Could there exist a sixth Fermat prime? I believe it is *not impossible.*

For my wife, Mary, and in memory of my parents,
Annie Sandes (1900-67) and Sean Cosgrave (1906-95)

John Cosgrave, Mathematics Department, St. Patrick's College, Drumcondra, Dublin 9, IRELAND.

0. SYNOPSIS. I present some work which should cause doubt concerning the assertion that there are no Fermat primes after the first five. An equivalent restatement of that assertion is: *no Fermat prime may follow a Fermat composite*, meaning

if F_n *is composite then* F_{n+1} *is also composite*.

To cause this doubt to be felt, I propose a new definition of *generalised Fermat number*. This definition incorporates the classic Fermat numbers in a satisfying manner, and in the process establishes an integral connection with the Mersenne numbers. Indeed, the Mersenne numbers will be seen to form the basis of the entire collection of proposed generalised Fermat numbers.

The proposed numbers fall into an infinite number of ranks, of which the classic Fermat numbers form the first. I identify one of those ranks−the 17th−whose first term $(M_{59} = 2^{59} - 1)$ is composite[1], but whose second term, a 1031-digit number, is prime. [Rather, it is almost certainly prime, but, even if it isn't, the spirit of the title of my paper will still stand. **Note to Editor/Referees**. With the permission of the Editor I will submit a request to the Number Theory List (Victor Miller, Univ. of North Dakota) about this number, so that *if* this paper is accepted by the *Monthly*, then that point may be tidied up.] The implication for *all* the ranks, and in particular for the Fermat numbers, is immediate.

I also pose some questions, and propose a number of computations, which may be of interest.

Readers−like myself−with an interest in undergraduate teaching may wish to see *how* I came to formulate my proposed definition, and so I include some detail about that.

1. INTRODUCTION. It is a sobering and humbling thought that we do not know the answer to the question: for which natural numbers m is $2^m + 1$ prime? According to Weil [**19**, p. 58] (see also Mahoney [**20**], p. 301]), Fermat first communicated his thoughts on this question in a letter to Frenicle in August 1640, followed by another[2] to Frenicle, dated Thursday, 18th October 1640.

[1] There is a connection−which will be clear later−between the '17' and '59'; 59 is the 17th prime.
[2] The texts of these letters (in French) have been made available by Antreas P. Hatzipolakis at http://users.hol.gr/~xpolakis/fermat/fac.html

Checking $2^m + 1$ for $m = 1, 2, 3, 4, 5, 6, 7, \ldots$, one finds it is prime for $m = 1, 2, 4, 8, \ldots$,
and immediately wonders–as all my students do, every year–if there is a 'pattern':

$$\text{Is } 2^m + 1 \text{ prime for } \textit{all } m = 1, 2, 4, 8, 16, 32, \ldots, 2^n, \ldots ?$$

An entirely elementary argument shows that if $2^m + 1$ is prime then m is power of 2:

Standard, simple result 1.[3] Let x and m be natural numbers such that $x^m + 1$ is prime, then $m = 2^n$ for some $n = 0, 1, 2, 3, \ldots$.

Standard proof: Suppose $m > 1$, and has an odd prime factor p. Then $m = m'\,p$ $(m' \in \mathbf{N})$ and so $x^m + 1 = x^{m'p} + 1 = X^p + 1 = (X+1)(X^{p-1} - X^{p-2} + \ldots + X^2 - X + 1)$, which, for $x > 1$, is the product of two natural numbers, each greater than 1, and so is composite. It follows that $m = 2^n$, some $n \in \mathbf{N}$ ($n = 0$ corresponds to $m = 1$).

The ***Fermat numbers*** are the $\{F_n\}$, with $F_n = 2^{2^n} + 1$ and $n = 0, 1, 2, 3, 4, 5, \ldots$.
They grow is size very rapidly. The first five are 3, 5, 17, 257 and 65537, and F_{10} is
1797693134862315907729305190789024733617976978942306572734300811577326758055009631327084773224075360211201138798713933576587897688144166224928474306394741243777678934248654852763022196012460941194530829520850057688381506823424628814739131105408272371633505106845862982399472459384797163048353563296242241372 17

As is well known–see *e.g.* Dickson [**1**, p. 375], Edwards[4] [**2**, p. 23-24], Weil [**19**, p. 58] or Mahoney [**20**, p.301]–the $\{F_n\}$ were believed by Fermat to be prime *without exception* (see also Guy [**3**], Klee and Wagon [**4**], Riesel [**5**], Cohen [**6**], BLSTW [**7**], Crandall [**8**]).

I quote from Fermat's letter to Frenicle of August 1640 [**20**, p.301]

> But here is what I admire most of all: it is that I am just about convinced that all progressive numbers augmented by unity, of which the exponents are numbers of
> the double progression, are prime numbers, such as
>
> 3, 5, 17, 65537, 4 294 967 297
>
> and the following of twenty digits

[3] The reader might like to prove the later, relevant result: if x and m are natural numbers such that $x^{2m} + x^m + 1$ is prime, then $m = 3^n$ for some $n = 0, 1, 2, 3, \ldots$.

[4] Letters from Fermat to Carcavi (one) and Frenicle (two)–referred to in Weil, Dickson, Edwards and Mahoney–concerning his views on his primes are available (in French) at
`http://users.hol.gr/~xpolakis/fermat/fac.html`

18 446 744 073 709 551 617, etc.

I do not have an exact proof of it, but I have excluded such a large quantity of divisors by infallible demonstrations, and my thoughts rest on such clear insights, that I can hardly be mistaken.

Fermat, however, erred.[5] In 1732 Euler [**1**, p. 375] found that

$$F_5 = 2^{32} + 1 = 4{,}294{,}967{,}297 = 641 \times 6{,}700{,}417,$$

and in 1880, Landry (at the ripe young age of 82!) [**1**, p. 377] announced–without giving any details–that

$$F_6 = 2^{64} + 1 = 18{,}446{,}744{,}073{,}709{,}551{,}617 = 274{,}177 \times 67{,}280{,}421{,}310{,}721.$$

(In a fascinating paper [**9**], H. C. Williams presents 'a likely reconstruction of Landry's technique.')

Much computational work has been done, and F_n is now known to be composite for $5 \le n \le 23$, the status of F_{24} is unknown, and F_n is known to be composite for quite a few values of n greater than 24. For the most up to date information one should consult Chris Caldwell's remarkable Web site [**10**].

So little–with proof–is known about Fermat numbers. There is the well known heuristic argument[6] in Hardy and Wright [**11**, p. 15] that there are only a finite number of prime Fermat numbers[7], but no one has been able to prove a result that says something like '*there is a constant, c, such that* F_n *is composite for all* $n \ge c$.' The only partial result I know of is[8] Exercise 7 [**6**, p. 435]: *Show that there exists infinitely many n for which at least one of* $2^{2^n} + 1$ *or* $6^{2^n} + 1$ *is composite*.

Thus no one has even proved that infinitely many Fermat numbers are composite, and it is even possible–though utterly unlikely!–that they are all eventually prime.

2. WHY DIDN'T FERMAT FIND THE EULER COUNTEREXAMPLE? Weil makes the observation [**19**, p. 58] that it is difficult to understand why Fermat did not do so. Fermat was aware that '*any prime divisor of* $F_5 = 2^{32} + 1$ *is of the form* $64n + 1$' which quickly leads to the discovery–and this is how Euler did it in the following century–of the factor 641, namely $10 \times 64 + 1$. Weil remarks [**19**, p. 58]

One may imagine that, when he first conceived the conjecture, he was so carried

[5] I like to tell my students that they are in good company.
[6] Of which Guy [**3**, p. 7] remarks, "Selfridge would like to see this [heuristic argument] strengthened to support the conjecture that *all the rest are composite* [my (J.C.) emphasis]."
[7] This argument is also available in a simplified form in Chris Caldwell's Web site at `http://www.utm.edu/research/primes/glossary/Heuristic.html`
[8] 'due to H. W. Lenstra.'

