THEOREMATVM QVORVNDAM AD NVMEROS PRIMOS SPECTANTIVM DEMONSTRATIO.

AVCTORE
Leonh. Eulero.

§. 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. Quamuis 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 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* 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 euincendam 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 $2^{2^n}+1$, quantumuis 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 theorematis, quae ego ipſe illi ſchediasmati, in quo de memorato theoremate *Fermatiano* numerisque perfectis tractaui, ſubieci, fidendum eſſe cenſerem, ſi tantum inductionibus, qua via quidem ſola tum temporis ad eorum cognitionem perueni, 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 inueſtigationibus vtilitatem

litatem 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 *diuidi poterit, niſi* a *per* p *diuidi queat.*

Ex hac enim propoſitione demonſtrata ſponte reliquorum 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 conueniet, 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 *diuidi poterit.*

Demonſtratio.

Loco 2 ponatur $1+1$, eritque $(1+1)^{p-1}=1+\frac{p-1}{1}+\frac{(p-1)(p-2)}{1.\ 2}+\frac{(p-1)(p-2)(p-3)}{1.\ 2.\ 3.}+\frac{(p-1)(p-2)(p-3)(p-4)}{1.\ 2.\ 3.\ 4}$ 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 $(1+1)^{p-1}-1=2^{p-1}-1=\frac{p-1}{1}+\frac{(p-1)(p-2)}{1.\ 2}+\frac{(p-1)(p-2)(p-3)}{1.\ 2.\ 3}+\frac{(p-1)(p-2)(p-3)(p-4)}{1.\ 2.\ 3.\ 4}+$ etc.

quorum

quorum numerus eſt $= p - 1$ et propterea par. Colligantur igitur bini quique termini in vnam ſummam, quo terminorum numerus fiat duplo minor; erit $2^{p-1} - 1 = \frac{p(p-1)}{1.\ 2} + \frac{p(p-1)(p-2)(p-3)}{1.\ 2.\ 3.\ 4} + \frac{p(p-1)(p-2)(p-3)(p-4)(p-5)}{1.\ 2.\ 3.\ 4.\ 5.\ 6}$ + etc. cuius ſeriei vltimus terminus ob p numerum imparem erit $\frac{p(p-1)(p-2) \cdots \cdots 2}{1.\ 2.\ 3 \cdots \cdots (p-1)} = p$. Apparet autem ſingulos terminos per p eſſe diuiſibiles, nam,cum p ſit numerus primus et maior quam vllus denominatorum factor, nusquam diuiſione 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 $2^p = (1 + 1)^p = 1 + \frac{p}{1} + \frac{p(p-1)}{1.\ 2} + \frac{p(p-1)(p-2)}{1.\ 2.\ 3} \cdots \cdots \frac{p}{1} + 1$. Quae ſeries terminis primo et vltimo truncata dat $\frac{p}{1} + \frac{p(p-1)}{1.\ 2} + \frac{p(p-1)(p-2)}{1.\ 2.\ 3} + \cdots \cdots \frac{p(p-1)}{1.\ 2} + p = 2^p - 2$. Perſpicuum autem eſt iſtius ſeriei quemuis terminum per p eſſe diuiſibilem, 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 quaeuis 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* $3^{p-1}-1$ *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 quicunque, et viciſſim. Eſt vero $3^p = (1+2)^p = 1 + \frac{p}{1}.2 + \frac{p(p-1)}{1.\ 2}4 + \frac{p(p-1)(p-2)}{1.\ 2.\ 3}8 - - - - + \frac{p}{1}.2^{p-1} + 2^p$, 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. I.

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

Theorema.

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

Demonstratio.

Resoluatur $(1+a)^p$ consueto more in seriem, erit $(1+a)^p = 1 + \frac{p}{1}a + \frac{p(p-1)}{1.\ 2}a^2 + \frac{p(p-1)(p-2)}{1.\ 2.\ 3}a^3 + \text{--------} \frac{p}{1}a^{p-1} + a^p$; 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 formula 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 numerum primum diuidi queat, per p quoque haec formula $(a+1)^p - a - 1$ diuisionem admittat; sequitur etiam $(a+2)^p - a - 2$, item $(a+3)^p - a - 3$ et generaliter $(a+b)^p - a - b$ per p diuidi posse. Posito autem $a = 2$, quia $2^p - 2$, vti iam demonstrauimus, per p diuidi potest, perspicuum est formulam $(b+2)^p - b - 2$ diuisionem 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.

ME-