Euler, Leonhard (1707-1783). (latin). 1911-19??]Opera mathematica . Series prima. Volumen II, Leonhardi Euleri commentationes arithmeticae. Volumen primum. 1995.

OBSERVATIONES DE THEOREMATE QUODAM FERMATIANO ALIISQUE AD NUMEROS PRIMOS SPECTANTIBUS

Commentatio 26 indicis ENESTROEMIANI
Commentarii academiae scientiarum Petropolitanae 6 (1732/3), 1738, p. 103—107

SUMMARIUM

Ex manuscriptis academiae scientiarum Petropolitanae nunc primum editum

Percelebris erat superioris saeculi Geometra Gallus FERMATIUS in investigandis numerorum proprietatibus. Inter quaestiones vero, quae de numerorum proprietatibus formari possunt, praecipua fere est ea, qua agitur de criteriis, quibus cognosci potest, utrum numerus propositus sit primus necne, i. e., an divisibilis sit per quendam numerum an secus; nec multo minoris facienda est quaestio de inveniendo numero primo quovis dato maiori. Affirmabat autem FERMATIUS omnes omnino numeros hac formula generali $2^{2^m}+1$ contentos esse primos, cuius theorematis ope altera dictarum quaestionum solvi posset. De hoc FERMATII asserto dubitari fere non poterat, quod inter numeros ab unitate usque ad 100000 progredientes nullus datur eius formae, qui non sit numerus primus. Etenim si pro m ponatur successive 1, 2, 3 et 4, prodeunt numeri 5, 7, 257 et 65537, qui revera omnes sunt numeri primi. Notavit vero celeb. EULERUS formulam FERMATIANAM fallere nonnunquam, id quod revera evenit, cum pro n ponitur 5; tunc enim prodit numerus 4294967297, qui divisibilis est per 641. Hac autem occasione auctor 6 alia proponit theoremata ad hanc rem pertinentia, quorum quidem demonstrationes non dantur, quamvis eorum veritas tentando comprobari possit.

Notum est hanc quantitatem $a^n + 1$ semper habere divisores, quoties n sit numerus impar vel per imparem praeter unitatem divisibilis. Namque $a^{2m+1} + 1$ dividi potest per $a + 1$ et $a^{p(2m+1)} + 1$ per $a^p + 1$, quicunque etiam

numerus loco a substituatur. Contra vero si n fuerit eiusmodi numerus, qui per nullum numerum imparem nisi unitatem dividi possit, id quod evenit, quando n est dignitas binarii, nullus numeri $a^n + 1$ potest assignari divisor. Quamobrem si qui sunt numeri primi huius formae $a^n + 1$, ii omnes comprehendantur necesse est in hac forma $a^{2^m} + 1$. Neque tamen ex hoc potest concludi $a^{2^m} + 1$ semper exhibere numerum primum, quicquid sit a; primo enim perspicuum est, si a sit numerus impar, istam formam divisorem habituram 2. Deinde quoque, etiamsi a denotet numerum parem, innumeri tamen dantur casus, quibus numerus compositus prodit. Ita haec saltem formula $a^2 + 1$ potest dividi per 5, quoties est $a = 5b \pm 3$, et $30^2 + 1$ potest dividi per 17 et $50^2 + 1$ per 41. Simili modo $10^4 + 1$ habet divisorem 73, $6^8 + 1$ habet divisorem 17 et $6^{128} + 1$ est divisibilis per 257. At huius formae $2^{2^m} + 1$, quantum ex tabulis numerorum primorum, quae quidem non ultra 100000 extenduntur, nullus detegitur casus, quo divisor aliquis locum habeat. Hac forte aliisque rationibus FERMATIUS adductus enunciare non dubitavit $2^{2^m} + 1$ semper esse numerum primum hocque ut eximium theorema WALLISIO aliisque Mathematicis Anglis demonstrandum proposuit. Ipse quidem fatetur se eius demonstrationem non habere, nihilo tamen minus asserit esse verissimum. Utilitatem eius autem hanc potissimum praedicat, quod eius ope facile sit numerum primum quovis dato maiorem exhibere, id quod sine huiusmodi universali theoremate foret difficillimum. Leguntur haec in WALLISII *Commercio Epistolico* tomo eius Operum secundo inserto, epistola penultima.[1]) Extant etiam in ipsius FERMATII operibus p. 115 sequentia[2]): „Cum autem numeros a binario quadratice in se ductos et unitate auctos esse semper numeros primos apud me constet et iam dudum Analystis illius theorematis veritas fuerit significata, nempe esse primos 3, 5, 17, 257, 65537 etc. in infinit., nullo negotio etc.“

