On numbers which are the sum of two squares *

Leonhard Euler

1. Arithmeticians are accustomed to investigating the nature of numbers in many ways where they show their source, either by addition or by multiplication. Of the aforementioned kind, the simplest is composition from units, by which all integers are understood to arise from units. Then numbers can also thus be considered as they are formed from the addition of two or more other integers, which pertains to the problem of the partition of numbers, the solution of which I have published in the last several years, in which is asked, in how many different ways any proposed number can result from the addition of two or more smaller numbers. This, however, creates an arrangement of numbers to analyze carefully, arising from the addition of two squares. In this way, seeing that not all numbers arise, since vast is the multitude which cannot be produced by the addition of two squares, I will investigate those which are sums of two squares, their nature and properties. Even though most of their properties are now known, elicited as it were by induction[1], still the greatest part remain without solid proof. Since a considerable part relies on the truth of Diophantine analysis, in this dissertation of many such propositions, which until now have been accepted without proofs, I will furnish proofs of their truth, while I will certainly also keep those in mind, which as far as I could see still could not be proved, although we cannot doubt their truth in any way.

2. First, therefore, since the square numbers are 0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, etc., it will be helpful to consider those numbers which arise from the sums of two squares, which, therefore, I list here, up to 200: 0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37, 40, 41, 45, 49, 50, 52, 53, 58, 61, 64, 65, 68, 72, 73, 74, 80, 81, 82, 85, 89, 90, 97, 98, 100, 101, 104, 106, 109, 113, 116, 117, 121, 122, 125, 128, 130, 136, 137, 144, 145, 146, 148, 149, 153, 157, 160, 162, 164, 169, 170, 173, 178, 180, 181, 185, 193, 194, 196, 197, 200, etc. These truly are all the numbers up to 200 which arise from the addition of two squares: and these numbers with all in sequences to infinity I will call the sums of two squares, which therefore it is clear are expressed in this general formula $xx + yy$, where all integers 0, 1, 2, 3, 4, 5, 6,

*Originally published as *De numeris, qui sunt aggregata duorum quadratorum*, Novi Commentarii academiae scientiarum Petropolitanae **4** (1758), pp. 3–40. E228 in the Enestr̈om index. Translated from the Latin by Paul R. Bialek, Department of Mathematics, Trinity International University, Deerfield, Illinois, email: pbialek@tiu.edu

[1]Translator: Logical induction, not mathematical induction.

etc. are successively substituted for x and y. Numbers, therefore, which are not found among these are not sums of two squares, which up to 200 are thus: 3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, 28, 30, 31, 33, 35, 38, 39, 42, 43, 44, 46, 47, 48, 51, 54, 55, 56, 57, 59, 60, 62, 63, 66, 67, 69, 70, 71, 75, 76, 77, 78, 79, 83, 84, 86, 87, 88, 91, 92, 93, 94, 95, 96, 99, 102, 103, 105, 107, 108, 110, 111, 112, 114, 115, 118, 119, 120, 123, 124, 126, 127, 129, 131, 132, 133, 134, 135, 138, 139, 140, 141, 142, 143, 147, 150, 151, 152, 154, 155, 156, 158, 159, 161, 163, 165, 166, 167, 168, 171, 172, 174, 175, 176, 177, 179, 182, 183, 184, 186, 187, 188, 189, 190, 191, 192, 195, 198, 199, etc. From this, it is evident, at least up to 200, that the multitude of numbers which are not sums of two squares is greater than the multitude which are sums of two squares. By examining the rest, it will be immediately clear that neither series of those numbers is to be composed by a fixed and assignable rule; and on account of this, it will be more difficult to investigate the nature of either.

3. Because each square number is either even, in which case it is divisible by 4 and contained in the form $4a$, or odd, in which case it is contained in the form $8b + 1$, each number formed from two squares will be either

first, a sum of two even squares and will be of the form $4a + 4b$, and will therefore be divisible by 4, or

second, a sum of two squares, one odd and one even, and therefore of the form $4a + 8b + 1$, or, really, will be contained in the form $4a + 1$: it will exceed a multiple of four by one, or

third, a sum of two odd squares and will thus be of the form $8a + 1 + 8b + 1$, or, really, will be contained in the form $8a + 2$. Namely, this will be an unevenly even number [2] and will exceed a multiple of eight by two.

Therefore because all odd numbers either exceed a multiple of four by one and are of the form $4n + 1$ or are one less than a multiple of four and are of the form $4n - 1$, it is evident that no odd numbers of the latter form $4n - 1$ are sums of two squares, and all numbers contained in this form $4n - 1$ are excluded from the series of numbers which are sums of two squares.

Then, because all unequally even numbers either exceed a multiple of eight by two so that they are $8n + 2$ or are two less than a multiple of eight so that they are $8n - 2$, it is evident that no numbers of the latter form are sums of two squares, and thus numbers of this form $8n - 2$ are excluded from the series of numbers which are sums of two squares.

Nevertheless, it is still to be properly observed that not all numbers contained in this form $4n + 1$ nor in this form $8n + 2$ are sums of two squares. And so, for example, the numbers of the former form which are excluded are 21, 33, 57, 69, 77, 93, 105, 129, etc. and certainly of the latter form are those numbers 42, 66, 114, 138, 154, etc. I will investigate their rule in turn.

[2] Translator: This is Euler's term for even numbers which are not divisible by four.

4. Nevertheless, still, numbers which are sums of two squares are so connected by a tie between themselves in a certain way that from one number of this kind, infinitely many others of the same nature can be formed. Because by it this will be more easily observed, I will add the following lemmas which are certainly known well enough by all.

I. If a number p is a sum of two squares, then the numbers $4p, 9p, 16p$ and, in general, nnp will be sums of two squares. Certainly, because $p = aa+bb$, we will have $4p = 4aa+4bb, 9p = 9aa+9bb, 16p = 16aa+16bb$ and $nnpp = nnaa+nnbb$, which are similarly sums of two squares.

II. If a number p is a sum of two squares, then so will be $2p$ and, in general, $2nnp$ will be a sum of two squares. Let $p = aa+bb$; we will have $2p = 2aa+2bb$. But $2aa+2bb = (a+b)^2+(a-b)^2$, from which we will have $2p = (a+b)^2+(a-b)^2$, and therefore also the sum of two squares. From this, moreover, we will have $2nnp = nn(a+b)^2 + nn(a-b)^2$.

