Fermat to Carcavi

August 1659

Relation of New Discoveries in the Science of Numbers,[1]

... 1. And since the ordinary methods found in the books, were insufficient to demonstrate such difficult propositions, I finally found a totally singular route to success.

I have called this manner of demonstration *infinite descent,* or *indefinite descent*, etc.; at first I only used it to demonstrate negative propositions, such as:

That there is no number, one less than a multiple of 3, composed of a square and the triple of another square;

That there is no right triangle in whole numbers whose area is a square number.

The proof is made by ἀπαγωγὴν εἰς ἀδύνατον[2] in this manner:

If there were a right triangle in whole numbers whose area were equal to a square, there would have to be another triangle smaller than it having the same property. If there were a second, less than the first, having the same property, then there would be, by a similar reasoning, a third less than the second, which would have the same property, and finally a fourth, a fifth, etc., descending infinitely. Yet given a number, there are not an infinite number of descending numbers smaller than it (I speak of whole numbers). Whence it is concluded that it is therefore impossible for there to be any right triangle with square area.

From this it is inferred that neither are there [right triangles] whose sides are fractions, having square areas; for, if there were one in fractions, there would be one in whole numbers, which cannot be, as can be proven by the *descent.*

[1] From a hand copy made by Huygens.

[2] proof by contradiction – literally, “leading down to an impossibility”

I do not add the reason by which I infer that, if there were a right triangle of this nature, there would be another of the same nature smaller than the first, because the discourse would be too long and there is the whole mystery of my method. I will be pleased to see the Pascals, the Robervals and other savants look for it following my outline.

2. For a long time I was without the means of applying my method to affirmative questions, because the path and the means of arriving there are much less easy that that which served me for the negative [questions]. So as soon as it was necessary for me to demonstrate that *every prime number, one greater than a multiple of 4, is composed of two squares,*[3] I found myself in great difficulty. But finally my frequent rumination brought me the light that I lacked, and affirmative questions were treated by my method, with the assistance of some new principles which were necessary to add. This progress of my reason for affirmative cases is such: if an arbitrarily taken prime number, which is one greater than a multiple of four, is not composed of two squares, then there will be another prime number of the same sort, less than the given, and further a third smaller still, etc., descending infinitely to the number 5, which is the least of all those of this nature, from which it would follow that it is not composed of two squares, which, however, it most certainly is. Whence it must be inferred, by the deduction of the impossible, that all those of this nature are consequently composed of two squares.

3. There are infinite questions of this type, but there are some which demand new principles before *descent* can be applied to them, and the study of them is sometimes so difficult that it cannot be performed without much trouble. Such is the following question that Bachet in his work on Diophantus avows to have never been able to demonstrate, and on which subject M. Descartes made the same declaration in one of his letters, where he confessed that it seemed so difficult that he saw no path to its discovery.

Every number is either square itself, or is composed of two, three, or four squares.

I have finally subdued it under my method and I demonstrate that, if a given number were not of this nature, there would be a smaller one which likewise would not be either, and thus a third, etc., to infinity; whence it is inferred that all numbers are of this nature.

[3] See his *Observations on Diophantus,* VII

4. That which I proposed to M. Frenicle and others[4] is just as difficult, if not more so: *Any non-square number is of such a nature that there are an infinite number of squares which, multiplying said number, make one less than a square.* I demonstrate it by the *descent* applied in a particular manner.

I maintain that M. Frenicle gave several particular solutions, and M. Wallis as well, but the general demonstration is to be found by duly and properly applied *descent*: which I will show them, in order that they may add the demonstration and general construction of the theorem and the problem to the specific solutions that they have given.

5. I then considered certain questions which, although negative, did not present any great difficulty, since the method of applying *descent* was completely different from the preceding, as it will be easy to prove. Such cases include the following:

There is no cube divisible into two cubes.[5]

There is only one square of whole numbers which, when two is added to it, makes a cube. Said square is 25.

