HISTORIA MATHEMATICA 18 (1991), 344–351

A Reconstruction of the Frenicle–Fermat Correspondence of 1640

COLIN R. FLETCHER

Department of Mathematics, The University College of Wales, Penglais, Aberystwyth Dyfed SY23 3BZ, United Kingdom

At the beginning of 1640 Frenicle asked Fermat to find a large perfect number. This question led to a correspondence between the two men in which Fermat disclosed the general statement of what is now known as Fermat's theorem. In this article missing letters are listed and their contents divined from the extant correspondence. © 1991 Academic Press, Inc.

Au début de 1640 Frenicle demanda à Fermat de trouver un grand nombre parfait. Cette requête mena à une correspondance entre les deux hommes contenant l'énoncé général de ce qu'on appelle de nos jours le théorème de Fermat. Cet article catalogue des lettres perdues et hasarde des conjectures sur leur contenu à partir de la correspondance entre les deux hommes qui existe encore. © 1991 Academic Press, Inc.

Anfang 1640 forderte Frenicle Fermat auf, eine große vollkommene Zahl zu finden. Diese Frage führte zwischen den beiden Männern zu einer Korrespondenz, in der Fermat die allgemeine Feststellung traf, die heute als Fermatscher Satz bekannt ist. In diesem Aufsatz werden die fehlenden Briefe aufgelistet und deren Inhalt aus der erhaltenen Korrespondenz erschlossen. © 1991 Academic Press, Inc.

AMS 1985 subject classifications: 10-03, 01A45.
KEY WORDS: Fermat, Fermat's theorem, Frenicle, Mersenne, perfect numbers.

1. INTRODUCTION

During the first half of the seventeenth century, mathematical ideas circulated in France, and to some extent throughout Western Europe, via a correspondence network, having its center in Paris, and with Marin Mersenne (1588–1648) as its driving force. Pierre de Fermat (1601?–1665), lawyer and mathematician living near Toulouse in the south of France, joined this circle in 1636. Bernard Frenicle de Bessy (1605?–1675), astronomer, physician, naturalist, and mathematician from Paris, had first communicated with Mersenne in 1634. It seems to have been mid-1640, however, before they were corresponding directly with each other, although both parties were using Mersenne as an intermediary earlier that year.

Fermat and Frenicle were each interested in the theory of numbers, and in questions concerning aliquot parts (divisors of positive integers). Indeed, as early as 26th December 1638, Fermat had written to Mersenne claiming that he could solve by his method all questions concerning aliquot parts, but in his usual way he had omitted any details. These claims no doubt aroused the interest of Frenicle, and at the beginning of 1640 he wrote to Mersenne with a question for Fermat: if

0315-0860/91 $3.00

it was not too much trouble for him, would he send Mersenne a perfect number of 20 digits, or the next biggest perfect number. (See Fletcher [1989] for an interpretation of this challenge and of Fermat's response.) This challenge from Frenicle was the beginning of a correspondence between the two men which led to Fermat's disclosing the general statement of the theorem which is now called Fermat's theorem. The modern version of the theorem is that $a^{p-1} \equiv 1 \pmod{p}$, where a and p are positive integers with p prime not dividing a. The extent of this 1640 correspondence was at least 11 letters, of which only six exist in full [1]. The correspondence, including four missing letters, will be reconstructed both mathematically and chronologically.

The letters are published in one or both of the collections of correspondence of Fermat and Mersenne [Fermat 1894; Mersenne 1965, 1967]. Below we give a list of these letters, including four missing ones, with a brief description of the contents as they relate to the determination of perfect numbers and to associated problems:

Date 1640	Writer/recipient	Contents
1. End of February/ beginning of March?	Frenicle to Mersenne	Challenge to find a perfect number of 20 digits or more
2. 1st April	Fermat to Mersenne (first reply to 1)	No mention of perfect numbers
3. 20th April/May?	Fermat to Mersenne (fragment)	No perfect number of 20 or 21 digits, $2^{37} - 1$ prime
4. May?	Frenicle to Fermat (lost; cited in 5)	($2^{37} - 1$ not prime)
5. Mid-June?	Fermat to Mersenne	Three propositions
6. June/August?	Fermat to Frenicle (mislaid then lost; first letter from Fermat to Frenicle; cited in 9)	(Fermat's theorem)
7. August/September?	Fermat to Frenicle (second letter from Fermat to Frenicle)	Numbers of the form $2^n + 1$, Fermat's conjecture
8. 21st September	Frenicle to Fermat (lost; cited in 9)	(Confirmation of Fermat's conjecture)
9. 18th October	Fermat to Frenicle	Fermat's theorem and its corollary
10. November/December?	Frenicle to Fermat (lost; cited in 11)	(?)
11. 25th December	Fermat to Mersenne	Three questions for Frenicle