III. If the even number $2p$ is a sum of two squares, then half of it, p, will also be a sum of two squares. Let $2p = aa + bb$; the numbers a and b will both be even or odd. From this, in either case, both $(a+b)/2$ and $(a-b)/2$ will be integers. Certainly $aa+bb = 2((a+b)/2)^2+2((a-b)/2)^2$, which, by substituting values, is $p = ((a+b)/2)^2 + ((a-b)/2)^2$.

From this, therefore, all even numbers which are sums of two squares, by continual halving, are finally returned to odd numbers of the same nature. Therefore, again, if only odd numbers which are sums of two squares are known, all such even numbers will be derived from these as well, by continual duplication.

5. Next it is proper to record the following theorem, by which the nature of the numbers which are sums of two squares is not usually shown.

Theorem

If p and q are two numbers, each of which is the sum of two squares, then their product pq will also be the sum of two squares.

Proof

Let $p = aa + bb$ and $q = cc + dd$. We will have $pq = (aa + bb)(cc + dd) = aacc + aadd + bbcc + bbdd$, which expression can be represented in this way so that $pq = aacc + 2abcd + bbdd + aadd - 2abcd + bbcc$ and for that reason $pq = (ac + bd)^2 + (ad - bc)^2$, from which the product pq will be a sum of two squares. Q. E. D.

From this proposition it follows that when however many numbers which individually are sums of two squares are multiplied together, the product will

always be a sum of two squares. And from the given general form, it is evident that the product of two such numbers doubled just recently[3] can be partitioned into two squares: so if $p = aa+bb$ and $q = cc+dd$, then $pq = (ac+bd)^2+(ad-bc)^2$ and $pq = (ac-bd)^2+(ad+bc)^2$, which will be a different formula, unless either $a = b$ or $c = d$. Thus, since $5 = 1 + 4$ and $13 = 4 + 9$, the product $5 \cdot 13$ will be the sum of two squares in two ways, namely $65 = (1 \cdot 3+2 \cdot 2)^2+(2 \cdot 3-1 \cdot 2)^2 = 49+16$, and $65 = (2 \cdot 2 - 1 \cdot 3)^2 + (2 \cdot 3 + 1 \cdot 2)^2 = 1 + 64$. Also, if a product of many numbers is considered, the terms of which are sums of two squares, it can be partitioned in many ways into the sum of two squares. So if the number $1105 = 5 \cdot 13 \cdot 17$ is put forward, its partitions into two squares will be these: $1105 = 33^2 + 4^2 = 32^2 + 9^2 = 31^2 + 12^2 = 24^2 + 23^2$, namely, the four partitions here.

6. Although it happens that if the factors p and q are sums of two squares then the product pq will also be a sum of two squares, the converse of this proposition does not follow from this; so if the product is a sum of two squares, neither the rules of logic prove the conclusion that its factors are also numbers of the same nature, nor does the nature itself of the thing. For example, the number $45 = 36 + 9$ is a sum of two squares, nevertheless, neither of its factors $3 \cdot 15$ is a sum of two squares. Rather, however, this firm conclusion is seen: if the product pq and one factor p are the sum of two squares, then the other factor q will be a sum of two squares also. Even though this conclusion is perhaps true, it is not confirmed by the rules of reasoning, nor because has been proved that if both factors p and q of the product pq are sums of two squares then pq itself will be a sum of two squares can the legitimate consequence therefore be inferred: if the product pq and one factor p are sums of two squares, then the other factor q will also be a sum of two squares. Truly, such a consequence is not legitimate; indeed this example clearly contradicts it: it is certain that if two factors p and q are even numbers, then their product will also be even. If however one wishes to conclude by this that if the product pq and one factor p are even numbers then the other factor q will also be even, that person is quite mistaken.

7. Therefore if it is true that when the product pq and either factor, say p, are the sum of two squares then the other factor q will be a sum of two squares also, this proposition cannot be inferred from what was shown above, but should be defended by a special proof. This proof however is not as clear as the preceding one and cannot be constructed apart from many details, and certainly the proof which I found seems to be constructed so that it does not require average reasoning ability. On account of this matter, the propositions, from which not only this truth is obtained but also other notable properties of numbers which are the sum of two squares, are known when I put forward here their own proofs sequentially, and I will be careful so that nothing whatsoever can be desired in rigor of proof. Though up to this point, these facts about

[3]Translator: Euler may be referring to the proof of Section 4, Lemma II, where he uses a similar argument.

the given numbers are trivial and in common knowledge, nevertheless I will use them in the form of lemmas for the following proofs.

Proposition I

8. If the product pq is a sum of two squares and one factor p is a prime number and similarly a sum of two squares, then the other factor q will also be a sum of two squares.

Proof

Let $pq = aa + bb$ and $p = cc + dd$; because p is a prime number, the numbers c and d will be prime between themselves. And so, $q = \frac{aa+bb}{cc+dd}$, and for this reason, because q is an integer, the numerator $aa + bb$ will be divisible by the denominator $cc + dd$. From this, the number $cc(aa + bb) = aacc + bbcc$ will also be divisible by $cc + dd$; and because the number $aa(cc + dd) = aacc + aadd$ is also divisible by $cc + dd$, it is necessary for the difference of these numbers, $aacc + bbcc - aacc - aadd$, or $bbcc - aadd$, to be divisible by $cc + dd$. However, because $cc + dd$ is a prime number, and $bbcc - aadd$ has factors $bc + ad$ and $bc - ad$, one of these factors, certainly $bc \pm ad$, will be divisible by $cc + dd$. So let $bc \pm ad = mcc + mdd$: however, whatever numbers a and b may be, they can expressed as $b = mc + x$ and $a = \pm md + y$, x and y appearing as either positive or negative integers. Certainly having substituted these values for b and a, the equation $bc \pm ad = mcc + mdd$ will take on this form: $mcc + cx + mdd \pm dy = mcc + mdd$, or, $cx \pm dy = 0$. From this, $\frac{x}{y} = \mp\frac{d}{c}$, and because d and c are prime between themselves, it is necessary that $x = nd$ and $y = \mp nc$, from which is obtained $a = \pm md \mp nc$ and $b = mc + nd$, namely, the numbers a and b ought to have values such that the number $pq = aa + bb$ is divisible by the prime number $p = cc + dd$. However, substituting those values for a and b makes $pq = mmdd - 2mncd + nncc + mmcc + 2mncd + nndd$, or, $pq = (mm + nn)(cc + dd)$. Now because $p = cc + dd$, we will have $q = mm + nn$; and therefore if the product pq is the sum of two squares and one factor p is a prime number and similarly a sum of two squares $cc + dd$, it necessarily follows that the other factor q will be a sum of two squares. Q. E. D.

