XLV.

Fermat à Mersenne.

Mardi 25 décembre 1640.

(A, folios 12-13 bis, B, folio 19)

Mon Révérend Père,

1. Je languissais 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, parce que les spéculations que j'y ai faites ne me satisfont pas pleinement :

1° La raison essentielle pour laquelle 3, 5, 17, 257, etc. à l'infini, sont tonjours des nombres premiers ;

2° Qu'il me donne quelqu'un de ses autres moyens pour trouver à l'infini des nombres premiers de tels nombres de figures qu'on voudra.
Sur quoi je voudrais être éclairci si une de mes pensées est vraie, qu'en la progression d'un nombre pair, comme 6, toutes les puissances +1 de la progression qui ont pour exposant : 1, 2, 4, 8, 16, etc. sont nombres premiers, si elles ne sont pas mesurées par un de ceux-ci : 3, 5, 17, 257. etc. ; laquelle proposition, si elle est vraie, est de très grand usage.
Si je puis une fois tenir la raison fondamentale que 3, 5, 17, etc. sont nombres premiers, il me semble que je trouverai de très belles choses en cette matière, car déjà j'ai trouvé des choses merveilleuses dont je vous ferai part, après que j'aurai eu votre réponse et celle de M. Frenicle.

3° Je lui demande un moyen plus général que celui que j'ai inventé pour savoir quels sont les multiples de l'exposant utiles à la division.

Après cela, je travaillerai aux propositions que vous me demandez.

2. Sur le sujet des triangles rectangles [2] voici mes fondements :

1° Tout nombre premier, qui surpasse de l'unité un multiple du quaternaire [3], est une seule fois la somme de deux carrés, et une seule fois l'hypoténuse d'un triangle rectangle.

2° Le même nombre et son carré sont chacun une fois la somme de deux carrés :
Son cube et le carré de son carré [4] sont chacun deux fois la somme de deux carrés ;
Le carré de son cube [5] et le cube de son cube [6] sont chacun trois fois la somme de deux carrés ;
Etc., à l'infini.

3° Ce même nombre étant une fois l'hypoténuse d'un triangle rectangle, son carré l'est deux fois, son cube trois, le carré de son carré quatre, etc. à l'infini.

4° Étant donné un nombre, pour savoir combien de fois il est l'hypoténuse d'un triangle rectangle, divisez-le par tous les nombres premiers, plus grands de l'unité qu'un multiple du quaternaire,

---

Transcription en LaTeX : Denise Vella-Chemla, juin 2026.

1. La réponse de Frenicle à la Lettre XLIV est perdue.
2. *Comparer, Tome I, l'Observation VII sur Diophante.*,
3. signifie 4.
4. son carrécarré.
5. son carrécube.
6. son cubecube.

qui le mesurent. Puis rangez les exposants des puissances des dits nombres premiers qui mesurent le nombre donné, en tel ordre que bon vous semblera, l'un après l'autre. Multipliez le premier par le second deux fois, et à cela ajoutez la somme du premier et du second ; puis multipliez cette dernière somme deux fois par le troisième, et ajoutez au produit tant la dite dernière somme que le troisième, etc. à l'infini. La dernière somme marquera à combien de triangles le nombre donné pent servir d'hypoténuse.

Les nombres premiers qui sont moindres de l'unité qu'un multiple du quaternaire, ni 2, non plus que leurs puissances, ne font rien à la question, et n'augmentent ni ne diminuent le nombre des dits triangles rectangles.

Soit, par exemple, un nombre donné mesuré par 5, par le carré de 13, par le cube de 17, et par le cube aussi de 29.

Nous aurons quatre diviseurs dont les exposants de leurs puissances, qui mesurent le nombre donné, sont :

$$1, 2, 3, 3.$$

Je multiplie le premier par le second deux fois : viendra 4 : ajoutez-y le premier et le second : viendra 7. Je multiplie par le troisième 3 deux fois viendra 42, auquel ajoutant 7 et 3, c'est 52. Je multiplie 52 par le quatrième (qui est 3) deux fois : viendra 312, auquel ajoutant 52 et 3, viendra 367.

Je dis donc que le nombre donné sera l'hypoténuse de 367 triangles rectangles et non plus.

