Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio

Auctore L. Eulero

A Proof of Certain Theorems Regarding Prime Numbers

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

Abstract

This paper contains the first published proof of Fermat's Little Theorem, that $a^{p-1} \equiv 1 \pmod{p}$, for all a relatively prime to p. Euler's proof is by induction on a, i.e., he begins by showing that $2^{p-1} \equiv 1 \pmod{p}$, for $p \neq 2$, then shows that $3^{p-1} \equiv 1 \pmod{p}$, for $p \neq 3$, and concludes that $a^{p-1} \equiv 1 \pmod{p}$, for all a relatively prime to p. It is important to note that this method of induction stands in stark contrast to what Euler calls 'induction', by which he means Fermat's habit of asserting the truth of conjectures based on 'inducting' from examples, and which he himself criticizes in the introduction. That is, Euler's method of proof is a genuine case of induction as it is known to us today.

According to the records, this paper was presented to the St. Petersburg Academy on August 2, 1736. It was later published in *Commentarii academiae scientiarum Petropolitanae* 8, 1741, pp. 141–146, and appears in Series 1, Volume 2, pp. 33–37 of the *Opera Omnia.* Its Eneström index is E54.

This translation was completed on August 30, 2004.

§1. Plurima quondam a Fermatio theoremata arithmetica sed sine demonstrationibus in medium sunt prolata, in quibus, si vera essent, non solum eximiae numerorum proprietates continerentur, verum etiam ipsa numerorum scientia, quae plerumque analyseos limites excedere videtur, vehementer esset promota. Quamvis autem iste insignis Geometra de pluribus, quae proposuit, theorematis asseruerit se ea vel demonstrare posse, vel saltem de eorum veritate esse certum: tamen nusquam, quantum mihi constat, demonstrationes exposuit. Quin potius Fermatius videtur maximam theorematum suorum numericorum partem per inductionem esse assecutus, quippe quae via fere unica ad huiusmodi proprietates eruendas patere videatur. At vero quam parum inductionibus in hoc negotio tribui possit pluribus exemplis possem declarare; ex quibus autem unicum ab ipso Fermatio desumtum attulisse sufficiat.

Loquor nimirum de illo theoremate, cuius falsitatem iam aliquot ab hinc annis ostendi, quo Fermatius asserit omnes numeros hac forma $2^{2^n}+1$ comprehensos esse numeros primos. Ad veritatem autem huius propositionis evincendam inductio omnino sufficere videatur. Nam praeterquam quod omnes isti numeri minores quam 100000 sint revera primi, demonstrari etiam facile potest nullum numerum primum, 600 non excedentem hanc formulam $2^{2^n}+1$, quantumvis magnus etiam numerus pro n substituatur, metiri. Cum tamen nihilominus constet hanc propositionem veritati non

§1. Many arithmetical theorems, though without proofs, were once brought to light by Fermat which (if they were true) not only would contain exceptional properties of numbers, but also would greatly promote the science of numbers itself, which seems for the most part to exceed the limits of analysis. However, although the famous geometer claimed, concerning many theorems that he proposed, that he either could prove them or that he was at least certain of their truth: nevertheless he never produced proofs for them at any time, insofar as I am aware. But on the other hand, Fermat seems to have grasped a large part of his numerical theorems through induction, which indeed seems to be an almost unique method for bringing to light properties of this kind. However, I could also speak of how little induction on many examples can yield in this matter; which was nevertheless sufficient for Fermat himself for eliciting unique observations.

I am speaking no less about that theorem, whose falsity I already pointed out several years ago, in which Fermat asserted that all numbers expressible in the form $2^{2^n}+1$ are prime numbers. However, induction may have seemed altogether to suffice for establishing the truth of this proposition. For apart from the fact that all numbers of that form less than 100,000 are in fact prime, it can still easily be proved that no prime number not exceeding 600 divides any number of the form $2^{2^n}+1$, for however large a number is taken for n. Nevertheless, although it is clear that this proposition esse consentaneam, facile intelligitur, quantum inductio in huiusmodi speculationibus valeat.

§2. Hanc ob rationem omnes huiusmodi numerorum proprietates, quae sola inductione nituntur, tam diu pro incertis habendas esse arbitror, donec illae vel apodicticis demonstrationibus muniantur vel omnino refellantur. Non plus etiam illis theorematis, quae ego ipse illi schediasmati, in quo de memorato theoremate Fermatiano numerisque perfectis tractavi, subieci, fidendum esse censerem, si tantum inductionibus, qua via quidem sola tum temporis ad eorum cognitionem perveni, niterentur. Nunc vero, postquam peculiari methodo demonstrationes horum theorematum firmissimas sum adeptus, de veritate eorum non amplius est dubitandum. Quocirca tam ad veritatem illorum theorematum ostendendam, quam ad methodum ipsam, quae forte etiam in aliis numerorum investigationibus utilitatem afferre poterit, in hac dissertatione meas demonstrationes explicare constitui.