2. PERFECT NUMBERS

The idea of a perfect number goes back to the Greeks. They discovered that some numbers have the property that the sum of all divisors (except the given number) is the number itself. For example, $6 = 1 + 2 + 3$. It is not very surprising (nor indeed interesting) that some numbers have this property. What gives the idea a certain piquancy is that there is a formula which generates such numbers. In Euclid's Elements, book IX (c. 300 B.C.), the final proposition reads as follows [Euclid 1908, 421]:

PROPOSITION 36. If as many numbers as we please beginning from an unit be set out continuously in double proportion, until the sum of all becomes prime, and if the sum multiplied into the last make some number, the number will be perfect.

In other words, the number $2^{n-1}(2^n - 1)$ will be perfect whenever $2^n - 1$ is prime. The proof of this is easy. However, two aspects of the theorem should be noted. First, Euclid is not claiming that all perfect numbers are of this form. In fact this is still an open question, although Euler (1707–1783) proved that all even perfect numbers are of this form [2]. Nevertheless, when Fermat and Frenicle discuss perfect numbers they are tacitly thinking only of those of Euclidean form. Frenicle's original challenge may have been in general terms, but any solution would have to come via Euclid's formula. The second comment is that Euclid's formula is not a formula in the sense that if a value of n is put in then an answer will come out. The expression will give a perfect number only when $2^n - 1$ is prime. It is this condition which causes the problems, and which leads to Fermat's theorem.

The first eight (Euclidean) perfect numbers are as follows:

n	$2^{n-1}(2^n - 1)$
2	6
3	28
5	496
7	8128
13	33,550,336
17	8,589,869,056
19	137,438,691,328
31	2,305,843,008,139,952,128

In Letter 1, Frenicle asks Fermat to find a perfect number of 20 digits or the next biggest one. When we look at the perfect number given by $n = 31$, it is clear why Frenicle chose 20 digits. It could have been simply a nice round number which was large enough to make Fermat do some work, but Frenicle was more astute than that. The number 20 was chosen so as to make the answer $n = 31$ unavailable. The perfect number $2^{30}(2^{31} - 1)$ has 19 digits.

3. THE RECONSTRUCTION (PART 1)

Fermat was away in the country when Frenicle's letter arrived from Mersenne. His reply, dated 1st April 1640, was taken up with matters other than perfect numbers (Letter 2). Fermat's first mention of the challenge is in Letter 3. This is an undated fragment which was sent toward the end of April [Mersenne 1965, 270] or in May [Fermat 1894, 194]. The fragment begins with Fermat's opening response to Frenicle's question, for he says immediately that there is no perfect number of 20 or 21 digits. This statement has little to do with perfect numbers but a lot to do with primes. When is $2^n - 1$ prime? Some pre-Fermat mathematicians thought that a sufficient condition was for n to be odd (see Dickson [1934, 7]). But Fermat was well aware that the value $n = 11$ gave a composite $2^n - 1$. If we jump ahead to Letter 5, the first of Fermat's propositions stated there is that a necessary condition for $2^n - 1$ to be prime is that n be prime. Armed with this result it is not difficult to prove that there is no perfect number of 20 or 21 digits. The value $n = 31$ gives a perfect number of 19 digits. The next prime is 37 but this would give a number lying between 94×10^{20} and 95×10^{20}, a number of 22 digits. This may or may not be perfect, but either way there is no perfect number of 20 or 21 digits.

Fermat begins Letter 5 by saying that he had received Mersenne's letter accompanied by that of M. Frenicle. This lost letter of Frenicle we have designated Letter 4, and given it the date May 1640? To guess at its contents we have to move forward once more to Letter 5, from Fermat to Mersenne, since this was an answer to Letter 4. The first part of the letter deals with magic squares and the second gives Fermat's three propositions which provide the short cut for finding perfect numbers. In the third part, Fermat returns to the case $n = 37$ and admits that he originally thought this gave a perfect number, in other words that $2^{37} - 1$ was prime. Fermat's previous Letter 3 exists only as a fragment, and it is more than likely that the lost portion of the letter contained his belief that $n = 37$ gave a perfect number and that this was the answer to Frenicle's challenge.

