Fermat's Little Theorem: Proofs That Fermat Might Have Used
Author(s): Bob Burn
Source: *The Mathematical Gazette*, Vol. 86, No. 507 (Nov., 2002), pp. 415-422
Published by: The Mathematical Association
Stable URL: http://www.jstor.org/stable/3621133
Accessed: 24/03/2010 21:19

Fermat's little theorem – proofs that Fermat might have used

BOB BURN

Fermat (1601-1665) is well-known for offering mathematical results without stating their proofs. In Mahoney's fine mathematical biography [1], suggestions are made giving possible lines of reasoning which Fermat may have used, suggestions which are easily recognised by those familiar with number theory. This article offers some conjectured reconstructions of Fermat's reasoning which may be more accessible to a beginner since they are linked to pattern recognition, and capitalise on the special cases with which Fermat illustrated his ideas. Generic examples played an essential part in Fermat's exposition and may well have played a larger part in his proofs than would be respectable in a textbook nowadays.

Mahoney used congruence notation ($a \equiv b$, $(\mathrm{mod}\, n)$ when n is a factor of $a - b$) to describe possible proofs that Fermat may have used. This notation was devised by Gauss 150 years later, and is avoided here. However it seems reasonable to use some algebra since we know that Fermat knew Viète's work well. Our discussion here focuses on three of Fermat's letters – two of which he wrote to Mersenne in April and June 1640, and one which he wrote to Frénicle de Bessy in October 1640. One of the conclusions which the reader may draw from these quotations is that Fermat does not seem to have reported his results in the chronological order of their discovery. His reporting depended on the current subjects of correspondence with Mersenne.

The original form of Fermat's little theorem

In the surviving literature, Fermat stated his 'little' theorem just once. He gave illustrations but no proof. He wrote on 18 October 1640 to Frénicle de Bessy:

> Without exception, every prime number measures [*i.e. divides*] one of the powers – 1 of any progression whatever, and the exponent of the said power is a sub-multiple of the given prime number – 1. Also, after one has found the first power that satisfies the problem, all those of which the exponents are multiples of the exponent of the first will similarly satisfy the problem. This proposition is generally true for all series and for all prime numbers; I would send you a demonstration of it, if I did not fear going on too long. [1, p. 295]

Fermat illustrated this by listing the powers of 3, the second row here. The other rows have been added to show how Fermat hunted for patterns.

n	1	2	3	4	5	6
3^n	3	9	27	81	243	729
$3^n - 1$	2	8	26	80	242	728
odd prime factors			13	5	11	7,13

If we put his proposition to Frénicle into algebraic form, Fermat claimed that

for any prime number p, and positive integer a,

there is a t such that p divides $a^t - 1$;

and that [the smallest] such t is a factor of $p - 1$.

Furthermore, for this smallest t, and any positive integer n, p divides $a^{tn} - 1$.

The exceptional case, when p is a factor of a, is not mentioned.

Fermat illustrated this in the table (taking $a = 3$, $p = 13$, giving the smallest $t = 3$) by claiming that

because $3^3 - 1$ has the least power of 3 giving a factor 13,

$3^{3n} - 1$ will have a factor 13 for all positive integers n.

$3^6 - 1$ is in the table and shows a factor 13, but $3^9 - 1$ and $3^{12} - 1$ will also have a factor 13. Fermat's claim that the least exponent, $t = 3$, is a factor of $13 - 1$ then follows from the unstated claim that there are no other powers of 3, less one, which have a factor 13, together with the conventional little theorem. We will consider a possible proof later on, after constructing some of the equipment that it needs.

The conventional form of Fermat's little theorem that appears in textbooks today is that a prime number p is a factor of $a^{p-1} - 1$ when p is not a factor of a. Fermat claimed more than this, and we will refer to the actual claim he made to Frénicle as the *strong* form of his little theorem.

Fermat and perfect numbers

How then did the idea of Fermat's little theorem arise?

Fermat wrote to Mersenne about mid-June 1640 presenting 'Three propositions I have found on which I hope to erect a great building.' [2, 11.C.4] Fermat was writing about perfect numbers. He knew the classical results on perfect numbers, and, in order to build on them, had investigated the prime factors of numbers which were one less than a power of 2. Fermat's little theorem is a generalisation, to powers of other numbers, of results he obtained for powers of 2.

Fermat's investigations of perfect numbers started from a theorem of Euclid (Euclid IX.36) that if $1 + 2 + 4 + 8 + \dots + 2^n$ is a prime number p, then $2^n p$ is a perfect number (that is, equal to the sum of its proper divisors; $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$ are both perfect numbers). More than one hundred years later, Euler showed (in work only published after his death) that every even perfect number is of this form.

