Observationes de Theoremate Quodam Fermatiano, Aliisque ad Numeros Primos Spectantibus

Auctore Leonh. Eulero

Observations on a Certain Theorem of Fermat and on Others Regarding Prime Numbers

Translated by David Zhao
Department of Computer Science
University of Texas at Austin

Abstract

According to the records, this was presented to the St. Petersburg Academy on September 26, 1732. It was originally published in *Commentarii academiae scientiarum Petropolitanae* 6, 1738, pp. 103-107, and reprinted in *Comment. acad. sc. Petrop.* 6, ed. nova, Bononiae 1743, pp. 98-102 and again in *Commentat. arithm.* 1, 1849, pp. 1-3. It appears in the *Opera Omnia* as Series 1, Volume 2, pp. 1 - 5, and its Eneström index is E26.

This translation was finished on December 17, 2006.

Notum est hanc quantitatem $a^n + 1$ semper habere divisores, quoties n sit numerus impar, vel per imparem praeter unitatem divisibilis. Namque $a^{2m+1} + 1$ dividi potest per $a + 1$ et $a^{p(2m+1)} + 1$ per $a^p + 1$, quicunque etiam numerus loco a substituatur. Contra vero si n fuerit eiusmodi numerus, qui per nullum numerum imparem nisi unitatem dividi possit, id quod evenit, quando n est dignitas binarii, nullus numeri $a^n + 1$ potest assignari divisor. Quamobrem si qui sunt numeri primi huius formae $a^n + 1$, ii omnes comprehendantur necesse est in hac forma $a^{2^m} + 1$. Neque tamen ex hoc potest concludi $a^{2^m} + 1$ semper exhibere numerum primum quicquid sit a; primo enim perspicuum est, si a sit numerus impar, istam formam divisorem habiturum 2.

Deinde quoque, etiamsi a denotet numerum parem, innumeri tamen dantur casus, quibus numerus compositus prodit. Ita haec saltem formula $a^2 + 1$ potest dividi per 5, quoties est $a = 5b \pm 3$, et $30^2 + 1$ potest dividi per 17, et $50^2 + 1$ per 41. Simili modo $10^4 + 1$ habet divisorem 73; $63^8 + 1$ habet divisorem 17, et $6^{128} + 1$ est divisibilis per 257. At huius formae $2^{2^m} + 1$ quantum ex tabulis numerorum primorum, quae quidem non ultra 100000 extenduntur, nullus detegitur casus, quo divisor aliquis locum habeat.

Hac forte aliisque rationibus *Fermatius* adductus enunciare non dubitavit $2^{2^m} + 1$ semper esse numerum primum, hocque ut eximium theorema *Wallisio* aliisque Matehmaticis Anglis demonstrandum proposuit. Ipse quidem fatetur se eius demonstrationem non habere, nihilo tamen minus asserit esse verissimum. Utilitatem eius autem hanc potissimum praedicat, quod eius ope facile sit numerum primum quovis dato maiorem exhibere, id quod sine huiusmodi universali theoremate

It is known that the quantity $a^n + 1$ always has divisors, whenever n is an odd number or is divisible by an odd number other than unity. For $a^{2m+1} + 1$ can be divided by $a+1$ and $a^{p(2m+1)} + 1$ by $a^p + 1$, for whatever number is substituted for a. But on the other hand, if n is a number that cannot be divided by an odd number except unity, it turns out that if n is a power of two, no number $a^n + 1$ can be assigned its divisor. For this reason, if any numbers of the form $a^n + 1$ are prime, it is necessary that they be of the form $a^{2^m} + 1$. However, it cannot be concluded from this that $a^{2^m} + 1$ always produces a prime number, whatever the value of a; since it is first clear that if a is an odd number, then that form will have 2 as a divisor.

But even if a denotes a prime number, there are still innumerable cases, in which a composite number arises. So at least the formula $a^2 + 1$ can be divided by 5, whenever $a = 5b \pm 3$, and $30^2 + 1$ can be divided by 17, and $50^2 + 1$ by 41. Likewise, $10^4 + 1$ has 73 as a divisor; $63^8 + 1$ has 17 as a divisor, and $6^{128} + 1$ is divisible by 257. And how many of the form $2^{2^m} + 1$ from the tables of prime numbers, which still extend no more than 100,000, no case exists, in which any divisor has a place.

