *Opera Omnia*, there are two consecutive paragraphs numbered 94.

95. Because the product of two sums of four squares is also a sum of four squares, it is evident that if all prime numbers are sums of four or fewer squares, then all numbers are sums of four or fewer squares.

Scholium

96. If the sum of four squares $aa + bb + cc + dd$ is divislble by the sum of four squares $pp + qq + rr + ss$, then the quotient is a sum of four squares, not just as fractions but also as integers–this is a most elegant theorem of Fermat, whose proof has eluded our grasp. I acknowledge that until now this proof could not be found, but nevertheless, from this, a way is disclosed for the following theorem to be proved, that any number can be expressed as a sum of four or fewer squares, that is, in the case in which fractional squares are not excluded; even if this theorem is always true for integers as well, it still seems not a little beyond me; I have proved it elsewhere using quotients of squares of integers. Indeed, although the proof after Fermat and until now has been sought in vain, I think I have come close to the target.

Theorem 20

97. Every number is the sum of four or fewer squares if fractional squares are not excluded.

Proof

This theorem is certainly true even if fractional squares are excluded; that is, Fermat asserted that every integer is a sum of four or fewer integer squares, but I confess that this proof is not yet possible for me to find; thus, I will give a proof for the case in which fractional squares are not excluded. Now I have noted that this proof is reduced to just prime numbers, so that it suffices to prove the theorem for these. Thus, since we have found that the smaller prime numbers, 2, 3, 5, 7, 11, 13, etc., can all be broken up into four or fewer squares, if anyone denies the following things, to him it must be said that there is some smallest prime number which is not the sum of four or fewer squares. Let p be that prime number, so that all prime numbers less than it, and thus also certainly all formed from them, are the sum of four or fewer squares. Now by a preceding theorem, there is a sum of three squares, say $aa + bb + cc$, divisible by that number p, where the individual squares are each less than $\frac{1}{4}pp$, so that

$$aa + bb + cc < \frac{3}{4}pp.$$

Thus, the quotient

$$\frac{aa + bb + cc}{p}$$

will be less than $\frac{3}{4}p$; since it is less than p, it will certainly be a sum of four or fewer squares; let $xx + yy + zz + vv$ be that quotient;

$$p = \frac{aa + bb + cc}{xx + yy + zz + vv}$$

and thus the number p itself will be a sum of four or fewer squares, which can also be written as fractions. Thus, since among prime numbers there is no smallest which cannot be divided up into four or fewer squares, there is no prime number whatsoever which is not a sum of four or fewer squares; since this is true of prime numbers, it will also be valid for all composite numbers and thus all numbers, so that there is no number whatsoever which is not a sum of four or fewer squares.

Corollary 1

98. Since every integer is a sum of four or fewer squares, this same property also extends to all fractional numbers. For example, let $\frac{m}{n}$ be any given fraction; this can be transformed into $\frac{mn}{nn}$. Now let

$$mn = \frac{aa}{pp} + \frac{bb}{qq} + \frac{cc}{rr} + \frac{dd}{ss};$$

then,[12]

$$\frac{mn}{nn} = \frac{m}{n} = \frac{aa}{nnpp} + \frac{bb}{nnqq} + \frac{cc}{nnrr} + \frac{dd}{nnss};$$

and thus every fractional number will be a sum of four or fewer squares.

Corollary 2

99. Since, if the discussion is about breaking fractional numbers into squares, that condition of integral squares disappears on its own, the theorem thus accepted in this broader sense, that all numbers whether integers or fractions can be broken into four or fewer squares, we can say I have proved without any rigid restriction.

Scholium

[12] Translator: The *Commentationes arithmeticae collectae* has $\frac{aa}{npp}$, which is a mistake. In the *Opera Omnia*, Ferdinand Rudio corrects this to $\frac{aa}{nnpp}$.

100. Therefore, while Fermat has asserted that every integer is a sum of four or fewer integer squares, this has now certainly been proved about squares considered in general, without excluding fractions. Thus, although this is satisfactory with respect to Fermat, it still remains for us prove that an integer, which can be broken into four square fractions, can also be written as four or fewer square integers. For example, in *Analysi*, certainly Diophantus usually assumes that no integer can be broken into four square fractions unless its representation consists of four or fewer square integers. So if this proof were confirmed, nothing further would be desired. Truly, until now nowhere has a proof of this sort been found. But because it can be extended to a theorem most broadly conceived by the words

Every number, whether integer or fraction,
is the sum of four or fewer squares,

the proof of this I have delivered up here; it is rigorous and nothing more can be desired of it at all; through this, it seems to truly restore a considerable part of the proofs of Fermat which had been denied me.