Fermat could sum $1 + 2 + 4 + 8 + \dots + 2^{n-1}$ in an old style:

$$2(1 + 2 + 4 + 8 + \dots + 2^{n-1}) - (1 + 2 + 4 + 8 + \dots + 2^{n-1}) = 2^n - 1.$$

So $1 + 2 + 4 + 8 + \dots + 2^{n-1} = 2^n - 1$.

If $2^n - 1$ is a prime number, then $2^{n-1}(2^n - 1)$ is perfect. This is Euclid's theorem, rewritten in modern notation. [*Proof.* If p is an odd prime number, then the proper factors of $2^{n-1}p$ are $1, 2, 2^2, \dots, 2^{n-1}$, p, $2p$, $\dots$, $2^{n-2}p$. The sum of these proper factors is $2^n - 1 + p(2^{n-1} - 1)$. This sum equals $2^{n-1}p$ if, and only if, $p = 2^n - 1$.]

Using Euclid's theorem to search for perfect numbers depends on finding prime numbers of the form $2^n - 1$.

In his letter to Mersenne, Fermat gave the first two rows of this table.

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$2^n - 1$	1	3	7	15	31	63	127	255	511	1023	2047	4095	8191
		prime	*prime*	fac 3	*prime*	fac 3	*prime*	fac 3	fac 7	fac 3	fac 23	fac 3	*prime*

The numbers in the second row he called *radicals*, and the numbers in the first row, their *exponents*. When a radical is prime it may be used to construct a perfect number by Euclid's theorem.

Fermat's first claim: when n is composite $2^n - 1$ is composite.

After displaying the numbers in this table, Fermat made his first claim.

This done I say that:

> When the exponent of a radical number is compound, its radical is also compound. Thus, because 6 the exponent of 63 is compound I say that 63 is also compound. [2, 11.C.4]

In other words, there are no prime numbers of the form $2^n - 1$ when the exponent n is composite.

Fermat gave no proof, but the old way of summing the terms of a geometric progression shows what is going on.

Suppose that the exponent has a factor 2.

Then the 'radical' $2^{2n} - 1 = 4^n - 1$.

Now $4(1 + 4 + 4^2 + \dots + 4^{n-1}) - (1 + 4 + 4^2 + \dots + 4^{n-1}) = 4^n - 1$.

So $3(1 + 4 + 4^2 + \dots + 4^{n-1}) = 4^n - 1$,

and $4^n - 1$ has a factor 3 (= $4 - 1$) and is composite for $n > 1$.

Suppose that the exponent has a factor 3.

Then the 'radical' $2^{3n} - 1 = 8^n - 1$.

Now $8(1 + 8 + 8^2 + \dots + 8^{n-1}) - (1 + 8 + 8^2 + \dots + 8^{n-1}) = 8^n - 1$.

So $7(1 + 8 + 8^2 + \dots + 8^{n-1}) = 8^n - 1$,

and $8^n - 1$ has a factor 7 (= $8 - 1$) and is composite for $n > 1$.

Clearly the argument may be extended to show that when the exponent has a factor t, $2^t - 1$ is a factor of $2^{tn} - 1$. (*)

We mark this result with an asterisk as it is needed repeatedly later on, together with its generalisation from changing the number 2 to any other positive integer.

Fermat's second claim: numbers of the form $2^p - 2$ have a factor $2p$.

To find prime numbers of the form $2^n - 1$ one need only consider prime numbers n, because of Fermat's first claim. But $2^{11} - 1 = 23 \times 89$, so

$2^p - 1$ does not have to be prime, even when p is prime. So Fermat investigated further, looking just at the prime exponents. This table was not displayed in Fermat's letter to Mersenne, but Fermat's discussion showed he was familiar with its contents.

exponent	2	3	5	7	11	13	17	19	p
radical	3	7	31	127	2047	8191	131071	524287	$2^p - 1$
radical – 1	2	6	30	126	2046	8190	131070	524286	$2^p - 2$
a factor	2	3	5	7	11	13	17	19	p why?

$$\begin{aligned}
2^3 - 2 &= 6 = 2 \times 3 \\
2^5 - 2 &= 20 = 2 \times 3 \times 5 \\
2^7 - 2 &= 126 = 2 \times 3 \times 3 \times 7 \\
2^{11} - 2 &= 2046 = 2 \times 3 \times 11 \times 31 \\
2^{13} - 2 &= 8190 = 2 \times 3 \times 3 \times 5 \times 7 \times 13 \\
2^{17} - 2 &= 131070 = 2 \times 3 \times 5 \times 17 \times 257 \\
2^{19} - 2 &= 524286 = 2 \times 3 \times 3 \times 3 \times 7 \times 19 \times 73
\end{aligned}$$

The matching of the first and fourth rows in the table suggests the next step.