There are only two squares of whole numbers which, when 4 *is added, make a cube.* Said squares are 4 and 121.[6]

All the square powers of two,[7] *with one added, are prime numbers.*[8]

This last question is a very subtle and ingenious study, and although it is stated in the affirmative, it is negative, since to say that a number is prime is to say that it cannot be divided by another number.

In this place I pose the following question, whose solution I have sent to M. Frenicle, after he swore to me and even affirmed in his written Work[9] that he was unable to find it:

There are only the two numbers 1 *and* 7 *which, being one less than twice a square, themselves make a square of the same nature* – that is, their squares are also one less than twice a square.

6. After having passed through all these questions, the majority of diverse

[4] see letters LXXX and LXXXI

[5] See *Observations on Diophantus,* II

[6] See letter LXXXIV, **5**, and *Observations on Diophantus*, XLII

[7] *toutes les puissances quarrées de 2*

[8] See letter XCVI, **3**, 1

[9] This work, *Solutio duorum problematum etc.,* has been lost.

natures and different means of demonstration, I moved on to the creation of general rules to solve the simple and double equations of Diophantus.

For example, let the question be posed:

$$2\text{ Q} + 7967 \text{ equals a square.}$$

I have a general rule to solve this equation, if it is possible, or to prove its impossibility, and so on for all cases and all numbers, both square and simple.

Let this double equation be proposed:

$$2\text{N} + 3 \quad \text{and} \quad 2\text{N} + 5 \text{ both be equal to a square.}$$

Bachet boasts, in his Commentaries on Diophantus,[10] to have found a rule for two particular cases: I give a general one applicable in all sorts of cases and determine by rule whether or not it is possible.

I afterwards re-established the majority of the defective propositions of Diophantus and I have solved those that Bachet confessed not to know, and the majority of those that Diophantus himself seemed to hesitate upon, for which I will produce proofs and examples at my first leisure.

7. I confess that my invention to discover whether a number is prime is not perfect, but I have many paths and methods to reduce the number of divisions and to greatly reduce them by shortening the usual labor. I believe it would be a considerable help for savants, were M. Frenicle to make his thoughts on this subject public.

8. The question which has occupied me without my yet finding a solution, is the following, which is the last of the book of Diophantus *De multangulus numeris.*

Dato numero, invenire quot modis multangulus esse possit.

Since the text of Diophantus has been corrupted, we can not guess his method; that of Bachet does not please me and it is too difficult for most. I have discovered a better one, but it does not yet satisfy me.

[10] See *Observations on Diophantus,* XLIV, and the Appendix to this Observation

9. It is necessary to seek from this proposition, the solution of the following problem.

Find a number which is polygonal as many times and no more than desired, and find the smallest of those which will satisfy the question.[11]

10. Here you have a summary account of my dreams[12] on the subject of numbers. I have only written it because I fear I will lack the leisure to fully express myself and to lay out the entirety of my demonstrations and methods; in any case, this outline will serve the savants to be able to prove for themselves that which I have not filled out, especially if MM. de Carcavi and Frenicle give them some demonstrations *by descent* that I have sent them on the subject of some negative propositions. And perhaps posterity will be thankful for my having let them know that which the Ancients did not, and this relation can enter the minds of those who will come after me to *traditio lampadis ad filios,* as the great Chancellor of England says,[13] according to the thought and the phrase to which I will add:

Multi pertransibunt et augebitur scientia.

FERMAT.

[11] Except for the smallest numbers, any number can be said to be a polygonal number in two ways – for example, 6 is the third triangular number and the first hexagonal number. The number 15 is the third hexagonal number, the fifth triangular number, and (less interestingly) the first 15-agonal number. I believe that 36 is the smallest number to be three non-degenerate polygonal numbers: the eighth triangular number, the sixth square number, and the third 13-agonal number.

[12] *rêveries*

[13] Bacon, *De dignitate et augmentis scientiarum*, book VI, ch. 2