

NOVAE DEMONSTRATIONES  
CIRCA DIVISORES NUMERORVM

FORMAE  $xx + nyy$ .

Auctore

L. EVLERO.

---

Conuent. exhib. d. 20 Nouembr. 1775.

---

Cum nuper eximia inuenta Illustris de la Grange super divisoribus numerorum formae  $xx + nyy$  recensuissem et cum meis obseruationibus, quas olim plerumque per inductionem erueram, contulissem, quippe quae inde haud exiguum firmitermentum acceperant, non dubitavi 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 perpensissem, mihi quoque contigit praecipua momenta, quibus istae exoptatae demonstrationes innituntur, perspicere, quae igitur hic exponere constitui.

Theorema I.

§. I. 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 ut forma  $xx + ny^2$  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 usque ad 100 est 46. Reliqui ergo numeri qui diuisorem 13 a formula  $xx + ny^2$  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  $xx + 13yy$ , vtrum diuisorem 13 accipiat, quaestio esse non potest, quia manifesto numerus deberet esse diuisibilis per 13.

### Scholion 2.

§. 10. Quoniam vis nostrae demonstrationis clarior 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  $xx + nyy$  diuisorem 19 recipere poterit, si numerus  $n$  in sequenti forma contineatur:

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

sin autem  $n$  contineatur in sequenti 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 est 47. Reliqui vero numeri ad hunc scopum inepti, exclusis multiplis ipsius 19, erunt numero 48 sequentes:

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, 85, 87, 92, 93, 96, 99, 100.

### Scholion 3.

§. II. Quo autem facilius intelligatur, quomodo quouis casu, vbi numerus  $n$  idoneum habet valorem, formula  $xx + nyy$  diuisibilis reddatur per numerum primum  $P$ , notetur, hoc semper fieri posse, dum pro  $x$  et  $y$  numeri non maiores quam  $\frac{1}{2}(P - 1)$  accipiantur, atque adeo alterum horum numerorum  $y$  pro lubitu accipi posse. Sit igitur  $y = 1$ , ita vt habeatur haec formula:  $xx + n$ , numerique  $n$  residuum nascatur  $r$ ; tum igitur pro  $xx$  id quaeratur quadratum, cui conueniat residuum  $P - r$ , ac manifesto summa  $xx + n$  per  $P$  erit diuisibilis. Hoc autem semper fieri posse euidens est, cum sit  $n = \lambda P - a$ , vnde fit residuum  $r = P - a$ , ideoque

G 3

P - r

$P - r = a$ , sicque pro  $xx$  id sumi debet quadratum, cui respondet residuum  $a$ . Ita sumto  $P = 13$  accipiatur pro  $n$ , pro lubitu, valor idoneus ex supra inuentis, veluti  $n = 82$ , et quaeratur  $x$  ita, vt fiat forma  $xx + 82$  per  $13$  diuisibilis. Hic autem fit residuum  $r = 4$ , hincque  $P - r = 9$ ; erit ergo  $x = 3$  et formula  $3^2 + 82$  per  $13$  diuidi potest. Simili modo si pro diuisore  $19$  sumatur  $n = 88$ , inde oritur residuum  $r = 12$ , ideoque  $P - r = 7$ ; quadratum autem, quod per  $19$  diuisum relinquit  $7$ , est  $64$ , sicque formula  $8^2 + 88$  prodit diuisibilis per  $19$ . Atque hinc deduci potest facilior et concinnior demonstratio nostri Theorematis.

### Alia Demonstratio Theorematis 2.

§. 12. Ostendi scilicet potest, si fuerit  $n = \lambda P - a$ , tum semper dari numerum  $x$ , vt formula  $xx + n$  diuisionem admittat: tantum enim pro  $xx$  id sumatur quadratum, quod per  $P$  diuisum relinquat  $a$ , quod ergo erit formae  $\mu P + a$ ; quare ob  $n = \lambda P - a$ , erit formula  $xx + n = (\mu + \lambda) P$ , ideoque manifesto diuisibilis per numerum  $P$ .

