The University of Melbourne
Internal Report

UM–P–92/14

The Properties of Fermat Moduli

John P. Costella

School of Physics, The University of Melbourne, Parkville, Vic. 3052, Australia

3 March 1992

Abstract

The properties of specific and universal Fermat moduli are investigated, from both a numerical and a theoretical point of view.

1 Introduction and Motivation[1]

The most popular pastime of amateur mathematicians the world over, at least during the last few centuries, has been to attempt to prove *Fermat's Last Theorem*,[2] namely, that

$$a^n + b^n = c^n \tag{1}$$

has *no* solutions in natural numbers for $n > 2$.[3] Despite proofs for the truth of this statement for an infinite number of values of n, no general (and correct) proof has, to date, been found. This report, unfortunately, has nothing to offer on this question. We shall, rather, investigate just a couple of the mathematical offshoots that have arisen from such investigations, which have somewhat intriguing properties.

[1] *Disclaimer:* The author of this report is not a professional mathematician, but is rather only an amateur, and a poor one at that. It is therefore most likely that the conclusions arrived at in this report have been previously obtained and reported in the professional literature. The current report should therefore be considered to be merely an introduction to that field (whatever it happens to be) for the layman.

[2] Some mathematicians claim that Fermat never had a proof for his Last Theorem, and therefore it should not be called a theorem at all. We shall not enter into the historical debate, but will rather simply refer to his conjecture by its popular name.

[3] See, for example [1], ch. 3.

It is obvious that Fermat's conjecture need only be verified for prime n (other than 2, of course) and for $n = 4$.[4] An interesting observation (which *a priori* may be of absolutely no use at all in the proof of the theorem) is the fact that, for *prime* n, the Fermat equation (1) is particularly simple *modulo* n, namely

$$a + b \equiv c \pmod{n}. \tag{2}$$

Of course, this provides but a very weak condition on the possible solutions of the Fermat equation. The reason that this observation is interesting is that its proof was first provided by Fermat himself—probably *after* writing his famous marginal note—via his *Little Theorem*,[5] which states that, for p prime,[6]

$$b^{p-1} \equiv 1 \pmod{p} \tag{3}$$

for *all* b, except if $b \equiv 0 \pmod{p}$, for which it obviously equals zero. Multiplying both sides by b, we then have

$$b^p \equiv b \pmod{p}, \tag{4}$$

which, of course, turns (1) into (2) modulo p. Writing Fermat's Little Theorem in the form (4) is arguably simpler than its conventional expression (3),[7] since it is obvious that we no longer have to treat the case $b \equiv 0 \pmod{p}$ in any special way.

Now, as noted, relation (4) may be completely irrelevant in proving Fermat's Last Theorem. But is is quite intriguing in its own right. Obviously, if we test (4) for some b and p, and find that it does *not* hold, then it shows that p cannot

[4] To see that this would be sufficient to prove the theorom for *all* n, take, as a simple case, $n = 6$. If Fermat's equation, (1), *did* have a solution with natural a, b and c for $n = 6$, *i.e.*

$$a^6 + b^6 = c^6,$$

or, equivalently,

$$\left(a^2\right)^3 + \left(b^2\right)^3 = \left(c^2\right)^3,$$

then we could simply define the three new numbers $x = a^2$, $y = b^2$ and $z = c^2$ which would then satisfy the equation

$$x^3 + y^3 = z^3.$$

It is clear that we could carry out this sort of procedure whenever n is not prime, and it implies that if Fermat's equation *did* have a solution for any composite n, then it would necessarily have at least one solution for *every* divisor of n. Obviously, this does not help us for $n = 4$, since we know there *are* solutions for $n = 2$; therefore, we need to prove $n = 4$ separately (which has, of course, been done). Once we have shown $n = 4$, then all other composite $n > 4$ follow, since every such n has at least one factor that is not equal to 2. For n a power of 2, we use the fact that 4 is a divisor; for all other n, we choose one of the *prime factors* of n. Thus, if we prove the theorem for *all* prime n except 2, as well as $n = 4$, then it will also hold true for all composite n. The trick, then, is to prove it for prime n!

[5] Or simply "Fermat's Theorem" to mathematicians, who, as noted, do not consider his Last Theorem a theorem.

[6] See, for example, [1], p. 18.