As it happened, led by this and other reasons, Fermat did not hesitate to declare that $2^{2^m} + 1$ is always a prime number, and proposed it to Wallis and to other English mathematicians as a distinguished theorem to be proven. Even he confessed that he did not have its proof, although he nevertheless asserted it to be very true. However, he advocated this utility of it above all, that with its aid it is easy to exhibit a prime number greater than any given number, which would be

foret difficillimum. Leguntur haec in *Wallisii* Commercio Epistolico Tomo Eius Operum secundo inserto, epistola penultima. Extant etiam in ipsius *Fermatii* operibus p. 115 sequentia. "Cum autem numeros a binario quadratice in se ductos et unitate auctos esse semper numeros primos apud me constet, et iam dudum Analystis illius theorematis veritas fuerit significata nempe esse primos 3, 5, 17, 257, 65537, etc. in infinit. nullo negotio etc."

Veritas istius theorematis elucet, ut iam dixi, si pro m ponatur 1, 2, 3 et 4, prodeunt enim hi numeri 5, 17, 257, et 65537, qui omnes inter numeros primos in tabula reperiuntur. Sed nescio, quo fato eveniat, ut statim sequens nempe $2^{2^5}+1$ cesset esse numerus primus, observavi enim his diebus longe alia agens posse hunc numerum dividi per 641, ut cuique tentanti statim patebit. Est enim $2^{2^5}+1 = 2^{32}+1 = 4294967297$. Ex quo intelligi potest, theorema hoc etiam in aliis, qui sequntur, casibus fallere, et hanc ob rem problema de inveniendo numero primo quovis dato maiore etiam nunc non esse solutum.

Considerabo nunc etiam formulam $2^n - 1$, quae quoties n non est numerus primus, habet divisores neque tantum $2^n - 1$ sed etiam $a^n - 1$. Sed si n sit numerus primus videri posset etiam $2^n - 1$ semper talem exhibere: hoc tamen asseuerare nemo est ausus quantum scio, cum tam facile potuisset refelli. Namque $2^{11} - 1$ i.e. 2047 divisores habet 23 et 89 et $2^{23} - 1$ dividi potest per 47. Video autem Cel. *Wolfium* non solum hoc in Elem. Matheseos editione altera non advertisse, ubi numeros perfectos investigat, atque 2047 inter primos numerat; sed etiam 511 seu $2^9 - 1$ pro tali habet, cum tamen sit divisibilis per $2^3 - 1$ i.e. 7.

Dat autem $2^{n-1}(2^n - 1)$ numerum perfectum, quoties $2^n - 1$ est primus, debet ergo etiam n esse numerus primus. Operae igitur pretium fore existimavi eos notare casus, quibus $2^n - 1$ non est numerus primus, quamvis n sit talis. Inveni autem hoc semper fieri, si sit $n = 4m - 1$, atque $8m - 1$ fuerit numerus primus, tum enim $2^n - 1$ semper poterit dividi per $8m - 1$. Hinc excludendi sunt casus sequentes, 11, 23, 83, 131, 179, 191, 239, etc. qui numeri pro n substituti reddunt $2^n - 1$ numerum compositum.

Neque tamen reliqui numeri primi omnes loco n positi satisfaciunt, sed plures insuper excipiuntur, sic observavi $2^{37} - 1$ dividi posse per 223, $2^{43} - 1$ per 431, $2^{29} - 1$ per 1103, $2^{73} - 1$ per 439, omnes tamen excludere non est in potestate. Attamen asserere audeo

very difficult without a universal theorem of this kind. This was written in the penultimate letter in the second inserted volume of his epistolary correspondence with Wallis. Indeed, the following is found on page 115 in the works of Fermat himself. "However, since the numbers taken from the powers of two and increased by unity seem to me always to be prime numbers, and since long ago the truth of the theorem was certainly known in analysis that 3, 5, 17, 257, 65537, etc. to infinity, are prime, with no trouble, etc."

