Observations on a theorem of Fermat and others on looking at prime numbers*

Leonhard Euler†

It has been noted that the quantity $a^n + 1$ always has divisors whenever n is an odd number, or is divisible by an odd number aside from unity. Namely $a^{2m+1} + 1$ is able to be divided by $a + 1$ and $a^{p(2m+1)} + 1$ by $a^p + 1$ for whatever number is substituted in place of a. On the other hand, if n is a number such that it is not able to be divided by any odd number aside from unity, whenever no divisor can be assigned for the number $a^n + 1$ then n is a rank of two. For this reason, all prime numbers in the form $a^n + 1$ must necessarily be expressed in the form $a^{2^m} + 1$. It cannot, however, be concluded for $a^{2^m} + 1$ to always produce a prime number for any a; it is at once clear that if a is an odd number, then this form has 2 as a divisor. Then also, even if a denotes an even number, countless other cases can be given where this produces a composite number. At the least, the formula $a^2 + 1$ is able to be divided by 5 whenever $a = 5b \pm 3$, and indeed $30^2 + 1$ is able to be divided by 17 and $50^2 + 1$ by 41. In a similar way, $10^4 + 1$ has the divisor 73, $6^8 + 1$ has the divisor 17, and $6^{128} + 1$ is divisible by 257. Yet for the form $2^{2^m} + 1$, no incidence has been found with a divisor that has any place in the table of prime numbers, which indeed has not been extended beyond 100000. Because of this and perhaps other reasons, Fermat was led to declare there to be no doubt for $2^{2^m} + 1$ to always be a prime number, and proposed

*Originally published as *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus*, Commentarii academiae scientiarum Petropolitanae **6** (1738), 103-107, and republished in *Leonhard Euler, Opera Omnia*, Series 1: Opera mathematica, Volume 2, Birkhäuser, 1992. A copy of the original text is available electronically at the Euler Archive, at www.eulerarchive.org. This paper is E26 in the Enestr̈om index.

†Date of translation: January 8, 2005. Translated from the Latin by Jordan Bell, 2nd year undergraduate in Honours Mathematics, School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada. Email: jbell3@connect.carleton.ca

for a demonstration of this extraordinary theorem to be given by Wallis and other English mathematicians. Indeed, although he confesses not to have a demonstration of this himself, nevertheless he claimed it to be certain. He recommended as easy work that it would be especially useful to produce a large prime number given in this way, in so far as without this a universal theorem would be most difficult. This is taken from a business letter in the second volume of his works, as the penultimate letter; furthermore, it is also recorded in the works of Fermat himself, p. 115, as the following: "It appears in my writings that the numbers made by a quadrature of two and increased by unity are always prime numbers, and analysis of this so far has of course shown the primes 3, 5, 17, 257, 65537, and without much difficulty the truth of this theorem will have been extended to infinity."

The truth of this theorem is clear, as I have already said, if for m is set 1, 2, 3 and 4, which produce the numbers 5, 17, 257 and 65537, all of which appear in the table of prime numbers. But not knowing how the ones that follow turns out, I have observed this for a time, and by a long route delivered this number to be able to be divided by 641, such that at once the way is cleared for any other to be attacked. Indeed $2^{2^5} + 1 = 2^{32} + 1 = 4294967297$. From this it can be understood for the theorem to be mistaken with this and also some of the others that follow, and because of this problem, this is now indeed not a solution for finding a larger prime number.