> away by his enthusiasm that he made a numerical error, and then never checked his calculation again … ,

and Weil further remarks

> … as to $2^{64}+1$, it has the prime factor 247177, but this was undoubtedly beyond Fermat's range, and even beyond Frenicle's, though the latter was the more stubborn calculator of the two.

3. SOME COMMENTS OF BOMBIER1 (1974) ON THE FERMAT NUMBERS. In May 1974 the AMS sponsored a special Symposium on the mathematical consequences of the Hilbert problems, and the Proceedings were published by the AMS [**12**]. In his Introduction [**12**, p. vii-viii], F. E. Browder remarked that

> an additional unusual feature of the present volume is an article entitled *Problems of present day mathematics* … . The development of this material was initiated by Jean Dieudonné through correspondence with a number of mathematicians throughout the world. The resulting problems … appear in the form in which they were suggested by the mathematicians whose names are attached to them.

I quote part of the contribution of E. Bombieri [**12**, p. 36-37]:

> Decidability of classical problems. There are many old problems in arithmetic whose interest is practically nil[9], e.g. the existence of odd perfect numbers, problems about the iteration of numerical functions, the existence of infinitely many Fermat primes $2^{2^n}+1$, etc. Some of these questions may well be undecidable in arithmetic; the construction of arithmetical models in which questions of this type have different answers would be of great importance.

In this paper I am not proposing an alternative arithmetical model with its own undefined terms, axioms, etc. in which addition, multiplication and exponentiation can be defined, leading to some sort of resolution of the corresponding Fermat numbers problem. Rather I am staying with the standard model for the natural numbers, and exhibit a computation which *could* lead to a new, partial insight into the problem of the Fermat prime numbers. I am *not* claiming that there is a sixth Fermat prime−how could I? Rather I make−I believe−the reasonable point that it is *not impossible* for there to be a sixth Fermat prime.

4. FERMAT'S 'LITTLE' THEOREM, PRIMALITY TESTING AND PSEUDOPRIMES. All modern studies of primality testing begin with Fermat's 'little'
theorem: if p is prime, and a is any integer with $a \not\equiv 0 (\mathrm{mod}\ p)$, then $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

[9] Bombieri is not suggesting that these problems are not of interest, rather he is of the (eminently reasonable!) view that there would appear to be no hope of solving any of them.

For example, if p_1 is the 101-digit prime $10^{100}+987{,}654{,}649$ (found by applying **Maple**'s **nextprime** command to $10^{100}+987{,}654{,}321$) then $2^{p_1-1} \pmod{p_1}$ evaluates to '1', as may be verified using **Maple**'s command[10] **2&^(p[1]-1) mod p[1]**.
If, however, n is (say) the 221-digit number
1000000…09876546490…012345697300
0…0121932853334917477, then the computation of $2^{n-1} \pmod{n}$ – what is called subjecting n to Fermat's base 2 test – would produce an output which was not '1,' proving that n was not a prime. One says n has '*failed Fermat's test to the base 2*,' and so is composite.

There, in fact, I constructed n to be the product of the above 101-digit prime p_1, and the 121-digit prime $10^{120}+123{,}456{,}973$.

If, however, n is 1195068768795265792518361315725116351898245581 [**6**, p. 415] then not only does the computation of $2^{n-1} \pmod{n}$ produce an output of '1,' but the same occurs from the computation of $a^{n-1} \pmod{n}$ for $3 \le a \le 36$, and it is only at $a = 37$ that the latter n would be revealed to be composite using Fermat's test. That n is – in modern parlance – a *pseudoprime to the base 2* (and is also a pseudoprime for every base up to 36). In fact [**6**, p. 415] the latter n is a *strong pseudoprime* to bases 2, 3, 5, … , 31, and is the product of two primes: 24444516448431392447461 and 48889032896862784894921, which, you will notice, are related.

The above computations bring to mind the so-called 'Chinese Conjecture,' which stated – in modern parlance – that n is an odd prime if and only if $2^{n-1} \equiv 1 \pmod{n}$ [**14**, p. 109]. (See also [**15**, p. 3]).

5. A *SUGGESTED* REASON FOR FERMAT'S BELIEF THAT ALL THE $\{F_n\}$ WERE PRIME: It has been suggested ([**14**[11], p. 109], and [**15**, p. 6]) that Fermat believed the $\{F_n\}$ to be prime because each of them *passes Fermat's test to the base 2*. That is, we have

$$2^{F_n-1} \equiv 1 \pmod{F_n} \ (n \ge 0) \qquad (1)$$

How can one show that (1) is true? It is easy to do so, and can be shown to follow from a well known[12] functional equation connecting the F-values:

$$F_0 F_1 F_2 \ldots F_n = F_{n+1} - 2 \ (n \ge 0) \qquad (2)$$

---

[10] The '**&**' – together with '^' – invokes the square and multiply method for modular exponentiation.
[11] Stark attributes the suggestion to 'the Polish astronomer Banachiewicz,' and remarks that it is expounded in a paper of W. Sierpinski's [**16**].
[12] I don't know who first made this elementary observation (Fermat himself?), but I recall making it myself while a student in London in the mid 60's: waiting for a bus, a # 255 passed by, and factoring 255 produced $3 \times 5 \times 17$ – the product of the first three Fermat numbers, and the 255 was just 2 short of the fourth Fermat number 257!! A fluke or not? Since $3 \times 5 = 15$ – just 2 short of 17 (and 3 itself was just 2 short of 5) then it clearly wasn't, and once (2) was *suspected* a proof was *immediate*.

I would prefer–for later purposes–to rewrite (2) as

$$F_0F_1F_2\ \ldots F_n = 2^{2^{n+1}} + 1 - 2 = 2^{2^{n+1}} - 1\ (n \geq 0) \tag{3}$$

Proof of (3)*:*

$$\begin{aligned} 2^{2^{n+1}} - 1 &= (2^{2^n} - 1)(2^{2^n} + 1) = (2^{2^n} - 1)F_n \\ &= (2^{2^{n-1}} - 1)(2^{2^{n-1}} + 1)F_n = (2^{2^{n-1}} - 1)F_{n-1}F_n \\ &= \ldots = F_0F_1 \ldots F_{n-1}F_n. \end{aligned}$$

Proof of (1)*:* From (3) we have

$$2^{2^{n+1}} \equiv 1 (\text{mod } F_n), \tag{4}$$

For $n \geq 0$ we have $n+1 \leq 2^n$, $2^{n+1} \mid 2^{2^n}$, and so $2^{2^n} = m_n \times 2^{n+1}$, where m_n is a positive integer, which–for later reference–I would like to call the raising power.

Then, raising both sides of (4) to the power m_n gives

$$\left(2^{2^{n+1}}\right)^{m_n} \equiv 1^{m_n} \equiv 1 (\text{mod } F_n),\ 2^{m_n \times 2^{n+1}} \equiv 1 (\text{mod } F_n),\ 2^{2^{2^n}} \equiv 1 (\text{mod } F_n),$$

and so[13] $2^{F_n - 1} \equiv 1 (\text{mod } F_n)$, namely (1).