[7] Except when one is making contact with its generalisation by Euler.

be prime;[8] therefore, using (4) is a useful way, in practice, to eliminate the possibility of a given number p being prime.[9]

Let us leave aside the question of primality, for the moment, and instead look at relation (4) in a somewhat different way. Rather than taking the modulus to be *fixed*, what if we simply specified the base and exponent, and asked the following question: For *which moduli* x does

$$b^n \equiv b \pmod{x} \tag{5}$$

hold true, for a given choice of b and n? Obviously, from the above, we know that $x = n$ must be one such modulus when n is prime; it may or may not be so when n is composite. Nevertheless, regardless of the primality of n, there may well be *other* moduli x for which the equation (5) is satisfied. Now, consider the fact that Fermat's Little Theorem *itself* is extremely easy to *prove*,[10] but is not trivially *obvious* (as witnessed by the fact that noöne before Fermat noted it). We should therefore be justified in assuming that the solutions x of (5) (which *encompass* those of the Little Theorem) will probably not be too difficult to prove either; on the other hand, they must, of course, be at least as unobvious as those of the Little Theorem. We shall therefore endeavour to investigate such solutions, at least in an elementary way, to see what they reveal.

2 Specific and Universal Fermat Moduli

Our first task in investigating the solutions for x in (5) is to consider the practical problem of how one actually goes about *finding* these possible solutions, numerically, given specific values for b and n. As an example, we might want to find those x for which

$$3^7 \equiv 3 \pmod{x}. \tag{6}$$

Now, if we simply subtract 3 from both sides of this congruence, we have

$$3^7 - 3 \equiv 0 \pmod{x}.$$

But equality of a quantity to zero modulo x simply means that the quantity is some *multiple* of x; in our example, we require $3^7 - 3$ to be a multiple of x. Turning this around, this simply means that x is any *divisor* of the number $3^7 - 3$. Therefore, all we need to do is cut up the number $3^7 - 3$ into its prime factors, *i.e.*

$$3^7 - 3 = 2184 = 2^3 \cdot 3 \cdot 7 \cdot 13. \tag{7}$$

[8] Of course, the converse is *not* true.

[9] There are apparently more elaborate forms of this test that work more efficiently; see [1], ch. 2.

[10] Ref. [1], p. 18.

We thus find that the only x for which (6) holds true are

$$\begin{aligned} x &= 1, 2, 3, 4, 6, 7, 8, 12, 13, 14, 21, 24, 26, 28, \\ &\quad 39, 42, 52, 56, 78, 84, 91, 104, 156, 168, 182, \\ &\quad 273, 312, 364, 546, 728, 1092 \text{ and } 2184, \end{aligned} \tag{8}$$

where each value is simply a divisor of (7). As promised by the Little Theorem, the value 7 is one of the solutions listed in (8)—and, of course, being prime, is also displayed explicitly in (7). But (8) shows that there are also another *thirty-one* moduli for which (6) holds; therefore, we can already see that the more general question (5) reveals more than the Little Theorem alone. Of course, it is sufficient for this task to simply know what the value of $b^n - b$ is—or, more precisely, its divisors—and in this sense there is nothing extraordinary about (7) or (8). But it will be seen, in the remainder of this report, that it is *precisely* our splitting up this number into prime factors that is most intriguing, taking into account the fact that there is (to the author's knowledge) no *a priori* way of writing down the prime factorisation of the number $b^n - b$,[11] other than by prime factorising it explicitly.

At this point, we shall, unfortunately, need to introduce a few pieces of notation and nomenclature, to simplify the following discussions.[12] We shall refer to the number $b^n - b$ as the *specific Fermat modulus* of base b and exponent n,[13] with symbol $F(n; b)$, *i.e.*

$$F(n; b) = b^n - b.$$

For the above example, we have

$$F(7; 3) = 2184.$$

As such, these numbers $F(n; b)$ are nothing more than particular numbers that the author has decided would be interesting to investigate. However, we now ask a more subtle question: Given a certain value for the exponent, n, are there any moduli x for which (5) is satisfied *for all* bases b? This question is, of course, inspired by the result (4) of the Little Theorem, which answers this question in the affirmative when n is prime, and provides at least one answer $x = n$.

[11] Or, more precisely, $b^{n-1} - 1$, since $b^n - b$ itself obviously has the divisors of b among its divisors.

[12] However, the author shall endeavour to explain the *spirit* of all symbolic statements in words, so that the following sections do not become completely symbolic and ununderstandable.

[13] Named after Fermat since it is quite likely that he would have investigated their nature to some extent (witness his Little and Last Theorems), and the fact that it is quite *unlikely* that anyone before him did so (again by consideration of the priority of the above Theorems). This terminology should not be confused with the existing term *Fermat number*, used for any number of the form $2^{2^n} + 1$; in practice, these two types of object would rarely, if ever, be mentioned in the one breath anyway.

However, it is again not *a priori* obvious (at least to the author) whether there are, in fact, any *other* values of x that have this universal nature for prime n, or, indeed whether any such values of x exist *at all* for composite n.