I will now consider the formula $2^n - 1$, which has divisors whenever n is not a prime number, and indeed not only $2^n - 1$ but also $a^n - 1$. But if n is a prime number it can be seen that $2^n - 1$ always is produced such that no one is prepared to profess knowledge of this quantity, with it possible for such to be easily refuted. For and in fact $2^{11} - 1$ i.e. 2047 has the divisors 23 and 89, and $2^{23} - 1$ is able to be divided by 47. I see moreover that the celebrated Wolff not only did not give attention to this in the second edition of his *Elementa Matheseos* where he investigates perfect numbers and numbers 2047 among the prime numbers, but he even has 511, that is, $2^9 - 1$ of such a kind, with it however divisible by $2^3 - 1$ i.e. 7. He moreover gives $2^{n-1}(2^n - 1)$ as a perfect number whenever $2^n - 1$ is prime, but therefore also n ought to be a prime number. I have judged the work worthwhile of noting the cases where n is such that $2^n - 1$ is not a prime number. I have discovered it always to come about that if $n = 4m - 1$ and that also $8m - 1$ is a prime number, then $2^n - 1$ is able to be divided by $8m - 1$. This excludes the following cases of 11,

23, 83, 131, 179, 191, 239, etc., which when substituted for n render $2^n - 1$ a composite number. Even still, not all the remaining prime numbers are successfully put as n, for aside from these many more are to be removed, and in this way I have observed for $2^{37} - 1$ to be able to be divided by 223, $2^{43} - 1$ by 431, $2^{39} - 1$ by 1103, $2^{73} - 1$ by 439; however, it is impossible to exclude all powers. Nevertheless, I intend to consider cases besides those that have been discussed, all the prime numbers less than 50 and perhaps as much as 100 that make $2^{n-1}(2^n - 1)$ a perfect number; from the following numbers 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47, put in place of n, 11 perfect numbers come forth. I have drawn these observations from a certain theorem which is not inelegant, a demonstration of which I do not however have, though in fact I am most certain of the truth of this. The theorem is that $a^n - b^n$ is always able to be divided by $n + 1$ if $n + 1$ is a prime number and a and b are not able to be divided by it; however I believe that a demonstration of this is more difficult, because it is not true unless $n + 1$ is a prime number. From this it at once follows that $2^n - 1$ is always able to be divided by $n + 1$ if $n + 1$ is a prime number, with all prime numbers odd aside from 2, and by the conditions of the theorem, because $a = 2$ it is not possible for this to be applied; $2^{2m} + 1$ will always be able to be divided by $2m + 1$ if $2m + 1$ is a prime number. Therefore $2^m + 1$ or $2^m - 1$ will always be able to be divided by $2m + 1$. Moreover, I have also discovered $2^m + 1$ to be able to be divided if $m = 4p+1$ or $4p+2$, whereas $2^m - 1$ will have the divisor $2m+1$ if $m = 4p$ or $4p - 1$. I have produced from this many other theorems which are not less elegant, and I think that this will have to be considered more, because neither can these be clearly demonstrated, but the propositions which follow are seen to follow in an excellent way from this.

Theorem I. If n is a prime number, all powers with the exponent $n - 1$ when divided by n leave either nothing or 1.

Theorem II. By fixing n as a prime number, for all powers, $n^{m-n}(n - 1)$ divided by n^m leaves over either 0 or 1.

Theorem III. When m, n, p, q, etc. are unequal prime numbers and A is the smallest that is divided by each of them less unity, as $m - 1$, $n - 1$, $p - 1$, $q - 1$, etc., I offer that each one set with A its exponent a^A returns either 0 or 1 when divided by $mnpq$, unless a is able to be divided by one of the numbers m, n, p, q, etc.

Theorem IV. By denoting with $2n+1$ a prime number, 3^n+1 will be able to be divided by $2n+1$ if either $n=6p+2$ or $n=6p+3$. On the other hand 3^n-1 will be able to be divided by $2n+1$ if $n=6p$ or $n=6p-1$.

Theorem V. 3^n+2^n is able to be divided by $2n+1$ if n is equal to either $12p+3$, $12p+5$, $12p+6$ or $12p+8$. Moreover, 3^n-2^n is able to be divided by $2n+1$ if n is equal to either $12p$, $12p+2$, $12p+9$ or $12p+11$.

Theorem VI. Under these very same conditions for 3^n+2^n, 6^n+1 is also able to be divided by $2n+1$, and 6^n-1 too under those for 3^n-2^n.