In a nutshell then, F_n is either prime or a pseudoprime to the base 2.

Although I would have some difficulty in accepting the validity of this proposed theory, nevertheless I feel that the passing of the Fermat base 2 test is an *integral* part of the *personality* of the Fermat numbers: one of the first things that one does in testing a large number to see if it is prime or composite[14] is to subject it to Fermat's base 2 test. If the number fails that test, then one immediately knows it is composite. If it passes that test then one still doesn't know if it is prime, and one then tries a base 3 Fermat test, and … . Since all Fermat numbers pass the base 2 test it means that each of them is *at least* masquerading as a prime.

6. GENERALISED FERMAT NUMBERS, AND A FIRST LOOK AT MY PROPOSED *ALTERNATIVE* DEFINITION. Two versions of 'generalized Fermat numbers' are currently used, though one is simply a special case of the other. The

---

[13] A simpler proof–that doesn't appear to have been noted–is to note that $2^{2^n} \equiv -1 (\text{mod } F_n)$, and raise both sides to the power $2^{2^n - n}$, producing $2^{2^{2^n}} \equiv 1 (\text{mod } F_n)$, namely $2^{F_n - 1} \equiv 1 (\text{mod } F_n)$.

[14] Having already performed–perhaps–a gcd calculation to determine if the tested number has a small prime factor

numbers $G_n(a, b) = a^{2^n} + b^{2^n}$ –where a, b are natural numbers with $\gcd(a, b) = 1$ and have opposite parity–have been called[15] the *generalised Fermat numbers* [**5**, p. 102] on the grounds that they share certain properties of the regular Fermat numbers. Specifically they have the following properties (the first two are pointed out in Riesel):

property 1. Every odd prime divisor p of $a^{2^n} + b^{2^n}$ satisfies $p \equiv 1 (\mathrm{mod}\, 2^{n+1})$.
Indeed that is true even if the a and b have the same parity.

property 2. If $b = 1$ there are Pépin-type primality tests[16] for $G_n(a, 1)$.

property 3. They satisfy the same sort[17] of functional equation as (3) above, namely

$$G_0(a, b) \times G_1(a, b) \times \ldots \times G_n(a, b) = a^{2^{n+1}} - b^{2^{n+1}} \qquad (5)$$

However these numbers *singularly lack* what I have already suggested should be considered a *distinctive property* of the regular Fermat numbers: they fail Fermat's test on the very first non-trivial base, namely $a = 2$. Indeed, not only do they *fail* on the first Fermat hurdle–and thus are immediately revealed as being composite–but matters are *even worse*:

- $G_3(3, 2) = 3^{2^3} + 2^{2^3} = 6{,}817 = 17 \times 401$, passes Fermat's test to least base 20
- $G_4(3, 2) = 3^{2^4} + 2^{2^4} = 43{,}112{,}257 = 3{,}401 \times 14{,}177$, passes Fermat's test to least base 11,027
- $G_3(6, 1) = 6^{2^3} + 1 = 1679617 = 17 \times 98{,}801$, passes Fermat's test to least base 6
- $G_2(10, 1) = 10^{2^2} + 1 = 10{,}001 = 73 \times 137$, passes Fermat's test to least base 10

and finally–for anyone who has jumped to a too hasty response to the '6' and '10' in the last two examples–

- $G_1(18, 1) = 18^{2^1} + 1 = 325 = 5^2 \times 13$, passes Fermat's test to least base 7

Primes $GF(n, b)$ of the form $b^{2^n} + 1$ are also considered to be generalised Fermat primes, and a huge amount of computational material concerning them is available on the Web. At the time of writing, the record largest generalized Fermat

[15] Who first did so?

[16] Pépin's test (1877): F_n is prime (for $n \geq 1$) if and only if $3^{\frac{F_n - 1}{2}} \equiv -1 (\mathrm{mod}\, F_n)$.

[17] (3) is (5) with $a = 2$ and $b = 1$.

prime–announced by Yves Gallot on 12th Feb. '99–has 36,725 digits, and is $30{,}406^{2^{13}}+1$.

For the numbers I now propose[18] to be considered as *generalised Fermat numbers*, this failure does *not* occur, and, in fact, forms the basis for proving that–like the classic Fermat numbers themselves–they pass Fermat's test to the base 2.

Proposed *alternative* definition. I propose that the Fermat numbers be regarded as the first rank in the following infinite hierarchy of numbers:

rank 1 The classic Fermat numbers: 3, 5, 17, 257, 65537, 4294967297, … ,
where the n^{th} is given by $2^{2^n}+1\,(n\geq 0)$

rank 2 7, 73, 262657, 18014398643699713,
58460065493236116728147417487167713078820795842 57, … ,
where the n^{th} is given by $2^{2\times 3^n}+2^{3^n}+1\,(n\geq 0)$

rank 3 31, 1082401, 1267650638007162390353805312001,
32733906078961418700131896968275991522935990893953977566947738682917267921195301720402309834027339643468148580227654392909014964460069404903315865600001, … ,
where the n^{th} is given by $2^{4\times 5^n}+2^{3\times 5^n}+2^{2\times 5^n}+2^{5^n}+1\,(n\geq 0)$

and, in general

rank r The n^{th} is given by $2^{(p-1)\times p^n}+2^{(p-2)\times p^n}+\ldots+2^{2\times p^n}+2^{p^n}+1\,(n\geq 0)$,
where $\boldsymbol{p}$ is r^{th} the prime

Notation and nomenclature. I adopt the following notation:

$$F_{n,r}=2^{(p-1)\times p^n}+2^{(p-2)\times p^n}+\ldots+2^{2\times p^n}+2^{p^n}+1\,(n\geq 0,\ r\geq 1),$$

and refer to $F_{n,r}$ as being the n^{th} (generalised) Fermat number of the r^{th} rank. I will say that $F_{n,r}$ is at the n^{th} level, and of the r^{th} rank.

The convention with respect to the Fermat numbers is to refer–for example–to F_8 as being the 8th Fermat number, although it is, in fact, the 9th. I will follow a similar convention here. Thus, for example,

- $F_{0,3}=2^{4\times 5^0}+2^{3\times 5^0}+2^{2\times 5^0}+2^{5^0}+1=31$, is the 0th (generalised) Fermat number of the 3rd rank

[18] I will show later *how* I came upon these numbers.

- $F_{1,3} = 2^{4\times 5^1} + 2^{3\times 5^1} + 2^{2\times 5^1} + 2^{5^1} + 1 = 1{,}082{,}401$, is the 1st (generalised) Fermat of the 3rd rank

Note. The proposed, generalised Fermat numbers at the 0th level, of the 1st, 2nd, 3rd, …
ranks are $3, 7, 31, 127, \ldots$ – the Mersenne numbers $\{M_p\}$, namely $\{2^p - 1\}$, for prime p (the very numbers whose investigation by Fermat led him to the Fermat numbers):

$$F_{0,r} = 2^{(p-1)\times \boldsymbol{p}^0} + \ldots + 2^{2\times \boldsymbol{p}^0} + 2^{\boldsymbol{p}^0} + 1 = 2^{p-1} + 2^{p-2} + \ldots + 2 + 1 = 2^p - 1$$

One might like to visualise the $\{F_{n,r}\}$ as forming a doubly infinite square matrix, in which the classic Fermat numbers form the left vertical side, and the Mersenne numbers form the bottom horizontal side. The corner site is occupied by the number '3', giving – I feel – a satisfying accounting for the quirk that '3' is both the first Fermat, and the first Mersenne number. Also I would like to suggest that one think of the numbers at level 1 as being – as it were – the first cousins of the Mersenne numbers; one of those first cousins – $F_{1,17}$, the one arising from the 17th Mersenne number, M_{59} – will have a big role to play later.