Corollary 1

Therefore, if the sum of two squares is divisible by a prime number which itself is a sum of two squares, the quotient resulting from the division will also be a sum of two squares. So if the sum of two squares is divisible by some number from these prime numbers 2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc., the quotient will always be a sum of two squares.

Corollary 2

10. Therefore, if the letters $\alpha, \beta, \gamma, \delta$, etc. denote such prime numbers which are sums of two squares, it is evident from this that if the product αq is a sum of two squares, then the factor q will also be a sum of two squares.

Corollary 3

11. Furthermore, from this it is easily obtained later on that if the product $\alpha\beta q$ is a sum of two squares, the factor q will also be a sum of two squares. Indeed, because $\alpha\beta q$ is a sum of two squares, by the corollary above, βq will also be a sum of two squares; and by the same reasoning q will also be a sum of two squares.

Corollary 4

12. In the same way, it is evident that if the product $\alpha\beta\gamma\delta\epsilon q$ is a sum of two squares, then the factor q is also a sum of two squares; hence, if the product pq is a sum of two squares, and the factor p is a product of however many prime numbers, each of which is a sum of two squares, then the other factor q will also be a sum of two squares.

Scholium

13. The rules of logic do not permit this proposition to be inverted, that whenever the factor q is a sum of two squares,[4] then the other factor p can be declared either a sum of two squares, if it is prime, or a product of prime numbers, each of which is a sum of two squares. Indeed, this itself has not yet been established, whether a product of several prime numbers which themselves are not sums of two squares cannot be a sum of two squares: rather, to the contrary, we already have a case that the product $45 = 3 \cdot 3 \cdot 5$ is a sum of two squares although its factors 3 and 3 are not of this kind. In truth, the proposition can thus be inverted correctly only to the extent that if the consequent is negated, then the negation of the antecedent is concluded; because of its very great importance, I will deal with the converse in this proposition.

Proposition II

14. If the product pq is a sum of two squares but its factor q is not a sum of two squares, then the other factor p, if it is a prime number, will not be a sum of two squares, but if however it is not prime, it will certainly have at least one prime factor which is not a sum of two squares.

[4]Translator: Here it is assumed that the product pq is a sum of two squares.

Proof

Because one factor p is either a prime number or composite, it is proper to analyze each case separately. First, let p be a prime number; if it were a sum of two squares, the other factor q would also be a sum of two squares, which is false according to the hypothesis. It follows that the factor p is not a sum of two squares. Second, let p be a composite number; it has been established previously that if all of its prime factors are sums of squares, then the other factor q will also be of the same nature. Therefore, because according to hypothesis, q is not a sum of two squares, it follows that not all factors of p itself are sums of two squares. Q. E. D.

Corollary 1

15. If therefore the product pq is a sum of two squares, but one of its factors q cannot be expressed as two squares, then the other factor p is either itself not a sum of two squares or will have at least one prime factor which cannot be expressed as two squares. For example, if $pq = 45$ and $q = 3$, then $p = 15$, which has a factor 3 that is not the sum of two squares.

Corollary 2

16. From this however one cannot yet conclude that the other factor p is clearly not a sum of two squares, however certain this may be in the case when p is a prime number. It still has not yet been established in the case when p is a composite number, because p can have a factor which cannot be written as the sum of two squares even though p itself is a sum of two squares.

Corollary 3

17. However, one can conclude this: If p is a sum of two squares then it has not just one but at least two prime factors which cannot be written as the sum of two squares. For example, let $p = \alpha\beta\gamma\delta$, where δ is that factor which cannot be written as a sum of two squares; it is clear that if p is a sum of two squares, then, in light of the deleted factor δ, in addition the remaining factor $\alpha\beta\gamma$ should have a factor which cannot be written as the sum of two squares[5].

Scholion

[5]Translator: This follows from applying Proposition II to $q = \delta$ and $p = \alpha\beta\gamma$.

18. Although an inquiry has been undertaken concerning the divisors of numbers which are sums of two squares, about the sum of squares $aa + bb$, the cases are properly distinguished depending on whether the squares aa and bb, or, equivalently, their roots a and b, are prime between themselves or not. For instance, if a and b are not prime between themselves but have a common divisor n so that $a = nc$ and $b = nd$, the sum of squares will be $nncc + nndd = nn(cc + dd)$, and therefore will have a divisor n which can be any number. But if the roots a and b are numbers prime between themselves, then the sum of squares $aa + bb$ does not admit many numbers as divisors. For example, it is evident that such a sum of two squares $aa + bb$ is never divisible by 3. For by hypothesis, the squares cannot both be divisible by 3, because otherwise they would not be prime between themselves. If the sum were divisible by 3, then neither term could be divisible by 3. Therefore if either of these roots exist, they are of the form $3m + 1$ or $3m - 1$. But the sum of two such squares, divided by 3, always leaves a remainder 2, and is therefore never divisible by 3. In the same way, it is understood that the sum of two squares $aa + bb$, prime between themselves, is never divisible by 7 or 11 or 19, etc. In general, it is not easy to determine in this way which numbers can never be divisors of the sums of two squares prime between themselves. It is fitting therefore to prove the proposition certainly known well enough elsewhere, that the sum of two squares prime between themselves does not admit other prime divisors, unless they themselves are sums of two squares. But the following proposition should be given.

Proposition III

19. If the sum of two squares primes between themselves $aa + bb$ is divisible by a prime number p, a sum of two other squares $cc+dd$ can always be generated which is divisible by that same number p so that the sum $cc + dd$ is not greater than $\frac{1}{2}pp$.

Proof

Let the sum of two squares prime between themselves $aa + bb$ be divisible by the number p, and let a and b be numbers of any size. Therefore, because neither a nor b is divisible by p, the numbers a and b can be expressed as $a = mp \pm c$ and $b = np \pm d$, where one may select m and n so that c and d do not exceed $\frac{1}{2}p$. Therefore $aa + bb = mmpp \pm 2mcp + cc + nnpp \pm 2ndp + dd$. Because both this whole expression is divisible by p, by hypothesis, and a part of it, $mmpp \pm 2mcp + nnpp \pm 2ndp$ by itself has p as a divisor, it is necessary that the other part $cc + dd$, which is a sum of two squares, is similarly divisible by p. But because the roots c and d do not exceed $\frac{1}{2}p$, neither of the formulas in the sum of squares $cc + dd$ will exceed the square pp, and therefore a sum of two squares $cc + dd$ can be produced which is not greater than $\frac{1}{2}pp$, but is nonetheless divisible by p. Q. E. D.