We have already indicated that Frenicle was aware of the perfect number of 19 digits given by $n = 31$. It now seems as though he knew the status of the number given by $n = 37$, either when he made his challenge or when he received Fermat's answer (Letter 3). For Fermat had made a mistake; $n = 37$ does not give a perfect number. This was one reason for Frenicle's lost Letter 4. In great glee he would be writing to tell Fermat that $2^{37} - 1$ is not prime. But he did not give the prime factorization of $2^{37} - 1$ since in Letter 5 Fermat states that he found the smallest prime factor using the short cut given by the third of his three propositions. It is unlikely that Frenicle had a short cut, but in this case the long winded method is reasonably brief:

$$2^{37} - 1 = 137{,}438{,}953{,}471 = 223 \times 616{,}318{,}177.$$

The smallest prime factor is 223, and this is the 48th prime. Fermat's third proposition states that if n is prime then prime factors of $2^n - 1$ are of the form $2nk + 1$, where k is a positive integer. Fermat himself has therefore to check only 75, 149 and 223. In fact 75 is not prime, and so the factor 223 is only the second prime to test. This illustrates nicely why Fermat was looking for a short cut. Frenicle had to check 46 primes before getting the factor (the primes 2 and 5 hardly need checking) whereas Fermat had finished after two long divisions.

The main question left unanswered is how Fermat came to make a mistake. No answer can be given with supreme confidence, but certain points can be made and a tentative conclusion can be drawn. We can first discard the possibility that Fermat imagined a prime n gave a prime $2^n - 1$. As has already been indicated, he knew that $2^{11} - 1$ was composite. So Fermat knew that he had something to prove, and the only method open to him was to find, or not to find, a prime factor of $2^{37} - 1$. Did he have his short cut by the time of Letter 3? Yes he did, because his opening remark is precisely that he does have a short cut. How then did he come to miss a prime factor of $2^{37} - 1$? One relevant feature may be that

$$2^{37} - 1 = 223 \times 616{,}318{,}177$$

is a product of two prime numbers, so that if Fermat had missed the first prime factor 223, then he could not have found the second because he would necessarily have stopped at $(2^{37} - 1)^{1/2}$. A possible explanation begins to emerge. Fermat takes $2^{37} - 1$ and divides by 149. This is not a factor. He divides by 223 and makes an error. This seems not to be a factor. He divides by 593. This is not a factor. He carries on into the morass getting nowhere. Now the number of primes of the form $74k + 1$ up to $(2^{37} - 1)^{1/2}$ is 887. Fermat may have tried them all, but it seems unlikely. If he received Letter 1 at the beginning of March, and replied in Letter 3 at the beginning of May, then he would have had two months only in which to divide by the 887 primes. And, of course, the primes themselves would have had to be determined in the first place. This would have involved the use of the sieve of Eratosthenes on an array of 5009 numbers. To check the lot, Fermat needed to find, and divide by, an average of 15 primes per day. That is possible, even for Fermat holding down a full time job. But would he have had the stomach for the fight? After a month living off a diet of 15 primes per day, he would have thrown up his hands, and expended his energies trying to find an even shorter cut. But he would have been honest. He would have written to Mersenne, 'I believe that $2^{36}(2^{37} - 1)$ is perfect'; he would not have claimed to have proved it.

So the missing part of Letter 3 contains Fermat's assertion, or his belief, that $n = 37$ is the answer to Frenicle's question. In Letter 4 Frenicle writes to Fermat telling him that he is wrong. If Fermat had tested all 887 primes then he would have known he had made a mistake, and he would have begun again with 149 to check his arithmetic. If he had not tested all the primes, he would have had a choice, to carry on using bigger and bigger primes, or to assume he had made a mistake and start again at the beginning. Metamathematics rather than mathematics should have told him what to do. The premises

(i) Frenicle has found a factor (true),
(ii) Frenicle has no short cut (highly likely),

lead to the conclusion,

(iii) $2^{37} - 1$ has a small prime factor.

Fermat would have started again [3].

However, the embarrassment to Fermat may have been the spur to his revealing the three propositions which made up his short cut. If that is the case, we should be glad that Fermat's arithmetic was not infallible. The three propositions, given in Letter 5, are as follows.