In Fermat's letter to Mersenne, Fermat's second claim was:

> When the exponent is a prime number *[> 2]*, I say that its radical reduced by unity is measured by [i.e. has as a factor] the double of the exponent. Thus because 7 the exponent of 127 is a prime number, I say that 126 is a multiple of 14. [2, 11.C.4]

Algebraically, Fermat here claimed that for a prime number p, $2^p - 2$ has a factor $2p$. The factor 2 is obvious; the factor p is not. The claim that $2^p - 2$ has a factor p is a special case of Fermat's little theorem.

What follows is a collection of ideas, which were available to Fermat and would have been sufficient to prove that $2^p - 2$ has a factor p for any prime number p. The method assumes familiarity with Pascal's triangle. This was only given by Pascal in 1654, but known to some extent for several hundred years before that.

$$\begin{array}{ccccccccccccccc}
&&&&&&&1&&&&&&& \\
&&&&&&1&&1&&&&&& \\
&&&&&1&&2&&1&&&&& \\
&&&&1&&3&&3&&1&&&& \\
&&&1&&4&&6&&4&&1&&& \\
&&1&&5&&10&&10&&5&&1&& \\
&1&&6&&15&&20&&15&&6&&1& \\
1&&7&&21&&35&&35&&21&&7&&1
\end{array}$$

$2^3 = (1+1)^3 = 1+3+3+1$, so $2^3 - 2 = 3 + 3$.
$2^5 = (1+1)^5 = 1+5+10+10+5+1$, so $2^5 - 2 = 5+10+10+5$.
$2^7 = (1+1)^7 = 1+7+21+35+35+21+7+1$, so
$2^7 - 2 = 7+21+35+35+21+7$

Generally,

$$2^p = (1+1)^p = 1 + p(\ldots\ \ldots) + 1.$$

So $2^p - 2$ has a factor p.

(The coefficient of a^{n-r} in the expansion of $(a+1)^n$ (the $r+1$ th term in the $n+1$ th row of Pascal's triangle) is the number of individual terms of the form a^{n-r} in the expansion. Counting them is tantamount to counting the number of ways of choosing $n - r$ as from the n brackets, namely $n(n-1)(n-2)\ldots(n-r+1)/r!$. According to Weil [3, pp. 46-48], Fermat had a good knowledge of binomial coefficients by 1636. When n is a prime number p, and $0 < r < n$, $n(n-1)(n-2)\ldots(n-r+1)/r!$ has a factor p.)

Since p is a factor of $2^p - 2$, p is also a factor of $2^{p-1} - 1$.

Fermat's little theorem (standard form): p is a factor of $a^p - a$.

Before looking at the third claim in Fermat's letter of June 1640 we return to Fermat's letter to Frénicle of 18 October, and possible proofs of the claims that Fermat described.

The binomial coefficients which appear in the expansion of $(1+1)^p$ also appear in the expansion of $(2+1)^p$, so

$3^p = (2+1)^p = 2^p + p(\ldots\ldots) + 1^p = 2^p - 2 + p(\ldots\ldots) + 2 + 1$.
Thus $3^p - 3 = (2^p - 2) + p(\ldots\ldots)$.
Now p divides $2^p - 2$, so p divides $3^p - 3$.
Again, $4^p = (3+1)^p = 3^p + p(\ldots\ldots) + 1^p = 3^p - 3 + p(\ldots\ldots) + 3 + 1$.
Thus $4^p - 4 = (3^p - 3) + p(\ldots\ldots)$.
Now p divides $3^p - 3$, so p divides $4^p - 4$.

Continuing in this way we can establish that the prime p divides $a^p - a$, for any positive integer a, with the proof built up from the bottom. This is one of the standard forms of Fermat's little theorem.

It was not characteristic of the period to provide the inductive step in a general form though it is this step which is implied by 'continuing in this way'. In fact the inductive step comes directly from spotting the pattern in the cases above.

Since $(a+1)^p = a^p + p(\ldots\ldots) + 1^p$,
we get $(a+1)^p - (a+1) = a^p - a + p(\ldots\ldots)$.
So if p is a factor of $a^p - a$, p must be a factor of $(a+1)^p - (a+1)$.

