

570. Si numerus quispiam N duplici modo est summa duorum quadratorum, scilicet

$$N = aa + bb = cc + dd,$$

tum non est primus. Cum enim sit $aa - cc = dd - bb$, erit $d + b = \frac{n(a+c)}{n}$ et $d - b = \frac{n(a-c)}{m}$, unde $b = \frac{m(a+c)}{2n} - \frac{n(a-c)}{2m}$; hinc

$$N = aa + bb = \frac{(mm+nn)}{4mnn} (nn(a-c)^2 + mm(a+c)^2) = \frac{(mm+nn)}{4mn} ((a-c)^2 + (b+d)^2),$$

ubi denominatoris factorem tollere nequit. (*)

Caput XVI.

De divisoribus numerorum formae $xx + 2yy$.

571. Sumtis x et y inter se primis, vel ambo sunt impares, vel alteruter tantum par, ergo vel x , vel y erit par; ex quo tres resultant casus considerandi, qui cujusmodi numeros ratione paritatis et imparitatis praebeant, investigasse juvabit.

~~572. Si ambo numeri x et y sint impares, eorum quadrata sunt numeri formae $8n + 1$, fietque $xx + 2yy$ numerus formae $8n + 3$; sin autem x impar et y par, ob~~

$$xx = 8m + 1 \quad \text{et} \quad 2yy = 2 \cdot 4n,$$

~~fiet $xx + 2yy$ numerus formae $8n + 1$.~~

573. Si x sit par et y impar, ponatur $x = 2z$, et fiet $xx + 2yy = 2(2zz + yy)$; jam cum y sit impar, prout z fuerit vel par, vel impar, erit vel

$$xx + 2yy = 2(8n + 1), \quad \text{vel} \quad xx + 2yy = 2(8n + 3).$$

574. Omnes ergo numeri in forma $xx + 2yy$ contenti, dum x et y sunt primi inter se, vel saltem non ambo pares, si fuerint impares, pertinebunt vel ad formam $8n + 1$, vel ad $8n + 3$; sin autem illi numeri sint pares, vel ad formam $2(8n + 1)$, vel ad $2(8n + 3)$ erunt referendi, et casu hoc posteriori eorum semisses, scilicet $2zz + yy$ sunt etiam numeri formae $xx + 2yy$.

575. Numeri ergo impares, qui sunt vel formae $8n + 5$, vel formae $8n + 7$, certe non sunt numeri formae $xx + 2yy$, neque etiam dupla earum formarum in hac continentur, unde infiniti dantur numeri in forma $xx + 2yy$ non contenti.

576. Productum autem duorum numerorum hujus formae in eadem forma continentur; est enim $(aa + 2bb)(cc + 2dd) = (ac \pm 2bd)^2 + 2(ad \mp bc)^2$, unde simul patet talia producta duplici modo in ista forma contineri.

577. Jam demonstrandum est, si numerus $pp + 2qq$ dividi queat per $aa + 2bb$, fore quotum

(*) *Script. ad marg.* $(a+c)(a-c) = (b+d)(d-b) = pqrs$, $a+c = pq$, $a-c = rs$, $b+d = pr$, $d-b = qs$;
 $a = \frac{pq+rs}{2}$, $b = \frac{pr-qs}{2}$, $aa+bb = \frac{1}{4}(pp+ss)(qq+rr)$.

etiam istius formae. Notetur hic ob a et b primos ad $aa + 2bb$, infinitis modis fieri posse

$$p = m(aa + 2bb) \pm fa \quad \text{et} \quad q = n(aa + 2bb) \pm gb,$$

hincque fore $ffaa + 2ggbb$ per $aa + 2bb$ divisibile.

578. Si concedatur hoc modo omnes formulas $ffaa + 2ggbb$ per $aa + 2bb$ divisibiles obtineri, ibi etiam continebitur casus $gg = ff$, seu $g = \pm f$, unde prodit

$$\frac{pp + 2qq}{aa + 2bb} = \left\{ \begin{array}{l} mm(aa + 2bb) \pm 2mfa \\ 2nn(aa + 2bb) \pm 4ngb \end{array} \right. + ff = (f \pm ma \pm 2nb)^2 + 2(mb \mp na)^2.$$

579. Hoc autem, quod concedendum postulavi, ita confirmari potest. Sint $1, \alpha, \beta, \gamma, \delta$, etc. residua, quae ex divisione quadratorum per numerum $aa + 2bb$ oriuntur, atque in istis residuis continebuntur tam omnia quadrata, quam $-2bb$, et -2 , seu omnia quadrata negativa duplicata, hoc est $-2, -2\alpha, -2\beta, -2\gamma$, etc.

