1787

Novae demonstrationes circa divisores numerorum formae $xx + nyy$

Leonhard Euler

NOVAE DEMONSTRATIONES CIRCA DIVISORES NVMERORVM FORMAE $xx + nyy$.

Auctore

L. EVLERO.

Conuent. exhib. d. 20 *Nouembr.* 1775.

Cum nuper eximia inuenta Illustris *de la Grange* super diuisoribus numerorum formae $xx + nyy$ recensuissem et cum meis obseruationibus, quas olim plerumque per inductionem erueram, contulissem, quippe quae inde haud exiguum firmamentum acceperant, non dubitaui mox perfectas demonstrationes, quae adhuc desiderabantur, polliceri. Fretus scilicet eram sagacitate acutissimi viri *de la Grange*, qua iam plures huius generis demonstrationes felicissimo successu in lucem produxit. Postquam autem omnes circumstantias, ad quas in hac inuestigatione est attendendum, accuratius perpendissem, mihi quoque contigit praecipua momenta, quibus istae exoptatae demonstrationes innituntur, perspicere, quae igitur hic exponere constitui.

Theorema 1.

§. 1. *Si omnes numeri quadrati per numerum quemcunque primum P (binario excepto, quippe cuius ratio per se est manifesta) diuidantur, numerus omnium residuorum diuersorum, quae inde resultare possunt, semper est* $= \frac{1}{2}(P - 1)$.

Demon-

Scholion 1.

§. 9. Quo haec exemplo clariora reddantur, consideremus numerum primum 13, pro quo residua reperiuntur: 1, 4, 9, 3, 12, 10, non-residua vero: 2, 5, 6, 7, 8, 11; atque vt forma $xx + nyy$ diuisibilis esse queat per 13, numerus n in aliqua sex sequentium formularum contentus esse debet:

$$13\lambda - 1,\ 13\lambda - 4,\ 13\lambda - 3,\ 13\lambda - 12,\ 13\lambda - 10,$$

sicque valores idonei pro isto numero n ordine naturali dispositi erunt sequentes:

1, 3, 4, 9, 10, 12, 14, 16, 17, 22, 23, 25, 27, 29, 30, 35, 36, 38, 40, 42, 43, 48, 49, 51, 53, 55, 56, 61, 62, 64, 66, 68, 69, 74, 75, 77, 79, 81, 82, 87, 88, 90, 92, 94, 95, 100;

quorum numerus vsque ad 100 est 46. Reliqui ergo numeri qui diuisorem 13 a formula $xx + nyy$ penitus excludunt, deletis iis qui ipsi per 13 sunt diuisibiles, ordine erunt isti:

2, 5, 6, 7, 8, 11, 15, 18, 19, 20, 21, 24, 28, 31, 32, 33, 34, 37, 41, 44, 45, 46, 47, 50, 54, 57, 58, 59, 60, 63, 67, 70, 71, 72, 73, 76, 80, 83, 84, 85, 86, 89, 93, 96, 97, 98, 99,

quorum numerus est 47, ideoque tantum non aequalis priori. Ratio autem, cur multipla ipsius 13 exclusimus, est, quod de formula $xx + 13\nu yy$, vtrum diuisorem 13 accipiat, quaestio esse non potest, quia manifesto numerus deberet esse diuisibilis per 13.

Scholion 2.

§. 10. Quoniam vis nostrae demonstrationis clarius in exemplis perspicitur, contemplemur alium numerum primum 19, pro quo nouem residua sunt: 1, 4, 9, 16, 6, 17, 11, 7, 5, nouem vero non-residua: 2, 3, 8, 10, 12, 13, 14, 15, 18.

Hinc

Hinc igitur formula $xx+nyy$ diuiforem 19 recipere poterit, fi numerus n in fequenti forma contineatur:

$$n = 19\lambda - (1, 4, 9, 16, 6, 17, 11, 7, 5);$$

fin autem n contineatur in fequenti formula:

$$n = 19\lambda - (2, 3, 8, 10, 12, 13, 14, 15, 18),$$

tum nullus numerus formae $xx+nyy$ per 19 diuidi poterit. Valores igitur idonei pro numero n vsque ad centum ordine erunt

2, 3, 8, 10, 12, 13, 14, 15, 18, 21, 22, 27, 29, 31, 32, 33, 34, 37, 40, 41, 46, 48, 50, 51, 52, 53, 56, 59, 60, 65, 67, 69, 70, 71, 72, 75, 78, 79, 84, 86, 88, 89, 90, 91, 94, 97, 98,

quorum multitudo eft 47. Reliqui vero numeri ad hunc fcopum inepti, exclufis multiplis ipfius 19, erunt numero 48 fequentes:

1, 4, 5, 6, 7, 9, 11, 16, 17, 20, 23, 24, 25, 26, 28, 30, 35, 36, 39, 42, 43, 44, 45, 47, 49, 54, 55, 58, 61, 62, 63, 64, 66, 68, 73, 74, 77, 80, 81, 82, 83, 85, 87, 92, 93, 96, 99, 100.

Scholion 3.

§. 11. Quo autem facilius intelligatur, quomodo quouis cafu, vbi numerus n idoneum habet valorem, formula $xx+nyy$ diuifibilis reddatur per numerum primum P, notetur, hoc femper fieri poffe, dum pro x et y numeri non maiores quam $\frac{1}{2}(P-1)$ accipiantur, atque adeo alterum horum numerorum y pro lubitu accipi poffe. Sit igitur $y=1$, ita vt habeatur haec formula: $xx+n$, numerique n refiduum nafcatur r; tum igitur pro xx id quaeratur quadratum, cui conueniat refiduum $P-r$, ac manifefto fumma $xx+n$ per P erit diuifibilis. Hoc autem femper fieri poffe euidens eft, cum fit $n=\lambda P - a$, vnde fit refiduum $r = P - a$, ideoque

$P - r = a$, ficque pro xx id fumi debet quadratum, cui refpondet refiduum a. Ita fumto $P = 13$ accipiatur pro n, pro lubitu, valor idoneus ex fupra inuentis, veluti $n = 82$, et quaeratur x ita, vt fiat forma $xx + 82$ per 13 diuifibilis. Hic autem fit refiduum $r = 4$, hincque $P - r = 9$; erit ergo $x = 3$ et formula $3^2 + 82$ per 13 diuidi poteft. Simili modo fi pro diuifore 19 fumatur $n = 88$, inde oritur refiduum $r = 12$, ideoque $P - r = 7$; quadratum autem, quod per 19 diuifum relinquit 7, eft 64, ficque formula $8^2 + 88$ prodit diuifibilis per 19. Atque hinc deduci poteft facilior et concinnior demonftratio noftri Theorematis.