Let us, therefore, investigate how one might go about calculating such values of x, given some exponent n. Basically, we need to test (5) for *all* integers b, and find those values of x which satisfy them all. This does not, on the surface of it, appear to be a very palatable task at all. However, if we follow the same procedure as taken above for any one *specific* choice of b, we see that it is not all that hopeless after all. We first note that, naturally, (5) is satisfied for *all* $n > 0$ and $x \geq 0$ if $b = 0$ or $b = 1$, since

$$0^n \equiv 0 \pmod{x}$$

and

$$1^n \equiv 1 \pmod{x}$$

are always true in these cases. The first integer b that might give us non-trivial information, therefore, is 2. Inserting this into (5), we require

$$2^n \equiv 2 \pmod{x}.$$

Now, we have already seen that, for a given exponent n, the solutions x of this equation are simply the divisors of the specific Fermat modulus $F(n;2)$; for example, if our chosen value of n were 7, then we would have

$$F(7;2) = 126 = 2 \cdot 3^2 \cdot 7.$$

Similarly, the value $b = 3$, or

$$3^n \equiv 3 \pmod{x},$$

has as solutions x the divisors of the specific Fermat modulus $F(n;3)$; for the example $n = 7$, we have already seen that

$$F(7;3) = 2184 = 2^3 \cdot 3 \cdot 7 \cdot 13.$$

If we now require that x be a modulus solution of *both* of these equations, then it must, by the above, be a divisor of both $F(n;2)$ and $F(n;3)$. There are, of course, a number of such solutions that satisfy both equations, but it is obvious that these solutions all share the property that they are themselves divisors of the *greatest common divisor* (gcd) of $F(n;2)$ and $F(n;3)$. For our specific example case $n = 7$, the above prime factorisations show that the gcd of $F(7;2)$ and $F(7;3)$ is

$$\gcd\left[F(7;2), F(7;3)\right] = 2 \cdot 3 \cdot 7;$$

or, in other words, the only values of x that *simultaneously* satisfy both

$$2^7 \equiv 2 \pmod{x}$$

and

$$3^7 \equiv 3 \pmod{x}$$

are the divisors of $2 \cdot 3 \cdot 7$, namely

$$x = 1, 2, 3, 6, 7, 14, 21, 42.$$

Already, we see that insisting on the congruence (5) for *two* different bases b has cut down the number of solutions for x quite dramatically.

OK, then, we have not, so far, hit upon any insuperable obstacles. Let us continue our investigations to the next step, and look for those values of x for which (5) is satisfied not just for $b = 2$ and $b = 3$, but for $b = 4$ as well. Obviously, the same considerations as above hold again; we now simply need to find the greatest common divisor of all *three* specific Fermat moduli, namely

$$\gcd\left[F(n;2), F(n;3), F(n;4)\right].$$

In a practical case, we can, however, use our previous knowledge if

$$\gcd\left[F(n;2), F(n;3)\right]$$

to compute this result, since

$$\gcd\left[F(n;2), F(n;3), F(n;4)\right] = \gcd\left[\gcd\left[F(n;2), F(n;3)\right], F(n;4)\right].$$

For our specific example, we first note that[14]

$$F(7;4) = 16380 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13.$$

Obviously, the gcd of this and $2 \cdot 3 \cdot 7$ is just $2 \cdot 3 \cdot 7$, as the above prime factorisation of $F(7;4)$ shows.

We therefore increment our base again, and try $b = 5$. We now have

$$F(7;5) = 78120 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 31,$$

so that, yet again, the number $2 \cdot 3 \cdot 7$ comes through the gcd process unscathed. At this stage, it is starting to look as if $2 \cdot 3 \cdot 7$ is going to satisfy this procedure

[14] It should be noted that all *perfect squares*, $b = a^2$, are somewhat special cases, since for such bases

$$\begin{aligned} F(n;b) &= b\left(b^{n-1} - 1\right) = a^2\left(a^{2(n-1)} - 1\right) \\ &= a^2\left(a^{n-1} - 1\right)\left(a^{n-1} + 1\right) = a\left(a^{n-1} + 1\right)F(n;a). \end{aligned}$$

Since, following the method above, we are "counting up" the integer b, by the stage we reach $b = a^2$ we must have already calculated the case $b = a$. It is then clear that taking the gcd of $F(n;a)$ and $F(n;a^2)$ will simply yield $F(n;a)$, *i.e.* it is unnecessary to test $F(n;a^2)$, since it cannot possibly yield any new information. However, to make the arguments in the text most transparent and uncluttered as possible, we have simply ignored this fact for $b = 4$; in practical calculations, on the other hand, one may like to skip over perfect squares to speed up the process.

