debere, cujus singuli termini integrati tandem exhibebunt terminum generalem indefinitum, quem etiam sine usu arithmeticae differentialis infinitis modis produci posse constat.

Quod ad Fermatii observationem attinet, Tecum sentio, non credibile videri, eum ad sex terminos illius suae seriei exprimendos progressum fuisse, neque tanto labore opus est ad verisimilitudinem illius observationis; facile enim experimur, divisore quocunque accepto, residua ex terminis ordine, quo sequuntur, divisis in circulum redire; sic v. gr. terminus $2^{2^x}+1$, ubi $x=2$, divisus per 7 relinquit 3, ergo terminus sequens relinquit idem residuum, quod relinquitur ex divisione numeri $(3-1)^2+1$ per 7, nempe residuum 5; terminus hunc sequens idem residuum dabit, quod relinquitur ex divisione numeri $(5-1)^2+1$ per 7 divisi, nempe 3; ergo omnia residua possibilia omnium terminorum seriei divisorum per 7 (ubi scil. quotiens sit >0) sunt vel 3 vel 5. Simili ratione facile apparet nullum terminum seriei Fermatianae dividi posse per numerum <100; sed quidquid sit de Fermatii observatione, hoc certum est, omnem numerum 2^p+1, ubi p non sit $=$ alicui numero 2^n (in quo n est numerus integer affirmativus), esse non primum, cujus quidem divisores facillime inveniuntur. Sic numeri $2^{64}+1$ divisor est 17, numeri $2^{1736}+1$ divisor est 257 etc. Vale.

Goldbach.

LETTRE V.

=

Euler à Goldbach.

Sommaire. Recherches ultérieures sur le théorème de Fermat. Formule qui exprime le nombre des diviseurs d'un nombre donné. Chaque nombre est la somme de quatre quarrés. Formule pour la quadrature du cercle de Grégoire à St.-Vincent.

Petropoli die 4 Junii 1730.

Postquam ultimas ad Te misissem litteras, de theoremate Fermatiano diligentius cogitare coepi, idque non tam levi nixum fundamento, quam primum putaveram, perspexi. Quoties enim in 2^n+1 non est n numerus ex progressione geometrica 1, 2, 4, 8, etc., divisores semper, ut ipse, Vir Celeberrime, in postremis litteris monuisti, assignari possunt. Nam si n est numerus impar, binomium 2^n+1, vel etiam generalius a^n+b^n poterit dividi per $a+b$. Si praeterea fuerit n multiplum quodpiam numeri imparis, uti si $n=ki$, denotante i numerum quemcunque imparem, divisor erit a^k+b^k. Quamobrem, cum solae binarii potentiae hanc habeant proprietatem, ut per nullum numerum imparem dividi possint, praeter unitatem, sequitur tum solum binomii a^n+b^n

ex hoc fonte divisorem assignari non posse, quando n est potentia quaedam binarii. Hoc quidem multum ad evincendam theorematis veritatem, sed tamen non est prorsus sufficiens. Quanquam enim pro n assumitur dignitas quaedam binarii, tamen ex eo inferre non licet $a^n + b^n$ nullos habere divisores; ut si a sit $= 4$, et $b = 3$, etiamsi ponatur $n = 2$, potest $16 + 9$ dividi per 5. Conducit ergo investigare casus, quibus nihilominus divisores locum habent. Perspicuum est primum, si a et b fuerint numeri inter se compositi, ut cf et df, binomium $c^n f^n + d^n f^n$ habere divisorem f^n. Deinde si a et b utrumque fuerit numerus impar, dividi semper poterit per 2. Denique ut hos casus universalius evolvamus, sit $a = mc + \alpha$, et $b = mc + \beta$, erit

$$a^n = \alpha^n + n\alpha^{n-1}mc + \frac{n(n-1)}{2}\alpha^{n-2}m^2c^2 + \text{etc.},$$

et $$b^n = \beta^n + n\beta^{n-1}mc + \frac{n(n-1)}{2}\beta^{n-2}m^2c^2 + \text{etc.},$$

ergo $$a^n + b^n = (\alpha^n + \beta^n) + nmc(\alpha^{n-1} + \beta^{n-1}) + \frac{n(n-1)}{2}m^2c^2(\alpha^{n-2} + \beta^{n-2}) + \text{etc.}$$

Ex hoc apparet singulos progressionis terminos praeter primum dividi posse per mc. Quoties igitur $\alpha^n + \beta^n$ et mc communem habent divisorem, per eundem et $a^n + b^n$ dividi poterit. In his igitur aliisque, si qui forte hic non continentur, casibus, quibus $a^n + b^n$ non fit numerus primus, si non comprehenditur casus Fermatii, quo $a = 2$ et $b = 1$, tuto concludi potest $2^n + 1$ semper esse numerum primum. Sed forte et alia hujusmodi theoremata invenire licet, ut $3^n + 2^n$, si n fuerit dignitas binarii, semper numeros primos mihi dare videtur. Caeterum theorema hoc non tam saepe, si unquam fallit, mihi fallere videtur, quam quae de differentiis potentiarum enunciant, cujusmodi est hoc: $2^n - 1$

semper dare numerum primum si n sit numerus primus. Nam si ponatur $n = 11$, $2^{11} - 1$, vel 2047, habet divisorem 23, similiter 47 metitur $2^{23} - 1$, et 223 hoc $2^{37} - 1$. Occurrit mihi hic terminus generalis, quem aliquando inveni, vel functio quaedam ipsius x, quae hanc habet proprietatem, ut quicunque numerus loco x ponatur, ea det numerum divisorum ejusdem numeri; in divisoribus vero habeo et unitatem et numerum ipsum, ita ut numeri primi duos tantum habeant divisores. Est itaque haec mea formula terminus generalis hujus seriei