Alia Demonftratio Theorematis 2.

§. 12. Oftendi fcilicet poteft, fi fuerit $n = \lambda P - a$, tum femper dari numerum x, vt formula $xx + n$ diuifionem admittat: tantum enim pro xx id fumatur quadratum, quod per P diuifum relinquat a, quod ergo erit formae $\mu P + a$; quare ob $n = \lambda P - a$, erit formula $xx + n = (\mu + \lambda) P$, ideoque manifefto diuifibilis per numerum P.

Scholion 1.

§. 13. Cum igitur pro quolibet numero primo P facile omnes valores numeri n exhiberi queant, quibus forma $xx + nyy$ diuifionem per P admittere poteft, quandoquidem, denotante a refidua omnia ex diuifione quadratorum per P oriunda, inuenimus $n = \lambda P - a$: manifeftum eft, pro n etiam infinitos valores negatiuos dari, qui oriuntur, fi pro λ etiam numeri negatiui accipiantur. Quamobrem non inutile erit, pro numeris primis fimplicioribus formulas exhibere, quae omnes valores idoneos numeri n contineant, quibus forma $xx + nyy$ per numerum primum P diuifibilis reddi queat, quas igitur hic apponemus.

P

P	n
3	$3\lambda - 1$
5	$5\lambda - (1, 4)$
7	$7\lambda - (1, 4, 2)$
11	$11\lambda - (1, 4, 9, 5, 3)$
13	$13\lambda - (1.4, 9, 3, 12, 10)$
17	$17\lambda - (1, 4, 9, 16, 8, 2, 15, 13)$
19	$19\lambda - (1, 4, 9, 16, 6, 17, 11, 7, 5)$
23	$23\lambda - (1, 4, 9, 16, 2, 13, 3, 18, 12, 8, 6)$
29	$29\lambda - (1, 4, 9, 16, 25, 7, 20, 6, 23, 13, 5, 28, 24, 22)$
31	$31\lambda - (1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8)$
37	$37\lambda - (1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28)$
41	$41\lambda - (1, 4, 9, 16, 25, 36, 8, 23, 40, 18, 39, 21, 5, 32, 20, 10, 2, 37, 33, 31)$
43	$43\lambda - (1, 4, 9, 16, 25, 36, 6, 21, 38, 14, 35, 15, 40, 24, 10, 41, 31, 23, 17, 13, 11)$
47	$47\lambda - (1, 4, 9, 16, 25, 36, 2, 17, 34, 6, 27, 3, 28, 8, 37, 21, 7, 42, 32, 24, 18, 14, 12)$

Corollarium.

§. 14. Si ergo n fuerit numerus negatiuus, puta $n = -m$, ſumto λ negatiuo erit $m = \lambda P + a$, quae forma cum contineat omnes numeros quadratos, quicunque numerus primus pro P accipiatur; patet, ſi fuerit m numerus quadratus, ſcilicet $m = k^2$, numeros formae $xx - kkyy$ per omnes plane numeros primos diuiſibiles exſiſtere poſſe, quo ergo caſu nulli numeri primi excluduntur, id quod per ſe eſt manifeſtum, quoniam formula $xx - kkyy$ in genere factores habet $x + ky$ et $x - ky$, quorum vterque per omnes numeros primos diuiſibilis reddi poteſt, id quod nullo alio caſu fieri licet.

Scholion 2.

§. 15. Quemadmodum reſpectu cuiusuis numeri primi P omnes numeri in duas claſſes diſtinguuntur, quarum al-

tera

tera continet valores idoneos litterae n, vt formula $xx+nyy$ per eum numerum primum P diuisibilis reddi queat, altera vero eos numeros, qui talem diuisionem respuunt, ac praeterea multitudo numerorum in vtraque classe contentorum eadem deprehenditur: ita vicissim pro quolibet numero n omnes numeros primos etiam in duas classes distingui oportet, quarum altera continebit eos, qui diuisores exsistere possunt formae $xx+nyy$, altera vero reliquos, qui nullo modo huius formae diuisores exsistere possunt. Pro vtraque autem classe iam olim formulas dedi generales, similes illis, quibus hic pro quolibet numero primo valores idoneos numeri n ab ineptis distinxi: hoc tantum discrimine, quod, dum hic formulae diuisorem P respiciunt, ibi numerus $4n$ diuisoris locum obtineat. Scilicet pro diuisoribus primis numerorum formae $xx+nyy$ dedi talem formam: $4ni+A$, pro iis vero, qui nullo modo diuisores esse possunt, talem: $4ni+\mathfrak{A}$, vbi litterae A et $\mathfrak{A}$ simul complectuntur omnes numeros ad $4n$ primos ipsoque minores, ex quibus littera A continet eos qui ad diuisionem sunt apti, littera vero $\mathfrak{A}$ eos qui excluduntur. Cum igitur has formulas olim per inductionem elicuissem, nunc nullum amplius dubium superesse potest, quin prior formula $4ni+A$ complectatur omnes numeros primos, per quos formulam $xx+nyy$ diuidere licet, dum altera $4ni+\mathfrak{A}$ eos inuoluit, qui nullo modo diuisores exsistere possunt. Interim tamen has ambas formulas sequenti modo ex positis principiis deriuare licebit.

