



1741

# Theorematum quorundam ad numeros primos spectantium demonstratio

Leonhard Euler

Follow this and additional works at: <https://scholarlycommons.pacific.edu/euler-works>

 Part of the [Mathematics Commons](#)

Record Created:

2018-09-25

## Recommended Citation

Euler, Leonhard, "Theorematum quorundam ad numeros primos spectantium demonstratio" (1741). *Euler Archive - All Works*. 54. <https://scholarlycommons.pacific.edu/euler-works/54>

This Article is brought to you for free and open access by the Euler Archive at Scholarly Commons. It has been accepted for inclusion in Euler Archive - All Works by an authorized administrator of Scholarly Commons. For more information, please contact [mgibney@pacific.edu](mailto:mgibney@pacific.edu).

THEOREMATVM  
 QVORVNDAM  
 AD  
 NUMEROS PRIMOS SPECTANTIVM  
 DEMONSTRATIO.

AVCTORE

*Leonh. Eulero.*

§. I.

**P**Lurima quondam a *Fermatio* theoremata arithmetica sed sine demonstrationibus in medium sunt prolata, in quibus, si vera essent, non solum existimiae numerorum proprietates contingerentur, verum etiam ipsa numerorum scientia, quae plerumque analyseos limites excedere videtur, vehementer esset promotum. 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 affectus, quippe quae via fere vnica ad huiusmodi proprietates eruendas patere videatur. At vero quam parum inductionibus in hoc negotio tribui possit pluribus exemplis possem declarare; ex quibus autem vnicum ab ipso *Fermatio* desumptum attulisse sufficiat. Lo-

quor 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 reuera 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 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 theorematibus, quae ego ipse illi schediasmati, in quo de memorato theoremate *Fermatiano* numerisque perfectis tractavi, subieci, fidenter 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

litem afferre poterit, in hac dissertatione meas demonstrationes explicare constitui.

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

*Significante p numerum primum, formula  $2^{p-1} - 1$  semper per p diuidi poterit, nisi a per p diuidi queat.*

Ex hac enim propositione demonstrata sponte reliquorum theorematum veritas fuit. 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 conueniet, quo transitus ad generaliora eo facilius reddatur. Demonstranda igitur erit sequens propositio:

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

### Demonstratio.

Loco 2 ponatur  $1+1$ , eritque  $(1+1)^{p-1} = 1 + \frac{p-1}{1} + \frac{(p-1)(p-2)}{1 \cdot 2} + \frac{(p-1)(p-2)(p-3)}{1 \cdot 2 \cdot 3} + \frac{(p-1)(p-2)(p-3)(p-4)}{1 \cdot 2 \cdot 3 \cdot 4}$  etc. cuius seriei terminorum numerus est  $=p$  et proinde impar. Praeterea quilibet terminus, quamuis habeat fractionis speciem dabit numerum integrum; quisque enim numerator, vti satis constat, per suum denominatorem diuidi potest. Demto igitur seriei termino primo 1 erit  $(1+1)^{p-1} - 1 = 2^{p-1} - 1 = \frac{2^{p-1}}{1} + \frac{(p-1)(p-2)}{1 \cdot 2} + \frac{(p-1)(p-2)(p-3)}{1 \cdot 2 \cdot 3} + \frac{(p-1)(p-2)(p-3)(p-4)}{1 \cdot 2 \cdot 3 \cdot 4} +$  etc. quorum

quorum numerus est  $= p - 1$  et propterea par. Colligantur igitur bini quique termini in unam summam, quo terminorum numerus fiat duplo minor; erit  $2^{p-1} - 1 = \frac{p(p-1)}{1 \cdot 2} + \frac{p(p-1)(p-2)(p-3)}{1 \cdot 2 \cdot 3 \cdot 4} + \frac{p(p-1)(p-2)(p-3)(p-4)(p-5)}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} + \text{etc.}$  cuius seriei ultimus terminus ob  $p$  numerum imparem erit  $\frac{p(p-1)(p-2) \dots (p-2)}{1 \cdot 2 \cdot 3 \dots (p-1)} = p$ . 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  $2^{p-1} - 1$  diuidi poterit. Q. E. D.

