Fermat à Frenicle

Jeudi 18 Octobre 1640

Monsieur,

1. Les vacations, qui m'ont éloigné de Toulouse, m'ont en même temps éloigné de mon devoir et empêché de vous écrire plus tôt depuis la dernière de vos lettres en date du 21 septembre. Je tâcherai de réparer par celle-ci la longueur de l'attente et commencerai par la liberté que je prends de vous dire que je n'ai point vu encore aucune proposition de votre part que je n'eûsse plus tôt trouvée et considérée; et afin de vous rendre vous-même juge de cette vérité, et vous ôter en même temps le scrupule que vous pourriez avoir, que je n'en use comme quelqu'un de ceux du lieu où vous êtes, qui s'attribue impunément les inventions d'autrui, après qu'elles lui ont été communiquées, je commencerai par la proposition de la différence de deux quarrés, que vous trouverez dans Bachet sur le Diophante, au commentaire de la proposition 11 du deuxième Livre, en même façon que vous me l'avez envoyée, vous avouant pourtant que l'application, que j'estime beaucoup, est toute vôtre et que je l'ai apprise de vous.

2. Pour le sujet des progressions, je vous avois envoyé par avance les propositions qui servent à déterminer les parties des puissances -1, et, par ma seconde Lettre, je vous avois fait comprendre que j'avois considéré toutes les propositions qui servent aux puissances $+1$, de quoi je m'étois contenté de vous donner deux exemples, dont l'un étoit démontré par moi et par conséquent connu nécessairement, et l'autre ne m'étoit point entièrement connu par raison démonstrative, bien que je vous assurasse que je n'en doutais pas.

Or, pour venir à la connoissance de ce dernier, quoiqu'imparfaite encore et non achevée, je ne le pouvois sans avoir plus tôt examiné et prouvé par démonstrations toutes leurs propositions contenues en votre dernière, ce que vous n'aurez nulle peine de croire, puisque le seul exemple que je vous envoyai le marquoit assez, auquel j'ajoutois qu'en toutes progressions on pouvoit déterminer les diviseurs communs et généraux avec pareille aisance.

Fermat to Frenicle

Thursday, 18 October 1640

Translated by Amanda Bergeron and David Zhao

Sir,

1. The vacations, which took me out of Toulouse, at the same time took me away from my work and prevented me from writing you sooner in response to the last of your letters dated 21 September. I will attempt to make up for the length of your wait by beginning with the freedom that I take in telling you that I still have not seen any proposition on your part that I have not already found and considered; and so that you may recognize this truth for yourself, and at the same time for you to remove any scruple that you could have, that I mistreat your work like one of those people from where you are, who attribtes inventions of the past to himself with impunity, after they were already communicated to him, I will start with the proposition on the difference of two squares, that you would find in Bachet on Diophantus, on the commentary of proposition 11 in the second book, in the same way that you sent it to me, admitting to you however that the application, which I value highly, is entirely yours and that I learned it from you.

2. On the subject of progressions, I have sent to you in advance the propositions that serve to determine the properties of powers minus one, and, by my second letter, I have made you understand that I have considered all the propositions which serve for the powers plus one, for which I was content to give you two examples, of which one was proved by me and as a consequence necessarily known, and the other not entirely known to me by way of proof, although I assure you that I do not doubt it.

Now, to come to the knowledge of the latter, even though still imperfect and not achieved, I could not have examined and shown by proofs all the propositions contained in your last letter without having it, so that you would not have any difficulty in believing, since the only example that I sent you indicated this sufficiently, to which I have added that in all progressions one could determine the common and general divisors with the same facility.

Mais je vous avoue tout net (car par avance je vous avertis que, comme je ne suis pas capable de m'attribuer plus que je ne sais, je dis avec même franchise ce que je ne sais pas) que je n'ai pu encore démontrer l'exclusion de tous diviseurs en cette belle proposition que je vous avois envoyée et que vous m'avez confirmée, touchant les nombres 3, 5, 17, 257, 65537, etc. Car, bien que je réduise l'exclusion à la plupart des nombres et que j'aie même des raisons probables pour le reste, je n'ai pu encore démontrer nécessairement la vérité de cette proposition, de laquelle pourtant je ne doute non plus à cette heure que je faisois auparavant. Si vous en avez la preuve assurée, vous m'obligerez de me la communiquer; car après cela, rien ne m'arrêtera en ces matières.