Veritas istius theorematis elucet, ut iam dixi, si pro m ponatur 1, 2, 3 et 4; prodeunt enim hi numeri 5, 17, 257 et 65537, qui omnes inter numeros primos in tabula reperiuntur. Sed nescio, quo fato eveniat, ut statim sequens, nempe $2^{2^5} + 1$, cesset esse numerus primus; observavi enim his diebus longe alia

---

1) I. WALLIS (1616—1703), *Opera*, t. II, Oxoniae 1693, p. 857 (Epistola XLVI D. FERMATII ad D. KENELMUM DIGBY, 1658); P. DE FERMAT (1601—1665), *Oeuvres*, publiées par les soins de MM. P. TANNERY et CH. HENRY, t. II, Paris 1894, p. 402. F. R.

2) P. DE FERMAT, *Varia opera mathematica*, Tolosae 1679, p. 115; *Oeuvres de FERMAT*, t. I, Paris 1891, p. 131, t. II, Paris 1894, p. 206. F. R.

agens posse hunc numerum dividi per 641, ut cuique tentanti statim patebit.[1]) Est enim $2^{2^5}+1=2^{32}+1=4294967297$. Ex quo intelligi potest theorema hoc etiam in aliis, qui sequuntur, casibus fallere et hanc ob rem problema de inveniendo numero primo quovis dato maiore etiam nunc non esse solutum.

Considerabo nunc etiam formulam 2^n-1, quae, quoties n non est numerus primus, habet divisores, neque tantum 2^n-1, sed etiam a^n-1. Sed si n sit numerus primus, videri posset etiam 2^n-1 semper talem exhibere; hoc tamen asseverare nemo est ausus, quantum scio, cum tam facile potuisset refelli. Namque $2^{11}-1$, i. e. 2047, divisores habet 23 et 89, et $2^{23}-1$ dividi potest per 47. Video autem Cel. WOLFIUM non solum hoc in *Elem. Matheseos*[2]) editione altera non advertisse, ubi numeros perfectos investigat atque 2047 inter primos numerat, sed etiam 511 seu 2^9-1 pro tali habet, cum tamen sit divisibilis per 2^3-1, i. e. 7. Dat autem $2^{n-1}(2^n-1)$ numerum perfectum, quoties 2^n-1 est primus; debet ergo etiam n esse numerus primus. Operae igitur pretium fore existimavi eos notare casus, quibus 2^n-1 non est numerus primus, quamvis n sit talis. Inveni autem hoc semper fieri, si sit $n=4m-1$ atque $8m-1$ fuerit numerus primus; tum enim 2^n-1 semper poterit dividi per $8m-1$. Hinc excludendi sunt casus sequentes: 11, 23, 83, 131, 179, 191, 239 etc., qui numeri pro n substituti reddunt 2^n-1 numerum compositum. Neque tamen reliqui numeri primi omnes loco n positi satisfaciunt, sed plures insuper excipiuntur; sic observavi $2^{37}-1$ dividi posse per 223, $2^{43}-1$ per 431, $2^{29}-1$ per 1103, $2^{73}-1$ per 439; omnes tamen excludere non est in potestate. Attamen asserere audeo praeter hos casus notatos omnes numeros primos minores quam 50 et forte quam 100 efficere $2^{n-1}(2^n-1)$ esse numerum perfectum sequentibus numeris pro n positis 1, 2, 3, 5, 7, 13, 17, 19, 31, 41, 47, unde 11 proveniunt numeri perfecti. Deduxi has observationes ex theoremate quodam non inelegânti, cuius quidem demonstrationem quoque non habeo, verum tamen de eius veritate sum certissimus. Theorema hoc est: *a^n-b^n semper potest dividi per $n+1$, si $n+1$ fuerit numerus primus atque a et b non possint per eum dividi*;[3]) eo autem difficiliorem puto eius demonstrationem esse, quia non est verum, nisi $n+1$ sit numerus primus. Ex

1) Vide L. EULERI Commentationem 134 (indicis ENESTROEMIANI), p. 74 (§ 32) huius voluminis. F. R.