⋮	⋮	⋮	⋮	⋮	⋮
level 3	$F_3 = F_{3,1} = 257$	$F_{3,2}$	$F_{3,3}$	$F_{3,4}$	
level 2	$F_2 = F_{2,1} = 17$	$F_{2,2}$	$F_{2,3}$	$F_{2,4}$	
level 1	$F_1 = F_{1,1} = 5$	$F_{1,2} = 73$	$F_{1,3}$	$F_{1,4}$	
level 0	$F_0 = F_{0,1} = 3$	$F_{0,2} = 7$	$F_{0,3} = 31$	$F_{0,4} = 127$	
	rank 1	rank 2	rank 3	rank 4	**…**

Not surprisingly, these numbers grow *extraordinarily quickly* in the vertical direction[19]:

$F_5 = F_{\mathbf{5},1} = 2^{2^5} + 1 = 4{,}294{,}967{,}297$ has 10 digits,
$F_{\mathbf{5},2}$ has 147 digits,
$F_{\mathbf{5},3}$ has 3,763 digits,
$F_{\mathbf{5},4}$ has 30,357 digits,
$F_{\mathbf{5},5}$ has 484,812 digits.

The mental picture that one should entertain for these numbers is that each is of the form $x^{p-1} + x^{p-2} + \ldots + x + 1$, and the number following at the next higher level is $(x^{p-1})^p + (x^{p-2})^p + \ldots + (x)^p + 1$. In particular, the 'first cousin' of the Mersenne number $M_p = 2^p - 1 = 2^{p-1} + 2^{p-2} + \ldots + 2 + 1$ is $2^{(p-1)p} + 2^{(p-2)p} + \ldots + 2^p + 1$.

Claims[20].

[19] I used **Maple** for these calculations.

Claim 1. Let x and m be natural numbers such that $x^{(p-1)m} + x^{(p-2)m} + \ldots + x^m + 1$ is prime, then $m = p^n$ for some $n = 0, 1, 2, 3, \ldots$.

Claim 2. The $\{F_{n,r}\}$ are pairwise relatively prime *within* a rank; that is, for given r, and $n \neq m$, we have $\gcd(F_{n,r}, F_{m,r}) = 1$. Indeed they are pairwise relatively prime *across* ranks; that is $\gcd(F_{n,i}, F_{m,j}) = 1$ for all n and m, and $i \neq j$.

Claim 3. For fixed r the $\{F_{n,r}\}$ satisfy a functional equation identical to (5), and every $F_{n,r}$ passes Fermat's test to the base 2. (It is well known that all Mersenne numbers pass Fermat's test to the base 2.)

The elementary claim 1 is the natural analogue of the earlier, standard, simple result that if x and m are natural numbers such that $x^m + 1$ is prime, then $m = 2^n$ for some $n = 0, 1, 2, 3, \ldots$. That shows that the only possible primes of the form $2^m + 1$ are the Fermat primes. Claim 1 merely points out that a similar result is also true with respect to the proposed generalised Fermat numbers:

- if x and m are natural numbers such that $x^{2m} + x^m + 1$ is prime, then $m = 3^n$ for some $n = 0, 1, 2, 3, \ldots$. In particular, the only primes of the form $2^{2m} + 2^m + 1$ are of the form $2^{2\times 3^n} + 2^{3^n} + 1$, namely the generalised Fermat numbers of the 2nd rank.

- and in general, if x and m are natural numbers, and p a prime (the r^{th} one) such that $x^{(p-1)m} + x^{(p-2)m} + \ldots + x^m + 1$, is prime, then $m = p^n$ for some $n = 0, 1, 2, 3, \ldots$. In particular, the only primes of the form $2^{(p-1)m} + 2^{(p-2)m} + \ldots + 2^m + 1$, are of the form $2^{(p-1)\times p^n} + 2^{(p-2)\times p^n} + \ldots + 2^{2\times p^n} + 2^{p^n} + 1$, namely the generalised Fermat numbers of the r^{th} rank.

The simple, principal idea of the proof can be conveyed by a single example. Reflecting on the earlier, standard result for $x^m + 1$ one sees that the key idea was to argue that m could not be divisible by any odd prime (i.e., any prime but 2). Now turning ones attention to (e.g.) $x^{2m} + x^m + 1$, the argument one should make is that m cannot be divisible by any prime but 3. Suppose, e.g., that m had 5 as a factor, then $m = 5m'$ and

$$x^{2m} + x^m + 1 = x^{10m'} + x^{5m'} + 1 = X^{10} + X^5 + 1$$
$$= (X^2 + X + 1)(X^8 - X^7 + X^6 - X^5 + X^4 - X^3 + X^2 - X + 1),$$

---

[20] With proofs later. My wish is to first show *how* these numbers emerged in an entirely unforeseen way from one of my undergraduate teaching preparations.

which, if $x > 1,$ is the product of two natural numbers, and so is composite. It should be clear not only how one may continue the proof here, but also in the general case. Simply use the fact that if p and q are *different* primes then $(X^{pq} - 1)$ factors in two entirely different ways

$$\begin{aligned} & X^{pq} - 1 \\ &= (X^p - 1)(X^{(q-1)p} + X^{(q-2)p} + \ldots + X^p + 1) \\ &= (X^q - 1)(X^{(p-1)q} + X^{(p-2)q} + \ldots + X^q + 1), \end{aligned}$$

and use that to give a factorisation of $(x^{(p-1)m} + x^{(p-2)m} + \ldots + x^m + 1)$ when m is divisible by a prime $q \neq p$. There is quite a bit here for students to experiment with, using a CAS like **Maple**.

Claim 2 has no real bearing on the main thrust of my paper, and I only include it because of the off-quoted property of the Fermat numbers, that they are pairwise relatively prime. Claim 2, however, establishes that these generalised Fermat numbers are *genuinely different* from each other: any one of them that is composite is so for some genuine reason, and not because it is divisible by, or shares a proper factor with one of the others in the same rank, or is divisible by or shares a proper factor with one of the others of a different rank.

I will prove claim 2 now, and later prove claim 3 in its natural place.

Proof of claim 2: Suppose $\gcd(F_{n,r}, F_{m,r}) = d > 1$ for some n, m and r, with (say $n < m$). Then some prime p' divides d. Also, since $n < m,$ then $n + 1 \leq m,$ and so we have

$$(2^{p^{n+1}} - 1) \Big| (2^{p^m} - 1) \qquad \text{(a)}$$

Now from $F_{n,r} = 2^{(p-1)\times p^n} + 2^{(p-2)\times p^n} + \ldots + 2^{2\times p^n} + 2^{p^n} + 1 = \dfrac{2^{p^{n+1}} - 1}{2^{p^n} - 1}$

we obtain $p' \Big| (2^{p^{n+1}} - 1),$ and from (a) that $p' \Big| (2^{p^m} - 1),$ and then from

$F_{m,r} = 2^{(p-1)\times p^m} + 2^{(p-2)\times p^m} + \ldots + 2^{2\times p^m} + 2^{p^m} + 1 = \dfrac{2^{p^{m+1}} - 1}{2^{p^m} - 1}$ we obtain

$$\gcd(2^{p^m} - 1, 2^{(p-1)\times p^m} + 2^{(p-2)\times p^m} + \ldots + 2^{2\times p^m} + 2^{p^m} + 1) \geq p' \qquad \text{(b)}$$

However, it is well known (see almost any text on Number Theory) that if p is prime and x is any integer, then $\gcd(x - 1, x^{p-1} + x^{p-2} + \ldots + x + 1) = 1$ or $p,$ and it follows from (b) that $p' = p,$ and thus $2^{p^m} \equiv 1 (\text{mod } p)$. That, however, is impossible, since, by Fermat's 'little' theorem, we have $2^p \equiv 2 (\text{mod } p),$ and repeated powering of both

sides to the power of p produces $2^{p^m} \equiv 2^{p^{m-1}} \equiv 2^{p^{m-2}} \equiv \ldots \equiv 2^p \equiv 2 \not\equiv 1 (\mathrm{mod}\ p)$. Thus the $\{F_{n,r}\}$ are pairwise relatively prime *within* a rank.