Corollary 1

20. Therefore, if there is no sum of two squares prime between themselves, divisible by p, and not exceeding $\frac{1}{2}pp$, then there is no sum of two squares prime between themselves which is divisible by the number p.

Corollary 2

21. Therefore, if there is no sum of squares prime between themselves, less than $\frac{1}{2}3^2$ (namely $4\frac{1}{2}$), and divisible by 3, then it clearly follows that there is no sum of two squares prime between themselves which is divisible by 3. And in a similar way by the number 7, because there is no sum of two squares less than $\frac{1}{2}7^2$ (namely $24\frac{1}{2}$), and divisible by 7, it follows that certainly neither among larger numbers is there a sum of two squares prime between themselves which is divisible by 7.

Proposition IV

22. The sum of two squares prime between themselves cannot be divided by any number which itself is not a sum of two squares.

Proof

Concerning what is to be proved, let us suppose that the sum of two squares prime between themselves $aa+bb$ is divisible by the number p, which is not a sum of two squares. Therefore, another sum of two squares prime between themselves can be generated, $cc + dd$, which is not greater than $\frac{1}{2}pp$ and is divisible by p. Therefore, let $cc + dd = pq$. Since p is not a sum of two squares, either the number q itself will not be such a sum or will have at least one factor r which is not a sum of two squares. Indeed, because $pq < \frac{1}{2}pp$, we have $q < \frac{1}{2}p$ and, furthermore, $r < \frac{1}{2}p$. Therefore because $cc + dd$ is also divisible by $r < \frac{1}{2}p$, by the preceding proposition, a sum of two squares $ee + ff$ can be generated which is divisible by the same number r and does not exceed $\frac{1}{2}rr$ or, furthermore, $\frac{1}{8}pp$, And since r is not a sum of two squares, proceeding continuously in a similar way, one reaches smaller sums of two squares which are divisible by a number that is not a sum of two squares. On account of this, because there is no sum of two squares prime between themselves among the smallest numbers and divisible by a number that is not the sum of two squares, neither among the greatest numbers will there be such sums of two squares which are divisible by numbers that are not themselves sums of two squares. Q. E. D.

Corollary 1

23. If therefore the sum of two squares prime between themselves is not a prime number, all of its prime factors will also be sums of two squares. Therefore, just as the product of however many prime numbers which themselves are sums of two squares will similarly be a sum of two squares, so now the converse of this proposition is proved, that the sum of two squares prime between themselves cannot be created by multiplication except from numbers which themselves are sums of two squares.

Corollary 2

24. Therefore, all numbers which are sums of two squares prime between themselves are either themselves contained in this series of prime numbers: 2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, etc. or are constructed by multiplication of two or more numbers from this series. Moreover, all these prime numbers except 2 exceed a multiple of 4 by 1, or namely, are contained in the form $4n + 1$.

Corollary 3

25. Therefore, if the sum of two squares $aa + bb$ is divisible by a number which is not a sum of two squares, then from this it is understood that those squares aa and bb are not prime between themselves, and thus neither are their roots, a and b.

Corollary 4

26. Let $a = nc$ and $b = nd$. Since the sum of the two squares $aa + bb = nn(cc + dd)$ can be divided by any number n that is not a sum of two squares, it is divisible not only by n but also by nn. It is evident that if the sum of two squares is divisible by some number which is not a sum of two squares, then it will also be divisible by the square of this number. Thus, because $45 = 36 + 9$ is divisible by 3, it is also divisible by 9.

Corollary 5

27. Because no number contained in the form $4n-1$ is a sum of two squares, it is also clear that no sum of two squares prime between themselves can be divided by any prime number contained in the form $4n - 1$. These prime numbers are 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, 103, 107, etc.

Scholium

28. All prime numbers which are sums of two squares, except 2, form this series: 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, etc. Not only are these contained in the form $4n + 1$, but also, however far the series is continued, we find that every prime number of the form $4n+1$ occurs. From this, we can conclude by induction [6] that it is likely enough that there is no prime number of the form $4n+1$ which is not also a sum of two squares. Nevertheless, induction, however extensive, cannot fulfill the role of proof. Even if no one doubts the truth of the statement that all prime numbers of the form $4n+1$ are sums of two squares, until now mathematics could not add this to its established truths. Even Fermat declared that he had found a proof, but because he did not publish it anywhere, we properly extend confidence toward the assertion of this most profound man, and we believe that property of the numbers, but this recognition of ours rests on pure faith without knowledge. Although I labored much in vain on a proof to be discarded, nevertheless I have discovered another argument to be given for this truth, which, even it if it is not fully rigorous, still appears to be equivalent to induction connected with nearly rigorous proof.

Proposition V

28.[7] Every prime number which exceeds a multiple of four by one is a sum of two squares.

Attempt at a Proof

The prime numbers which this discussion concerns are contained in the form $4n + 1$. Now if the number $4n + 1$ is prime, I showed that the form $a^{4n} - b^{4n}$ is always divisible by it, regardless of what numbers are substituted for a and b, provided that neither is divisible by $4n+1$. Because $a^{4n}-b^{4n} = (a^{2n}-b^{2n})(a^{2n}+b^{2n})$, it is necessary that one of the factors, either $a^{2n} - b^{2n}$ or $a^{2n} + b^{2n}$, be divisible by the prime number $4n + 1$. Accordingly, as a and b assume some values or others, in some cases the formula $a^{2n} - b^{2n}$ and in other cases the formula $a^{2n} + b^{2n}$ will divisible by $4n + 1$. From this, one may assume, if indeed I am not yet able to overcome this with a solid proof, that such numbers can always be assigned for a and b so that the formula $a^{2n} - b^{2n}$ is not divisible by $4n + 1$; therefore, in these cases, the other formula $a^{2n} + b^{2n}$ must necessarily be divisible by $4n + 1$. Let $a^n = p$ and $b^n = q$. The sum of two squares $pp + qq$ obtained is divisible by $4n+1$ even though neither square pp nor qq individually has $4n+1$ as a divisor. And therefore, even if perhaps pp and qq have a common divisor mm, so that $pp + qq = mm(rr + ss)$, because the common factor mm does not have $4n + 1$ as a divisor, it is necessary that the sum of two squares prime between themselves $rr+ss$ has $4n+1$ as a divisor. Consequently, because such a sum of two squares does not allow other divisors, it is necessary that the prime number $4n + 1$ be a sum of two squares.

[6] Translator: Logical induction, not mathematical induction.

[7] Translator: Original version mistakenly has two sections numbered 28.