2) CHR. WOLF, *Elementa matheseos universae*, editio nova, Halae Magdeburgicae, t. I, 1730, p. 384; numerus autem 2047 etiam in editione novissima (1742) inter primos numeratur. F. R.

3) Vide Commentationem 134 huius voluminis, theorema 4. F. R.

hoc statim sequitur $2^n - 1$ semper dividi posse per $n+1$, si fuerit $n+1$ numerus primus, seu, cum omnis primus sit impar praeter 2 hicque ob conditiones theorematis, quia est $a = 2$, non possit adhiberi, poterit $2^{2m} - 1$ semper dividi per $2m+1$, si $2m+1$ sit numerus primus. Quare etiam vel $2^m + 1$ vel $2^m - 1$ dividi poterit per $2m+1$. Deprehendi autem $2^m + 1$ posse dividi, si fuerit $m = 4p+1$ vel $4p+2$; at $2^m - 1$ habebit divisorem $2m+1$, si $m = 4p$ vel $4p-1$. Haec persecutus in multa alia incidi theoremata non minus elegantia, quae eo magis aestimanda esse puto, quod vel demonstrari prorsus nequeant vel ex eiusmodi propositionibus sequantur, quae demonstrari non possunt; primaria igitur hic adiungere visum est.

THEOREMA 1

Si fuerit n numerus primus, omnis potentia exponentis $n-1$ *per n divisa vel nihil vel* 1 *relinquit.*[1])

THEOREMA 2

Manente n numero primo omnis potentia, cuius exponens est $n^{m-1}(n-1)$, *divisa per* n^m *vel* 0 *vel* 1 *relinquit.*[2])

THEOREMA 3

Sint m, n, p, q etc. numeri primi inaequales sitque A minimus communis dividuus eorum unitate minutorum, puta ipsorum $m-1$, $n-1$, $p-1$, $q-1$ *etc.; his positis dico omnem potentiam exponentis A ut* a^A *divisam per mnpq etc. vel* 0 *vel* 1 *relinquere, nisi a dividi possit per aliquem horum numerorum m, n, p, q etc.*

THEOREMA 4

Denotante $2n+1$ *numerum primum poterit* $3^n + 1$ *dividi per* $2n+1$, *si sit vel* $n = 6p+2$ *vel* $n = 6p+3$; *at* $3^n - 1$ *dividi poterit per* $2n+1$, *si sit vel* $n = 6p$ *vel* $n = 6p-1$.

---

1) Quod est celebre theorema FERMATIANUM. Vide Commentationes 54, 134, 262 huius voluminis. F. R.

2) Hoc theorema generalius, quod in se complectitur theorema FERMATIANUM, primum ab EULERO demonstratum est in Commentatione 271 huius voluminis. F. R.

THEOREMA 5

$3^n + 2^n$ potest dividi per $2n+1$, si sit $n =$ vel $12p+3$ vel $12p+5$ vel $12p+6$ vel $12p+8$. Atque $3^n - 2^n$ potest dividi per $2n+1$, si sit $n =$ vel $12p$ vel $12p+2$ vel $12p+9$ vel $12p+11$.

THEOREMA 6

Sub iisdem conditionibus, quibus $3^n + 2^n$, poterit etiam $6^n + 1$ dividi per $2n+1$; atque $6^n - 1$ sub iisdem, quibus $3^n - 2^n$. [1])

---

1) Confer haec theoremata 4—6 nec non, quod occurrit in ipsa dissertatione, theorema de divisibilitate formularum $2^m + 1$ et $2^m - 1$ cum theorematis 42, 43, 50 Commentationis 164 huius voluminis. Vide etiam theorema 11 Commentationis 134 et theorema inversum, quod in Commentatione 262 (§ 72) huius voluminis continetur. F. R.