3. Reste à vous parler de la proposition fondamentale des parties aliquotes, laquelle m'étoit tellement connue que je vous l'avois envoyée par la première lettre que je vous écrivis, laquelle on m'a dit depuis s'être égarée. Pourtant, si le Père Mersenne veut prendre le soin de la faire chercher dans le bureau de la poste, elle se trouvera dans un paquet que j'adressois à M. ....

Outre que cette proposition est si naturelle, qu'il est impossible de déterminer et de trouver la moindre chose sur ce sujet, qu'elle ne se présente d'abord; de sorte qu'ayant depuis fort longtemps trouvé et envoyé les propositions des deux nombres 17 296 et 18 416 et autres pareilles, il falloit par nécessité que j'eûsse passé par la dite proposition.

Pour votre application, il me semble qu'elle n'ôte pas la longueur que je trouvois en cette sorte de questions, qui est la seule difficulté que j'y ai toujours reconnue; sinon que je ne l'aie bien comprise, de quoi je vous prie m'avertir et me rendre certain.

4. Il me semble après cela qu'il m'importe de vous dire le fondement sur lequel j'appuie les démonstrations de tout ce qui concerne les progressions géométriques, qui est tel:

Tout nombre premier mesure infailliblement une des puissances -1 de quelque progression que ce soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné -1; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.

Exemple: soit la progression donnée

1	2	3	4	5	6	
3	9	27	81	243	729	etc.

avec ses exposants en dessus.

But I clearly admit to you (because as above I will make you aware that I am not capable of attributing to myself more than I know, I will speak with the same frankness about that which I do not know) that I still cannot prove the exclusion of all divisors in this lovely proposition which I have sent to you and which you have confirmed for me, touching the numbers 3, 5, 17, 257, 65537, etc. For, although I have reduced the exclusion to most of the numbers and also have probable reasons for the rest, I still cannot prove with necessity the truth of this proposition, although I still do not doubt to this hour that I have done it already. If you have assured the proof, you would oblige me in communicating it to me; because, after this, nothing would hinder me in these matters.

3. The rest of this concerns a fundamental proposition of uniform divisors, which was so firmly known to me that I sent it to you in the first letter which I wrote you, but which I have been told has since been misplaced. However, if Father Mersenne wants to take the time to look for it in the post office, it would be found in a packet which I addressed to Mr. Carcavi (?).

Furthermore, this proposition is so natural that it is impossible to determine and to find the least matter on this subject, and that it does not present itself at first; so that having found and sent a long time ago the propositions of the two numbers 17,296 and 18,416 and other similar numbers, it follows by necessity that I am finished with the stated proposition.

For your application, it seems to me that it does not detract from the length that I have found in these sorts of questions, which is the only difficulty that I always recognize; or else that I do not understand it well enough, in which case I would hope that you would inform me and render me certain.

4. It seems to me after this that it is important for me to tell you the basis on which I apply the proofs of everything that concerns geometric progressions, such as:

Every prime number evenly divides one of the powers minus one of any progression in which the exponent of the given power is a factor of the given prime number minus one; and after one has found the first power which satisifies this property, all those numbers having exponents that are multiples of the exponent of the first satisfy all of the same properties.

Example: consider the given progression

1	2	3	4	5	6	
3	9	27	81	243	729	etc.

with the exponents listed above.

Prenez, par exemple, le nombre premier 13. Il mesure la troisième puissance -1, de laquelle 3, exposant, est sous-multiple de 12, qui est moindre de l'unité que le nombre 13, et parce que l'exposant de 729, qui est 6, est multiple du premier exposant, qui est 3, il s'ensuit que 13 mesure aussi la dite puissance $729 - 1$.

Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.

5. Mais il n'est pas vrai que tout nombre premier mesure une puissance $+1$ en toute sorte de progressions: car, si la première puissance -1, qui est mesurée par le dit nombre premier, a pour exposant un nombre impair, en ce cas il n'y a aucune puissance $+1$ dans toute la progression qui soit mesurée par le dit nombre premier.

Exemple: parce qu'en la progression double, 23 mesure la puissance -1 qui a pour exposant 11, le dit nombre 23 ne mesurera aucune puissance $+1$ de la dite progression à l'infini.

Que si la première puissance -1 qui est mesurée par le nombre premier donné a pour exposant un nombre pair, en ce cas la puissance $+1$ qui a pour exposant la moitié dudit premier exposant sera mesurée par le nombre premier donné.