Now, suppose $\gcd(F_{n,r}, F_{n',r'}) = D > 1$ for some n, r, n' and r' with $r \neq r'$, and corresponding *different* primes be p and p'. Then some prime q divides D.

From $F_{n,r} = 2^{(p-1)\times p^n} + 2^{(p-2)\times p^n} + \ldots + 2^{2\times p^n} + 2^{p^n} + 1 = \dfrac{2^{p^{n+1}} - 1}{2^{p^n} - 1}$

and $F_{n',r'} = 2^{(p'-1)\times p'^{n'}} + 2^{(p'-2)\times p'^{n'}} + \ldots + 2^{2\times p'^{n'}} + 2^{p'^{n'}} + 1 = \dfrac{2^{p'^{m'+1}} - 1}{2^{p'^{m'}} - 1}$ we have

$2^{p^{n+1}} - 1 \equiv 0 (\mathrm{mod}\ q)$ and $2^{p'^{n'+1}} - 1 \equiv 0 (\mathrm{mod}\ q)$, and so have $2^{p^{n+1}} \equiv 1 (\mathrm{mod}\ q)$ and $2^{p'^{n'+1}} \equiv 1 (\mathrm{mod}\ q)$.

Now, letting $R = ord_q 2$, we have $R \mid p^{n+1}$ and $R \mid p'^{n'+1}$, from which $R = p^a$ for some a with $0 \le a \le n+1$, and $R = p'^{a'}$ for some a' with $0 \le a' \le n'+1$.

It follows that $p^a = p'^{a'}$, and thus, since p and p' are *different* primes, we have (by unique factorisation) $a = a' = 0$, and so $R = ord_q 2 = 1$, which implies $q = 2$. But that is impossible since all the F numbers are odd. Thus the $\{F_{n,r}\}$ are pairwise relatively prime *across* the ranks.

7. HOW I CAME UPON THE ABOVE NUMBERS. I teach a basic undergraduate course[21] on Number Theory and Cryptography[22], and this year while preparing notes to give my students in connection with

Proth's theorem (which is a generalisation of Pépin's). Let $N = s \times 2^r + 1$, where $s, r \in \mathbf{N}$ and[23] $s < 2^r$. Suppose there is an $a \in \mathbf{Z}$ such that $a^{\frac{N-1}{2}} \equiv -1 (\mathrm{mod}\ N)$, then N is prime,

I improved the '$s < 2^r$' condition (which is used awkwardly in the standard proof) to the more natural $s \le 2^r + 1$, with this

Proof: First, note the standard result about prime divisors of the Fermat numbers: let x be an integer and m a non-negative integer, then every odd prime divisor q of $x^{2^m} + 1$ satisfies $q \equiv 1 (\mathrm{mod}\ 2^{m+1})$. Next let p be any prime divisor of N, then

[21] The vast majority of my students are preparing to be primary schoolteachers, who have chosen Mathematics as an 'academic' subject as part of their B.Ed. degree programme.
[22] Several of my **Maple** worksheets are viewable at David Joyner's US Naval Academy Web site, **[18]**.
[23] Some texts add an entirely irrelevant requirement that s be *odd*.

$a^{\frac{N-1}{2}} = \left(a^s\right)^{2^{r-1}} \equiv -1 (\text{mod } p)$, and so $p \equiv 1 (\text{mod } 2^r)$. Thus, if N is composite, N will be the product of at least two primes each of which has minimum value $2^r + 1$, and so $N = s \times 2^r + 1 \geq (2^r + 1)(2^r + 1) = 2^r \times 2^r + 2 \times 2^r + 1$. That leads to $s \geq 2^r + 2$, which is incompatible with $s \leq 2^r + 1$. Thus N is prime.

8. LEADING TO THE DISCOVERY OF THE PROPOSED DEFINITION OF GENERALISED FERMAT NUMBERS. Having made the above improvement–and thus having two extra values of s to play with–I wanted to show my students that it was worth making the improvement by exhibiting some examples of numbers whose primality could be established with the increased range for s. Thus I wanted to find examples of primes N of the following form[24]:

$$N = (2^r + 1) \times 2^r + 1 = 2^{2r} + 2^r + 1$$

Two obvious cases are $r = 1$ and $r = 3$, producing the primes $N = 7$ and $N = 73$, but I wanted more examples quickly[25], and resorted to **Maple**'s **isprime** command[26]:

```
> seq(isprime(2^(2*(2*k + 1)) + 2^(2*k + 1) + 1), k=0..9);
```

produced the output:

true, true, false, false, true, false, false, false, false, false

The first two '***true***' correspond to the primes 7 and 73, and the third one (**k=4**) corresponds to the prime $2^{18} + 2^9 + 1$.

I continued doing this type of calculation for ranges of **k**–up to **k=350**, in fact–and at that point (to reduce computation times) I tried subjecting the numbers $2^{2r} + 2^r + 1$–with odd r starting at 701–to a base 2 Fermat test. The command

```
> for r from 701 by 2 to 801 do
  if 2&^(2^(2*r) + 2^r ) mod (2^(2*r) + 2^r + 1) = 1
  then print(r) fi od;
```

produced the single output ***729***.

At that point I felt a surge of excitement: 729 is 3 to the power of 6, and that tied in with the three earlier values of r, namely 1, 3 and 9. They too are powers of 3!! I was

---

[24] Pépin's theorem is, in fact, the case $s = 2^r$.

[25] Intending that any further examples would then be subjected to Proth's theorem for a primality *proof*. It is generally known that **no** CAS primality test carries a primality *certificate*; certainly not for large values of the candidate.

[26] I used *odd* values for r since the well known factorisation $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x - 1)$, would have produced composites from $2^{2r} + 2^r + 1$ when r was even. That's related to claim 1 above.

utterly convinced the resulting $N = 2^{1458} + 2^{729} + 1$ must be prime, and I subjected it to the Proth test. However, the commands[27]:

```
> N := 2^1458 + 2^729 + 1:
  mods(2&^((N-1)/2), N);
```

(the latter is computing the value of $2^{\frac{N-1}{2}} \bmod N$) produced the output '**1**', meaning that N could not be proved prime by choosing $a = 2$ in Proth's theorem. Thus I tried $a = 3,$ but the command

```
> mods(3&^((N-1)/2), N);
```

produced an output which was neither '**1**' nor '$-$**1**', and so N is composite since it *fails* Fermat's test to the base 3. Actually, this is not strictly the Fermat base 3 test, but **N** fails Fermat's base 3 test as a consequence of $3^{\frac{N-1}{2}} \not\equiv \pm 1 (\bmod N)$.