for *arbitrary* b. Are we doomed to continue this process forever? Fortunately, we are not; by the following reasoning: Imagine that $2 \cdot 3 \cdot 7 = 42$ *does* satisfy (5) with $n = 7$ for arbitrary b.[15] That would mean that, in particular,

$$b^7 \equiv b \pmod{p} \text{ for all } b,$$

where p equals 2, 3 or 7; conversely, if it *does* hold for these prime factors, then it will necessarily hold for $x = 42$ also. Now, if we have verified this statement for all $b < 7$, where 7 is the *largest* prime factor p, then we know from the theory of congruences that it will automatically be satisfied for all $b \geq 7$ too. Therefore, we need only need test the relation for values of b up to 7. In the *general* case, rather than our specific example $n = 7$, what we do is this: calculate the "running gcd", as above, of the quantities

$$F(n;2), F(n;3), F(n;4), F(n;5), \ldots, F(n;b).$$

If, at any stage, we find that the base b that we are testing is greater than or equal to the greatest prime factor of the "running gcd", then we know we can stop—the gcd thus obtained will then be our answer. We shall call this quantity the *universal Fermat modulus* of exponent n, and denote it by the symbol $F(n)$, so that

$$F(n) = \operatorname*{gcd}_{b=2}^{\infty} \left[F(n;b) \right].$$

Given these definitions, and the above algorithm, it is a fairly simple task, in principle, to compute the universal Fermat moduli for various exponents n, since the gcd operation (via the Euclidean algorithm) is quite efficient. The only hassle we have, in practice, is the fact that we must handle numbers of rather long length, indeed far too long for a handheld calculator. (Consider, as a relatively simple example, the specific modulus $F(101;41)$, which is a 163-digit number.) We also cannot apply the various tricks that are usually available when one is computing numbers congruent to some modulus, since the whole point of the current report is to *find* the moduli for which certain equations are satisfied. The only alternative[16] is to sit down and write a few routines for one's computer to handle integer arithmetic for arbitrarily[17] long integers.[18]

Having overcome the above technical problems, it is then a fairly simple task to compute the first few universal Fermat moduli.[19] All of the $F(n)$ for $n < 100$ are listed in table 1. There are two facts that immediately stand out, that are so simply stated that it seems likely that *even the author* should be able to prove

[15] The author does *not* believe that this is the question that Douglas Adams was referring to.

[16] Unless there is some trick that the author has not woken up to.

[17] Limited by the resources of the computer in question, of course.

[18] This is, unfortunately, most likely a deterrent to the interested layman who might otherwise like to investigate the numerical results which follow. To offset this deterrent, the author will readily give any interested reader a copy of the C source files that perform these tasks, if

n	$F(n)$	n	$F(n)$	n	$F(n)$	n	$F(n)$
2	2	27	6	52	2	77	30
3	6	28	2	53	1590	78	2
4	2	29	870	54	2	79	3318
5	30	30	2	55	798	80	2
6	2	31	14322	56	2	81	230010
7	42	32	2	57	870	82	2
8	2	33	510	58	2	83	498
9	30	34	2	59	354	84	2
10	2	35	6	60	2	85	3404310
11	66	36	2	61	56786730	86	2
12	2	37	1919190	62	2	87	6
13	2370	38	2	63	6	88	2
14	2	39	6	64	2	89	61410
15	6	40	2	65	510	90	2
16	2	41	13530	66	2	91	272118
17	510	42	2	67	64722	92	2
18	2	43	1806	68	2	93	1410
19	798	44	2	69	30	94	2
20	2	45	690	70	2	95	6
21	330	46	2	71	4686	96	2
22	2	47	282	72	2	97	4501770
23	138	48	2	73	140100870	98	2
24	2	49	46410	74	2	99	6
25	2730	50	2	75	6		
26	2	51	66	76	2		

Table 1: The universal Fermat moduli $F(n)$ for all $n < 100$. As noted in the text, this explicit listing shows three distinctive features: (a) $F(n) = 2$ for even n; (b) $F(n)$ is even for all n; and (c) the values of the magnitudes of the $F(n)$, as they are displayed here, do not show any apparent pattern.

them rigorously. The first observation is that $F(n) = 2$ for all even n. Despite some work, the author is ashamedly unable to report having found any proof of this statement on elementary grounds, although our later findings *will* lead to an "explanation" (of sorts) of the phenomenon. On the other hand, the second noteworthy feature of table 1—that all $F(n)$ are even—is easy to prove, since it simply imples that

$$b^n \equiv b \pmod 2.$$

But this just states that an odd number to any power is odd, and that an even number to any power is even, which is of course obviously true.