### Scholion I.

§. 13. Cum igitur pro quolibet numero primo  $P$  facile omnes valores numeri  $n$  exhiberi queant, quibus forma  $xx + nyy$  diuisionem per  $P$  admittere potest, quandoquidem, denotante  $a$  residua omnia ex diuisione quadratorum per  $P$  oriunda, inuenimus  $n = \lambda P - a$ : manifestum est, pro  $n$  etiam infinitos valores negatiuos dari, qui oriuntur, si pro  $\lambda$  etiam numeri negatiui accipiantur. Quamobrem non inutile erit, pro numeris primis simplicioribus formulas exhibere, quae omnes valores idoneos numeri  $n$  contineant, quibus forma  $xx + nyy$  per numerum primum  $P$  diuisibilis 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  $\lambda$  negatiuo erit  $m = \lambda P + a$ , quae forma cum contineat omnes numeros quadratos, quicumque numerus primus pro  $P$  accipiatur; patet, si fuerit  $m$  numerus quadratus, scilicet  $m = k^2$ , numeros formae  $xx - kky$  per omnes plane numeros primos diuisibiles existere posse, quo ergo casu nulli numeri primi excluduntur, id quod per se est manifestum, quoniam formula  $xx - kky$  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 cuiusvis numeri primi  $P$  omnes numeri in duas classes distinguuntur, quarum altera

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 existere possunt formae  $xx + nyy$ , altera vero reliquos, qui nullo modo huius formae diuisores existere possunt. Pro vtraque autem classe iam olim formulas dedi generales, similes illis, quibus hic pro quolibet numero primo valores idoneos numeri  $n$  ab ineptis distinxī: 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:  $4ni + \mathcal{A}$ , vbi litterae  $A$  et  $\mathcal{A}$  simul complectuntur omnes numeros ad  $4n$  primos ipsoque minores, ex quibus littera  $A$  continet eos qui ad diuisionem sunt apti, littera vero  $\mathcal{A}$  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  $4ni + \mathcal{A}$  eos inuoluit, qui nullo modo diuisores existere possunt. Interim tamen has ambas formulas sequenti modo ex positis principiis derivare licebit.

### Problema.

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

Solutio.

### Solutio.

§. 16. Denotet  $P$  diuisorem quemcunque primum formae propositae  $xx + ny, y$ , sitque  $\lambda$  quotus ex hac diuisione oriundus, atque habebimus hanc aequationem:  $\lambda P = xx + ny, y$ , 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  $\lambda i$ , vt scilicet prius membrum per  $\lambda$  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  $\lambda$  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  $ab, ac,$

$ac, bc$ , 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  $\lambda$  non fuerit unitas, seu qui tantum sint diuifores formae  $ss + nuu$ , quorum multitudo videri posset indefinita, recurrere debemus ad theorema Illustris *de la Grange*, quo demonstrauit, omnes diuifores numerorum formae  $ss + nuu$  semper contineri in hac formula:  $fpp + 2gpq + bqq$ , existente  $fb = gg + n$ , neque has formulas vterius continuari opus esse, quamdiu fuerit vel  $2g < f$ , vel  $2g < b$ , quarum formarum numerus semper est satis modicus. Hinc igitur semper pro  $A$  accipere licebit vel  $f$  vel  $b$ , nisi forte ad  $4n$  non fuerint primi. Hoc enim casu pro  $A$  sumi conueniet vel numeros  $f + 2g + b$ , vel  $4f + 4g + b$ , vel  $f + 4g + 4b$ , 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  $\alpha, \beta, \gamma, \delta$ , etc. hi dabunt omnes valores litterae  $\mathcal{A}$  pro formula  $4ni + \mathcal{A}$ , quae omnes  
conti-



continet numeros primos, qui nullo modo diuifores esse possunt vllius numeri in forma  $x x + n y y$  contenti.

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

§. 22. Cum igitur formula  $4 n i + A$  certe omnes numeros contineat, qui nullo modo esse possunt diuifores formae  $x x + n y y$ , necesse est vt omnes numeri primi in forma  $4 n i + A$  contenti simul sint diuifores cuiuspiam formae  $x x + n y y$ .

### Corollarium 1.

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

### Corollarium 2.

§. 24. Quoniam pro quouis numero  $n$  forma diuisorum *Grangiana*  $f p p \pm 2 g p q + b q q$  exiguam variationem  
H 2
reci-

recipit, quandoquidem ea semper ita reduci potest, ut  $2g$  fiat minus quam  $f$  vel  $b$ , si valores isti minores designentur littera  $f$ , tum omnes diuisores primi numerorum formae  $xx + nyy$  vel ipsi erunt eiusdem formae, vel per  $f$  multiplicati, unde si  $f$  alios non habeat valores praeter unitatem, quod euenit casibus  $n = 1$ ,  $n = \pm 2$  et  $n = \pm 3$ , tum omnes diuisores primi his casibus quoque ipsi habebunt eandem formam.