5° Pour trouver, par exemple, le moindre nombre de tous ceux qui sont 367 fois seulement l'hypoténuse d'un triangle rectangle, je double le nombre donné et au dit double j'ajoute l'unité : viendra 735, duquel je prends tous les diviseurs séparément. Quoiqu'un nombre mesure et par soi et par ses puissances, j'entends tous les diviseurs qui sont nombres premiers ; le dit nombre se trouve donc divisé aux dites conditions par 3, 5, 7, 7. J'ôte de chacun des dits diviseurs l'unité et prends la moitié du reste : viendra 1, 2, 3, 3.

Il faut donc prendre quatre nombres premiers plus grands de l'unité qu'on multiple du quaternaire, et prendre leurs puissances exposées par les dits quatre nombres. En quoi faisant, vous satisferez à la question généralement en multipliant les dites quatre puissances entre elles.

Que si vous voulez le moindre nombre satisfaisant à la question, il faudra prendre les quatre plus petits nombres premiers de la qualité requise, qui sont 5, 13, 17, 20, et pour leurs puissances, il faut que celle du plus petit ait le plus grand exposant, et ainsi des antres. Nous prendrons done le cabe de 5, le cube de 13, le carré de 17, et 29, ef multipliant tous les uns par les autres, nous aurons le moindre nombre de tous ceux qui servent d'hypoténuse à 367 triangles rectangles et non plus.

3. Il s'ensuit de la que si le double du nombre donné, plus 1, est nombre premier, en ce cas le nombre cherché ne peut être divisé que par un seul nombre premier plus grand de l'unité qu'un multiple du quaternaire.

Comme si vous demandez un nombre qui serve d'hypoténuse à 20 triangles rectangles et non plus, parce[7] que 41 est nombre premier, il faut prendre la 20^{eme} puissance d'un nombre premier de la qualité requise.

Vous trouverez, par conséquence aisée, un nombre qui ait autant de diviseurs différents que vous voudrez et qui puisse satisfaire à la question, lorsqu'elle est possible. J'entends des diviseurs de la qualité requise, car vous y en pouvez mettre, comme nous avons dit, autant que vous voudrez de

7. pource.

ceux qui sont moindres de l'unité qu'un multiple de 1, ou bien 2 et telle de ses puissances que vous voudrez.
Je vous écris ceci si fort à la hâte que je ne prends pas garde si je fais des fautes, et omets beaucoup de choses dont je vous dirai le menu une autre fois.

4. Pour la question des ellipses[8], elle se déduira fort aisément de ce que vous venez de voir, car la question va là à trouver un nombre qui serve d'hypoténuse à 12 triangles et non plus, de telle qualité que la dite hypoténuse ait plus grande proportion au plus grand des deux autres côtés que le dit plus grand au moindre c'est-à-dire que chacun des dits triangles soit comme, par exemple, 20, 21, 20. Ce qui est aisé, et ayant trouvé le dit nombre, son carré sera le demi-diamètre des ellipses. Il faut l'élever au carré[9], afin que la perpendiculaire sur le foyer soit un nombre entier. J'en dis assez pour me faire entendre à M. Frenicle.

5. J'ajoute encore qu'une toute pareille règle à la précédente des hypoténuses sert à cette question : Étant donné un nombre, déterminer combien de fois il est la différence de deux nombres desquels le produit est un nombre carré.
Et n'y a que cette différence, qu'en cette question tous les nombres premiers hormis 2 sont utiles, ce qui n'est pas en la précédente des hypoténuses.
Comme, si un nombre est mesuré par 3 et par le carré de 5, les exposants étant 1 et 2, multipliez le premier par le second deux fois, à quoi ajoutant leur somme, viendra 7. Vous pouvez donc assurer que 75 est 7 fois la différence de deux nombres desquels le produit fait un carré.
Pour avoir le plus petit, vous userez de même voie. Or, pour trouver tous les triangles et aussi les dits nombres en cette question, la chose est assez aisée, de quoi je vous écrirai séparément, si vous voulez.
De cette dernière question, on peut tirer l'invention d'hyperholes au lieu d'ellipses, etc.
Dès que M. de Frenicle m'aura écrit, je lui donnerai des propositions que je juge, sans me flatter, qu'il estimera incomparablement plus belles que tout ce dont nous avons encore parlé.

Je suis,

Mon Révérend Père,

Votre très humble serviteur.

Fermat.

À Toulouse, le 23 décembre 1640.