§3. Propositio autem, quam hic demonstrandum suscepi, est sequens:

Significante p numerum primum, formula $a^{p-1}-1$ semper per p dividi poterit, nisi a per p dividi queat.

Ex hac enim propositione demonstrata sponte relinquorum theorematum veritas fluit. Casum quidem formulae propositae, quo est $a = 2$, iam ab aliquo tempore demonstratum dedi; attamen tum demonstrationem ad generalem formulam extendere non licuit. Quamobrem primo huius casus probationem afferre conveniet, quo transitus ad generaliora eo facilior reddatur. Demonstranda igitur erit sequens propositio:

Significante p numerum primum imparem quemcunque, formula $2^{p-1} - 1$ semper per p dividi poterit.

Demonstratio.

Loco 2 ponatur $1 + 1$, eritque $(1 + 1)^{p-1} = 1 + \frac{p-1}{1} + \frac{p-1}{1}\frac{p-2}{2} + \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3} + \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4}$ etc. cuius seriei terminorum numerus est $= p$ et proinde impar. Praeterea quilibet terminus, quamvis habeat fractionis speciem dabit numerum integrum; quisque enim numerator, uti satis constat, per suum denominatorem dividi potest. Demto igitur seriei termini primo 1 erit $(1+1)^{p-1}-1 = 2^{p-1}-1 = \frac{p-1}{1}+\frac{p-1}{1}\frac{p-2}{2}+\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}+\frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4}+$ etc. quorum numerus est $= p - 1$ et propterea par. Colligantur igitur bini quique ter-

is not consistent with truth, it is still easy to see how much induction can be of use in speculations of this sort.

§2. For this reason, all such properties of numbers, which rested upon induction alone, I now judge to have uncertainty, until they are either supplied with clearly valid proofs or altogether refuted. I have submitted to judgment no more than those theorems, which I myself judge to be resting on extempore speech, in which I dealt with the aforementioned theorem of Fermat and with perfect numbers, if they should rest only on induction, by which way alone, certainly, I arrived at recognizing them in the first place. But now, as I have attained the firmest proofs of these theorems by my own method, there can be no more doubt concerning their truth. And on this account, in order to establish the truth of those theorems, which is a method in itself and which may even bear usefulness in other investigations of numbers, I have resolved to set forth my proofs in this paper.

§3. Now, the proposition, which I am prepared to prove, is the following:

Letting p denote a prime number, the formula $a^{p-1} - 1$ can always be divided by p, unless a can be divided by p.

Now, the truth of the remaining theorems follows if this proposition is proved. Indeed, I already gave the proof of the case of the proposed statement in which $a = 2$ at an earlier time; but nonetheless it was not clear that the proof would extend to the general case. So for this reason, it is fitting to offer an examination of this case first, whereby the transition to the more general case would be easier from there. Therefore, the following proposition will be proved:

Letting p be any odd prime number, the formula $2^{p-1} - 1$ can always be divided by p.

Proof.

In place of 2, take $1 + 1$, and the formula becomes $(1 + 1)^{p-1} = 1 + \frac{p-1}{1} + \frac{p-1}{1}\frac{p-2}{2} + \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3} + \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4}$, and so on. The number of terms of this series is equal to p and consequently odd. For this reason, even though every term has the form of a fraction, each still gives a whole number; because each numerator, as is clearly sufficient, can be divided by its denominator. Then take away the initial term of 1 from the series to obtain: $(1 + 1)^{p-1} - 1 = 2^{p-1} - 1 = \frac{p-1}{1} + \frac{p-1}{1}\frac{p-2}{2} + \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3} + \frac{p-1}{1}\frac{p-2}{2}\frac{p-3}{3}\frac{p-4}{4} + \dots$. So mini in unam summam, quo terminorum numerus fiat duplo minor; erit $2^{p-1}-1 = \frac{p}{1}\frac{p-1}{2} + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\frac{p-3}{4} + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\frac{p-3}{4}\frac{p-4}{5}\frac{p-5}{6} +$ etc. cuius seriei ultimus terminus ob p numerum imparem erit $\frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\cdots\frac{2}{p-1} = p$. Apparet autem singulos terminos per p esse divisibiles, nam, cum p sit numerus primus et maior quam ullus denominatorum factor, nusquam divisione tolli poterit. Quamobrem si fuerit p numerus primus impar, per illum semper $2^{p-1}-1$ dividi poterit. Q.E.D.

