contentos, tentet, cum demonſtratum ſit omnes reliquos numeros primos huius formae diuiſores eſſe non poſſe.

Theorema 8.

29. Summa duarum huiusmodi poteſtatum $a^{2^m}+b^{2^m}$ quarum exponens eſt dignitas binarii alios diuiſores non admittit, niſi qui contineantur in hac forma $2^{m+1}n+1$.

Demonſtratio.

Quemadmodum demonſtrauimus omnes diuiſores formae a^2+b^2 in hac forma $4n+1$ contineri, hincque vlterius diuiſores omnes formae a^4+b^4 in $8n+1$ et formae a^8+b^8 in $16\,n+1$ contineri euicimus; ita ſimili modo oſtendi poteſt formam $a^{16}+b^{16}$ nullos alios diuiſores admittere niſi in formula $32n+1$ contentos. Dehinc porro intelligemus formas $a^{32}+b^{32}$; $a^{64}+b^{64}$ etc. alios diuiſores habere non poſſe, niſi qui in formulis $64n+1$, $128n+1$ etc. includantur. Sicque in genere patebit formae $a^{2^m}+b^{2^m}$ alios non dari diuiſores, niſi qui in formula $2^{m+1}n+1$ contineantur. Q. E. D.

Coroll. 1.

30. Nullus ergo numerus primus, qui in hac forma $2^{m+1}n+1$ non includitur, vnquam eſſe poteſt diuiſor vllius numeri in hac forma $a^{2^m}+b^{2^m}$ contenti.

Coroll. 2.

31. Diuiſores ergo huiusmodi numeri $a^{2^m}+b^{2^m}$ inquiſiturus inutiliter operam ſuam comſumeret, ſi aliis numeris primis praeter eos, quas forma $2^{m+1}n+1$ ſuppeditat, diuiſionem tentare vellet.

Scholion

Scholion 1.

32. Fermatius affirmauerant, etiamſi id ſe demonſtrare non poſſe ingenue eſſet confeſſus, omnes numeros ex hac forma $2^{2^m}+1$ ortos eſſe primos; hincque problema alias difficillimum, quo quaerebatur numerus primus dato numero maior, reſoluere eſt conatus. Ex vltimo theoremate autem perſpicuum eſt, niſi numerus $2^{2^m}+1$ ſit primus eum alios diuiſores habere non poſſe praeter tales, qui in forma $2^{m+1}n+1$ contineantur. Cum igitur veritatem huius effati Fermatiani pro caſu $2^{32}+1$ examinare voluiſſem, ingens hinc compendium ſum nactus, dum diuiſionem aliis numeris primis, praeter eos, quos formula $64n+1$ ſuppeditat, tentare non opus habebam. Huc igitur inquiſitione reducta mox deprehendi ponendo $n=10$ numerum primum 641 eſſe diuiſorem numeri $2^{32}+1$, vnde problema memoratum, quo numerus primus dato numero maior requiritur, etiamnum manet inſolutum.

Scholion 2.

33. Summa duarum poteſtatum eiusdem gradus vti a^m+b^m ſemper habet diuiſores algebraice aſſignabiles, niſi m ſit dignitas binarii. Nam ſi m ſit numerus impar, tum a^m+b^m ſemper diuiſorem habet $a+b$, atque ſi p fuerit diuiſor ipſius m, tum quoque a^p+b^p formam a^m+b^m diuidet. Sin autem m ſit numerus par, in hac formula $2^n p$ continebitur, ita vt p ſit numerus impar, hocque caſu $a^{2^n}+b^{2^n}$ diuiſor erit formae a^m+b^m exiſtente $m=2^n p$. Atque ſi p habeat diuiſorem q, tum