Problema.

Proposito numero quocunque n *positiuo, assignare omnes numeros primos, per quos numeri formae* $xx+nyy$ *diuisionem admittere queant.*

Solutio.

Solutio.

§. 16. Denotet P diuiſorem quemcunque primum formae propoſitae $xx+nyy$, ſitque λ quotus ex hac diuiſione oriundus, atque habebimus hanc aequationem: $\lambda P = xx+nyy$, quam expreſſionem transformemus ponendo $x = 2nr+s$ et $y = 2t+u$, prodibitque iſta aequatio:

$$\lambda P = 4n(nrr+rs+tu+tt)+ss+nuu,$$

cuius loco, quia $nrr+rs+tu+tt$ omnes numeros deſignare poteſt, ſcribamus breuitatis gratia λi, vt ſcilicet prius membrum per λ diuidi poſſit, atque habebimus hanc aequalitatem: $P = 4ni+\frac{ss+nuu}{\lambda}$.

§. 17. Hoc igitur modo iam nacti ſumus formam ſupra memoratam: $4ni+A$, ſimulque patet loco A ſumi debere omnes numeros ex formula $\frac{ss+nuu}{\lambda}$ reſultantes, vbi cum λ quemcunque numerum deſignare poſſit, littera A tam omnes numeros ipſos in forma $ss+nuu$ contentos, quam eorum diuiſores omnes in ſe comprehendet. Quoniam autem noſtra forma numeros primos exhibere debet, loco A alios numeros accipere non licebit, niſi qui ad $4n$ fuerint primi, quos ergo oportebit eſſe impares ſimulque primos ad ipſum numerum n, ſiue cum n nullum habere debent diuiſorem communem.

§. 18. Primo igitur inter valores litterae A, ſumendo $u=0$ et $\lambda=1$, occurrent omnes numeri quadrati ss impares et ad n primi, vel ipſi, vel diuiſione per $4n$ facta depreſſi. Deinde ſumendo $u=1$, manente $\lambda=1$, etiam occurrent omnes numeri in forma $ss+n$ contenti, quatenus ſcilicet ad $4n$ fuerint primi; vbi quidem plurimum notaſſe iuuabit, poſtquam iam aliquot numeri idonei pro A fuerint inuenti, qui ſint a, b, c, d, e, etc. etiam omnia producta ex binis, ſcilicet ab,

ac, bc, etc. ibidem occurrere debere, cuius rei ratio eſt, quod producta ex pluribus numeris formae $ss + nuu$ ſemper ad eandem formam reducere licet.

§. 19. Quod vero ad eos valores ipſius A attinet, qui oriuntur ſi λ non fuerit vnitas, ſeu qui tantum ſint diuiſores formae $ss + nuu$, quorum multitudo videri poſſet indefinita, recurrere debemus ad theorema Illuſtris *de la Grange*, quo demonſtrauit, omnes diuiſores numerorum formae $ss + nuu$ ſemper contineri in hac formula: $fpp \pm 2gpq + hqq$, exſiſtente $fh = gg + n$, neque has formulas vlterius continuari opus eſſe, quamdiu fuerit vel $2g < f$, vel $2g < h$, quarum formarum numerus ſemper eſt ſatis modicus. Hinc igitur ſemper pro A accipere licebit vel f vel h, niſi forte ad $4n$ non fuerint primi. Hoc enim caſu pro A ſumi conueniet vel numeros $f \pm 2g + h$, vel $4f \pm 4g + h$, vel $f \pm 4g + 4h$, etc. quatenus ſcilicet hi numeri fuerint primi ad $4n$. Simulac vero vnicus talis valor fuerit repertus, is per eos, qui iam ante ſunt inuenti, multiplicatus, dabit totidem nouos valores idoneos pro A.

§. 20. Hoc autem modo mox omnes valores idoneos pro A adipiſcemur, cum eorum numerus ſemper aequetur ſemiſſi omnium numerorum minorum quam $4n$ ad eumque primorum. Hinc ſi multitudo omnium iſtorum numerorum fuerit $= 2k$ (eum enim ſemper eſſe parem aliunde conſtat), multitudo valorum litterae A ſemper erit $= k$, ſolo caſu excepto, quo n eſt numerus quadratus negatiuus, quippe quo omnes plane hi numeri locum inueniunt: reliquis vero caſibus omnibus multitudo numerorum excluſorum itidem erit $= k$, qui ſi deſignentur litteris graecis α, β, γ, δ, etc. hi dabunt omnes valores litterae $\mathfrak{A}$ pro formula $4ni + \mathfrak{A}$, quae omnes

conti-

continet numeros primos, qui nullo modo diuisores esse possunt vllius numeri in forma $xx + nyy$ contenti.

§. 21. Quod ad ipsos valores ipsius A attinet, qui oriuntur ex forma $fpp \pm 2gpq + hqq$, quia haec forma, siue per f siue per h multiplicetur, reducitur ad formam $xx + nyy$, ob $fh = gg + n$, his casibus erit siue $\lambda = f$, siue $\lambda = h$, ita vt tum pro numeris primis inde natis tam fP quam hP semper futurus sit numerus formae $xx + nyy$, vbi ergo sufficiet minorem horum duorum numerorum f et h accepisse, ita vt pronunciare liceat: quoties numerus primus P fuerit diuisor cuiuspiam numeri formae $xx + nyy$, tum vel ipsum hunc numerum P, vel eius multiplum fP, fore quoque numerum formae eiusdem $xx + nyy$.

§. 22. Cum igitur formula $4ni + \mathfrak{A}$ certe omnes numeros contineat, qui nullo modo esse possunt diuisores formae $xx + nyy$, necesse est vt omnes numeri primi in forma $4ni + $ A contenti simul sint diuisores cuiuspiam formae $xx + nyy$.

Corollarium 1.