The third most noticeable feature of table 1 is that, if there *is* some pattern to the $F(n)$ for odd n, then writing the $F(n)$ as per table 1 isn't going to reveal it! Indeed, the only thing to be gleaned from that table about the $F(n)$ for odd n is that—unlike the case of even n—*none* of them are equal to 2.[20] We can, however, glean some insight into their apparently random pattern by returning to the example treated above—namely,

$$F(7) = 42 = 2 \cdot 3 \cdot 7.$$

Now 42 is not, in itself, an obviously meaningful number. But its prime factors, 2, 3 and 7, seem much simpler, because no prime factor is repeated, and the largest is equal to 7—the value of n that we are testing. It is therefore plausible that the universal Fermat moduli would look much simpler if we broke them *all* down into their prime factors.[21] To this end, we have listed all the $F(n)$ (for odd n) in table 2, broken up into their prime factors.

There are several features of table 2 that hit one in the face immediately. The first is that, not only are all the $F(n)$ (for odd n) *even*, they are in fact multiples of *six*. Secondly, the *largest* prime factor $F(n)$ is no larger than n itself. But the most remarkable feature of table 2 of all is the fact that *none of them have repeated prime factors* (*i.e.* they are *squarefree*). Now, if Fermat's Little Theorem is not a trivially obvious statement, then the above

requested and supplied with a 3.5 inch IBM diskette for the purpose.

[19] In fact, one finds that, when computing the universal Fermat moduli, the gcd algorithm only reduces the "running gcd" for *prime* bases b; furthermore, the number of primes necessary to reduce the gcd to its final value is *extremely* small—in fact, the author has not found any case (for exponents less than a few hundred) for which the "work" is done by numbers other than $2, 3, 5, 7$ and 11. Thus, it suffices, in practice, to keep an eye on the gcd algorithm and quit it after the gcd does not reduce further, rather than test the more excessive number of values suggested by the earlier analysis (*i.e.* the largest prime factor of the "running gcd"). It will be seen shortly that the universal Fermat moduli *do*, in fact, follow a rather remarkable set of rules; one can use this knowledge to *test* the gcd algorithm and see how quickly it homes in on the correct answer, and to actually *verify* that only prime bases b give any new information in the process—at least, for some finite number of cases!

[20] The reason for this will be seen to be elementary shortly.

[21] Note that performing prime factorisation *after* obtaining the moduli by gcd methods is *not* a difficult task, since most of the prime factors are eliminated in the gcd process. This will be clearer shortly.

n	$F(n)$	n	$F(n)$
3	$2 \cdot 3$	53	$2 \cdot 3 \cdot 5 \cdot 53$
5	$2 \cdot 3 \cdot 5$	55	$2 \cdot 3 \cdot 7 \cdot 19$
7	$2 \cdot 3 \cdot 7$	57	$2 \cdot 3 \cdot 5 \cdot 29$
9	$2 \cdot 3 \cdot 5$	59	$2 \cdot 3 \cdot 59$
11	$2 \cdot 3 \cdot 11$	61	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$
13	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	63	$2 \cdot 3$
15	$2 \cdot 3$	65	$2 \cdot 3 \cdot 5 \cdot 17$
17	$2 \cdot 3 \cdot 5 \cdot 17$	67	$2 \cdot 3 \cdot 7 \cdot 23 \cdot 67$
19	$2 \cdot 3 \cdot 7 \cdot 19$	69	$2 \cdot 3 \cdot 5$
21	$2 \cdot 3 \cdot 5 \cdot 11$	71	$2 \cdot 3 \cdot 11 \cdot 71$
23	$2 \cdot 3 \cdot 23$	73	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73$
25	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	75	$2 \cdot 3$
27	$2 \cdot 3$	77	$2 \cdot 3 \cdot 5$
29	$2 \cdot 3 \cdot 5 \cdot 29$	79	$2 \cdot 3 \cdot 7 \cdot 79$
31	$2 \cdot 3 \cdot 7 \cdot 11 \cdot 31$	81	$2 \cdot 3 \cdot 5 \cdot 11 \cdot 17 \cdot 41$
33	$2 \cdot 3 \cdot 5 \cdot 17$	83	$2 \cdot 3 \cdot 83$
35	$2 \cdot 3$	85	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 29 \cdot 43$
37	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37$	87	$2 \cdot 3$
39	$2 \cdot 3$	89	$2 \cdot 3 \cdot 5 \cdot 23 \cdot 89$
41	$2 \cdot 3 \cdot 5 \cdot 11 \cdot 41$	91	$2 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 31$
43	$2 \cdot 3 \cdot 7 \cdot 43$	93	$2 \cdot 3 \cdot 5 \cdot 47$
45	$2 \cdot 3 \cdot 5 \cdot 23$	95	$2 \cdot 3$
47	$2 \cdot 3 \cdot 47$	97	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 97$
49	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$	99	$2 \cdot 3$
51	$2 \cdot 3 \cdot 11$		