1. If n is not prime then $2^n - 1$ is not prime.
2. When p ($\neq 2$) is prime, $2^p - 2$ is divisible by $2p$.
3. When q ($\neq 2$) is prime, the prime factors of $2^q - 1$ are of the form $2kq + 1$, where k is a positive integer.

Proposition 2 is simply the modern version of Fermat's theorem ($a^{p-1} \equiv 1 \pmod p$) with $a = 2$. Proposition 3 is the use of Fermat's general theorem to find prime factors of $2^q - 1$. Fermat expressed his theorem in the following form.

FERMAT'S THEOREM. If a and p are positive integers, where p is a prime not dividing a, then p divides $a^n - 1$ for some positive n. Let d be the least such n. Then d divides $p - 1$, and the exponents n for which p divides $a^n - 1$ are precisely all multiples of d.

So if p divides $2^q - 1$ then d divides q, and since q is prime, $d = q$. Then q divides $p - 1$ and p and q both being odd, p has the form $2kq + 1$.

4. THE RECONSTRUCTION (PART 2)

The remainder of the correspondence produced only one new idea, but the course of true communication did not run smoothly. Sometime during the summer Fermat wrote his first letter to Frenicle (Letter 6). This letter is now lost, and was in fact 'mislaid' when Fermat wrote Letter 9 on 18th October. Fermat had sent Frenicle the statement of his general theorem in Letter 6, and he repeated it in Letter 9. Meanwhile Fermat had switched his attention from powers with 1 subtracted to powers with 1 added.

In Fermat's second letter (7) to Frenicle (designated thus in Letter 9) he claims to have a method of finding the factors of $2^n + 1$, where n is not a power of 2. His example indicates that he used his main theorem. If p divides $2^n + 1$ then p divides $(2^n + 1)(2^n - 1) = 2^{2n} - 1$, and d, a factor of $2n$, divides $p - 1$.

He ends this letter with his conviction that if n is a power of 2 then $2^n + 1$ is prime. This is the oldest surviving evidence of Fermat's (false) conjecture. Once again he does not claim too much. "I do not have a proof," he says, but "I am almost persuaded." It is a mystery why he was not very easily persuaded to the contrary. He must have examined the first few cases. Indeed, in Letter 7, he seems to be saying that the first six are prime, perhaps even the first seven. His exact (and ambiguous) words are

. . . 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 65,537 4,294,967,297

et le suivant de 20 lettres

18,446,744,073,709,551,617; etc.

The first five are prime, almost by inspection, so he surely must have tested the sixth using his powerful method. A small prime divisor is easily found this way, so the suspicion must arise that his arithmetic was at fault yet again. For suppose p divides $2^{32} + 1$ then p divides $2^{64} - 1$, and $d = 1, 2, 4, 8, 16, 32$ or 64. But if $d \neq 64$ then p divides $2^{32} - 1$ which is impossible. So $d = 64$ and using his theorem Fermat would prove that

$$p = 1 + 64k.$$

So

$$p = 65, 129, 193, 257, 321, 385, 449, 513, 577, 641, \ldots.$$

Omitting the nonprimes

$$p = 193, 257, 449, 577, 641, \ldots.$$

Since $2^{32} + 1 = 641 \times 6{,}700{,}417$, Fermat needed to test five primes only. (And it is perhaps significant that once again if the smaller prime is missed, the factorization cannot be achieved since the larger factor is also prime.)

Frenicle's reply (Letter 8) is lost but we know that one piece of information was not contained within. Frenicle did not point out Fermat's mistake, for Fermat was claiming the existence of the theorem until the end of his days. It would be straining credulity too much to expect Frenicle also to have made a mistake with $2^{32} + 1$, so we must assume that he did not check Fermat's arithmetic. On the other hand since

$$2^{64} + 1 = 274{,}177 \times 67{,}280{,}421{,}310{,}721,$$

where both these factors are prime, no amount of investigation here would have produced an answer. Frenicle must have made some suitable noises in the lost Letter 8, perhaps confirming Fermat's conjecture or verifying his assertions, because Fermat comments on Frenicle's reaction in Letter 9. But these comments show that Frenicle had been none too specific. For Fermat talks of "this fine proposition that I sent you and which you have corroborated," and later "if you have a positive proof, you would oblige me by informing me of it." Clearly, Frenicle did not have a proof, and it is more than likely that he did not spend much time trying to find a counterexample. Fermat seemed to have verified all the easy cases. Why should Frenicle spend a lot of time verifying something much more difficult? The reward for finding a factor would have been very satisfying, but to Frenicle the theorem probably looked right.