### Corollarium 3.

§. 25. Quoniam omnes valores pro littera  $A$  debent esse numeri impares, omnes formae  $fp p \pm 2gpq + bqq$  hinc sunt excludendae, in quibus ambo numeri  $f$  et  $b$  pares. Quare cum sit  $fb = gg + n$ , numerum  $gg + n$  ita in duos factores resolui conuenit, ut alter saltem euadat impar, unde si numerus  $gg + n$  plures habeat diuisores pares, plures resolutiones tanquam inuiles erunt reiiciendae.

### Scholion 1.

§. 26. Quemadmodum valores litterae  $A$  pro forma  $4ni + A$  sunt minores quam  $4n$ , ita si negativos introducere velimus, eos infra  $2n$  deprimere licebit. Obseruauimus autem porro, pro omnibus casibus, quibus  $n$  est numerus positius, multitudinem istorum valorum ipsius  $A$  ad semissem redigi posse, ita ut 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	$6i \pm 1$	1
4	$8i \pm 1, -3$	1
5	$10i \pm 1, \pm 3$	1, 2
6	$12i \pm 1, \pm 5$	1, 2
7	$14i \pm 1, -3, +5$	1
8	$16i \pm 1, +3, -5, -7$	1, 3
9	$18i \pm 1, \pm 5, \mp 7,$	1, 2
10	$20i \pm 1, +3, \pm 7, \pm 9$	1, 2
11	$22i \pm 1, +3, +5, -7, +9$	1, 3
12	$24i \pm 1, -5, +7, -11,$	1, 3
13	$26i \pm 1, +3, +5, \pm 7, \pm 9, \pm 11$	1, 2
14	$28i \pm 1, \pm 3, \pm 5, \pm 9, \mp 11, \pm 13$	1, 2, 3
15	$30i \pm 1, -7, -11, -13,$	1, 3

H 3

"

<i>n</i>	Diuifores P	<i>f</i>
16	$32i + 1, -3, +5, -7, +9, -11, +13, -15,$	1,4
17	$34i \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \pm 13, \pm 15,$	1,2,3
18	$36i \pm 1, \pm 5, \pm 7, \pm 11, \pm 13, \pm 17,$	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	$42i \pm 1, \pm 5, \pm 11, \pm 13, \pm 17, \pm 19,$	1,2,3
22	$44i \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 13, \pm 15, \pm 17, \pm 19,$ $\pm 21$	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	$50i \pm 1, \pm 3, \pm 7, \pm 9, \pm 11, \pm 13, \pm 17, \pm 19, \pm 21,$ $\pm 23,$	1,2
26	$52i \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \pm 15, \pm 17, \pm 19,$ $\pm 21, \pm 23, \pm 25,$	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	$58i \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \pm 13, \pm 15, \pm 17,$ $\pm 19, \pm 21, \pm 23, \pm 25, \pm 27$	1,2,3,5
30	$60i \pm 1, \pm 7, \pm 11, \pm 13, \pm 17, \pm 19, \pm 23, \pm 29$	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	$66i \pm 1, \pm 5, \pm 7, \pm 13, \pm 17, \pm 19, \pm 23, \pm 25, \pm 29,$ $\pm 31$	1,2,3
34	$68i \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \pm 13, \pm 15, \pm 19, \pm 21,$ $\pm 23, \pm 25, \pm 27, \pm 29, \pm 31, \pm 33$	1,2,5
35	$70i + 1, +3, +9, +11, +13, +17, -19, -23, +27, +29,$ $-31, +33$	1,4,5