The binomial expansion of $(a+1)^p$ may be used to construct another proof.

Since $(a + 1)^p = a^p + p(......) + 1^p$,

$(a + 1)^p - a^p - 1^p$ has a factor p.

Putting $a = n, n - 1, \ldots, 2, 1$, we get

$(n + 1)^p - n^p - 1$ has a factor p,
$n^p - (n - 1)^p - 1$ has a factor p,
$(n - 1)^p - (n - 2)^p - 1$ has a factor p,
$\ldots\ldots$
$3^p - 2^p - 1$ has a factor p,
$2^p - 1^p - 1$ has a factor p.

If these n numbers, each with a factor p, are added, we get

$$(n + 1)^p - 1^p - n \text{ has a factor } p.$$

So $(n + 1)^p - (n + 1)$ has a factor p.

Euler (in 1735, according to Weil [3, p. 176]), used reasoning of this kind to construct an inductive argument to show p divides $a^p - a$. The induction is implicit in what has been written here. It follows that p is a factor of $a^{p-1} - 1$, provided p is not a factor of a, although Fermat did not mention this exception.

The strong form of Fermat's little theorem

Fermat claimed more. His generic example was that since 13 was a factor of $3^3 - 1$, every number of the form $3^{3n} - 1$ had a factor 13. This followed directly from his first claim (*), putting 3 instead of 2 in the argument, since $3^3 - 1$ is a factor of $3^{3n} - 1$. To use the little theorem to show that 13 – 1 is of the form $3n$, Fermat would have needed to show that for *all* numbers of the form $3^s - 1$ which have a factor 13, s is a multiple of 3. To see how Fermat may have convinced himself of this, we pretend that $3^s - 1$ might have a factor 13 when s is not a multiple of 3. Suppose, for example, that $3^{17} - 1$ has a factor 13. Since we know $3^{15} - 1$ has a factor 13, we can deduce that $[(3^{17} - 1) - (3^{15} - 1)]$ also has a factor 13. But $[(3^{17} - 1) - (3^{15} - 1)] = 3^{15}(3^2 - 1)$ and 13 does not divide either of these factors. So we have made a mistake; our supposition must be false and 13 is *not* a factor of $3^{17} - 1$.

Fermat claimed that if t were the least exponent such that the prime p divided $a^t - 1$, then p divided $a^{tn} - 1$. This follows from the first claim (*) putting a instead of 2 in the argument. Fermat also claimed that t was a factor of $p - 1$. This follows from the little theorem when it is shown that *every* s such that p divides $a^s - 1$ is a multiple of t.

The generic proof given above provides the structure of a general proof by contradiction. If p divides $a^s - 1$ for some positive integer s which is not a multiple of t, then s lies between two consecutive multiples of t, so $tn < s < t(n + 1)$ for some integer n. Now p divides $a^{tn} - 1$ and therefore p also divides $(a^s - 1) - (a^{tn} - 1) = a^{tn}(a^{s-tn} - 1)$.

If p is not a factor of a, p divides $a^{s-tn} - 1$. But $0 < s - tn < t$, and this contradicts the definition of t. So there is no such s. Now since p divides $a^{p-1} - 1$ (Fermat's little theorem), t is a factor of $p - 1$.

It also follows that if p divides $a^q - 1$ for some prime q, then $q = t$. This is exactly what is needed to establish Fermat's third claim.

Fermat's third claim: when q is prime, a prime factor of $2^q - 1$ has the form $2kq + 1$.

We return to Fermat's letter to Mersenne of June 1640. The example $2^{11} - 1 = 2047 = 23 \times 89$ is particularly tantalising. Might there be some structure linking the factors 23 and 89 to the exponent 11?

The classical way to find the factors of a number is to use the idea behind Eratosthenes sieve.

Because $45^2 < 2047 < 46^2$, if 2047 were composite it would have a prime factor less than 45. So to find out whether 2047 is composite the primes between 3 and 43 can be tested as possible factors. This could be a long job. We propose an argument by which Fermat may have shortened the list of primes that needed to be tested.

Suppose p divides $2^{11} - 1$. By the strong form of the little theorem, 11 is a multiple of t where t is the smallest number such that p divides $2^t - 1$. But the only factors of 11 are 1 and 11 itself, so $t = 1$ or 11. $t = 1$ is absurd, so $t = 11$. But t is a factor of $p - 1$, so 11 divides $p - 1$ and $p = 11k + 1$ (§§).

