quotient ne pourra être divisé que par un nombre qui surpasse de l'unité ou le double de 13 exposant susdit, ou un multiple dudit double de 13, etc., à l'infini.

Que si l'exposant est un nombre composé, qui pourtant ne soit pas un de ceux de la progression double, je puis trouver tous les diviseurs fort aisément.

3. Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé (1) que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double, sont nombres premiers, comme

3 5 17 257 65537 4 294 967 297

et le suivant de 20 lettres

18 446 744 073 709 551 617; etc.

Je n'en ai pas la démonstration exacte, mais j'ai exclu si grande quantité de diviseurs par démonstrations infaillibles, et j'ai de si grandes lumières, qui établissent ma pensée, que j'aurois peine à me dédire.

XLIV.

FERMAT A FRENICLE.

JEUDI 18 OCTOBRE 1640.

(*Va*, p. 162-164.)

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

(1) C'est là le plus ancien énoncé donné par Fermat de la célèbre proposition dont Euler a reconnu la fausseté. *Voir* Tome I, page 131, note 1. Le sixième nombre ($2^{32}+1$) indiqué ici par Fermat comme premier est divisible par 641. Le septième ($2^{64}+1$) est divisible par 274 177.

la dernière de vos lettres en date du 21 septembre (1). 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 (2) 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 (3) les propositions qui servent à déterminer les parties des puissances -1, et, par ma seconde Lettre (4), 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.

Mais je vous avoue tout net (car par avance je vous avertis que,

(1) Lettre perdue.
(2) Construction de deux carrés entiers ayant une différence donnée.
(3) *Voir* Lettre XL, 6.
(4) Lettre XLIII.

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 (1), 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. ... (2).

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 (3), 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 pas 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 fonde-

(1) Lettre perdue, qui doit avoir été écrite entre les Lettres XL et XLIII.
(2) Carcavi?
(3) *Voir* Pièce IV$_A$.

ment sur lequel j'appuie les démonstrations de tout ce qui concerne les progressions géométriques, qui est tel :

Tout nombre premier (1) 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.

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

(1) C'est de cet énoncé qu'a été tirée la proposition connue sous le nom de *Théorème de Fermat*, à savoir que si p est premier et ne divise pas a, il divise $a^{p-1} - 1$.

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 donnée : 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 ôtez 2 ou 8 ou 32 etc., les nombres premiers moindres de l'unité qu'un multiple 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 5e 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 29e 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 mesuré par le premier diviseur (1).

Exemple : 121 est mesuré 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.

10. Que si le second diviseur est plus grand que le premier, en ce

(1) C'est-à-dire que si l'on a

$$a = bq = b_1 q_1 + r,$$

si l'on a $b > b_1$, b divise $q_1(b - b_1) - r$. Si au contraire $b < b_1$, b divise $q_1(b_1 - b) + r$.

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 mesuré 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 à lire cette longue lettre, qui vous confirmera que je suis etc.

XLV.

FERMAT A MERSENNE.

MARDI 25 DÉCEMBRE 1640.

(A, f^{os} 12-13 *bis*, B, f° 19.)

MON RÉVÉREND PÈRE,

1. Je languissois dans l'attente de vos lettres et de M. de Frenicle. Je suis bien aise qu'il approuve ce que j'ai fait (1); et afin qu'il ne soit plus en doute de ce que je lui demande, voici trois questions que je lui propose, pource que les spéculations que j'y ai faites ne me satisfont pas pleinement :

1° La raison essentielle pourquoi 3, 5, 17, 257, etc. à l'infini, sont toujours nombres premiers;

2° Qu'il me donne quelqu'un de ses autres moyens pour trouver

(1) La réponse de Frenicle à la Lettre XLIV est perdue.