Immediately I returned to test the three 'missing' values of r between 9 and 729$-$ $r = 3^3, 3^4$ and 3^5 $-$to see why they had not been passed as primes earlier, and to my great delight it turned out that they all *passed* Fermat's test to the base 2, but *failed* it to the base 3!

At that point I realised there must be some sort of connection with Fermat numbers: each of the numbers $2^{2r} + 2^r + 1 = 2^{2\times 3^n} + 2^{3^n} + 1$ ($n = 0, 1, 2, 3, \ldots$) *appeared* to be prime or a pseudoprime to the base 2.

Another question immediately, and naturally arose: the numbers $2^{2r} + 2^r + 1$ are simply values of the irreducible[28] *quadratic* $x^2 + x + 1,$ and an obvious leap to make was to the irreducible $x^{p-1} + x^{p-2} + \ldots + x + 1,$ for prime p, under the substitution $x = 2^{p^m}$. Those are the numbers I earlier proposed might be considered as generalised Fermat numbers.

When those numbers jumped out at me, the obvious question also presented itself[29]: do those numbers behave in the *same*, *apparent way* as Fermat numbers? Meaning that for fixed p and varying n (starting at $n = 0),$ do their values proceed:

- prime, … , prime (end of block of them), composite, … (possibly *ad infinitum*)?

  or perhaps

- composite, composite, … (possibly *ad infinitum*)?

---

[27] The **mods** command produces the least absolute remainder, and the '**&**' invokes the fast square-and-multiply modular exponentiation command.

[28] There would be no point in considering the reducible $x^3 + x^2 + x + 1,$ as it would produce only composite values. Of course, numbers like $2^3 + 2^2 + 2 + 1$ are pseudoprimes to the base 4 … .

[29] All subject to being able to prove that the revealed numbers really were like Fermat numbers … .

Whatever might be the case, however, there was no point in proceeding unless I could prove that each $F_{n,r}$ passes Fermat's test to the base 2.

I could give a formal proof immediately that they do−I will shortly−but as someone who is concerned that my students don't just see proofs, but get some idea as to how proofs come into being, I would like to share with my reader some thoughts with respect to proving that $F_{n,r}$ passes Fermat's test to the base 2.

For brevity, then, setting

$$f_n = F_{n,r} = 2^{(p-1)\times p^n} + 2^{(p-2)\times p^n} + \ldots + 2^{2\times p^n} + 2^{p^n} + 1,$$

how can one prove that

$$2^{f_n - 1} \equiv 1 (\text{mod } f_n) \tag{6}$$

The obvious approach is to return to the proof of (1)−which uses (3)−and ask, here, what is the analogue of (3)?

Are the $\{f_n\}$ related in some way like the $\{F_n\}$ in (3)?

One quickly finds that they are. I began with the first two numbers of rank 2−namely 7 and 73−and on multiplying them obtained 511. That gave the game away immediately since it is $2^9 - 1,$ and it was clear that one had−in general, with elementary proof−that the following formulated part of claim 3 held:

First part of Claim 3. $$F_{0,r} \times F_{1,r} \times \ldots \times F_{n,r} = 2^{p^{n+1}} - 1 \tag{7}$$

Proof of first part of Claim 3: It is simple. Repeatedly factor the right hand side

$$\begin{aligned} 2^{p^{n+1}} - 1 &= (2^{p^n} - 1)(2^{(p-1)p^n} + 2^{(p-2)p^n} + \ldots + 2^{p^n} + 1) \\ &= (2^{p^n} - 1)F_{n,r} \\ &= (2^{p^{n-1}} - 1)F_{n-1,r}F_{n,r} = \ldots = F_{0,r}F_{1,r} \ldots F_{n-1,r}F_{n,r} \end{aligned}$$

Returning to the problem of proving (6)

From (7), which I simplify as $f_0 f_1 \ldots f_n = 2^{p^{n+1}} - 1,$ one now has

$$2^{p^{n+1}} \equiv 1 (\text{mod } f_n) \tag{8}$$

Now, would (6) follow from (8) in the same way that (1) followed from (4)? Would there be−as before, after (4)−a helpful, perhaps obvious, 'raising power'? One quickly realises that if one is to succeed in proving (6) then somehow one is going to

have to argue that p^{n+1} divides $f_n - 1$, and that's because it is easy to argue that $ord_{f_n} 2 = p^{n+1}$.

A small consideration. Let's consider the case $p = 3$, and look at the first few f−values:

First we have $f_0 = 2^2 + 2^1 + 1 = 7$ and $2^3 \equiv 1 (\mathrm{mod}\ 7)$, and we would like $2^{7-1} \equiv 1 (\mathrm{mod}\ 7)$.

Next $f_1 = 2^6 + 2^3 + 1 = 73$ and $2^9 \equiv 1 (\mathrm{mod}\ 73)$, and we would like $2^{73-1} \equiv 1 (\mathrm{mod}\ 7)$.

Then $f_2 = 2^{18} + 2^9 + 1 = 2626577$ and $2^{27} \equiv 1 (\mathrm{mod}\ 262657)$, and we would like to have $2^{262657-1} \equiv 1 (\mathrm{mod}\ 262657)$.
In the first two of those, the raising powers are $\frac{7-1}{3} = 2$ and $\frac{73-1}{9} = 8$, which could lead one to jump to a wrong conclusion (that, somehow, it's going to be a suitable power of 2 that is the requisite raising power), but the next one−

$$\frac{262657-1}{27} = 9728 = 2^9 \times 19$$

−and the next two:

$$\frac{18014398643699713-1}{81} = 222399983255552 = 2^{27} \times 19 \times 87211, \text{ and}$$

$$\frac{58460065493236116728147417487167713078820795842 57-1}{243}$$

$$= 240576401206732990650812417642665485921073233 92$$

$$= 2^{81} \times 19 \times 163 \times 87211 \times 135433 \times 272010961,$$

−and other similar examples for $p = 5, 7, 11, \ldots$ −lead one to realise that all is not so straightforward when $p \neq 2$.

I confess that I lost a lot of sleep, and tried many, many unsuccessful approaches before coming up with the following

Theorem (the second part of claim 3). *$F_{n,\,r}$ passes Fermat's test to the base 2*.

Proof: For p prime, then, by Fermat's 'little' theorem, we have $2^p \equiv 2 (\mathrm{mod}\ p)$, and successively raising to the power p gives $2^{p^2} \equiv 2^p (\mathrm{mod}\ p^2)$, $2^{p^3} \equiv 2^{p^2} (\mathrm{mod}\ p^3)$, … , $2^{p^{n+1}} \equiv 2^{p^n} (\mathrm{mod}\ p^{n+1})$. Then $2^{p^{n+1}} - 1 \equiv 2^{p^n} - 1 (\mathrm{mod}\ p^{n+1})$, and so

$$(2^{p^n} - 1)(2^{(p-1)\times p^n} + 2^{(p-2)\times p^n} + \ldots + 2^{p^n} + 1) \equiv 2^{p^n} - 1 (\mathrm{mod}\ p^{n+1}) \qquad (9)$$

But $2^{p^n} \equiv 2^{p^{n-1}} \equiv \ldots \equiv 2^p \equiv 2 (\mathrm{mod}\ p)$, and so $2^{p^n} - 1 \equiv 2 - 1 \equiv 1 \not\equiv 0 (\mathrm{mod}\ p)$, and $\gcd(2^{p^n} - 1,\ p^n) = 1$. It follows then from (8) that

$$2^{(p-1)\times p^n} + 2^{(p-2)\times p^n} + \ldots + 2^{2\times p^n} + 2^{p^n} + 1 \equiv 1 (\text{mod } p^{n+1}) \qquad (10)$$

Thus $F_{n,r} \equiv 1 (\text{mod } p^{n+1})$, and it follows from earlier that $F_{n,r}$ passes Fermat's test to the base 2.