Table 2: The universal Fermat moduli $F(n)$ for all odd $n < 100$, as given in table 1, but broken up into their prime factors. The remarkable squarefree nature of each modulus is evident, as is the fact that none of the prime factors of $F(n)$ are greater than n. For prime n, n is itself a prime factor (and, by the above observation, the largest), as it must be by Fermat's Little Theorem. (The exact structure of each $F(n)$ is detailed in the text.)

considerations are even less so; in particular, the author cannot think of any good intuitive argument why the last such phenomenon—the squarefree nature of the moduli—should hold.

Remarkable as the above may seem (at least to the author), we can, in fact, go even further in our analysis of the universal Fermat moduli for odd exponents. To do this, one should first note some suspicious-looking *largest* prime factors in table 2 for odd n that are *not* prime. (For *prime* n, $F(n)$ must, by the Little Theorem, contain n as a factor; the above observations show that it is also the largest.) One of these is $F(57)$,

$$F(57) = 2 \cdot 3 \cdot 5 \cdot 29.$$

The prime factor 29 seems to stick out like a sore thumb, since

$$57 - 1 = 2(29 - 1).$$

In fact, we find that this occurs for the largest prime factor of $F(n)$ for a number of *other* composite n in table 2—namely $n = 9, 21, 25, 33, 45, 57, 81$ and 93. Now, these "coïncidences" should raise our suspicions even further—unexplainable coïncidences being a rare animal in mathematics. Let us, then, investigate in more detail one n for which $F(n)$ seems to have an inordinately large number of prime factors—say, $n = 61$ in table 2. For this case, one notes immediately that

$$F(61) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$$

can be rewritten

$$\begin{aligned} F(60+1) &= (1+1)\cdot(2+1)\cdot(4+1)\cdot(6+1) \\ &\quad \cdot(10+1)\cdot(12+1)\cdot(30+1)\cdot(60+1), \end{aligned} \tag{9}$$

where, of course, the numbers $1, 2, 4, 6, 10, 12, 30$ and 60 are *all divisors of 60*—the number on the left hand side. This, surely, cannot be a coïncidence, so let us look at the question a little more closely. Take, for example, the prime factor $7 = 6 + 1$ in the above. Let us, first, introduce another trivial piece of terminology, to avoid an excess of words in further descriptions, and call the number $a + 1$ the *increment* of the number a, and likewise for the *decrement* of a. Now, we know that Fermat's Little Theorem assures us that

$$b^6 \equiv \begin{cases} 1 & \text{if } b \not\equiv 0 \pmod 7, \\ 0 & \text{if } b \equiv 0 \pmod 7. \end{cases}$$

But raising both sides of this to the tenth power (where $10 = 60/6$) we then find that

$$b^{60} \equiv \begin{cases} 1 & \text{if } b \not\equiv 0 \pmod 7, \\ 0 & \text{if } b \equiv 0 \pmod 7, \end{cases}$$

since 1 and 0 remain unchanged by this operation. Multiplying through by an extra factor of b, at this last stage, we find that, of course, $b^{61} \equiv b \pmod 7$

must hold for all b. Now, we could repeat this for *any* of the divisors of 60, *as long as the increment of the divisor is prime*—since Fermat's Little Theorem says *nothing at all* about numbers that are not prime.[22] Since this (single) congruence for b^{61} would then hold for all these *various* moduli, then by the previous explanations it should be clear that these moduli *must* all be prime factors of $F(61)$.

The above reasoning, therefore, tells us what prime factors *must* appear in $F(61)$. But that argument does *not*, however, say anything about what *other* prime factors might appear in $F(61)$. For example, let us look more closely at the list of the divisors of 60:

$$1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.$$

Now, not all of these divisors were actually used in $F(61)$—recall, only 1, 2, 4, 6, 10, 12, 30 and 60 were used. What about the others? For example, imagine that the congruence

$$b^{21} \equiv b \pmod{21}$$

happened to hold for all b (it doesn't, in actual fact, but for the purposes of argument ignore the fact that we know this).[23] By the above arguments, we would then (again, hypothetically) find that

$$b^{61} \equiv b \pmod{21}$$

so that $F(61)$ would then have to be a multiple of 21. But $F(61)$ is *already* a multiple of $21 = 3 \cdot 7$, by virtue of the (somewhat coïncidental) fact that $2 = 3 - 1$ and $6 = 7 - 1$ are divisors of 60. The question that then arises is this: would $F(61)$ then contain the *squares* of 3 and 7 as prime factors, or would it somehow know that it "should be" squarefree? And if it *did* "know" to keep itself squarefree, how would it "know" what to do if those prime factors (3 and 7, in the above example) were *not* already present?