6. Toute la difficulté consiste à trouver les nombres premiers qui ne mesurent aucune puissance $+1$ en une progression donée: car cela sert, par exemple, à trouver quels des nombres premiers mesurent les radicaux des nombres parfaits et à mille autres choses, comme, par exemple, d'où vient que la 37^{e} puissance -1 en la progression double est mesurée par 223. En un mot, il faut déterminer quels nombres premiers sont ceux qui mesurent leur première puissance -1 en telle sorte que l'exposant de la dite puissance soit un nombre impair, ce que j'estime fort malaisé, en attendant un plus grand éclaircissement de votre part et qu'il vous plaise d'étendre cet endroit de votre lettre, où vous dites qu'après avoir trouvé que le diviseur doit être multiple $+1$ de l'exposant, il y a aussi des règles pour trouver le quantième des dits multiples $+1$ de l'exposant doit être le diviseur.

7. Voici une mienne proposition (que peut-être vous aurez aussi trouvée) que j'estime beaucoup, bien qu'elle ne découvre pas tout ce que je cherche, que sans doute j'achèverai d'apprendre de vous:

En la progression double, si d'un nombre quarré, généralement parlant, vous otez 2 ou 8 ou 32 etc., les nombres premiers moindres de l'unité qu'un multiple

Take for example the prime number 13. It divides the third power minus one, of which the exponent 3 is a factor of 12, which is less than the number 13 by one, and because the exponent of 729, which is 6, is a multiple of the first exponent, which is 3, it follows that 13 also divides the given power 729 minus one.

And this proposition is generally true for all progressions and for all prime numbers; the proof of which I would send to you, if I were not afraid that it would be too long.

5. But it is not true that every prime number measures a power plus one in every possible progression: since, if the first power minus one that is measured by the given prime number has an odd number for its exponent, then in this case there exists no power plus one in the entire progression that is measured by the given prime number.

Example: because in the binary progression, 23 measures the power that has 11 as its exponent minus one, the given number 23 will not measure any power plus one of the given progression to infinity.

But if the first power that is measured by the given prime number minus one has an even number for its exponent, then in this case the power plus one, which has half of the aforementioned first exponent, will be measurable by the given prime number.

6. All the difficulty consists of finding the prime numbers that do not measure any power plus one in a given progression: thus it allows, for example, us to find which of the prime numbers measure the bases of the perfect numbers and to do a thousand other things, like, for example, whence the 37^{th} power minus one in the given binary progression is measurable by 223. In a word, one must determine which prime numbers are those that measure their first power minus one in such a way that the exponent of the given power is an odd number, something which I consider very difficult, in waiting for a greater solution on your part and which it would please you to elaborate on that part of your letter, where you say that after having found that the divisor must be a multiple of the exponent plus one, there are also rules for finding which of the given multiples of the exponent plus one must be the divisor.

7. Here is one of my propositions (which perhaps you may have also discovered) which I value greatly, although it does not reveal all that I am looking for, which without doubt I will be able to learn from you:

In the binary progression, if from a square number, generally speaking, you subtract 2 or 8 or 32, etc., the prime numbers less than a multiple of four by one,

du quaternaire, qui mesureront le reste, feront l'effet requis.

Comme de 25, qui est un quarré, ôtez 2; le reste 23 mesurera la 11^{e} puissance -1.

Otez 2 de 49, le reste 47 mesurera la 23^{e} puissance -1.

Otez 2 de 225, le reste 223 mesurera la 37^{e} puissance -1; etc.

En la progression triple, si d'un nombre quarré *ut supra* vous ôtez 3 ou 27 ou 243 etc., les nombres premiers moindres de l'unité qu'un multiple du quaternaire, qui mesureront le reste, feront l'effet requis. Comme:

Otez 3 de 25, le reste 22 est divisé par 11, qui est premier et moindre de l'unité qu'un multiple du quaternaire; aussi 11 mesure la 5^{e} puissance -1.

Otez 3 de 121; le reste 118 est mesuré par 59 moindre de l'unité qu'un multiple du quaternaire; aussi 59 mesure la 29^{e} puissance -1.

En la progression quadruple, il faut ôter 4 ou 64 ou 1024, etc. à l'infini en toutes progressions, en procédant de même façon.

8. J'ajouterai encore cette petite proposition.

Si d'un quarré vous ôtez 2, le reste ne peut être divisé par aucun nombre premier qui surpasse un quarré de 2.

