An inquiry into whether or not 1000009 is a prime number*

Leonhard Euler†

December 2, 2004

1. Since this number is clearly the sum of two squares, namely 1000^2+3^2, the the question becomes: can this number can be separated into two squares in more than one way? For if this can be done in no other way, then this number will clearly be prime, but on the other hand, if there is another way to decompose it, then it will not be prime, as indeed it would then be possible to determine its divisors. Therefore, if we take as one square xx, it is to be investigated whether another square can be found, namely $1000009 - xx$, aside of course from the case $x = 3$ and $x = 1000$. This will be considered in the following way.

2. If the chosen square number ends in 9, the other square must necessarily be divisible by 5, and indeed by 25. Therefore we take the expression $1000009-xx$ to be divisible by 25, and it is clear that it must then necessarily be $x = 25a + 3$; thus this expression is attained:

$$1000000 - 6 \cdot 25a - 25^2 \cdot aa,$$

*Originally published as *Utrum hic numerus: 1000009 sit primus, nec ne, inquiritur*, Nova Acta Academiae Scientarum Imperialis Petropolitinae **10** (1797), 63-73, and republished in *Leonhard Euler, Opera Omnia*, Series 1: Opera mathematica, Volume 4, Birkhäuser, 1992. A copy of the original text is available electronically at the Euler Archive, at www.eulerarchive.org. This paper is E699 in the Eneström index.

†Translated from the Latin by Jordan Bell, II year undergraduate in Honours Mathematics, School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada. Email: jbell3@connect.carleton.ca

which when divided by 25 changes into this: $40000-6a-25aa$, which therefore must also be of a square form.

3. At this point two cases are to be considered, according to whether a is an even or odd number. In the first case it is $a=2b$, and by dividing by 4, this resulting formula must also be a square:

$$A = 10000 - 3b - 25bb.$$

For the other case, taking $a = 4c+1$ yields this square formula:

$$B = 39969 - 224c - 400cc,$$

which is clearly able to be an odd square; on the other hand, in the same case, if we take $c = 4d-1$, then the formula that results is:

$$C = 39981 + 176d - 400d,$$

which when divided by 8 leaves a remainder of 5, and thus is not able to be a square in any circumstances. Hence only the two formulas for A and B will be examinded.

The decomposition of the formula $B = 39969 - 224c - 400cc$.

4. Here we can take for the letter c all the successive positive and negative values 0, 1, 2, 3, etc., and for the absolute value, 39969 is subtracted from the expression $400cc \pm 224c$, for both c positive and negative. Here we note the successive numbers being subtracted in the second column, with the differences between them in the first:

c	$400cc-224c$	Diff.	c	$400cc+224c$	Diff.
0	0		0	0	
		176			624
1	176		1	624	
		976			1424
2	1152		2	2048	
		1776			2224
3	2928		3	4272	
		2576			3024
4	5504		4	7296	

from which it is immediately clear that the differences along each of the sides are increasing each time by 800.

5. Then these differences are continuously subtracted from the absolute number 39969, and for convenience is done in two columns, so that it can be seen whether the numbers that result from this area squares.

39969	39969	31089	28849
176	624	4176	4624
39793	39345	26913	24225
976	1424	4976	5424
38817	37921	21937	18801
1776	2224	5776	6224
37041	35697	16161	12577
2576	3024	6576	7024
34465	32673	9585	5553
3376	3824	7376	
31089	28849	*2209	