Corollary 1

29. This proof would therefore be perfect if one could only prove that there always exist such values to be substituted for a and b for which the formula $a^{2n} - b^{2n}$ would not be made divisible by the prime number $4n + 1$, namely, in these cases, the formula $a^{2n} + b^{2n}$ is necessarily divisible by $4n + 1$.

Corollary 2

30. But if anyone attacks this matter by calculation, he will discover not only many cases but infinitely many cases of the formula $a^{2n} - b^{2n}$ for which it is not divisible by a prime number $4n + 1$, but also one can set b equal to one so that this simpler formula $a^{2n} - 1$ is again and again not divisible by $4n + 1$.

Scholium

31. These cases of a for which the formula $a^{2n} - 1$ is divisible by the prime number $4n + 1$ can be easily determined. First, for instance, if $a = pp$, then the formula $a^{2n} - 1 = p^{4n} - 1$ is always divisible by $4n + 1$, provided that p does not equal $4n + 1$ or a multiple of it. Next, if $a = pp \pm (4n + 1)q$, the formula $a^{2n} - 1$ also has $4n + 1$ as a divisor, for $a^{2n} = (pp \pm (4n + 1)q)^{2n}$ can be broken up into a series of terms, of which the first is p^{4n}, and each of the subsequent terms is divisible by $4n + 1$. From this, it is evident that the appropriate values for a are all the residues which remain after the squares p^2 are divided by $4n + 1$. However, whether r or $4n + 1 + r$ or $(4n + 1)q + r$ is substituted for a, these same residues occur, from which all possible residues are obtained if p is set equal to successive numbers 1, 2, 3, 4, 5, up to $4n$. But setting p equal to the value $4n$ yields the same residue as the value 1, and in a similar way, the values 2 and $4n - 1$ give the same residue; so do 3 and $4n - 2$; so do 4 and $4n - 3$, etc. Thus, whenever two residues arising from the numbers 1, 2, 3, up to $4n$ for the roots of squares are equal, the number of different such resulting residues will be $2n$, and therefore this many numbers will be generated less than $4n + 1$, numbers which cannot be residues arising from division of square numbers by $4n + 1$. And these numbers substituted for a always produce a number $a^{2n} - 1$ which is not divisible by $4n + 1$. Indeed, this similarly cannot be proven. And yet, because in making the attempt, however many numbers are explored in this way, not a single case will occur which contradicts this rule, its truth should be acknowledged. I will attach several examples in which these things are observed more clearly. First, let $4n + 1 = 5$; cases for which the formula $a^2 - 1$ is divisible by 5 will be obtained if for a is substituted the residues arising from division of squares by 5; these residues are 1, 4. But if a is set equal to either 2 or 3, the formula $a^2 - 1$ will not be divisible by 5; in these cases therefore the formula $a^2 + 1$ will have 5 as a divisor. Now let $4n + 1 = 13$, namely, let $n = 3$. The

residues which are left after the division of square numbers by 13 are 1, 4, 9, 3, 12, 10. Consequently, if any of the remaining numbers 2, 5, 6, 7, 8, 11, are substituted for a, then not the formula $a^6 - 1$, but $a^6 + 1$ will be divisible by 13. Next, if $4n + 1 = 17$, that is, if $n = 4$, because the residues of squares divided by 17 are 1, 4, 9, 16, 8, 2, 15, 13, if any of the remaining numbers 3, 5, 6, 7, 10, 11, 12, 14 is set equal to a, then the formula $a^8 - 1$ will not be divisible by 17, but $a^8 + 1$ will be. Therefore, because this principle is observed continually, this proof via induction will be judged almost complete. Hence, this proposition seems so confirmed that one may not voice much doubt about its truth. Nevertheless, it would be all the more worthwhile if anyone could show a rigorous proof of this proposition by which we are more certain of its truth. Indeed, there is no doubt that such a proof, sought in vain for so long, may lead us to many other important properties of the numbers. Although the truth of this proposition is beyond doubt, nevertheless, I will diligently note that I will distinguish the consequences which depend on it from the others which are supported by solid proof; however, from this unproved proposition follow these corollaries which I wish to be designated by that name.

Corollary 3

32. Therefore, if a number of the form $4n + 1$ cannot be written in any way as the sum of two squares, this is a sure sign that the number is not prime. For if the number $4n + 1$ were prime, it could certainly be written as the sum of two squares. Thus, since the numbers 21, 33, 57, 69, 77, 93, etc., which are contained in the form $4n + 1$, are not sums of two squares, from this fact itself it is evident that they are not prime.

Corollary 4

33. Therefore, in the series of numbers which are sums of two squares, first, all prime numbers of the form $4n + 1$ are included, and all products of two or more such prime numbers, and then products of these individual numbers in pairs and any square numbers.

Corollary 5

34. All numbers n for which a prime number is generated by the formula $4n + 1$ are sums of two triangular numbers. For when $4n + 1$ is a sum of two squares, its double $8n + 2$ will be a sum of two unequal squares [8]. Therefore, let $8n + 2 = (2x + 1)^2 + (2y + 1)^2$ so that $n = \frac{xx+x}{2} + \frac{yy+y}{2}$. Thus, if n is not a sum of two triangular numbers, then the number $4n + 1$ is certainly not prime.

[8] Translator: Proved in Section 4.

Proposition VI

35. If a number of the form $4n+1$ can be written in only one way as a sum of two squares prime between themselves, then it is certainly a prime number.

Proof

Since this number is a sum of two squares prime between themselves, if it is not prime, then its individual factors are sums of two squares [9]. Thus, if this number is not prime, then at least two factors in such a number can be written so that $4n+1 = (aa+bb)(cc+dd)$; in this case, however, there are two ways to write it as a sum of two squares [10], namely,

I. $4n+1 = (ac+bd)^2 + (ad-bc)^2$

II. $4n+1 = (ad+bc)^2 + (ac-bd)^2$.

And these resolutions are always different, unless either $ac+bd = ad+bc$ or $ac+bd = ac-bd$. In the former case, $ac+bd-ad-bc = 0$, or namely, $(a-b)(c-d) = 0$, and therefore either $a = b$ or $c = d$ and hence either $aa+bb$ or $cc+dd$ is an even number which could not be a divisor of $4n+1$ itself, since it is odd. In the latter case, either $b = 0$ or $d = 0$ and therefore $4n+1$ equals either $aa(cc+dd)$ or $cc(aa+bb)$, from which the two squares cannot be prime between themselves, contrary to hypothesis. By these cases which have been noted, it follows that $4n+1$ is a composite number if it can be written as a sum of two squares prime between themselves and can be written in at least two ways as the sum of two squares. Therefore, if the number $4n+1$ can be written in only one way as the sum of two squares, then it will certainly not be composite, but consequently will be prime. Q. E. D.