This shows that if there is a $p \leqslant 45$ which divides $2^{11} - 1$, it must be in the list 12, 23, 34, 45; and of these numbers, only 23 is prime. So only one possible prime factor needs to be tested.

There are two points to note.

(i) If k is odd then p is even and so not prime, so k must be even and, putting $2k$ for $k, p = 22k + 1$.

(ii) The four lines of argument leading up to (§§) apply to any prime number p that divides 2047.

$2047/23 = 89$, another prime number of the form $22k + 1$.

The third claim in Fermat's letter to Mersenne was:

> When the exponent is a prime number, I say that its radical is not measured by any prime number except those which exceed by unity either a multiple of the double of the exponent or the double of the exponent. Thus because 11, the exponent of 2047, is a prime number, I say that it cannot be measured except by a number which is greater by unity than a multiple of 22; in fact 2047 is only measured by 23 or 89, from which, if you remove unity, 88 remains, a multiple of 22. [2, 11.C.4]

Algebraically, Fermat claimed here that if a prime p divides $2^q - 1$, where q is also prime, then $p = 2kq + 1$, for some positive integer k.

7 divides $2^3 - 1$ and $7 = 6 + 1$;

31 divides $2^5 - 1$ and $31 = 3 \times 10 + 1$;

127 divides $2^7 - 1$ and $127 = 9 \times 14 + 1$;

$2047 = 23 \times 89$, so 23 divides $2^{11} - 1$ and $23 = 22 + 1$; and 89 divides $2^{11} - 1$ and $89 = 4 \times 22 + 1$;

8191 divides $2^{13} - 1$ and $8191 = 315 \times 26 + 1$;
131071 divides $2^{17} - 1$ and $131071 = 3855 \times 34 + 1$;
524287 divides $2^{19} - 1$ and $524287 = 13797 \times 38 + 1$.

Now we generalise the generic example of factorising $2^{11} - 1$ by expressing the argument algebraically to determine when a prime number p may be a factor of $2^q - 1$ when q is a given prime.

If p is a factor of $2^t - 1$ and t is minimal, then q is a multiple of t, from the strong form of the little theorem. But q is prime, so $t = 1$ or q. Now p does not divide $2^1 - 1$, so $t \neq 1$. Thus $t = q$, and therefore q divides $p - 1$ applying the strong form of the little theorem again.

So $p - 1 = kq$ and $p = kq + 1$.

Now p is odd and q is odd, so k must be even and $p = 2kq + 1$, for some positive integer k.

In fact $2^q - 1$ is prime for $q = 17, 19, 31$ and 61. But, for example, $2^{23} - 1$ has a factor 47 and $2^{29} - 1$ a factor 233.

An application of Fermat's third claim about factors of numbers of the form $2^n - 1$

Fermat had claimed earlier in a letter to Mersenne (20 April 1640) that there was no perfect number with 21 or 22 digits. This related to a much earlier (false) conjecture, going back to Nicomachus (c.100 AD) that each consecutive interval in the series 1,10, 100, 1000, ... contained a perfect number. Fermat's claim meant that there were no numbers n such that $10^{20} < 2^{n-1}(2^n - 1) < 10^{22}$, with $2^n - 1$ being prime. Now $10^{20} < 2^{2n-1} - 2^{n-1} < 10^{22}$ requires $66 \leqslant 2n - 1 \leqslant 73$, or $67 \leqslant 2n \leqslant 74$, or $33 < n \leqslant 37$. 34, 35 and 36 are not prime numbers, so these values for n cannot make $2^n - 1$ prime from Fermat's first claim (*). Thus $n = 37$ is the only possibility that must be tested. Fermat's third claim, above, implied that any prime factor of $2^{37} - 1$ must be of the form $74k + 1$. 75 is not prime. But 149 and 223 are primes. Fermat found that 223 was a factor of $2^{37} - 1$. So his third claim had reduced this huge problem to a still large, but manageable problem. So it seems that Fermat had his three results of June 1640, and the little theorem as well, by April of 1640.

References

1. M. S. Mahoney, *The mathematical career of Pierre de Fermat, 1601 – 1665*, (2nd edn), Princeton University Press (1994).
2. J. Fauvel and J. Gray, *The history of mathematics: a reader*, Macmillan (1987).
3. A. Weil, *Number theory, an approach through history; From Hammurapi to Legendre*, Birkhäuser (1984).

R. P. BURN
Sunnyside, Barrack Road, Exeter EX2 6AB
e-mail: *R.P.Burn@exeter.ac.uk*