1, 2, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6,
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,

cujus quilibet terminus indicat, quot index subscriptus habeat divisores, ut 6 habet quatuor 1, 2, 3, 6. Significet nunc x numerum quemcunque, erit numerus divisorum ipsius x hic

$$\frac{3 + (-1)^x + 1 + (-1)^A + 1 + (-1)^B + 1 + (-1)^C + 1 + (-1)^D + \text{etc.}}{2}$$

Designant vero A terminum generalem seriei 1, 1, 4, 7, 13, 22, etc., cujus quivis terminus summa est duorum praecedentium et 2; B terminum generalem seriei 1, 1, 1, 6, 11, 21, 41, etc., cujus quilibet terminus est summa trium praecedentium + 3; C terminum generalem seriei 1, 1, 1, 1, 8, 15, 29, 57, etc., cujus quivis terminus est summa quatuor praecedentium + 4. Similis ratio est reliquarum litterarum D, E, etc. Quaeratur binc numerus divisorum senarii, erit $x = 6$, $A = 22$, $B = 21$, $C = 15$, $D = 10$, $E = 1$, $F = 1$, et reliquae omnes erunt 1. His positis erit numerus divisorum senarii =

$$\frac{3 + (-1)^6 + 1 + (-1)^{22} + 1 + (-1)^{21} + 1 + (-1)^{15} + 1 + (-1)^{10} + 1 + (-1)^1 + 1 + (-1)^1 \text{etc.}}{2}$$

quia autem — 1 elevatum ad numerum parem dat + 1 et ad numerum imparem — 1, erit numerus divisorum

$$= \frac{3+1+1+1+1-1+1-1+1+1+1+1-1+1-1}{2} = 4,$$

qui sunt 1, 2, 3, 6. Si igitur quis potuerit, formula illa posita $= 2$, eruere quid sit x, haberetur terminus generalis pro serie numerorum primorum; sed isthuc pertingere non spero. Incidi nuper, opera Fermatii legens, in aliud quoddam non inelegans theorema: *Numerum quemcunque esse summam quatuor quadratorum*, seu semper inveniri posse quatuor numeros quadratos, quorum summa aequalis sit numero dato, ut $7 = 1 + 1 + 1 + 4$. Sed tria quadrata nunquam invenientur, quorum summa sit 7. Ad hoc theorema demonstrandum requiritur, ut generaliter quatuor quadrata inveniantur z^2, y^2, x^2, v^2 quorum summa aequalis sit summae quinque datorum $1 + a^2 + b^2 + c^2 + d^2$. Alia ibi habentur theoremata de resolutione cujusvis numeri in trigonales, pentagonales, cubos etc., quorum demonstratio magnum afferret incrementum analysi. Ut pagina haec impleatur transcribam quadraturam quandam circuli, quam ex propositione aliqua Gregorii a St. Vincentio elicui, cujus falsitatem nemo adhuc ostendit. Ea haec est: Si peripheria sit p et diameter d, erit $\frac{p}{d} = \frac{3(1+A)\sqrt{3}}{2(2A-1)}$, est vero $A = \left(\frac{11}{5}\right)^{\frac{l11:5}{l203:53}}$, ubi $l\,11:5$ denotat logarithmum fractionis $\frac{11}{5}$ et $l.\,203:53$ logarithmum hujus $\frac{203}{53}$. Haec expressio prope ad $\frac{22}{7}$ accedit, et si vera esset, magnum sane esset inventum.

Vale et favere perge, Vir Celeb., Tui observantissimo

Eulero.

LETTRE VI.

GOLDBACH à EULER.

SOMMAIRE. Réflexions ultérieures sur le théorème de Fermat et réponse à la lettre précédente.

Moscuae d. $\frac{15}{26}$ Junii 1730.

Etiamsi vera non esset Fermatii propositio, tamen laude digna mihi videtur propterea quod, cum ejus demonstrationem investigamus, in alia incidimus theoremata quorum veritas solidis argumentis evinci potest, quale est illud quod de numero $a^n + b^n$ divisibili per $a + b$, si n fuerit numerus impar, observasti.

Praeterea 1) si a, b, n sint numeri integri, et $\asymp$ significet aequationem impossibilem, posito $\frac{a \pm n}{n^2+1} \asymp b$, sequitur $a^2 + 1$ esse numerum primum; id quod demonstrari potest.