9. THE PRIME/COMPOSITE BEHAVIOUR OF THE $\{F_{n,r}\}$. As I was about to submit this paper to the *Monthly* I was proposing that colleagues with knowledge of the implementation of a modern primality test[30] and access to more computational power than myself would carry out some searches of the following type: for a given rank of the above generalised Fermat numbers, investigate the numbers $F_{n,r}$ for $n = 0, 1, 2, 3, 4, \ldots$. Do they proceed:

- prime, prime, … , prime, (*end* of prime block), and then: composite, composite, … (*ad infinitum*?), or
- composite, composite, … , (with not a single prime, *ad infinitum*?)

In short, I wished to ask the following

Question. For a *fixed* rank $r (r \geq 2)$ of the proposed generalised Fermat numbers, is the *apparent* pattern of behaviour–in terms of which are prime, and which are composite– *always* the same as the *apparent* (conjectured) behaviour of the Fermat numbers (the generalised ones of rank 1), in the following sense:

if $F_{n,r}$ ***= composite, is*** $F_{n+1,r}$ ***(also) = composite?***

I decided to do try one small, **Maple** assisted check, and tested all ranks from 2 to 25; that is I tested the primes $3 \leq p \leq 97$. Of those twenty-four primes, fourteen lead to composite for the initial numbers in the corresponding generalised Fermat numbers, the composite Mersennes: $M_{11} = 2^{11} - 1$, $M_{23} = 2^{23} - 1, \ldots, M_{97} = 2^{97} - 1$.

For each of those fourteen ranks I subjected the 1st level numbers $F_{1,r}$ (the 'first cousins' of those Mersenne numbers) to a base 3 Fermat test. *Expecting* all fourteen to be composite I was therefore expecting all fourteen to fail the Fermat base 3 test[31]. To my very, very great surprise I found that for $r = 17$ (*i.e.* for $p = 59$), the 1031-digit number $F_{1,17}$, namely

$$P = 2^{58\times 59} + 2^{57\times 59} + 2^{56\times 59} + \ldots + 2^{2\times 59} + 2^{59} + 1 \qquad (11)$$

passed the test.[32]

---

[30] Methods due to Adleman, Pomerance and Rumley, H.Cohen and H.Lenstra, Goldwasser, Kilian and Atkin.

[31] Of course there are numbers that are pseudoprimes to bases 2 *and* 3, not to mention the Carmichael numbers *n* that pass Fermat's test to all bases relatively prime to *n*.

[32] I was so astonished that I checked it several times … .

Of course I *wanted P* to be a prime, but *is* it? I subjected *P* to more Fermat tests, and it passed all of them to prime bases as far as 137 (I had to stop somewhere). I further subjected *P* to twenty-five (again, I had to stop somewhere) Miller tests, with the following outcomes, which are consistent with *P* being prime:

$$2^{\frac{P-1}{2^{59}}} \equiv 1 (\mathrm{mod}\ P),$$

$$b^{\frac{P-1}{2^1}} \equiv -1 (\mathrm{mod}\ P), \text{ for } b = 5, 7, 13, 17, 23, 29, 31, 37, 43, 61, 73, 79 \text{ and } 97,$$

$$b^{\frac{P-1}{2^2}} \equiv -1 (\mathrm{mod}\ P), \text{ for } b = 11, 19, 47, 53, 59 \text{ and } 71,$$

$$b^{\frac{P-1}{2^3}} \equiv -1 (\mathrm{mod}\ P), \text{ for } b = 3, \text{ and } 41,$$

$$b^{\frac{P-1}{2^4}} \equiv -1 (\mathrm{mod}\ P), \text{ for } b = 67 \text{ and } 89, \text{ and}^{33}$$

$$b^{\frac{P-1}{2^8}} \equiv -1 (\mathrm{mod}\ P), \text{ for } b = 83.$$

I resorted to using **Maple**'s '**isprime**' command, which returned 'true,' but as is known that does *not guarantee* that *P* is prime, since **Maple**–like all other computer algebra systems uses a probabilistic algorithm for testing primality; I quote from **Maple**'s own Help section:

> The function isprime is a probabilistic primality testing routine. It returns false if
>
> n is shown to be composite within one strong pseudo-primality test and one Lucas test and returns true otherwise. If isprime returns true, n is ``very probably'' prime - see Knuth ``The art of computer programming'', Vol 2, 2nd edition, Section 4.5.4, Algorithm P for a reference and H. Reisel, ``Prime numbers and computer methods for factorization''. No counter example is known
>
> and it has been conjectured that such a counter example must be hundreds of digits long.

It would be pleasing to prove that *P* is prime by using one of the classical methods (Lucas, Proth, Pocklington, Kraitchik, Lehmer, Selfridge). I teach such methods to my students, and, as is well known, such methods require having a complete factorisation of $n-1$, in the case of the LKLS method, and a not necessarily complete one in the case of Proth or Pocklington.

In the LKLS case one has:

> Let $n-1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ be the complete prime factorisation of $n-1$, and suppose there are integers $a_1, a_2, \ldots, a_r$ (not necessarily distinct) such

[33] What a lovely surprise–in terms of those powers of 2! If it hadn't been for those two '2^3's,' one might have jumped to a Fermat type guess!!

that $a_i^{n-1} \equiv 1 (\mathrm{mod}\, n)$ and $a_i^{\frac{n-1}{p_i}} \not\equiv 1 (\mathrm{mod}\, n)$ for all $i, 1 \le i \le r$, then n is prime.
[This is Selfridge's highly effective 'change of base' theorem.]

In the Pocklington case one has:

Let $n-1 = UF = Up_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ be an incomplete factorisation of $n-1$ (where U is the 'unfactored part' of $n-1$, and $F = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ is its factored part) with $U < p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ and $\gcd(U, F) = 1$. Suppose there is an a such that $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ and $\gcd(a^{\frac{n-1}{p_i}} - 1, n) = 1$ for all $i, 1 \le i \le r$, then n is prime.

Favourable circumstances are for $n-1$ to have only a small number of prime factors, or for $n-1$ to have a large prime power factor, or perhaps only a small number of such factors. For details see [**5**], [**6**], [**7**], [**21**], [**22**], [**23**], [**24**] or [**25**].

I have used LKLS to prove the primality of the 1006-digit $(2^{50}(p_1 p_2 \ldots p_{20})^3 + 1)$, and the primality of the 1405-digit $(2^{37} \times 1!2!3!4! \ldots 48!49!50! + 1)$. Also I have used Pocklington to establish the primality of the (serendipitously found) 2000-digit $(p_1 p_2 \ldots p_{325} p_{326}^{325} + 1)$, (**[17]**. See **[18]** for the **Maple** worksheet details), and also the primality of the 3318-digit $(p_1 p_2 \ldots p_{346} p_{347}^{346} p_{348}^{346} + 1)$, where p_r is the r^{th} prime.

In view of those last examples, why can't I similarly establish the primality of the above 1031-digit *P*? That is the question I now address.

The difficulty encountered in attempting a proof of the primality of *P* using classical methods, and a tentative accounting of its *possible* primality.

