Fermat and Prime Number Theorems

JIM ADAMS

It is interesting to reverse engineer the considerations that led Fermat to ask whether all Fermat numbers are prime, which Euler disproved. These are related to cyclotomic equations.

In fact, a result proved in [1], there are generalisations for *any* real numbers, not just for the numbers 2, or just for subtraction or addition by 1, of the relation we give below between generalised Mersenne numbers $M_n = (2^{(2^n)} - 1)$ and Fermat numbers $F_n = (2^{(2^n)} + 1)$.

The first four values for Fermat numbers are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$ and $F_3 = 257$, and we have

$$M_3 = F_3 - 2 = 255$$
$$= 17 \times 5 \times 3$$
$$= F_2 \times F_1 \times F_0.$$

This is a special case of

$$M_n = \Pi(r = 0, n - 1)\, F_r,$$

which as a first stage can be put as

$$(2^{(2^n)} - 1) = (2^{(2^{n-1})} - 1)(2^{(2^{n-1})} + 1),$$

and which can be written inductively as

$$(2^{(2^n)} - 1) = (2 - 1)(2^{(2^{n-1})} + 1)(2^{(2^{n-2})} + 1) \ldots (2^{(2^0)} + 1). \quad \square$$

These ideas led us to investigate the following two simple prime number theorems based on real cyclotomics – equations of type (1) below, which are not usually stated in this generality, e.g. not in the excellent [2] or [3], and are amongst the 70 results described in [1].

Theorem. *Suppose* a, b *and* n *are positive whole numbers*. *Then*

$$a^n - b^n$$

is not prime except for the possibilities $n = 1$, *or* $b = (a - 1)$ *and* n *prime*.

Proof.

(1) $a^n - b^n = (a - b)\{\Sigma(r = 0, n - 1)\, a^{n-r-1}b^r\}$,

so if $a^n - b^n$ is prime, either the first factor $(a - b) = 1$, or the second factor equals 1. But if the second factor equals 1, then $n = 1$, so consider the case $(a - b) = 1$.

Assume n is *not* prime, so $n = km$, say. We prove a contradiction. It is generally true that

$$a^{km} - b^{km} = (a^k)^m - (b^k)^m = (a^k - b^k)\{\Sigma(r = 0, m - 1)\, a^{k(m-r-1)}b^{kr}\}.$$

Now we cannot have $m = 1$, because n factorises, so the assumption leads to

$$a^k - b^k = 1.$$

But if $a > b \geq 1$, then

$$1^k = (a - b)^k < a^{k-1}(a - b) < a^k - b^k.$$

This is the required contradiction, that $a^k - b^k \neq 1$, so n is prime. $\square$

Examples. If $n = 3$, $a = 10$ and $b = 9$, then $(a - b) = 1$ and in this particular instance

$$10^3 - 9^3 = 271$$

is prime, so this is a possibility. On the other hand

$$7^5 - 6^5 = 9031 = 11 \times 821,$$

so not all such numbers with n prime and (a – b) = 1 are prime. We have indicated that for n = 4, which is not prime, and for a = 10, b = 9, so (a – b) = 1, that $a^n – b^n$ will factorise, and we verify

$$10^4 – 9^4 = 3439 = 19 \times 181$$

is composite. We also know that the case n = 3, a = 10 and b = 7 will factorise, since (a – b) ≠ 1, and

$$10^3 – 7^3 = 657 = 3 \times 3 \times 73.$$

Theorem. *Let* a, b *and* n *be positive whole numbers, as before. No numbers of the form*

$$a^n + b^n$$

are prime except for the possibilities a = b = 1 *or* n = 1, *or* n *a power of* 2, *so all the latter such numbers can be represented as sums of squares.*

Proof. We assume to begin with that n is an *odd* whole number – we will prove a contradiction. We can easily see, if in formula (1) we put (-b) instead of (b), *provided* n *is odd*

(2) $a^n + b^n = (a + b)\{\Sigma(r = 0, n – 1)a^{n-r-1}(-b)^r\}$.

Now if $a^n + b^n$ is prime, either (a + b) = 1, which is impossible, or the expression in curly brackets is 1. So

$$a^n + b^n = (a + b),$$

which is clearly the case only for a = b = 1 or n = 1.

So in all other circumstances, n is not odd. But if n is even and not a power of 2, there exists an odd factor m ≠ 1 so that n = jm, and

$$a^n + b^n = (a^j)^m + (b^j)^m$$

is prime, which we have proved is not the case.

So a = b = 1 or n = 1, or n is a power of 2, call it 2z, so all the latter such primes can be written as

$$(a^z)^2 + (b^z)^2. \ \square$$

Examples. If we put a = 10, b = 3 and choose an odd n = 5, we get the factorisation

$$10^5 + 3^5 = 100{,}243 = 13 \times 7711.$$

For n a power of 2, say n = 2 or 4, we find there are some sums of nth powers that are primes, e.g.

$$4^2 + 1 = 2^4 + 1 = 17,$$

and others that are not, e.g.

$$6^4 + 5^4 = 1921 = 17 \times 113.$$

But for n = 6 (not a power of 2), the result must factorise, and indeed

$$4^6 + 3^6 = 4825 = 5 \times 5 \times 193.$$

We are now in a position to see how relevant our discussion of Fermat numbers $F_n = (2^{(2^n)} + 1)$ was. If we choose a = 2 and b = 1, then the F_n are the only sums of powers of this type which can be prime.

Acknowledgements. I would like to thank Doly García for discussions and acknowledge the help of the anonymous referees.

References.

[1] Jim Adams, *Exponential Factorisation Theorems,* http://www.jimhadams.com/math/ExponentialFactorisationTheorems.pdf, (15th August 2008).
[2] John Conway and Richard K. Guy, *The Book of Numbers*, Copernicus Books, (2006).
[3] Paulo Ribenboim, *The Book of Prime Number Records*, Springer, (1989).

 14 Sept. 2008