Corollary 1

36. If therefore one learns upon examination that some given number of the form $4n+1$ can be written in only one way as the sum of two squares prime between themselves, then from this we may safely conclude that the number is prime, even if we have not tested its divisibility by prime numbers as is usually done. Thus, because 73 is the sum of two squares in only one way, obviously 64 + 9, we know that it is certainly prime.

Corollary 2

[9] Translator: Proved in Section 22.
[10] Translator: Proved in Section 5.

37. Therefore, if a method is considered expedient, and with the use of it one may easily investigate whether and in how many ways a given number in the form $4n+1$ can be written as the sum of two squares, then we can quickly judge whether the number is prime; for instance, if it can be written in only one way as the sum of two squares and the two squares are prime between themselves, then it will certainly be regarded as prime.

Corollary 3

38. Moreover, it is clear that if some number is written as a sum of two squares not prime between themselves, then that number is not prime. If however the given number is found to be $nnaa + nnbb$, then it will have divisors n and nn. Also, it is understood that if the given number is itself a square, say $aa + 0$, then it will have a as a divisor.

Scholium

39. This rule about testing prime numbers is restricted to odd numbers of the form $4n + 1$; for instance, when even numbers can be written in one way as a sum of two squares, they are still not prime; so 10 can be written in only one way as a sum of two squares, and yet it is not prime, the reason of which is that in the product $(aa + bb)(cc + dd)$, to which numbers of this form are equal, either $a = b$ or $c = d$, in which case the twofold solution (which is seen to hold in general), reduces to a single one, just as explained in the demonstration. Neither is this given rule diminished by this exception, because the case of even numbers by themselves is easy. However, odd numbers of the other form, $4n-1$ are thus themselves excluded, since they clearly cannot be written as a sum of two squares. As for the other form, if a number $4n+1$ either cannot be written as a sum of two squares or can successfully be written in several ways, we have already noted by the prior case that this number is certainly not prime, and yet this depends on the preceding proposition, which was not proved with sufficient rigor. Truly, this contention for the latter case will be conveyed in the following proposition.

Proposition VII

40. A number which can be written in two or more different ways as a sum of two squares is not prime but is composed of at least two factors.

Proof

Let N be the proposed number which can be written in two ways as a sum of two squares , namely, $N = aa + bb = cc + dd$. Since these squares are not equal, otherwise N itself would not be prime, let $a > b$ and $c > d$. Because these two representations are different, $a \neq c$ and $b \neq d$. Therefore, if $a > c$, then $b < d$, so that one can set $a = c + x$ and $d = b + y$. So because $aa + bb = cc + dd$, $2cx + xx = 2by + yy$ as a result . Let either form be xyz, because one side is divisible by x and the other side is divisible by y. Then[11], $c = \frac{yz-x}{2}, b = \frac{xz-y}{2}, a = \frac{yz+x}{2}, d = \frac{xz+y}{2}$, so that $N = aa + bb = \frac{xxzz+yy+yyzz+xx}{4}$, that is, $N = \frac{(yy+xx)(1+zz)}{4}$. Therefore, unless $xx + yy$ is divisible by 4, $xx + yy$ will be a divisor of N itself; but if $xx + yy$ is divisible by 4 or is somehow a composite number, some factor of it will certainly be a divisor of N itself. Therefore, because $x = a - c$ and $y = d - b$, the given number $N = aa + bb = cc + dd$ will have as a divisor either the number $(a-c)^2 + (d-b)^2$ itself or a half or a quarter of it. And because one may permute the numbers a, b and c, d in any way, the factors of N itself will be also be $(a-d)^2 + (c-b)^2$, or because the roots a, b, c, d may assume negative values, $(a \pm c)^2 + (d \pm b)^2$ or $(a \pm d)^2 + (c \pm b)^2$ or half of these formulas or some other portion. Thus, when a number can be written in more than one way as a sum of two squares, that number will certainly not be prime, but composite. Q. E. D.

Corollary 1

41. Therefore, when the number $N = aa + bb = cc + dd$ is composite, it will be of the form $N = (pp + qq)(rr + ss)$. This, in turn, results in two ways to express it as a sum of two squares; these will certainly be $a = pr + qs$, $b = ps - qr$ and $c = ps + qr$, $d = pr - qs$. Furthermore, from this is obtained $a - d = 2qs$ and $c - b = 2qr$, so $\frac{r}{s} = \frac{c-b}{a-d}$. Therefore, if the fraction $\frac{c-b}{a-d}$ is reduced to lowest terms so that $\frac{c-b}{a-d} = \frac{r}{s}$, from the fraction $\frac{r}{s}$ arises a divisor $rr + ss$ of the number N, unless it is even, for if it is even, then it should be assumed to be half of this.

Corollary 2

42. In a similar way, when one permits a, b and c, d to be permuted between themselves and to take on negative values, if one reduces the fractions $\frac{a \pm c}{b \pm d}$ or $\frac{a \pm d}{b \pm c}$ to lowest terms, they become $\frac{r}{s}$, and $rr + ss$ will always be a divisor of the given number N.

Corollary 3

[11] Translator: Original version has $x = \frac{yz-x}{2}$ instead of $c = \frac{yz-x}{2}$.

43. Although from this more than two divisors appear to arise, different formulas lead to the same divisor, so not more than two are produced, if indeed the given number can be written in only two ways as a sum of two squares. Thus, if $N = 85 = 9^2 + 2^2 = 7^2 + 6^2$, the formulas $\frac{9\pm7}{6\pm2}$, $\frac{9\pm6}{7\pm2}$ supply only these four fractions in lowest terms: $\frac{2}{1}, \frac{4}{1}, \frac{5}{3}, \frac{3}{1}$, of which the last two generate such a double value, which arise from the first two. From this, it is clear that the factors will be the two numbers $2^2 + 1 = 5$ and $4^2 + 1 = 17$. Very briefly, these factors are found only if the roots of the odd and even squares are separately combined in turn, and the combination of the evens with the odds is totally omitted, because from this, fractions arise having odd numerator and denominator.