§. 23. Quod multitudo valorum litterae $\mathfrak{A}$ semper aequalis sit multitudini valorum ipsius A, quos ponimus a, b, c, d, e, etc. inde patet, quod si vnicus innotuerit, veluti α, ad $\mathfrak{A}$ referendus, tum etiam omnia producta αa, αb, αc, αd, etc. ad eandem classem pertinere, vnde tamen vnicum casum, quo $n = -mm$, excipi oportet, quoniam hoc casu nulli prorsus valores pro $\mathfrak{A}$ dantur.

Corollarium 2.

§. 24. Quoniam pro quouis numero n forma diuisorum *Grangiana* $fpp \pm 2gpq + hqq$ exiguam variationem recipit, quandoquidem ea ſemper ita reduci poteſt, vt $2g$ fiat minus quam f vel h, ſi valores iſti minores deſignentur littera f, tum omnes diuiſores primi numerorum formae $xx + nyy$ vel ipſi erunt eiusdem formae, vel per f multiplicati, vnde ſi f alios non habeat valores praeter vnitatem, quod euenit caſibus $n = 1$, $n = + 2$ et $n = + 3$, tum omnes diviſores primi his caſibus quoque ipſi habebunt eandem formam.

Corollarium 3.

§. 25. Quoniam omnes valores pro littera A debent eſſe numeri impares, omnes formae $fpp \pm 2gpq + hqq$ hinc ſunt excludendae, in quibus ambo numeri f et h pares. Quare cum ſit $fh = gg + n$, numerum $gg + n$ ita in duos factores reſolui conuenit, vt alter ſaltem euadat impar, vnde ſi numerus $gg + n$ plures habeat diuiſores pares, plures reſolutiones tanquam inutiles erunt reiiciendae.

Scholion 1.

§. 26. Quemadmodum valores litterae A pro forma $4ni + A$ ſunt minores quam $4n$, ita ſi negatiuos introducere velimus, eos infra $2n$ deprimere licebit. Obſeruaui autem porro, pro omnibus caſibus, quibus n eſt numerus poſitiuus, multitudinem iſtorum valorum ipſius A ad ſemiſſem redigi poſſe, ita vt ſinguli non ſuperent ipſum numerum n, ſi ſcilicet non ad formam $4ni$, ſed ad eius dimidium tantum $2ni$ referantur. Hic autem duos caſus probe a ſe inuicem diſtingui oportet, prouti n vel in alterutra harum formularum: $4k$ et $4k - 1$, vel in alterutra harum: $4k + 1$ et $4k + 2$ continetur. Hoc enim poſteriori caſu ſingulis valoribus ipſius A ſignum ambiguum, ſiue $\pm$, ſiue $\mp$, praefigi debet, quorum ſignorum ſuperiora

periora valeant, quoties i fuerit numerus par, inferiora autem quoties impar. Hoc igitur modo sequens tabula est constructa tres columnas complexa, quarum prima exhibet valores numeri n ordine naturali procedentes, secunda formulas pro diuisoribus P. tertia vero indices littera f supra indicatos, quos ita interpretari decet, vt, quoties P fuerit numerus primus, eius productum per quempiam indicum f fiat numerus formae $xx + nyy$.

Tabula exhibens omnes diuisores primos pro numeris formae $xx + nyy$, vna cum indicibus f.

Vbi circa signa ambigua est obseruandum, superiora valere quoties i numerus par, inferiora vero, quoties i numerus impar.

n	Diuisores P	f
1	$2i \pm 1$	1
2	$4i \pm 1$	1
3	$6i + 1$	1
4	$8i + 1, - 3$	1
5	$10i \pm 1, \pm 3$	1, 2
6	$12i \pm 1, \pm 5$	1, 2
7	$14i + 1, - 3, + 5$	1
8	$16i + 1, + 3, - 5, - 7$	1, 3
9	$18i \pm 1, \pm 5, \mp 7,$	1, 2
10	$20i \pm 1, \mp 3, \pm 7, \pm 9$	1, 2
11	$22i + 1, + 3, + 5, - 7, + 9$	1, 3
12	$24i + 1, - 5, + 7, - 11,$	1, 3
13	$26i \pm 1, \mp 3, \mp 5, \pm 7, \pm 9, \pm 11$	1, 2
14	$28i \pm 1, \pm 3, \pm 5, \pm 9, \mp 11, \pm 13$	1, 2, 3
15	$30i + 1, - 7, - 11, - 13,$	1, 3

n	Diuisores P	f
16	$32i + 1, - 3, + 5, - 7, + 9, - 11, + 13, - 15,$	1,4
17	$34i \pm 1, \pm 3, \mp 5, \pm 7, \pm 9, \pm 11, \pm 13, \mp 15,$	1,2,3
18	$36i \pm 1, \mp 5, \mp 7, \pm 11, \mp 13, \pm 17,$	1,2,3
19	$38i + 1, - 3, + 5, + 7, + 11, - 13, - 15, + 17,$	1,4
20	$40i + 1, + 3, + 7, + 9, - 11, - 13, - 17, - 19.$	1,3,4
21	$42i \pm 1, \pm 5, \pm 11, \mp 13, \pm 17, \pm 19,$	1,2,3
22	$44i \pm 1, \mp 3, \mp 5, \mp 7, \pm 9, \pm 13, \pm 15, \mp 17, \pm 19, \pm 21$	1,2
23	$46i + 1, + 3, - 5, - 7, + 9, - 11, + 13, - 15, - 17, - 19, - 21$	1,3,4
24	$48i + 1, + 5, + 7, + 11, - 13, - 17, - 19, - 23,$	1,3,5
25	$50i \pm 1, \mp 3, \mp 7, \pm 9, \mp 11, \pm 13, \mp 17, \mp 19, \pm 21, \mp 23,$	1,2
26	$52i \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \mp 11, \pm 15, \pm 17, \mp 19, \pm 21, \mp 23, \pm 25,$	1,2,3
27	$54i + 1, + 5, + 7, - 11, - 13, + 17, - 19, - 23, + 25.$	1,4
28	$56i + 1, - 3, - 5, + 9, + 11, - 13, + 15, - 17, - 19, - 21, + 23, + 25, - 27$	1,4
29	$58i \pm 1, \pm 3, \pm 5, \mp 7, \pm 9, \pm 11, \pm 13, \pm 15, \mp 17, \pm 19, \mp 21, \mp 23, \pm 25, \pm 27$	1,2,3,5
30	$60i \pm 1, \mp 7, \pm 11, \pm 13, \pm 17, \mp 19, \pm 23, \pm 29$	1,2,3,5
31	$62i + 1, - 3, + 5, + 7, + 9, - 11, - 13, - 15, - 17, + 19, - 21, - 23, + 25, - 27, - 29,$	1,5
32	$64i + 1, + 3, - 5, - 7, + 9, + 11, - 13, - 15, + 17, + 19, - 21, - 23, + 25, + 27, - 29, - 31,$	1,3,4
33	$66i \pm 1, \mp 5, \pm 7, \mp 13, \pm 17, \pm 19, \pm 23, \pm 25, \pm 29, \mp 31$	1,2,3
34	$68i \pm 1, \mp 3, \pm 5, \pm 7, \pm 9, \mp 11, \mp 13, \mp 15, \pm 19, \mp 21, \pm 23, \pm 25, \mp 27, \pm 29, \pm 31, \pm 33$	1,2,5
35	$70i + 1, + 3, + 9, + 11, + 13, + 17, - 19, - 23, + 27, + 29, - 31, + 33$	1,4,5