Of course, it is a little silly to use the above numbers as an example, since we know that 21 is not a Carmichael number anyway, so we cannot answer the questions one way or the other. Let us, therefore, use the fact that we know that $561 = 3 \cdot 11 \cdot 17$ *is* a Carmichael number (the smallest, in fact), and construct an example that would test the various choices offered above. A good test case is the number $F(1121)$, which we have rigged by noting that

$$1121 = 2 \cdot 560 + 1.$$

Now, since we know that

$$b^{561} \equiv b \pmod{561}$$

[22] More precisely, there are an abundant number of examples of non-prime numbers n (most of them, in fact) such that $a^{n-1} \equiv 1 \pmod{n}$ does *not* hold for all b; on the other hand, the so-called "Carmichael numbers" ([1], p. 21) are composite n such that this congruence *does* hold for all b.

[23] Of course, 21 would be a Carmichael number if this were true, and we know that it is not.

holds for all b, then it follows from the above that

$$b^{1121} \equiv b \pmod{561}$$

must too. Therefore, $F(1121)$ must be a multiple of $561 = 3 \cdot 11 \cdot 17$. On the other hand, we also know that, by Fermat's Little Theorem, the other factor of 2 in $2 \cdot 560$ *separately* leads to the result

$$b^3 \equiv b \pmod{3}$$

since 3 is a prime; therefore, it follows that

$$b^{1121} \equiv b \pmod{3}$$

must too—and, thus, we "independently" know that $F(1121)$ must be a multiple of 3. The question raised above is then the following: will the prime factor 3 appear *once* or *twice* in $F(1121)$? Well, it is a fairly straightforward[24] to check this, using the gcd algorithm described earlier, and in fact one finds that

$$F(1121) = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 17 \cdot 29 \cdot 41 \cdot 71 \cdot 113 \cdot 281,$$

so that, in fact, $F(1121)$ "decides" that it *will* remain squarefree, despite the two "sources" of the prime factor 3 that one might, *a priori*, imagine might appear.[25] Thus, as far as the Fermat modulus is concerned, the only relevant property of 561 is the fact that 560 has the divisors it has; the fact that 561 *itself* satisfies Fermat's Little Theorem, despite the fact that it is not prime, is merely a *by-product* of the coïncidence that $(3-1)$, $(11-1)$ and $(17-1)$ happen to divide $(561-1)$.[26]

It will also be noted that, so far, we have only looked into the question of why there are no *repeated* prime factors in $F(n)$. Of an altogether different nature is the question of why there are no *other* prime factors in $F(n)$ that do not follow the "increment–divisor" rule above. For example, why should the equation

$$b^{1121} \equiv b \pmod{x}$$

never be satisfied for all b if x were, say, 89, or 167, or in general *any* prime whose decrement is not a divisor of 1120? If it is satisfied, as it is, for the large modulus

[24] *Warning:* this involves manipulating integers up to 784 digits in length!

[25] Note that there is no *a priori* reason why $b^{1121} \equiv b \pmod{9}$ could not be satisfied for all b—Fermat's Little Theorem says nothing on this question. The proof of this result must, therefore, be based on deeper results than simply the Little Theorem.

[26] For this to be true in general, it would require *all* Carmichael numbers to be simply "by-products" of the fact that the decrements of their prime factors divide the decrement of themselves, *i.e.* that *no* composite number satisfying Fermat's Little Theorem exists apart from those of this form. The author, having access only to a handful of Carmichael numbers, knows not whether it has been shown that they are, in fact, all of this form, or indeed whether contrary examples are known.

$5 \cdot 11 \cdot 29 \cdot 41 = 65395$, then why shouldn't it be satisfied for the prime 65393? One might argue that this would imply 65393 irreducible solutions, which does not really work well with only an 1121-th order equation (if the normal rules of algebra apply here), and, if that were so, then it would follow that $F(n)$ could have *no* prime factor larger than n. But that still does not answer the previous question—why prime factors *smaller* than n but not following the above rules never appear. It seems as if there is a type of "minimalist" approach taken with these numbers, in that *only* those solutions required by Fermat's Little Theorem are accommodated in the Fermat moduli, and no more.