n	Divisores P	f
36	$72i + 1, +5, -7, -11, +13, +17, -19, -23, +25, +29, -31, -35$	1, 3, 4, 5
37	$74i + 1, +3, +5, +7, +9, +11, +13, +15, +17, +19, +21, +23, +25, +27, +29, +31, +33, +35$	1, 2
38	$76i + 1, +3, +5, +7, +9, +11, +13, +15, +17, +21, +23, +25, +27, +29, +31, +33, +37$	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	$82i + 1, +3, +5, +7, +9, +11, +13, +15, +17, +19, +21, +23, +25, +27, +29, +31, +33, +35, +37, +39$	1, 2, 3, 5, 6
42	$84i + 1, +5, +11, +13, +17, +19, +23, +25, +29, +31, +37, +41$	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	$90i + 1, +7, +11, +13, +17, +19, +23, +29, +31, +37, +41, +43$	1, 2, 3, 5, 7
46	$92i + 1, +3, +5, +7, +9, +11, +13, +15, +17, +19, +21, +25, +27, +29, +31, +33, +35, +37, +39, +41, +43, +45$	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	$f$
48	$98i \pm 1, \pm 3, \pm 5, \pm 9, \pm 11, \pm 13, \pm 15, \pm 17, \pm 19, \pm 23,$ $\pm 25, \pm 27, \pm 29, \pm 31, \pm 33, \pm 37, \pm 39, \pm 41, \pm 43,$ $\pm 45, \pm 47$	1, 2, 5
50	$100i \pm 1, \pm 3, \pm 7, \pm 9, \pm 11, \pm 13, \pm 17, \pm 19, \pm 21,$ $\pm 23, \pm 27, \pm 29, \pm 31, \pm 33, \pm 37, \pm 39, \pm 41, \pm 43,$ $\pm 47, \pm 49$	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 ultra  $\frac{1}{2}n$  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  $4k$ , unde omnes valores  $A$  signis simplicibus afficien-

ficientur. 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  $+$  affiendi 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 diuisoribus 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 ultra  $x = 18$  continuare est opus, quia maximus numerus primus infra 41 est 37, cuius dimidium est 18; haec ergo operatio vt ante instituitur.

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

$$\S 2i \pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11, \mp 13, \pm 15, \mp 17, \pm 19, \pm 21, \mp 23, \pm 25, \pm 27, \mp 29, \mp 31, \pm 33, \pm 35, \pm 37, \mp 39.$$

### Scholion 3.

§. 28. Quod ad indices  $f$  pro quouis numero  $n$  atinet, forma generalis, quam illustris *de la Grange* pro diuisoribus formae  $xx + ny$  dedit, considerari debet, quae erat  $fpp + 2gpq + bqq$ , existente  $fb = n + gg$ , 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  $b$  sit par, hocque pacto facile erit, omnes indices  $f$  assignare. Ita pro priori exemplo supra allato, vbi  $n = 40$ , sumatur primo  $g = 0$ , eritque  $fb = 40 = 5 \cdot 8$ ,  
sicque



ficque erit  $f = 5$ ; deinde sumto  $g = 1$  fiet  $fb = 41$ , ideo-  
 que  $f = 1$ ; sumto porro  $g = 2$  erit  $fb = 44$ , ideoque  $f = 4$ ;  
 sumto autem  $g = 3$ , ob  $fb = 49$  esse poterit  $f = 7$ , unde  
 omnes valores ipsius  $f$  erunt 1, 4, 5, 7. Pro altero exemplo,  
 quo  $n = 41$ , valor  $g = 0$  tantum dat  $f = 1$ ; valor  $g = 1$  prae-  
 bet  $fb = 42$ , hincque vel  $f = 2$ , vel  $f = 3$ , vel  $f = 6$ ;  
 porro valor  $g = 2$  praebet  $fb = 45$ , unde colligitur  $f = 5$ ;  
 denique valor  $g = 3$  dat  $fb = 50$ , unde iterum sequitur  
 $f = 5$ , ficque 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  $14^2 + 41 \cdot 1^2$ . Simili modo pro P etiam re-  
 peritur numerus primus 73, qui neque ipse, neque eius du-  
 plum, neque triplum in proposita forma continetur, at vero  
 eius quintuplum 365 est  $= 18^2 + 41 \cdot 1^2$ .

### Problema.

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

### Solutio.

§. 29. Solutio huius problematis instituat uti prae-  
 cedentis, scribendo scilicet  $-m$  loco  $n$ , tum vero si P deno-  
 tet diuisorem primum formulae propositae, quoniam is neces-  
 sario esse debet positiuus, etiam numerum  $i$  negatiuum accipi

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 positue quam negatiue accipi posse, ita vt generatim habeamus  $P = 4mi \pm A$ , vbi  $A$  denotat omnes diuifores, siue formulae  $ss - m$ , siue formulae  $m - ss$ , qui quidem ad  $4n$  sint primi, vnde ex his diuiforibus excluduntur primo omnes numeri pares, deinde etiam ii impares, qui cum numero  $m$  communem inuoluunt diuiforem.

§. 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 diuifor formae  $m - ss$ , vel  $ss - m$ , tum quoties  $4mi \pm a$  fuerit numerus primus, is semper erit diuifor numeri cuiuspiam formae propositae; contra autem, si  $a$  fuerit numerus hinc exclusus, tum certe affirmare licet, nullum numerum formae  $4mi \pm a$  vnquam diuiforem esse posse formae propositae.