Aliter

Si $2^{p-1}-1$ per numerum primum p dividi potest, dividi quoque poterit eius duplum 2^p-2 et vicissim. At est $2^p = (1+1)^p = 1 + \frac{p}{1} + \frac{p}{1}\frac{p-1}{2} + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\cdots\frac{p}{1} + 1$. Quae series terminis primo et ultimo truncata dat $\frac{p}{1} + \frac{p}{1}\frac{p-1}{2} + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3} + \cdots \frac{p}{1}\frac{p-1}{2} + p = 2^p - 2$. Perspicuum autem est istius seriei quemvis terminum per p esse divisibilem, si quidem p fuerit numerus primus. Quamobrem etiam semper 2^p-2 per p et propterea quoque $2^{p-1}-1$ per p dividi poterit, nisi sit $p=2$. Q.E.D.

§4. Cum igitur $2^{p-1}-1$ per numerum primum imparem p dividi queat; facile intelligitur per p quoque dividi posse hanc formulam $2^{m(p-1)}-1$ denotante m numerum quemcunque integrum. Quare sequentes formulae quoque omnes $4^{p-1}-1$, $8^{p-1}-1$, $16^{p-1}-1$ etc. per numerum primum p dividi poterunt. Demonstrata igitur est veritas theorematis generalis pro omnibus casibus, quibus a est quaevis binarii potestas, et p quicunque numerus primus praeter binarium.

§5. Demonstrato nunc hoc theoremate eius ope sequens quoque demonstrabimus.

Theorema.

Denotante p numerum primum quemcunque praeter 3, per illum semper haec formula $3^{p-1}-1$ dividi poterit.

Demonstratio.

Si $3^{p-1}-1$ per numerum primum p excepto 3 dividi potest, tum 3^p-3 per p dividi poterit, quoties p fuerit numerus primus quicunque, et vicissim. Est vero $3^p = (1+2)^p = 1 + \frac{p}{1}\cdot 2 + \frac{p}{1}\frac{p-1}{2}\cdot 4 + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\cdot 8 \cdots + \frac{p}{1}\cdot 2^{p-1} + 2^p$, cuius seriei singuli termini praeter primum et ultimum per p dividi poterunt, si quidem p fuerit numerus primus. Per p igitur dividi potest ista formula 3^p-2^p-1, quae aequalis est huic 3^p-3-2^p+2. At 2^p-2 semper per p numerum primum dividi potest; ergo etiam 3^p-3. Quare $3^{p-1}-1$ semper per p dividi potest, quoties p fuerit numerus primus excepto 3. Q.E.D.

the number of terms is $p-1$ and therefore even. Now, collect each pair of terms into one sum, so that the number of terms is less by a half, to obtain: $2^{p-1}-1 = \frac{p}{1}\frac{p-1}{2} + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\frac{p-3}{4} + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\frac{p-3}{4}\frac{p-4}{5}\frac{p-5}{6} +$, and so on. Since p is an odd number, the last term of this series is $\frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\cdots\frac{2}{p-1} = p$. So it is clear that each term is divisible by p, because, as p is a prime number and greater than every factor in the denominators, it can never be removed by division. For this reason, if p is an odd prime number, $2^{p-1}-1$ can always be divided by it. □

Or Alternately:

If $2^{p-1}-1$ can be divided by a prime number, then its alternate form 2^p-2 can in turn also be divided. And $2^p = (1+1)^p = 1 + \frac{p}{1} + \frac{p}{1}\frac{p-1}{2} + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\cdots\frac{p}{1} + 1$. And this series, with the first and last terms removed, gives $\frac{p}{1} + \frac{p}{1}\frac{p-1}{2} + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3} + \cdots \frac{p}{1}\frac{p-1}{2} + p = 2^p - 2$. Now it is clear that each term of this series is divisible by p, if indeed p is a prime number. For this reason, 2^p-2 can also always be divided by p, and accordingly so can $2^{p-1}-1$, unless $p=2$. □

§4. Therefore since $2^{p-1}-1$ can be divided by an odd prime number p; it is easy to see that the formula $2^{m(p-1)}-1$ can also be divided by p, with m as any whole number. For this reason, all the following formulas: $4^{p-1}-1$, $8^{p-1}-1$, $16^{p-1}-1$, and so on, can be divided by a prime number p. Therefore the truth of the general theorem has been proven for all cases, in which a is any power of two, and p is any prime number except two.