The truth of this theorem is clear, as I have already said, if 1, 2, 3 and 4 are taken for m, since the numbers 5, 17, 257 and 65537 are produced, which are found among the prime numbers in the table. But I do not know by what fate it became clear, that the number immediately following, $2^{2^5}+1$, ceases to be a prime number, for I have observed after working for many days that this number can be divided by 641, as it will immediately be clear to anyone who tries. Indeed, $2^{2^5}+1 = 2^{32}+1 = 4294967297$. From this it can be seen that this theorem also fails in some cases, which follows, and for this reason the problem of finding a prime number greater than a given one is still not yet solved.

I will now also consider the formula $2^n - 1$. Whenever n is not a prime number, not only $2^n - 1$ but also $a^n - 1$ has divisors. But if n is a prime number still $2^n - 1$ can be seen to exhibit one, although no one has ventured to assert this insofar as I am aware, since it could easily have been refuted. Moreover, I see that the celebrated Wolf not only did not perceive this in the other edition of the *Elements of Mathematics*, where he investigates perfect numbers, and enumerates 2047 primes; but also has 511 or $2^9 - 1$ as such, even though it is divisible by $2^3 - 1$, i.e., 7.

However, $2^{n-1}(2^n - 1)$ gives a perfect number, whenever $2^n - 1$ is prime, and therefore n ought to be a prime number. I believe therefore that it will be of value to this work to note those cases, in which $2^n - 1$ is not a prime number, even though n is such. I discovered however that it always turns out that if $n = 4m - 1$ and $8m - 1$ is a prime number, then $2^n - 1$ can always be divided by $8m - 1$. The following cases are then excluded from this, 11, 23, 83, 131, 179, 191, 239, etc., which make $2^n - 1$ a composite number when substituted for n.

However, not all of the remaining prime numbers taken in the place of n prove sufficient, but but more in addition are excepted, as I have observed that $2^{37} - 1$ can be divided by 223, $2^{43} - 1$ by 431, $2^{73} - 1$ by 439, although it is not possible to exclude everything. But

praeter hos casus notatos, omnes numeros primos minores quam 50, et forte quam 100, efficere $2^{n-1}(2^n-1)$ esse numerum perfectum, sequentibus numeris pro n positis, 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47, unde 11 proveniunt numeri perfecti.

Deduxi has observationes ex Theoremate quodam non ineleganti, cuius quidem demonstrationem quoque non habeo, verum tamen de eius veritate sum certissimus. Theorema hoc est, $a^n - b^n$, semper potest dividi per $n+1$, si $n+1$ fuerit numerus primus atque a et b non possint per eum dividi; eo autem difficiliorem puto eius demonstrationem esse, quia non est verum nisi $n+1$ sit numerus primus.

Ex hoc statim sequitur $2^n - 1$ semper dividi posse per $n+1$, si fuerit $n+1$ numerus primus, seu cum omnis primus sit impar praeter 2, hicque ob conditiones theorematis, quia est $a = 2$, non possit adhiberi, poterit $2^{2m} - 1$ semper dividi per $2m+1$ si $2m+1$ sit numerus primus. Quare etiam vel $2^m + 1$ vel $2^m - 1$ dividi poterit per $2m+1$. Deprehendi autem $2^m + 1$ posse dividi, si fuerit $m = 4p+1$ vel $4p+2$, at $2^m - 1$ habebit divisorem $2m+1$, si $m = 4p$ vel $4p-1$. Haec persecutus in multa alia incidi theoremata non minus elegantia, quae eo magis aestimanda esse puto, quod vel demonstrari prorsus nequeant, vel ex eiusmodi propositionibus sequantur, quae demonstrari non possunt, primaria igitur hic adiungere visum est.

Theorema I. Si fuerit n numerus primus, omnis potentia exponentis $n-1$ per n divisa vel nihil vel 1 relinquit.

Theorema II. Manente n numero primo, omnis potentia, cuius exponens est $n^{m-1}(n-1)$, divisa per n^m vel 0 vel 1 relinquit.