Problem

44. To explore whether a given number of the form $4n + 1$ is prime or not.

Solution

According to the operation to be explained shortly, let a given number be investigated as to whether or not it can be written as a sum of two squares, and if it can, whether more than one way is successful. If there is no way to write it as a sum of two squares, then by Section 32, this is a sure sign that the given number is not prime, even if this conclusion follows from Proposition 5, which was not satisfactorily proved. Indeed, in this case, nothing is known about its divisors. However, we can still certainly conclude that it has prime divisors of the form $4m - 1$, because if all its divisors were of the form $4m + 1$, these certainly could be written as sums of two squares. But if the given number can be written as a sum of two squares in only one way, then infallibly it will be regarded as a prime. However, if it can be successfully represented as a sum of squares in more than one way, then not only will it be known that it is not prime, but also its divisors can be distributed according to Section 43. With these matters carefully considered, I will pass on this rule with the help of which the representation as sum of two squares can be explored.

A given number ends in 1, 3, 7, or 9. Here I omit the case in which it ends in 5, because then 5 is clearly a divisor, which indicates that the number is not prime. Then let square numbers starting with the greatest less than the given number itself be subtracted from it, so that it is evident whether a square number ever remains; indeed, however often this happens is the number of ways it can be successfully written as a sum of two squares.

Now because square numbers cannot end in any of the numbers 2, 3, 7, or 8, the subtraction of the square numbers which produce residues ending in these numbers can be omitted. Consequently, the only work left is to find which squares produce residues ending in 0, 1, 4, 5, 6, or 9 when they are subtracted from the given number. Of course,

if the given number ends in	the squares to be subtracted end in	and the roots of these squares end in
1	0, 1, 5, 6	0, 1, 4, 5, 6, 9
3	4, 9	2, 3, 7, 8
7	1, 6	1, 4, 6, 9
9	0, 4, 5, 9	0, 2, 3, 5, 7, 8

Therefore, for any given number $4n + 1 = N$, however many operations are separately undertaken, that many are suitable endings of roots. So let pp be the greatest square of its kind which can be subtracted from a given number N; and then the squares $(p-10)^2, (p-20)^2, (p-30)^2, (p-40)^2$, etc. are subtracted successively. Certainly from this, the residues emerging can be found readily in this way by continual addition:

$$\begin{array}{rl} \text{The given number} & N \\ \text{from which is subtracted} & pp \\ & \overline{= (N - pp)} \\ \text{is added} & (20p - 100) \\ & \overline{= (N - (p-10)^2)} \\ \text{is added} & (20p - 300) \\ & \overline{= (N - (p-20)^2)} \\ \text{is added} & (20p - 500) \\ & \overline{= (N - (p-30)^2)} \end{array}$$

Therefore, the numbers to be added successively are $20p - 100$, $20p - 300$, $20p - 500$, $20p - 700$, etc. which decrease in an arithmetic progression with difference -200. Such an operation for individual numbers p, of which squares are just less than the given number and which end in some of the figures indicated above, is arranged and not contained beyond which half of the given number N is reached. Indeed, if the number N is a sum of two squares, it is certainly necessary for one to be less than half of N itself. When this is observed, however many squares will be produced by this operation, in that many ways the given number can be written as a sum of two squares.

The following examples will show that this long-anticipated operation is not very burdensome compared with all other methods of searching for prime numbers.

Example 1

45. To test whether or not the number 82421 is prime. The operation is arranged in the following six columns:

p	82421	p	82421	p	82421	p	82421	p	82421	p	82421
286	81796	285	81225	284	80656	281	78961	280	78400	279	77841
	□ 625		1196		1765		3460		4021		4580
	5620		5600		5580		5520		5500		5480
	6245		6796		7345		8980		9521		10060
	5420		5400		5380		5320		5300		5280
	11665		12196		12725		14300		14821		15340
	5220		5200		5180		5120		5100		5080
	16885		17396		17905		19420		19921		20420
	5020		5000		4980		4920		4900		4880
	21905		22396		22885		24340		24821		25300
	4820		4800		4780		4720		4700		4680
	26725		27196		27665		29060		29521		29980
	4620		4600		4580		4520		4500		4480
	31345		31796		32245		33580		34021		34460
	4420		4400		4380		4320		4300		4280
	35765		36196		36625		37900		38321		38740
	4220		4200		4180		4120		4100		4080
	39985		40396		40805		42020		42421		42820

So then, because here a square, 625, occurs only once, and thus the given number 82421 can be written in only one way as a sum of two squares, namely, $25^2 + 286^2$, the number 82421 will be prime.

Scholium

46. In this computation, four columns where the remaining numbers end in either 5 or 0 notably can be assembled omitting the columns which do not end in 25 or 00. Because of this, in the columns in which the remainders end in 5 or 0, first the next square which produces a remainder ending in 25 or 00 is subtracted, and let this square be designated pp so that the remainder is $N - pp$; then, in the same way, the squares from the remainders of which the endings arise will be $(p-50)^2$, $(p-100)^2$,$(p-150)^2$, etc., and therefore these remainders will be obtained if, to $N - pp$, is continually added these numbers: $100p - 2500$, $100p - 7500$, $100p - 12500$,[12] which decrease arithmetically by a second constant difference 5000; from this, these columns are next spread out until the end, while the ones that are not more than half of the given number is a work to be continued. Therefore, one will have the shortened situation in numbers ending in 1 or 9, which are thus more easily arranged even if six columns are required, as long as four columns are sufficient for the remaining ones.

Example 2

[12]Translator: Original version has $100p - 2500$, $100p - 17500$, $100p - 125000$.

47. To test whether or not the number 100981 is prime.

p	100981	p	100981	p	100981	p	100981
316	99856	315	99225	309	95481	310	96100
	1125		1756		5500		4881
	29100		6200		28400		6100
	30225		7956		33900		10981
	24100		6000		23400		5900
	$*$ 54325		13956		$*$ 57300		16881
			5800				5700
p	100981		19756	p	100981		22581
284	80656		5600	291	84681		5500
	20325		25356		16300		28081
	25900		5400		26600		5300
215^2	$= 46225$		30756		42900		33381
			5200		21600		5100
			35956		$*$ 64500		38481
			5000				4900
			40956				43381
			4800				4700
			45756				48081
			4800				
			50356				

Therefore, because only one square occurs (namely, $46225 = 215^2$), $100981 = 215^2 + 234^2$ will be a prime number.