n

n	Diuisores P	f
36	$72i+1,+5,-7,-11,+13,+17,-19,-23,+25,+29,$ $-31,-35$	1,3,4,5
37	$74i\pm1,\mp3,\mp5,\mp7,\pm9,\mp11,\mp13,\pm15,\mp17,\pm19,$ $\pm21,\pm23,\pm25,\mp27,\mp29,\pm31,\pm33,\pm35$	1,2
38	$76i\pm1,\pm3,\mp5,\pm7,\pm9,\mp11,\pm13,\mp15,\pm17,\pm21,$ $\pm23,\pm25,\pm27,\pm29,\mp31,\mp33,\mp37,$	1,2,3,6
39	$78i+1,+5,-7,+11,-17,-19,-23,+25,-29,-31,$ $-35,-37,$	1,3,5
40	$80i+1,-3,+7,+9,+11,+13,-17,+19,-21,+23,$ $-27,-29,-31,-33,+37,-39$	1,4,5,7
41	$82i\pm1,\pm3,\pm5,\pm7,\pm9,\pm11,\mp13,\pm15\mp17,\pm19,$ $\pm21,\mp23,\pm25,\pm27,\mp29,\mp31,\pm33,\pm35,\pm37,$ ∓39	1,2,3,5,6
42	$84i\pm1,\mp5,\mp11,\pm13,\pm17,\mp19,\pm23,\pm25,\pm29,$ $\pm31,\mp37,\pm41$	1,2,3,6
43	$86i+1,-3,-5,-7,+9,+11,+13,+15,+17,-19,$ $+21,+23,+25,-27,-29,+31,-33,+35,-37,$ $-39,+41$	1,4
44	$88i+1,+3,+5,-7,+9,-13,+15,-17,-19,-21,$ $+23,+25,+27,-29,+31,-35,+37,-39,$ $-41,-43$	1,3,4,5
45	$90i\pm1,\pm7,\mp11,\mp13,\mp17,\mp19,\pm23,\pm29,\mp31,$ $\mp37,\pm41,\pm43$	1,2,3,5,7
46	$92i\pm1,\mp3,\pm5,\mp7,\pm9,\pm11,\mp13,\mp15,\mp17,\pm19,$ $\pm21,\pm25,\mp27,\mp29,\pm31,\mp33,\mp35,\pm37,\pm39,$ $\pm41,\pm43,\pm45$	1,2,5
47	$94i+1,+3,-5,+7,+9,-11,-13,-15,+17,-19,+21$ $-23,+25,+27,-29,-31,-33,-35,+37,-39,$ $-41,-43,-45$	1,3,7
48	$96i+1,-5,+7,-11,+13,-17,+19,-23,+25,$ $-29,+31,-35,+37,-41,+43,-47$	1,3,4,7

n	Diuisores P	f
49	$98i \pm 1, \mp 3, \pm 5, \pm 9, + 11, \pm 13, \mp 15, \pm 17, + 19, + 23, \pm 25, \mp 27, \pm 29, \mp 31, \pm 33, \pm 37, \mp 39, \pm 41, \mp 43, \pm 45, \mp 47$	1, 2, 5
50	$100i \pm 1, \pm 3, \mp 7, \pm 9, \pm 11, \mp 13, \pm 17, \pm 19, \mp 21, \mp 23, \pm 27, \mp 29, \mp 31, \pm 33, \mp 37, \mp 39, \pm 41, \pm 43, \mp 47, \pm 49$	1, 2, 3, 6

Scholion 2.

§. 27. Haec tabula facili negotio quousque libuerit continuari poteſt. Propoſito enim quocunque numero n, pro formula $2ni + A$ quaerantur primo omnes numeri primi minores quam n ſimulque ad n primi, quibus ſignum $+$ tribuatur, ſi n fuerit formae vel $4k$ vel $4k - 1$; caſibus autem quibus n eſt formae $4k + 1$ vel $4k + 2$, praefigendum eſt ſignum ambiguum $\pm$; reliquis vero numeris primis praefigatur ſiue ſignum $-$ ſiue ambiguum $\mp$. Quodſi n diuiſores habeat impares, eos omnes ex valoribus ipſius A excludi oportet, reliqui vero numeri primi deſumantur ex diuiſoribus numerorum in hac formula $n + xx$ contentorum, dum loco x ſucceſſiue ſcribuntur ordine numeri 1, 2, 3, 4, 5, etc. quos autem non vltra $\frac{1}{2}n$ continuare opus eſt. Si enim p denotet maximum numerum primum minorem quam n, niſi is fuerit diuiſor formae $n + xx$, ſumto $x < \frac{1}{2}p$, tum certe non erit diuiſor, quantumuis magni numeri ſcribantur. Hoc ergo modo facile omnes numeri loco A ſcribendi deteguntur, quibus inuentis numeri compoſiti facile ex ipſa compoſitione colliguntur, dum ſignum cuiusque producti ex ſignis factorum more ſolito formatur. Totam hanc operationem operae pretium erit aliquot exemplis declarare. Sit igitur primo $n = 40$, ideoque formae $4k$, vnde omnes valores A ſignis ſimplicibus afficienficientur. Quia iam 37 eſt maximus numerus primus infra 40, ſufficiet numeros x vsque ad 18 continuaſſe. Hos ergo valores formae $40 + xx$ hic vna cum ſingulis diuiſoribus primis infra 40, praeter 5, apponamus:

$n + xx$	Diuiſores.	$n + xx$	Diuiſores.
41	—	140	7
44	11	161	7, 23
49	7	184	23
56	7	209	11, 19
65	13	236	—
76	19	265	—
89	—	296	37
104	13	329	7
121	11	364	7, 13

Hinc ergo numeri primi ſigno + afficiendi ſunt +1, +7, +11, +13, +19, +23, +37, reliqui vero numeri primi minores quam 40 habebunt ſignum —, eruntque —3, —17, —29, —31, atque ex his numeri compoſiti erunt +9, —21, —27, —33, —39, quocirca formula pro diviſoribus primis P erit ſequens:

$$80i + 1, -3, +7, +9, +11, +13, -17, +19, -21, +23 -27, -29, -31, -33, +37, -39.$$

Pro altero exemplo ſumatur $n = 41$, qui numerus cum ſit formae $4k + 1$, ſigna ambigua erunt adhibenda. Quaerantur igitur primo omnes diuiſores primi numerorum formae $41 + xx$, quos non vltra $x = 18$ continuare eſt opus, quia maximus numerus primus infra 41 eſt 37, cuius dimidium eſt 18; haec ergo operatio vt ante inſtituatur.

$n+xx$	Diuisores.	$n+xx$	Diuisores.
42	3, 7	141	3 —
45	3, 5	162	3
50	5	185	5, 37
57	3, 19	210	3, 5, 7
66	3, 11	237	3
77	7, 11	266	7, 19
90	3, 5	297	3, 11
105	3, 5, 7	330	3, 5, 11
122	—	365	5

Numeri ergo primi ſigno $\pm$ afficiendi ſunt ± 1, ± 3, ± 5, ± 7, ± 11, ± 19, ± 37, reliqui vero ſigno $\mp$ afficiendi ſunt ∓ 13, ∓ 17, ∓ 23, ∓ 29, ∓ 31, vnde numeri compoſiti colliguntur ± 9, ± 15, ± 21, ± 25, ± 27, ± 33, ± 35, ∓ 39, quare formula pro diuiſoribus primis P ita ſe habebit:

$$82i \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \mp 13, \pm 15, \mp 17, \pm 19, \pm 21, \mp 23, \pm 25, \pm 27, \mp 29, \mp 31, \pm 33, \pm 35, \pm 37, \mp 39.$$

Scholion 3.

§. 28. Quod ad indices f pro quouis numero n attinet, forma generalis, quam illuſtris *de la Grange* pro diuiſoribus formae $xx+nyy$ dedit, conſiderari debet, quae erat $fpp+2gpq+hqq$, exſiſtente $fh=n+gg$, vbi notetur, plures huiusmodi formulas quouis caſu non opus eſſe formari, quam vbi $2g$ non excedit f; praeterea autem hic pro f ſumimus minorem factorem formulae $n+gg$; tum vero neceſſe eſt, vt alter numerorum f et h ſit par, hocque pacto facile erit, omnes indices f aſſignare. Ita pro priori exemplo ſupra allato, vbi $n=40$, ſumatur primo $g=0$, eritque $fh=40=5.8$,

ſicque

ſicque erit $f = 5$; deinde ſumto $g = 1$ fiet $fh = 41$, ideoque $f = 1$; ſumto porro $g = 2$ erit $fh = 44$, ideoque $f = 4$; ſumto autem $g = 3$, ob $fh = 49$ eſſe poterit $f = 7$, vnde omnes valores ipſius f erunt 1, 4, 5, 7. Pro altero exemplo, quo $n = 41$, valor $g = 0$ tantum dat $f = 1$; valor $g = 1$ praebet $fh = 42$, hincque vel $f = 2$, vel $f = 3$, vel $f = 6$; porro valor $g = 2$ praebet $fh = 45$, vnde colligitur $f = 5$; denique valor $g = 3$ dat $fh = 50$, vnde iterum ſequitur $f = 5$, ſicque omnes valores pro f ſunt 1, 2, 3, 5, 6. Hinc ergo colligimus, quoties pro formula $xx + 41yy$ prodeat P numerus primus, tum ſemper fore vel P, vel 2P, vel 3P, vel 5P, vel 6P, certum numerum formae $xx + 41yy$. Veluti ſumto $i = 1$, quia eſt $82 - 3 = 79$, ideoque numerus primus, ſtatim patet, hunc ipſum numerum 79 in forma $xx + 41yy$ non contineri, neque etiam eius duplum 158: at eius triplum 237 eſt $14^2 + 41 . 1^2$. Simili modo pro P etiam reperitur numerus primus 73, qui neque ipſe, neque eius duplum, neque triplum in propoſita forma continetur, at vero eius quintuplum 365 eſt $= 18^2 + 41 . 1^2$.

Problema.

Si n *fuerit numerus negatiuus, puta* $n = -m$, *inuenire formulam generalem pro omnibus numeris primis, qui exſiſtere posſunt diuiſores cuiuspiam numeri formae* $xx - myy$, *vel etiam formae* $myy - xx$.