6. Over both sides, the single square that occurs is $*2209$. From this is seen that the proposed number is not prime, but rather has divisors, even though it is included in the work, "De tabula numerorum primorum usque ad millionem et ultra continuande", *Novi Commentarii academiae scientiarum imperialis Petropolitanae* **19**. To find the divisors of it, it is noted that this square is generated from the value $c = -10$, because of which it is $a = -39$, and then of course $x = 25a + 3 = -927$ is deduced, and then

$$1000009 - xx = 55225 = 235^2.$$

Therefore we have these two decompositions for it:

$$1000^2 + 3^2 = 927^2 + 235^2,$$

and then by rearranging,

$$1000^2 - 235^2 = 972^2 - 3^2,$$

from which it follows

$$(1000 - 235)(1000 + 235) = (927 - 3)(927 + 3),$$

that is, $1235 \cdot 765 = 969 \cdot 975$. Then it is $\frac{1235}{975} = \frac{969}{765}$, and by simplifying these fractions, it can be brought into its lowest terms: $\frac{19}{15}$, and then indeed it can be concluded that our number has a common divisor with the sum of the squares $19^2 + 15^2$, which is therefore 293. So thus we can see that

$$1000009 = 293 \cdot 3412.$$

From this, it appers that an error has crept into the table in the above mentioned work, in which all the prime numbers between 1000000 and 1002000 are given; perhaps the reason for this is because consideration of the prime divisor 293 was missed.

The decomposition of the formula $A = 10000 - 3b - 25bb$.

7. This formula is a hundredth part of the formula $1000009 - xx$, and for its decomposition again two cases are distinguished, according to whether b is an even number, or whether it's an odd number. For the first case, it is clear that unless b is itself made of a pair of even parts the given formula could not be made a square. Therefore it will be $b = 4c$, and the resulting formula when divided by 4 would be $2500 - 3c - 100cc$, for which it is not hard to see that it will never be a square except for the case $c = 0$: Firstly, it is clear that it will not be one when $c = \pm 1$, and then similarly it could not be one for $c = \pm 2$, For $c = \pm 3$, our formula comes out as $2500 - 900 \pm 9 = 1600 \pm 9$, which cannot be a square. Furthermore, if it is supposed that $c = \pm 4$, it would be

$$2500 - 1600 \pm 12 = 900 \pm 12,$$

which will certainly not be a square. Indeed, even by taking $c = \pm 5$, it can still not be brought forth as a square, for it appears as

$$2500 - 2500 \pm 15 = 0 \pm 15.$$

8. For the second case, in which b is an odd number, at first it is taken $b = 4d + 1$, and the expression that follows is

$$9972 - 212d - 400dd,$$

which when divided by 4 is

$$2493 - 53d - 100dd,$$

which for the case of $d = 0$ is seen to not be a square. It is then taken $d = \pm 1$, which produces 2393 ± 53; similarly, that is not a square. For the case $d = \pm 2$, 2093 ± 106 is produced. The case $d = \pm 3$ gives 1593 ± 159, and both ways no square can result, neither as well from the case $d = \pm 4$, which of course gives 893 ± 212. Then for the case of $d = -5$, $-7 + 265$ follows. In the end, for a number b in the form $4d - 1$, this is produced:

$$9978 + 188d - 400d$$

which must be an even number, but which when divided by 4 cannot be a square.

9. Following this method, with the numerous calculations that have been developed for it, we will examine another number which can be resolved into two squares, which is $1000081 = 1000^2 + 9^2$, and we will see whether it can be decomposed into two squares in more than this one way. Like in the last case, one or the other of them must necessarily be divisible by 5. Therefore one is set to be the square xx, and we see that the remaining part $1000081 - xx$ can be a square divisible by 5 or by 25.

10. At this point, we now set $x = 25y + 9$, which makes the formula $1000000 - 18 \cdot 25y - 25^2 yy$, which, when divided by 4, is simplified into this: $40000 - 18y - 25yy$. Now, for the first term with a y, it is even, and so it will be $y = 2a$, and by dividing this formula again by 4, it becomes:

$$A = 10000 - 9a - 25aa.$$

The second number is odd, and for it, it is set, #1 $y = 4b + 1$, which produces

$$B = 39957 - 272b - 400b,$$

which is an odd number and leaves a remainder of 5 when divided by 8, and so cannot be a square; because of this, the formula for B is omitted. #2. We set $y = 4c - 1$, and its formula will be:

$$C = 39963 + 128c - 400cc,$$

where the number 39939, when divided by 8 has a remainder 1; the investigation is advanced by examining this now.