Comme prenez pour quarré 1 000 000, duquel, ôté 2 reste 999 998. Je dis que le dit reste ne peut être divisé ni par 11, ni par 83, ni par 227 etc.

Vous pouvez éprouver la même règle aux quarrés impairs et, si je voulois, je vous la rendrois belle et générale; mais je me contente de vous l'avoir indiquée seulement.

9. Avant que finir, voici une autre proposition, laquelle vous fournira peut-être quelque application, comme vous y êtes très heureux.

Si un nombre est mesuré par un autre et que le nombre divisé soit encore divisé par un autre nombre moindre que le premier diviseur, en ce cas, si vous ôtez du quotient de la seconde division, multiplié par la différence des deux diviseurs, le reste de la seconde division, ce qui restera sera mesure par le premier divisuer.

Exemple: 121 est mesure par 11. Divisez encore 121 par 7; le quotient sera 17 et le reste de la division 2.

Multipliez le quotient 17 par 4, différence du premier et du second diviseur, et du produit 68 ôtez-en 2; reste 66 qui sera aussi mesuré par 11, premier diviseur.

which will measure the rest, will produce the required effect.

For example, from 25, which is a square, subtract 2; the remaining 23 will measure the 11^{th} power minus one.

Subtract 2 from 49, the remaining 47 will divide the 23^{th} power minus one.

Subtract 2 from 225, the remaining 223 will measure the 37^{th} power minus one; etc.

In a ternary progression, if you subtract from a square number (as above) 3 or 27 or 243 etc., the prime numbers less than a multiple of four by one, which will measure the rest, will produce the required effect. Like:

Subtract 3 from 25, the remaining 22 is divisible by 11, which is prime and less than a multiple of four by one; also 11 measures the 5^{th} power minus one.

Subtract 3 from 121; the remaining 118 is measured by 59, less than a multiple of four by one; also 59 measures the 29^{e} power minus one.

In the powers of four, you must subtract 4 or 64 or 1024, etc. in all progressions, to proceed in the same manner.

8. I will also add this small proposition.

If you subtract 2 from a square, the remaining value cannot be divided by any prime number which is greater than a square by 2.

For example, take for a square 1,000,000, from which, subtracted by two, remains 999,998. I say that the given remainder can not be divided by 11 or by 83, by 227, and so on.

You can prove the same rule for odd squares and, if I wanted, I would give you the lovely and general rule; but I am content with having only indicated it to you.

9. Before ending, here is another proposition, which will perhaps furnish you with some application, as to make you very happy.

If a number is measured by another and the divided number can still be divided by another number number less than the first divisor, in this case, if you subtract from the quotient of the second division multiplied by the difference of the two divisors, the remainder of the second division, that which remains will be measurable by the first divisor.

Example: 121 is measurable by 11. Further divide 121 by 7; the quotient is 17 and the remainder of the division is 2.

Multiply the quotient 17 by 4, which is the difference between the first and the second divisors, and subtract 2 from the product 68; the remainder 66 which will also be measurable by 11, the first divisor.

10. Que si le second diviseur est plus grand le premier, en ce cas, si vous ajoutez au quotient de la seconde division, multiplié par la différence des deux diviseurs, le reste de la seconde division, ce qui restera sera mesure par le premier diviseur.

Exemple: 117 est mesuré par 3. Divisez encore 117 par 4; le quotient sera 29 et le reste de la division 1.

Ajoutez au quotient 29, multiplié par la différence des diviseurs (qui ne change ici rien, parce que c'est l'unité), le reste de la dite division, qui est 1; la somme 30 sera aussi mesurée par 3, premier diviseur.

J'ai déjà trop écrit et il me semble qu'il est temps que vous parliez, après avoir employé si mal votre temps a lire cette longue lettre, qui vous confirmera que je suis etc.

10. But if the second divisor is larger than the first, in this case, if you add to the quotient of the second division, multiplied by the difference fo the two divisors, the remainder of the second division, that which remains will be divisible by the first divisor.

Example: 117 is measurable by 3. Further divide 117 by 4; the quotient will be 29 and the remainder of the division 1.

Add tot he quotient 29, multiplied by the difference of the divisors (which does not change anything here, because it is unity), the remainder of the given division, which is 1; the sum 30 will also be measurable by 3, the first divisor.

I have already written too much and it seems to me that it is time for you to speak, after having employed your time so poorly in reading this long letter, which will confirm to you that I exist etc.