Solutio.

§. 29. Solutio huius problematis inſtituatur vti praecedentis, ſcribendo ſcilicet $-m$ loco n, tum vero ſi P denotet diuiſorem primum formulae propoſitae, quoniam is neceſſario eſſe debet poſitiuus, etiam numerum i negatiuum accipi

 conuenit

conuenit, vnde formula ſupra inuenta euadet

$$P = 4mi + \frac{ss - muu}{\lambda},$$

vel etiam

$$P = 4mi - \frac{ss + muu}{\lambda},$$

ex quo manifeſtum eſt, omnes numeros primo membro $4mi$ adiungendos tam poſitiue quam negatiue accipi poſſe, ita vt generatim habeamus $P = 4mi \pm A$, vbi A denotat omnes diuiſores, ſiue formulae $ss - m$, ſiue formulae $m - ss$, qui quidem ad $4n$ ſint primi, vnde ex his diuiſoribus excluduntur primo omnes numeri pares, deinde etiam ii impares, qui cum numero m communem inuoluunt diuiſorem.

§. 30. Quodſi multitudo omnium numerorum ad $4n$ primorum eoque minorum ſit $= 4k$, numerus valorum ipſius A tantum erit $= k$, qui autem ob ſigna ambigua cenſendus eſt $= 2k$, ita vt numerus excluſorum itidem ſit $= 2k$. Hoc obſeruato, ſi a fuerit diuiſor formae $m - ss$, vel $ss - m$, tum quoties $4mi \pm a$ fuerit numerus primus, is ſemper erit diuiſor numeri cuiuſpiam formae propoſitae; contra autem, ſi α fuerit numerus hinc excluſus, tum certe affirmare licet, nullum numerum formae $4mi \pm \alpha$ vnquam diuiſorem eſſe poſſe formae propoſitae.

§. 31. Ex theoremate autem illuſtris *de la Grange* omnes diuiſores formae propoſitae continentur in hac formula generali: $fpp \pm 2gpq - hgg$, exſiſtente $fh = m - gg$, quas autem formulas eo vsque tantum continuare opus eſt, donec $2g$ ſuperet f; ſemper enim nobis denotet f minorem binorum factorum, in quos numerus $m - gg$ reſoluitur. Praeterea vero, vt caſu praecedente, alter numerorum f et h ſumi debet impar; vnde intelligitur, pro quouis caſu multitudinem valo-

valorum ipſius f ſatis fore modicam, quibus inuentis omnes diuiſores primi P, vel ipſi, vel per quempiam valorem ipſius f multiplicati, in forma propoſita continebuntur, idque non vnico modo, vti caſu praecedente vſu venit, ſed infinitis adeo modis.

§. 32. Hinc autem merito excludimus caſus quibus m eſt numerus quadratus, quia tum omnes plane numeri primi, nullo excluſo, euadere poſſunt diuiſores formae propoſitae, id quod etiam inde patet, quod pro A ſumi debent omnes diviſores formulae $ss - m$; hinc enim ſi fuerit $m = ll$, et capiatur $s = l$, haec formula fit o, at vero ciphra per omnes plane numeros eſt diuiſibilis.

Corollarium 1.

§. 33. Quodſi ergo a fuerit diuiſor cuiuspiam numeri formae $xx - myy$, tum omnes numeri primi tam in hac forma $4mi + a$, quam in hac: $4mi - a$, certe erunt diviſores cuiuspiam numeri formae propoſitae; tum vero etiam vel ipſi, vel per quempiam valorem ipſius f multiplicati, in eadem forma continebuntur.

Corollarium 2.

§. 34. Quoniam omnes valores ipſius A tam poſitiue quam negatiue accipiuntur, eos non vltra terminum $2m$ continuari neceſſe eſt, ideoque ſi numeri $m - ss$, vel $ss - m$, ordine ſcribantur, valores litterae s non vltra $\frac{1}{2}p$ continuare opus eſt, ſiquidem p denotet maximum numerum primum minorem quam $2m$.

Corollarium 4.

§. 35. Cum valores producti fh ſint m, $m-1$, $m-4$, $m-9$, $m-16$, $m-25$, etc., qui ab initio decreſcunt, ſi ex quopiam maiore ſumatur fh, in minoribus vero occurrant ſiue fk, ſiue kk, ita vt k ſit $< f$, tum in indices loco f referri debet k; vnde ſi fuerit $k = 1$, multitudo indicum hinc non augebitur: ſi enim fuerit fP formae $xx - myy$, ſiue $myy - xx$, tum etiam ſemper hP eandem habebit formam, ideoque etiam kP eandem formam habebit.

Scholion 1.

§. 36. Poſtquam omnes numeri primi ipſo $4m$ minores ſimulque ad eum primi, fuerint notati, qui ſint a, b, c, d, etc. reliqui etiam notentur, qui ſint α, β, γ, δ, etc. et numeri compoſiti vel erunt producta ex numeris a, b, c, d, etc. vel producta ex binis excluſorum α, β, γ, δ, etc. Quodſi ergo P denotet omnes diuiſores primos numerorum formae $xx - myy$, ſumamus Π pro denotandis numeris inde excluſis, erit

$$P = 4mi \pm (a, b, c, d, e, \text{etc.}),$$
$$\Pi = 4mi \pm (\alpha, \beta, \gamma, \delta, \varepsilon, \text{etc.}),$$

vnde pro quouis numero m iſtae binae formulae facile conſtruentur; ſemper autem ambae pari terminorum numero conſtabunt. Veluti ſi fuerit $m = 21$, ita vt ex diuiſoribus excludi debeant numeri 3 et 7 cum ſuis multiplis, euoluantur numeri ex forma $21 - ss$ oriundi, nullo reſpectu habito ſiue ſint poſitiui ſiue negatiui, et pro quouis notentur diuiſores primi, praeter 3 et 7, non ſuperantes $2m = 42$, quae operatio hoc modo inſtituatur.