The decomposition of the formula $C = 39993 + 128c - 400cc$.

11. It is clear that numbers in the form $400 \cdot cc \pm 128c$ should be subtracted from this absolute number 39993, and these calculations are simplified, like before, by taking away the differences between the other numbers, whether c is positive or negative; we set these up in the following table:

c	$400cc - 128c$	Diff.	c	$400cc + 128c$	Diff.
0	0		0	0	
		272		528	
1	272		1	528	
		1072			1328
2	1344		2	1856	
		1872			2128
3	3216		3	3984	

where again the differences continually increase by 800.

12. Therefore we subtract these increasing differences of 800 from the absolute number 39993, which will have these calculations:

39993	39993	30633	29353
272	528	4272	4528
39721	39465	26361	24825
1072	1328	5072	5328
38649	38137	21289	19497
1872	2128	5872	6128
36777	36009	15417	13369
2672	2928	6672	6928
34105	33081	8745	6441
33472	3728	7472	
30633	29353	1273	

Clearly no square occurs in this.

The decomposition of the formula $A = 10000 - 9a - 25aa$.

13. In place of a we will place an equal number, which ought to be made of equal parts, and on that account it will be $a = 4e$, such that by dividing by 4, this expression will be seen: $2500 - 9e - 100ee$. Then at this point, numbers in the form $100ee \pm 9e$ should be successively subtracted from the absolute number; this is given in the following table, in which the number e can be either a positive or negative number:

e	$100ee - 9e$	Diff.	$100ee + 9e$	Diff.
0	0		0	
		91		109
1	91		109	
		291		309
1	382		418	
		491		509
3	873		927	

Then we continually subtract these differences increasing by 200 from the absolute number 2500, in the following way:

2500	2500
91	109
2409	2391
291	309
2118	2082
491	509
1627	1573
691	709
936	864
891	
45	

where no squares occur aside from 2500, which however leads to a square beyond the noted 1000^2.

9. Now, if a is an odd number, first of the form $4f + 1$, our formula will come out as

$$9966 - 236f - 4ff,$$

which is a number with unequal parts, and it cannot be a square. Therefore we then set $a = 4f - 1$, and the formula produced is

$$9984 + 164f - 4ff,$$

which therefore has equal parts; thus dividing this by 4 changes it into this:

$$2496 + 41f - 100f.$$

Then numbers in the form $100ff \pm 41f$ are subtracted from the absolute number, and, for f a positive or negative number, it will thus be:

f	$100ff - 41f$	Diff.	f	$100ff + 41f$	Diff.
0	0		0	0	
		59			141
1	59		1	141	
		259			341
2	318		2	482	
		459			541
3	777		3	1023	

Then these differences of two hundred are successively subtracted from the absolute number:

2496	2496
59	141
2437	2355
259	341
2178	2014
459	541
1719	1473
659	741
1060	732
859	
201	

Therefore, because in all these calculations no squares occur, it is certain that the given number 1000081 can be resolved into two squares in only one way, and thus is clearly a prime number. This is shown in the table of the earlier paper; yet what is most remarkable about this is the ease of the calculation with which we were able to verify this for certain.

15. However, it is sad that this method is not able to be used for investigating all the numbers, but rather is limited to numbers which not only are the sum of two squares, but on top of this end in a 1 or 9, because with these it follows that the other square will be divisibe by 5.

16. Still though, clearly all numbers that are of the form $4n + 1$ and that end in either a 1 or a 9 are suitable and they are thus able to be examined with success; if we know that such a number can be resolved into two squares, the other one is certain to be divisible by 5. Then, by following the instructions that have been given here, if it is found that the given number is only able to be resolved into two squares in one way, then there will be a sure proof that it will be prime; but if on the other hand it could be made from two squares in multiple ways, from this it will be possible to assign factors, in the same way we did earlier. However, if it comes out that the given number is completely not able to be broken into two squares, then this itself is a proof that it is not prime, even if the factors themselves cannot be determined, as it can be concluded that at a minimum it has two factors, with the first of the form $4n - 1$.