If we conjecture that the above conclusions about the Fermat moduli are true in general, and not just for the rather small number of numerical cases investigated here, then we can go on and write down an *exact* formula for $F(n)$, that has nothing to do with the way we have computed the moduli above (*i.e.* via an infinite gcd operation), but is rather based on the prime numbers. To do this, we must first define a simple *primality function* $\theta(n)$ such that

$$\theta(n) = \begin{cases} 1 & \text{if } n \text{ is prime,} \\ 0 & \text{if } n \text{ is composite.} \end{cases}$$

(Of course, one of the problems with prime numbers is the fact that evaluating $\theta(n)$ is, in general, not a trivial task. For this reason, it is interesting to find any relation that *uses* $\theta(n)$ in a non-trivial way, since it might conceivably tell us something about the prime numbers that we didn't already know.)[27] Employing the commonly used notation that $d|n$ means that d is a divisor of n, and that, for example,

$$\sum_{d\,|n}$$

implies a sum over *all* of the divisors d of n,[28] then our above observations

[27] For example, the number of primes less than x,

$$\pi(x) = \sum_{n<x} \theta(n),$$

and the Riemann zeta function ([1], p. 125),

$$\zeta(z) = \sum_{n=1}^{\infty} n^{-z} = \prod_{n=1}^{\infty} \left(1 - \theta(n) n^{-z}\right)^{-1},$$

both seem to be of some importance in a number of areas of mathematics, some quite unrelated to prime numbers.

[28] And similarly for products, *etc.*

suggest the general formula[29]

$$F(n) = \operatorname*{gcd}_{b=2}^{\infty} [F(n;b)] = \prod_{d\,|n-1} (d+1)^{\theta(d+1)}, \tag{10}$$

where, recall, the specific Fermat modulus function $F(n;b)$ is simply given by[30]

$$F(n;b) = b^n - b. \tag{11}$$

Ignoring, for the moment, our reasons for constructing the Fermat moduli in the first place, then the result (10)—which relates an infinite set of gcd operations to the properties of primality and divisibility—is, at least to the author, an unexpected and intriguing connection. Finally, returning to the problem which we originally posed—namely, to find those moduli for which (5) is satisfied for *all* integers b—we now have the answer that

$$b^n \equiv b \pmod{d\,|F(n)} \quad \text{for all } b, \tag{12}$$

where $F(n)$ is given by (10) and (11), and, most importantly, such divisors d are the *only* moduli for which this congruence holds for all integers b, if the conjectures above are, in fact, true.

It should again be emphasised that the results (10), (11) and (12) are, most likely, plainly obvious to any professional mathematician, and their proof can undoubtedly be written on the back of an envelope by any such expert. Nevertheless, the author hopes that this account is as entertaining for any amateur number theorist reading this report as it has been for himself; the strange and beautiful properties that numbers themselves can throw our way never cease to amaze.

3 Acknowledgments

Extensive philosophical, physical and mathematical discussions with R. E. Behrend, going back two and a half decades, are gratefully acknowledged.

[29] It should be noted that our numerically-observed result that $F(n) = 2$ for even n is *implied* by this formula, since, for n even, the number $n-1$ is odd, whose divisors must therefore also be odd, and thus $d+1$ is even. Then, since no even number greater than 2 is prime, the θ function in (10) will simply kill them all off except 2 (which is, of course, always present, since 1 is a divisor of every number).

[30] It should be noted at this point that it is strictly *not* permissible to replace $F(n;b)$ by $F(n;b)/b$, *i.e.* $\left(b^{n-1}-1\right)$, in the gcd operation in (10), since if one *did* do so, then all of the factors of $F(n)$ would simply disappear. To see why these factors would disappear, one only need note that the quantity $b^{n-1} - 1 \equiv -1 \pmod{b}$, and therefore it *cannot* be a multiple of b (if $b > 1$). Consider, now, those values of b which are equal to one of the prime factors of $F(n)$; by the above, such a prime factor will not be contained in the quantity $b^{n-1}-1$. If we *were* then to replace $F(n;b)$ by $b^{n-1}-1$, then the gcd operation would, upon hitting each of these particular bases in turn, eliminate *every* prime factor if $F(n;b)$; the corresponding infinite gcd would therefore give the meaninigless result 1 for all n.

This work was supported in part by the Australian Research Council and an Australian Postgraduate Research Allowance.

The original form of this report was created on an IBM PS/2 Model 70–386 using Microsoft Word for OS/2 and printed on an IBM 4019 PostScript printer. This document was converted to LaTeX format on 11 November 1992; the contents were not modified at that time, apart from several minor typographical corrections. The numerical calculations for this report were written using the Microsoft C Professional Development System version 6.0 and computed under OS/2 on the abovementioned IBM PS/2. The author will provide the source code for these computations free of charge to any interested reader, if a 3.5 inch IBM diskette accompanies such a request.

References

[1] I. Stewart, *The Problems of Mathematics* (Oxford University Press, Oxford, 1987).