§. 31. Ex theoremate autem illustris *de la Grange* omnes diuifores formae propositae continentur in hac formula generali:  $fpp \pm 2gpq - bgg$ , existente  $fb = m - gg$ , 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  $b$  sumi debet impar; vnde intelligitur, pro quouis casu multitudinem

vale-

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 unico modo, vti casu praecedente vsu venit, sed infinitis adco 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 diuisores formulae  $ss - m$ ; hinc enim si fuerit  $m = ll$ , et capiatur  $s = l$ , haec formula fit 0, 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 diuisores 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 positive quam negative 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  $fb$  sint  $m, m-1, m-4, m-9, m-16, m-25, \text{etc.}$ , qui ab initio decrefcunt, fi ex quopiam maiore fumatur  $fb$ , in minoribus vero occurrant fiue  $fk$ , fiue  $kk$ , ita vt  $k$  fit  $< f$ , tum in indices loco  $f$  referri debet  $k$ ; vnde fi fuerit  $k=1$ , multitudo indicum hinc non augebitur: fi enim fuerit  $fP$  formae  $xx - myy$ , fiue  $myy - xx$ , tum etiam femper  $bP$  eandem habebit formam, ideoque etiam  $kP$  eandem formam habebit.

### Scholion 1.

§. 36. Postquam omnes numeri primi ipfo  $4m$  minores fimulque ad eum primi, fuerint notati, qui fint  $a, b, c, d, \text{etc.}$  reliqui etiam notentur, qui fint  $\alpha, \beta, \gamma, \delta, \text{etc.}$  et numeri compositi vel erunt producta ex numeris  $a, b, c, d, \text{etc.}$  vel producta ex binis exclusorum  $\alpha, \beta, \gamma, \delta, \text{etc.}$  Quodfi ergo  $P$  denotet omnes diuifores primos numerorum formae  $xx - myy$ , fumamus  $\Pi$  pro denotandis numeris inde exclusis, erit

$$P = 4mi \pm (a, b, c, d, e, \text{etc.}),$$

$$\Pi = 4mi \pm (\alpha, \beta, \gamma, \delta, \epsilon, \text{etc.}),$$

vnde pro quouis numero  $m$  istae binae formulae facile confluentur; femper autem ambae pari terminorum numero conflabunt. Veluti fi fuerit  $m=21$ , ita vt ex diuiforibus excludi debeant numeri 3 et 7 cum fuis multiplis, euoluantur numeri ex forma  $21 - ss$  oriundi, nullo respectu habito fiue fint pofitiui fiue negatiui, et pro quouis notentur diuifores primi, praeter 3 et 7, non fuperantes  $2m=42$ , quae operatio hoc modo inflituatur.

21 — 55	Diuisores.	21 — 55	Diuisores.
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  $a, b, c, d$ , sunt 5, 17, 37, 41, exclusi vero, litteris  $\alpha, \beta, \gamma, \delta$ , etc. denotati, sunt 11, 13, 19, 23, 29, 31: ad illos igitur accedit compositus 25, ita vt ambae nostrae formulae futurae sint

$$P = 84i \pm (1, 5, 17, 25, 37, 41),$$

$$\Pi = 84i \pm (11, 13, 19, 23, 29, 31).$$

Sicque vtraque forma eodem terminorum numero constat, id quod semper fieri necesse est. Pro productis autem  $fb$ , 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 esse 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 diuisores esse possunt, quas in superiori tabula superfluum fuisset adiungere, quoniam si in formulis pro P datis singula signa in contraria mutantur, tum eae praebebunt omnes numeros II.

Tabula

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

Vbi perpetuo signa ambigua simul locum inueniunt.

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

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

### Scholion 2.

§. 37. Manifestum hic est, formulas P et II 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 causam tales casus a se inuicem distinximus. His igitur expeditis coronidis loco subiungam duo theoremata, quibus in casibus prioris problematis formulae P

ad membrum  $2ni$  sunt reductae, et quorum veritatem ex  
hactenus traditis haud difficulter cognoscere licebit.

### Theorema 3.

§. 38. Si fuerit  $n = 4k + 1$ , vel  $n = 4k + 2$ , quo-  
ties fuerit  $4ni + 2n + 1$  numerus primus, is erit diuisor  
formae  $xx + ny$ .

### Theorema 4.

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