Example 3

48. To test whether or not the number 1000009 is prime. [13]

[13]Translator: In the last two columns, the original version erroneously lists 69784 instead of 68784, 88984 instead of 87984, 107984 instead of 106984, etc.

p	1000009		p	1000009	p	1000009	p	1000009	
1000	1000000		978	956484	997	994009	995	990025	
3^2	$= 9$	277509		43525		6000		9984	285984
	19900	16900		95300		97200		19800	16800
	19909	294409		138825		103200		29784	302784
	19700	16700		90300		92200		19600	16600
	39609	311109		229125		195400		49384	319384
	19500	16500		85300		87200		19400	16400
	59109	327609		314425		282600		68784	335784
	19300	16300		80300		82200		19200	16200
	78409	343909		394725		364800		87984	351984
	19100	16100		75300		77200		19000	16000
	97509	360009		470025		442000		106984	367984
	18900	15900						18800	15800
	116409	375909	p	1000009	p	1000009		125784	383784
	18700	15700	972	944784	953	908209		18600	15600
	135109	391609	235^2	$= 55225$		91800		144384	399384
	18500	15500		94700		92800		18400	15400
	153609	407109		149925		184600		162784	414784
	18300	15300		89700		87800		18200	15200
	171909	422409		239625		272400		180984	429984
	18100	15100		84700		82800		18000	15000
	190009	437509		324325		355200		198984	444984
	17900	14900		79700		77800		17800	14800
	207909	452409		404025		433000		216784	459784
	17700	14700		74700				17600	14600
	225609	467109		478725				234384	474384
	17500	14500						17400	14400
	243109	481609						251784	488784
	17300	14300						17200	
	260409	495909						269984	
	17100							17000	
	277509							285984	

Therefore, this number 1000009 can be written in two ways as the sum of two squares, obviously $1000^2 + 3^2$ and $235^2 + 972^2$, so it will not be prime; indeed, its factors will be found from the formula $\frac{1000 \pm 972}{235 \pm 3}$ reduced to lowest terms, from which arises

$$\frac{1000 + 972}{235 + 3} = \frac{1972}{238} = \frac{986}{119} = \frac{58}{7}, \text{ so a factor is 3413,}$$[14]

$$\frac{1000 + 972}{235 - 3} = \frac{1972}{232} = \frac{493}{58} = \frac{17}{2}, \text{ so a factor is 293;}$$ [15]

[14] Translator: Based on Corollary 1, a factor is $58^2 + 7^2$.
[15] Translator: Based on Corollary 1, a factor is $17^2 + 2^2$.

The factors will be easily found from the formula

$$\frac{1000-972}{235\pm 3}=\frac{28}{238}=\frac{14}{119}=\frac{2}{17},\text{ and }\frac{28}{232}=\frac{7}{58}.$$

Therefore, we have learned that $1000009 = 293 \cdot 3413$, factors which had not been so easily discovered by any other method.

Example 4

49. To test whether or not the number 233033 is prime.

482^2	$233033 - 232324$	477^2	$233033 - 227529$	473^2	$233033 - 223729$	478^2	$233033 - 228484$
	709		5504		9304		4549
	9540		9440		9360		9460
	10249		14944		18664		14009
	9340		9240		9160		9260
	19589		24184		27824		23269
	9140		9040		8960		9060
	28729		33224		36784		32329
	8940		8840		8760		8860
	37669		42064		45544		41189
	8740		8640		8560		8660
	46409		50704		54104		49849
	8540		8440		8360		8460
	54949		59144		62464		58309
	8340		8240		8160		8260
	63289		67384		70624		66569
	8140		8040		7960		8060
	71429		75424		78584		74629
	7940		7840		7760		7860
	79369		83264		86344		82489
	7740		7640		7560		7660
	87109		90904		93904		90149
	7540		7440		7360		7460
	94649		98344		101264		97609
	7340		7240		7160		7260
	101989		105584		108424		104869
	7140		7040		6960		7060
	109129		112624		115384		111929
	6940		6840		6760		6860
	116069		119464		122144		118789

Therefore, because this number, although it is of the form $4n + 1$, is not a sum of two squares, by the use of Proposition 5 we conclude that it is not a

prime number. Indeed, we cannot determine its factors from this. Nevertheless, we still conclude that it has at least two factors of the form $4m - 1$, which by investigation are found to be $467 \cdot 499$.

Example 5

50. To test whether or not the number 262657 is prime.

262657	262657	262657	262657
$511^2 = 261121$	$509^2 = 259081$	$506^2 = 256036$	$504^2 = 254016$
1536	3576	6621	8641
10120	10080	10020	9980
11656	13656	$129^2 = 16641$	18621
9920	9880	9820	9780
21576	23536	26461	28401
9720	9680	9620	9580
31296	33216	36081	37981
9520	9480	9420	9380
40816	42696	45501	47361
9320	9280	9220	9180
50136	51976	54721	56541
9120	9080	9020	8980
59256	61056	63741	65521
8920	8880	8820	8780
68176	69936	72561	74301
8720	8680	8620	8580
76896	78616	81181	82881
8520	8480	8420	8380
85416	87096	89601	91261
8320	8280	8220	8180
93736	95376	97821	99441
8120	8080	8020	7980
101856	103456	105841	107421
7920	7880	7820	7780
109776	111336	113661	115201
7720	7680	7620	7580
117496	119016	121281	122781
7520	7480	7420	7380
125016	126496	128701	130161
7320	7280	7220	7180
132336	133776	135921	137341

Therefore, because only one square occurs here, $16641 = 129^2$, so that there is only one way, $262657 = 129^2 + 496^2$, and these numbers 129 and 496 are prime between themselves, it is certain that the number 262657 is prime.

Example 6

51. To test whether or not the number 32129 is prime.

	32129		32129		32129		32129
152^2	$= 23104$	177^2	$= 31329$	175^2	$= 30625$	170^2	$= 28900$
95^2	$= 9025$		800		1504		3229
	12700		15200		3400		3300
	21725		16000		4904		6529
					3200		3100
	32129		32129		8104		9629
148^2	$= 21904$	173^2	$= 299294$		3000		2900
	10225		2200		11104		12529
	12300		14800		2800		2700
	22525		17000		13904		15229
					2600		2500
					16504		17729

Therefore, this number can also be written in just one way as a sum of two squares, $95^2 + 152^2$, but because these numbers 95 and 152 are not prime between themselves but have common divisor 19, the given number is not prime but has factor $19^2 = 361$, and $32129 = 19^2 \cdot 89$.

Scholium

52. Although this method of testing whether or not numbers are prime has been extended only to numbers contained in the form $4n + 1$, very often it can provide great assistance in judging numbers. But as for how much this same rule surpasses other rules, anyone who wishes to make an attempt in this matter will easily try. The one who will wish to examine a number not less than one million in the ordinary way should attempt its division by all prime numbers up to one thousand, a work which will not be finished for many hours, while with the help of this rule by itself, the work will scarcely be a half hour.