$P = x^{p-1} + x^{p-2} + \ldots + x + 1$, with $p = 59$ and $x = 2^{59}$. Then $q = \frac{p-1}{2} = 29$, and in order to attempt a classical proof of the primality of *P*, one forms $P - 1$:

$$\begin{aligned} P - 1 &= x^{p-1} + x^{p-2} + \ldots + x \\ &= x(x^{p-2} + x^{p-2} + \ldots + x + 1) \\ &= \frac{x(x^{p-1} - 1)}{x - 1} = \frac{x(x^q - 1)(x^q + 1)}{x - 1} \\ &= x(x^{q-1} + x^{q-2} + \ldots + x + 1)(x + 1)(x^{q-1} - x^{q-2} + \ldots + x^2 - x + 1) \end{aligned} \qquad (12)$$

Now, with q being prime, both the *polynomials* $(X^{q-1} + X^{q-2} + \ldots + X + 1)$ and $(X^{q-1} - X^{q-2} + \ldots + X^2 - X + 1)$ are irreducible, and so have no trivial algebraic factors. The classic [**7**] contains 22 pages of factorisations of $(2^n - 1)$ and $(2^n + 1)$ for all odd n with $n < 1200$. Unfortunately those tables do not afford me a complete factorisation of $(x^{q-1} + x^{q-2} + \ldots + x + 1)$ and $(x^{q-1} - x^{q-2} + \ldots + x^2 - x + 1)$, since $(x^q - 1) = (2^{59})^{29} - 1 = 2^{1711} - 1$ and $(x^q + 1) = (2^{59})^{29} + 1 = 2^{1711} + 1$ are outside the ranges of the tables in [**7**].

A perusal of those tables suggests a result which I feel certain is suspected–but which I have never seen explicitly stated–namely: both $(2^n - 1)$ and $(2^n + 1)$ have a relatively large prime factor (frequently a few), which is greater the larger is the largest prime factor of *n*. It would appear, then, highly likely that *P*'s primality is a consequence of one of the classical tests, using the fact that P passes Fermat's test to base 3. I am not, of course, suggesting that in general (looking at p's other than 59) the mere fact that $P - 1$ is a product of primes, some of which are quite large would imply *P*'s primality.

What one lacks here, of course, is a tailor made primality test for these generalised Fermat numbers–something along the lines of a Pépin type test. For the classic Fermat
numbers the Pépin test is that F_n is prime for $n \geq 1$ if and only if $3^{\frac{F_n - 1}{2}} \equiv -1 (\text{mod } F_n)$ –and there is the classic Lucas-Lehmer test for the Mersenne numbers (which is quite unlike the Pépin test).

10. SOME RELATED QUESTIONS, AND PROPOSED COMPUTATIONS.

Question. *Could* it be that the required test is this: let f be any generalised Fermat number $(f \neq 3)$, then f is prime if and only if f passes Fermat's test to base 3? (The exceptional case $(f \neq 3)$ could be brought under the umbrella if one replaced (as is frequently done) $3^{f-1} \equiv 1 (\text{mod } f)$, for $3 \not\equiv 0 (\text{mod } f)$, with $3^f \equiv 3 (\text{mod } f)$. In short, is it true that a generalised Fermat number f $(f \neq 3)$, is prime if and only if $3^{f-1} \equiv 1 (\text{mod } f)$?

In asking that, I realise that since the Mersenne numbers are the level 0 (proposed) generalised Fermat numbers, then I am asking–as a special case–if it is true that M_p is prime for odd prime *p* if and only if M_p passes Fermat's test to base 3? I find it difficult to believe that this could be true, and it surely would be remarkable if it was.

Of course Fermat numbers that pass Pépin's test (and so are prime–all five of them!) automatically pass Fermat's test to base 3. Are there composite Mersenne numbers that pass Fermat's test to base 3? Perhaps this is a question that has been investigated. I have tested–using modest computing power–every odd prime *p* up to 4000 for which M_p is composite (there are 532 such primes), and in no case does M_p pass Fermat's test to base 3.

Suggested computation 1. Find some more (with proof!) first cousin Mersenne primes at level 1 (it will be of interest irrespective of whether M_p is composite or prime), or at least find some at level 1 that pass Fermat's test to base 3.

Suggested computation 2. Find more composite-prime pairs $(F_{n,r}, F_{n+1,r})$, with r as small as possible (ideally with $r = 1$!)

11. SUMMARY. I consider the central point of this paper simply to be this: the classic Fermat numbers have a certain *apparent* behaviour–five primes followed by a sea of composites. Is there another Fermat prime? Who knows? A definitive proof that there are none would be utterly remarkable (I have often remarked to my students that if someone were to find a proof that F_n is composite for all $n > 4,$ then he/she would surely die of happiness).

What I have done is to place–in, I believe, a very natural way–the Fermat numbers in a larger setting, and point out that in that larger setting–almost certainly at the 17^{th} rank–the corresponding behaviour is different. If that can happen at the 17^{th} rank, then surely it is fair to note that it could happen at *any* rank, and therefore that it is not impossible (until proven otherwise) for a sixth Fermat prime to exist.

REFERENCES[34]

1. L. E. Dickson, *History of the Theory of Numbers*, vol. 1, Chelsea, New York, 1971.
2. H. M. Edwards, *Fermat's Last Theorem*, Springer-Verlag, 1977.
3. R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, 1981.
4. V. Klee and S. Wagon, *Old and New Unsolved Problems in Plane Geometry and Number Theory*, MAA, 1991.
5. H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, 1994.
6. H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.
7. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$ ($b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*), AMS (Contemporary Mathematics Series), Vol. 22, 2nd edition, 1988.
8. R. E. Crandall, *Topics in Advanced Scientific Computation*, Springer-Verlag, 1996.
9. H. C. Williams, How was F_6 factored? *Math. Comp.* **61** (1993) 463–474.
10. C. Caldwell's site, `http://www.utm.edu/research/primes/`
11. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford, 5th edition. 1979.
12. Mathematical Developments arising from Hilbert Problems, Proceedings of Symposia in Pure Mathematics, Vol. XXVIII, AMS, (1976)
13. Yves Gallot's site, `http://perso.wanadoo.fr/yves.gallot/primes/gfn.html`
14. H. M. Stark, *An Introduction to Number Theory*, MIT Press, 1978
15. R. Honsberger, *Mathematical Gems 1*, Dolciani Mathematical Expositions, MAA, 1973.
16. W. Sierpinski, L'Induction incomplète dans la théorie des nombres, *Scripta Math.* **28** (1967) 5–13
17. Ivars Peterson's Math Trek column, *Science News*[35], Jan.16, 1999.
18. David Joyner's site, `http://web.usna.navy.mil/~wdj/crypto.htm`

[34] In compiling my references I am entirely relying upon my own personal books and the Web, and have undoubtedly omitted some valuable sources.

[35] `http://www.sciencenews.org/sn_arc99/1_16_99/mathland.htm`

19. A. Weil, *Number Theory* (*An approach through history*) *From Hammurapi to Legendre*, Birkhäuser, 1984.
20. M. S. Mahoney, *The Mathematical Career of Pierre de Fermat*, Princeton University Press, 2nd edition, 1994.
21. D. M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag, 1989.
22. D. E. Knuth, *Seminumerical Algorithms, The Art of Computer Programming*, vol. 2, Addison-Wesley, 1981.
23. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, 1994.
24. E. Bach and J. Shallit, *Algorithmic Number Theory*, MIT Press, 1996.
25. A. Lenstra, Primality Testing (in *Cryptology and Computational Number Theory*), Proceedings of Symposia in Applied Mathematics, Vol. 42, AMS, 1990.