*Aliter*

Si  $2^{p-1} - 1$  per numerum primum  $p$  diuidi potest, diuidi quoque poterit eius duplum  $2^p - 2$  et vicissim. At est  $2^p = (1 + 1)^p = 1 + \frac{p}{1} + \frac{p(p-1)}{1 \cdot 2} + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} + \dots + \frac{p}{1} + 1$ . Quae series terminis primo et ultimo truncata dat  $\frac{p}{1} + \frac{p(p-1)}{1 \cdot 2} + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} + \dots + \frac{p(p-1)}{1 \cdot 2} + p = 2^p - 2$ . Perspicuum autem est istius seriei quemuis 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  $p$  diuidi poterit, nisi sit  $p = 2$ . Q. E. D.

§. 5. Cum igitur  $2^{p-1} - 1$  per numerum primum imparem  $p$  diuidi queat; facile intelligitur per  $p$  quoque diuidi 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.

etc. per numerum primum  $p$  diuidi poterunt. Demonstrata igitur est veritas theorematis generalis pro omnibus casibus, quibus  $a$  est quacuis binarii potestas, et  $p$  quicumque 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  $3^{p-1} - 1$  diuidi poterit.

Demonstratio.

Si  $3^{p-1} - 1$  per numerum primum  $p$  excepto 3 diuidi potest, tum  $3^p - 3$  per  $p$  diuidi poterit, quoties  $p$  fuerit numerus primus quicumque, et vicissim. Est vero  $3^p = (1 + 2)^p = 1 + \frac{p}{1} \cdot 2 + \frac{p(p-1)}{1 \cdot 2} \cdot 4 + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} \cdot 8 + \dots + \frac{p}{1} \cdot 2^{p-1} + 2^p$ , cuius seriei singuli termini praeter primum et vltimum per  $p$  diuidi poterunt, si quidem  $p$  fuerit numerus primus. Per  $p$  igitur diuidi 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 diuidi potest; ergo etiam  $3^p - 3$ . Quare  $3^{p-1} - 1$  semper per  $p$  diuidi potest, quoties  $p$  fuerit numerus primus excepto 3. Q. E. L.

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

Theorema.

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

Demonstratio.

Resoluator  $(1 + a)^p$  consueto more in seriem,  
erit  $(1 + a)^p = 1 + \frac{p}{1} a + \frac{p(p-1)}{1 \cdot 2} a^2 + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} a^3 +$   
 $\dots + \frac{p}{1} a^{p-1} + a^p$ ; cuius seriei singuli termini  
per  $p$  diuidi possunt praeter primum et vltimum; si  
quidem  $p$  fuerit numerus primus. Quamobrem  $(1 + a)^p$   
 $- a^p - 1$  diuisionem per  $p$  admittet; haec autem for-  
mula congruit cum hac  $(1 + a)^p - a - 1 - a^p + a$ . At  
 $a^p - a$  per hypothesin per  $p$  diuidi potest, ergo et  
 $(1 + a)^p - a - 1$ . Q. E. D.

§. 7. Cum igitur, posito quod  $a^p - a$  per  $p$  nu-  
merum primum diuidi queat, per  $p$  quoque haec for-  
mula  $(a + 1)^p - a - 1$  diuisionem admittat; sequitur  
etiam  $(a + 2)^p - a - 2$ , item  $(a + 3)^p - a - 3$  et ge-  
neraliter  $(a + b)^p - a - b$  per  $p$  diuidi posse. Posito  
autem  $a = 2$ , quia  $2^p - 2$ , vti iam demonstrauius,  
per  $p$  diuidi potest, perspicuum est formulam  $(b + 2)^p$   
 $- b - 2$  diuisionem per  $p$  admittere debere, quicumque  
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.