§5. Now with this theorem proved we prove the following with its help.

Theorem.

If p is any prime number except 3, then $3^{p-1}-1$ can always be divided by it.

Proof.

If $3^{p-1}-1$ can be divided by any prime number p except 3, then 3^p-3 can be divided by p, whenever p is any prime number, and in turn. But $3^p = (1+2)^p = 1 + \frac{p}{1}\cdot 2 + \frac{p}{1}\frac{p-1}{2}\cdot 4 + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}\cdot 8 \cdots + \frac{p}{1}\cdot 2^{p-1} + 2^p$. Each term of this series can be divided by p, except for the first and last, provided that p is a prime number. Therefore, the formula 3^p-2^p-1 can be divided by p, and this is equal to 3^p-3-2^p+2. And 2^p-2 can always be divided by p; therefore so can 3^p-3. For this reason, $3^{p-1}-1$ can always be divided by p, whenever p is a prime number except 3. □

§6. Eodem modo ulterius progredi liceret ab hoc ipsius a valore ad sequentem unitate maiorem. Sed quo demonstrationem generalis theorematis magis concinnam magisque genuinam efficiam, sequens praemitto.

Theorema.
Denotante p numerum primum, si $a^p - a$ per p dividi potest; tum per idem p quoque formula $(a+1)^p - a - 1$ dividi poterit.

Demonstratio.
Resolvatur $(1+a)^p$ consueto more in seriem, erit $(1+a)^p = 1 + \frac{p}{1}a + \frac{p}{1}\frac{p-1}{2}a^2 + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}a^3 + \cdots \frac{p}{1}a^{p-1} + a^p$; cuius seriei singuli termini per p dividi possunt praeter primum et ultimum; si quidem p fuerit numerus primus. Quamobrem $(1+a)^p - a^p - 1$ divisionem per p admittet; haec autem formula congruit cum hac $(1+a)^p - a - 1 - a^p + a$. At $a^p - a$ per hypothesin per p dividi potest, ergo et $(1+a)^p - a - 1$. Q.E.D.

§7. Cum igitur, posito quod $a^p - a$ per p numerum primum dividi queat, per p quoque haec formula $(a+1)^p - a - 1$ divisionem admittat; sequitur etiam $(a+2)^p - a - 2$, item $(a+3)^p - a - 3$ et generaliter $(a+b)^p - a - b$ per p dividi posse. Posito autem $a = 2$, quia $2^p - 2$, uti iam demonstravimus, per p dividi potest, perspicuum est formulam $(b+2)^p - b - 2$ divisionem per p admittere debere, quicunque integer numerus loco b substituatur. Metietur ergo p formulam $a^{p-1} - 1$, nisi fuerit $a = p$ vel multiplo ipsius p. Atque haec est demonstratio generalis theorematis, quam tradere suscepi.

§6. In the same manner as above, we may proceed from one value of a to the value larger by one. But in order to make the proof of the general theorem more concise and more genuine, I advance the following.

Theorem.
Letting p be a prime number, if $a^p - a$ can be divided by p, then $(a+1)^p - a - 1$ can also be divided by the same value p.

Proof.
If $(1+a)^p$ is expanded in the usual manner into a series, we have $(1+a)^p = 1 + \frac{p}{1}a + \frac{p}{1}\frac{p-1}{2}a^2 + \frac{p}{1}\frac{p-1}{2}\frac{p-2}{3}a^3 + \cdots \frac{p}{1}a^{p-1} + a^p$. The individual terms of this series can all be divided by p, except for the first and last, provided that p is a prime number. For this reason, $(1+a)^p - a^p - 1$ admits division by p; but this formula is equivalent to $(1+a)^p - a - 1 - a^p + a$. And $a^p - a$ can be divided by p by hypothesis, so therefore $(1+a)^p - a - 1$ also. □

§7. Therefore, since by assuming that $a^p - a$ can be divided by the prime number p, the formula $(a+1)^p - a - 1$ also admits division by p; it also follows that $(a+2)^p - a - 2$, $(a+3)^p - a - 3$ and in general $(a+b)^p - a - b$ can be divided by p. Then by setting $a = 2$, because $2^p - 2$, as we have proven, can be divided by p, it is clear that the formula $(b+2)^p - b - 2$ ought to admit division by p, for whatever whole number is substituted in place of b. Therefore p divides the formula $a^{p-1} - 1$, unless $a = p$ or a is a multiple of p. And so this is the proof of the general theorem, which I undertook to provide.