Letter 9 continues with the general statement of the Fermat theorem, repeated since Letter 6 did not get through to Frenicle. Fermat then gives the necessary and sufficient condition for a prime p to divide $a^n + 1$ for some n.

FERMAT'S COROLLARY ON POWERS PLUS 1. Let a and p be positive integers where p is a prime not dividing a. Let d be the least positive integer such that p divides $a^d - 1$. Then if d is odd, p does not divide $a^n + 1$ for any n; if d is even, then p divides $a^{d/2} + 1$.

The example he gives is of 23 dividing $2^{11} - 1$, where 11 is the least such positive integer. It therefore follows from the corollary that 23 does not divide $2^n + 1$ for any n. As an example where d is even, we may take $p = 41$ and $a = 3$. Then 41 divides $3^8 - 1$ and by the corollary 41 divides $3^4 + 1$.

Returning to Frenicle's lost Letter 8, it seems he must have made a rash statement concerning the multiples of the exponent in Fermat's third proposition. Fermat had stated that when q is an odd prime, the prime factors of $2^q - 1$ are of the form $2kq + 1$. Could k take any value or could we narrow the search still further? In Letter 9 Fermat asks Frenicle to enlarge on that part of his letter where "there are rules for finding the number of multiples +1 of the exponent."

Frenicle's reply (Letter 10) is lost, but its general tone must have been unsatisfactory for Fermat, because on Christmas Day 1640 he is writing to Mersenne (Letter 11) and including in this letter three questions for Frenicle ("so that he is no longer in any doubt what I am asking him"). The first question again asks why $2^{2^n} + 1$ is prime. The second is a new question but is related to the first. Is it true that $(2a)^{2^n} + 1$ is prime if it is not divisible by one of the numbers $2^{2^m} + 1$? The third question repeats his demand for a method for finding the multiples of the exponent.

5. CONCLUSION

So the year 1640 came to an end. Little had been learnt about perfect numbers although the case $n = 37$ had been dealt with. But number theory had taken a major leap forward, although probably only Fermat realized it at the time. Fermat's theorem is one of the corner stones of modern number theory, and in this year of its 350th anniversary, it is fitting to remember its birth.

NOTES

1. Only one 1640 letter to Fermat survives. This was written by Gilles Personne de Roberval (1602–1675) and is dated 4th August 1640.

2. In a recent article [Rashed 1989] it is claimed that the Arabs had proved this theorem seven centuries before Euler.

3. It is true that Fermat, in his letters, praises the achievements of Frenicle (e.g., "Je ne doute pas que M. Frenicle ne soit allé plus avant . . ." in Letter 5). But it was his habit to write in this way (e.g., ". . . je serai bien aise d'apprendre le sentiment de M. de Roberval," also in Letter 5). This may have been due to his nature, or it may have been Fermat's way of trying to get information out of his correspondents, or indeed it may have been an attempt to confirm that his correspondents had no useful information to impart. In any case, we cannot deduce that Fermat believed Frenicle to be ahead of him in the theory of the divisors of numbers of the form $2^n - 1$. But the question is of no great importance; either at once, or eventually, Fermat found the factor 223.

REFERENCES

Dickson, L. E. 1934. *History of the theory of numbers*. Vol. 1. New York: Stechert.

Euclid. 1908. *The thirteen books of his Elements*. Translated from the text of Heiberg with introduction and commentary by T. L. Heath. Cambridge: Cambridge Univ. Press. Reprinted New York: Dover, 1956.

Fermat, P. 1894. *Oeuvres*. Tome 2. *Correspondance*, P. Tannery & C. Henry, Eds. Paris: Gauthier–Villars.

Fletcher, C. R. 1989. Fermat's theorem. *Historia Mathematica* **16,** 149–153.

Mersenne, M. 1965. *Correspondance*. Tome IX. C. de Waard, Ed. Paris: Editions du Centre National de la Recherche Scientifique.

——— 1967. *Correspondance*. Tome X. C. de Waard, Ed. Paris: Editions du Centre Nationale de la Recherche Scientifique.

Picutti, E. 1989. Pour l'histoire des sept premiers nombres parfaits. *Historia Mathematica* **16,** 123–136.

Rashed, R. 1989. Ibn al-Haytham et les nombres parfaits. *Historia Mathematica* **16,** 343–352.

Weil, A. 1983. *Number theory*. Boston: Birkhäuser.