Theorema III. Sint m, n, p, q, etc. numeri primi inaequales, sitque A minimus communis dividuus eorum unitate minutorum, puta ipsorum $m-1$, $n-1$, $p-1$, $q-1$, etc. his positis dico omnem potentiam exponentis A ut a^A divisam per $mnpq$ etc. vel 0 vel 1 relinquere, nisi a dividi possit per aliquem horum numerorum, m, n, p, q, etc.

Theorema IV. Denotante $2n+1$ numerum primum poterit $3^n + 1$ dividi per $2n+1$, si sit vel $n = 6p+2$ vel $n = 6p+3$: at $3^n - 1$ dividi poterit per $2n+1$ si sit vel $n =$ vel $6p$ vel $n = 6p-1$.

Theorema V. $3^n + 2^n$ potest dividi per $2n+1$ si sit $n =$ vel $12p+3$, vel $12p+5$, vel $12p+6$, vel $12p+8$. Atque $3^n - 2^n$ potest dividi per $2n+1$, si sit $n =$ vel $12p$ vel $12p+2$, vel $12p+9$, vel $12p+11$.

yet I will venture to asser that except for these noted cases, all prime numbers less than 50, greater than 100, and of the form $2^{n-1}(2^n-1)$ are perfect numbers, with the following numbers taken for n: 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47, and so 11 perfect numbers come about.

I have deduced these observations from a certain not inelegant theorem, whose proof indeed I also do not have, but nevertheless concerning its truth I am most certain. The theorem is this, that $a^n - b^n$ can always be divided by $n+1$, if $n+1$ is a prime number and a and b cannot be divided by it; but so far I think its proof is more difficult, because it is not true unless $n+1$ is a prime number.

From this it immediately follows that $2^n - 1$ can always be divided by $n+1$, if $n+1$ is a prime number; or, since every prime number except two is odd, and due to the conditions of the theorem, because $a = 2$, it cannot be applied, $2^{2m} - 1$ can always be divided by $2m+1$ if $2m+1$ is a prime number. Thus, either $2^m + 1$ or $2^m - 1$ can be divided by $2m+1$. Moreover, I have perceived that $2^m + 1$ can be divided, if m is $4p+1$ or $4p+2$, and $2^m - 1$ has $2m+1$ as a divisor, if m is $4p$ or $4p-1$. Having followed this into many others, I have fallen into theorems no less elegant, but which I think should be judged more so, because either they cannot be proved straightforwardly, or they follow from propositions of the sort that cannot be proven, and therefore seemed to connect to distinguished ones.

Theorem I. If n is a prime number, every number raised to power $n-1$ and divided by n leaves either 0 or 1.

Theorem II. Letting n be a prime number, every number raised to power $n^{m-1}(n-1)$ and divded by n^m leaves either 0 or 1.

Theorem III. Let m, n, p, q, etc. be unequal prime numbers, and let A be least common divisor of them decreased by one, think of them as $m-1$, $n-1$, $p-1$, $q-1$, etc. With these values, I say that every number raised to A, or a^A, divided by $mnpq$ etc. leaves either 0 or 1, unless a can be divided any of the numbers m, n, p, q, etc.

Theorem IV. Letting $2n+1$ be a prime number, 3^n+1 can be divided by $2n+1$, if either $n = 6p+2$ or $n = 6p+3$: and $3^n - 1$ can be divided by $2n+1$ if either $n = 6p$ or $n = 6p-1$.

Theorem V. $3^n + 2^n$ can be divided by $2n+1$ if n is $12p+3$, $12p+5$, $12p+6$ or $12p+8$. And $3^n - 2^n$ can be divided by $2n+1$, if n is $12p$, $12p+2$, $12p+9$ or $12p+11$.

Theorema VI. Sub iisdem conditionibus quibus $3^n + 2^n$ poterit etiam $6^n + 1$ dividi per $2n + 1$; atque $6^n - 1$ sub iisdem, quibus $3^n - 2^n$.

Theorem VI. Under the same conditions by which $3^n + 2^n$ can, also $6^n + 1$ can be divided by $2n + 1$; and $6^n - 1$ under the same conditions as $3^n - 2^n$.