$21 - ss$	Diuifores.	$21 - ss$	Diuifores.
21		79	—
20	5	100	5
17	17	123	41
12	—	148	37
5	5	175	5
4	—	204	17
15	5	235	—
28	—	268	—
43	—	303	—
60	5	340	17, 5

Hinc ergo valores pro litteris a, b, c, d, funt 5, 17, 37, 41, exclufi vero, litteris α, β, γ, δ, etc. denotati, funt 11, 13, 19, 23, 29, 31: ad illos igitur accedit compofitus 25, ita vt ambae noftrae formulae futurae fint

$$P = 84 i \pm (1, 5, 17, 25, 37, 41),$$
$$\Pi = 84 i \pm (11, 13, 19, 23, 29, 31).$$

Sicque vtraque forma eodem terminorum numero conftat, id quod femper fieri neceffe eft. Pro productis autem fh, prouti ex terminis decrefcentibus oriuntur, habebimus fequentia: 3.7, 4.5, 3.4, 1.5, 1.4, ex quorum minimis 5 et 4 patet, vnitatem tantum inter indices effe referendam. Hinc ex 3.4 etiam 3 ad vnitatem reducitur, vnde concluditur, vnicum dari indicem 1. Hic conueniebat etiam formulas afferre pro numeris qui nullo modo diuifores effe poffunt, quas in fuperiori tabula fuperfluum fuiffet adiungere, quoniam fi in formulis pro P datis fingula figna in contraria mutentur, tum eae praebebunt omnes numeros Π.

Tabula

Tabula exhibens omnes diuifores primos pro numeris formae vel $xx - myy$ vel $myy - xx$, vna cum indicibus f.

Vbi perpetuo figna ambigua fimul locum inueniunt.

m	P et Π.	f
2	$8i \pm 1$	1
	$8i \pm 3$	
3	$12i \pm 1$	1
	$12i \pm 5$	
5	$20i \pm (1, 9)$	1
	$20i \pm (3, 7)$	
6	$24i \pm (1, 5)$	1
	$24i \pm (7, 11)$	
7	$28i \pm (1, 3, 9)$	1
	$28i \pm (5, 11, 13)$	
8	$32i \pm (1, 7, 9, 15)$	1
	$32i \pm (3, 5, 11, 13)$	
10	$40i \pm (1, 3, 9, 13)$	1, 2
	$40i \pm (7, 11, 17, 19)$	
11	$44i \pm (1, 5, 7, 9, 19)$	1
	$44i \pm (3, 11, 13, 17, 21)$	
12	$48i \pm (1, 11, 13, 23)$	1
	$48i \pm (5, 7, 17, 19)$	
13	$52i \pm (1, 3, 9, 17, 23, 25)$	1
	$52i \pm (5, 7, 11, 15, 19, 21)$	
14	$56i \pm (1, 5, 9, 11, 13, 25)$	1
	$56i \pm (3, 15, 17, 19, 23, 27)$	
15	$60i \pm (1, 7, 11, 17)$	1, 2
	$60i \pm (13, 19, 23, 29)$	

m	P et Π.	f
17	$68\,i \pm (1, 9, 13, 15, 19, 21, 25, 33)$	1
	$68\,i \pm (3, 5, 7, 11, 23, 27, 29, 31)$	
18	$72\,i \pm (1, 7, 17, 23, 25, 31)$	1
	$72\,i \pm (5, 11, 13, 19, 25, 35)$	
19	$76\,i \pm (1, 3, 5, 9, 15, 17, 25, 27, 31)$	1
	$76\,i \pm (7, 11, 13, 21, 23, 29, 33, 35, 37)$	
20	$80\,i \pm (1, 9, 11, 19, 21, 29, 31, 39)$	1
	$80\,i \pm (3, 7, 13, 17, 23, 27, 33, 37)$	
21	$84\,i \pm (1, 5, 17, 25, 37, 41)$	1
	$84\,i \pm (11, 13, 19, 23, 29, 31)$	
22	$84\,i \pm (1, 3, 7, 9, 13, 21, 25, 27, 29, 39)$	1
	$84\,i \pm (5, 15, 17, 19, 23, 31, 35, 37, 41, 43)$	
23	$92\,i \pm (1, 7, 9, 11, 13, 15, 19, 25, 29, 41, 43)$	1
	$92\,i \pm (3, 5, 17, 21, 27, 31, 33, 35, 37, 39, 45)$	
24	$96\,i \pm (1, 5, 19, 23, 25, 29, 43, 47)$	1
	$96\,i \pm (7, 11, 13, 17, 31, 35, 37, 41)$.	

Scholion 2.

§. 37. Manifeſtum hic eſt, formulas P et Π pro caſu $m = 24$ non differre ab iis, quae pro caſu $m = 6$ ſunt datae, quemadmodum rei natura poſtulat, quoniam forma $xx - 6yy$ redigitur ad formam $xx - 24yy$, dum in priore loco y ſcribitur $2y$, quae conuenientia in genere locum habere debet, ſi numerus m per 4, aliumue numerum quadratum, multiplicetur. Eadem quoque harmonia reperitur in formulis prioris problematis: interim tamen diſcrimen intercedere poteſt ratione indicum f, quam ob cauſſam tales caſus a ſe inuicem diſtinximus. His igitur expeditis coronidis loco ſubiungam duo theoremata, quibus in caſibus prioris problematis formulae P ad ad membrum $2ni$ ſunt reductae, et quorum veritatem ex hactenus traditis haud difficulter cognoſcere licebit.

Theorema 3.

§. 38. Si fuerit $n = 4k + 1$, vel $n = 4k + 2$, quoties fuerit $4ni + 2n + 1$ numerus primus, is erit diuiſor formae $xx + nyy$.

Theorema 4.

§. 39. Si fuerit vel $n = 4k$, vel $n = 4k - 1$, tum, quoties fuerit $4ni - 2n + 1$ numerus primus, is erit diuiſor formae $xx + nyy$.

INVESTI-