---

8. Voir sur cette question, antérieurement proposée par Frenicle à Descartes, les Lettres de ce dernier, du 20 décembre 1638 (éd. Clerselier, II, 95), du 9 février 1639 (II, 97), du 30 avril 1639 (III, 81). Frenicle avait demandé de construire sur le même grand axe ($2a$) un nombre déterminé d'ellipses telles que pour chacune la distance des foyers ($2c$) fût supérieure au petit axe ($2b$) et qu'on pût exprimer en nombres entiers le grand axe, le petit axe, la distance ($a-c$) d'un foyer au sommet voisin, et l'excès $\left(\frac{a^2+c^2}{a}\right)$ sur la distance des foyers, de la distance de l'un d'eux à l'extrémité de l'ordonnée passant par l'autre.

9. Il le faut quarrer.

XXXVI.

Fermat à Mersenne [10].

Dimanche 26 décembre 1638.

(A, folios 23-24, B, folio 25 verso)

1. Pour les nombres, je peux trouver par ma méthode toutes les questions des parties aliquotes [11], mais la longueur des opérations me rebute et la recherche des nombres premiers, à laquelle toutes ces questions aboutissent. Sur lequel sujet je ne sais point de méthode que la vulgaire, sinon qu'il suffit de faire la division jusques à la plus petite racine carrée du nombre donné, car si on n'a point trouvé de diviseur jusque-là, on n'a garde d'en trouver de plus grands, parce que leur quotient serait moindre que la racine carrée, ce qui est impossible, par l'expérience qu'on aura déjà faite.

[...]

Exemple : Soit donné 84. Le plus grand carré qui le mesure est 4. le quotient 21, lequel est mesuré par 3 ou bien par 7, moindres de l'unité qu'un multiple de 4. Je dis que 81 n'est ni carré, ni composé de deux carrés, ni en entiers, ni en fractions.
Soit donné 77. Le plus grand carré qui le mesure est l'unité ; le quotient 77, qui est ici le même que le nombre donné, se trouve mesuré par 11 ou par 7, moindres de l'unité qu'un multiple du quaternaire. Je dis que 77 n'est ni carré, ni composé de deux carrés, ni en entiers ni en fractions. Etc.
Je vous avoue franchement que je n'ai rien trouvé en nombres qui m'ait tant plu que la démonstration de cette proposition, et je serai bien aise que vous fassiez effort de la trouver, quand ce ne serait que pour apprendre si j'estime plus mon invention qu'elle ne vaut.

5. J'ai démontré ensuite cette proposition, qui sert à l'invention des nombres premiers :

> *Si un nombre est composé de deux carrés premiers entre eux, je dis qu'il ne peut être divisé par ancun nombre premier moindre de l'unité qu'un multiple de 4.*

Comme, par exemple, ajoutez l'unité, si vous voulez, à un carré pair, soit le carré 10 000 000 000, lequel avec 1 fait 10 000 000 001. Je dis que 10 000 000 001 ne peut être divisé par aucun nombre premier moindre de l'unité qu'un multiple de 4, et ainsi, lorsque vous voudrez éprouver s'il est nombre premier, il ne faudra point le diviser ni par 3, ni par 7, ni par 11, etc.

[...]

3. Mais voici ce que j'admire le plus : c'est que je suis quasi persuadé [12] que tous les nombres progressifs augmentés de l'unité, desquels les exposants sont des nombres de la progression double,

10. Cette Pièce est un extrait d'une Lettre perdue, déjà publié par M. Charles Henry (*Recherches, etc.*, pp. 177-178) d'après le brouillon d'Arbogast, qui dérive d'une copie de Mersenne.

11. *Voir* Lettre XXXIII, 4.

12. 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 $(2^{2^4}+1)$ indiqué ici par Fermat comme premier est divisible par 641. Le septième $(2^{2^6}+1)$ est divisible par 274 177.

sont nombres premiers, comme

$$3 \quad 5 \quad 17 \quad 257 \quad 65\,537 \quad 4\,294\,967\,297$$

et le suivant de 20 lettres [13]

$$18\,446\,744\,073\,709\,551\,617 \; ; \quad \text{etc.}$$

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'aurais peine à me dédire.

13. Les suivants sont
$59649589127497217 \times 5704689200685129054721 = 2^{2^7} + 1 = 340282366920938463463374607431768211457$
ou bien
$1238926361552897 \times 93461639715357977769163558199606896584051237541638188580280 32 = 2^{2^8} + 1$
$= 115792089237316195423570985008687907853269984665640564039457584007913129639937.$