580. Jam quodcumque residuum quadratum qq per $aa + 2bb$ divisum relinquat, cum poni possit $q = n(aa + 2bb) \pm gb$, id per $ggbb$ exhiberi potest, et residuum, ex divisione ipsius $2qq$ ortum, per $2ggbb$; quadratum ergo pp per $aa + 2bb$ divisum relinquere debet $-2ggbb$; cujus loco poni potest $aagg$, sicque quadrata pp et $aagg$ paria relinquent residua, sicque fieri potest

$$p = m(aa + 2bb) \pm ag.$$

581. At haec demonstratio est rejicienda, nisi sit $aa + 2bb$ numerus primus, nam si sit primus, ob $ffaa + 2ggbb$ et $ggaa + 2ggbb$ divisibile per $aa + 2bb$, necesse est sit $ff - gg$, ideoque vel $f - g$, vel $f + g$ divisibile; utrovis autem casu, ob $aa + 2bb$ jam in altera parte contentum, prodit vel $g = +f$, vel $g = -f$; quae conclusio locum non habet, si $aa + 2bb$ sit numerus compositus, cum tunc $f - g$ per alterum ejus factorem, et $f + g$ per alterum divisibile esse posset.

582. Si numerus $pp + 2qq$ per numerum \mathcal{A} , qui non sit formae $xx + 2yy$, dividi queat, quotus non erit numerus primus formae $xx + 2yy$, quare si quotus sit primus, non erit formae $xx + 2yy$; at si sit compositus, certe non omnes factores primi erunt hujus formae.

583. Denotent enim A, B, C, D , etc. numeros primos formae $xx + 2yy$, ac si $pp + 2qq$ esset divisibile per $ABCD$ etc., quotus certe esset formae $xx + 2yy$; ergo si quotus, seu alter multiplicator non sit formae $xx + 2yy$, fieri nequit, ut alter factor sit productum talium numerorum primorum.

584. Quare si $pp + 2qq$ dividi queat per numerum \mathcal{A} ex forma $xx + 2yy$ exclusum, quotus, si sit primus, non erit hujus formae, vel si sit compositus, factorem certe habebit non hujus formae. (*)

585. Denotent $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$, etc. numeros primos ex forma $xx + 2yy$ exclusos, et vidimus $pp + 2qq$ non esse posse $\mathcal{A}\mathcal{A}$, neque $AB\mathcal{A}$, neque $ABC\mathcal{A}$, quare certum est, inter factores primos numerorum $pp + 2qq$ vel nullum, vel duos ad minimum numeros \mathcal{A}, \mathcal{B} contineri.

(*) *Script. ad marg.* Ergo $pp + 2qq$ per nullos numeros primos formae $8n + 5$ et $8n + 7$ dividi potest; unde si quadrata per tales numeros primos dividantur, inter non-residua erit -2 .

$$\text{Si } \frac{xx + nyy}{aa + nbb} = \text{integro, erit } \frac{bbxx - aayy}{aa + nbb} = \text{int. et } \frac{aaxx - nbbyy}{aa + nbb} = \text{int.}$$

586. Hinc autem nondum concludi potest, si unus factor, etiamsi sit compositus, ipsius $pp + 2qq$ fuerit formae $xx + 2yy$, etiam alterum fore hujus formae. Demonstrandum restat numerum $pp + 2qq$ non esse posse formae vel $2\mathfrak{B}$, vel $A2\mathfrak{B}$, vel $AB2\mathfrak{B}$, quod si esset, foret utique $2\mathfrak{B}$ numerus hujus formae.

587. Visuri autem an $pp + 2qq$ per numerum \mathfrak{A} non formae $xx + 2yy$ dividi queat, quod si fieri posset, foret $p < \frac{1}{2}\mathfrak{A}$ et $q < \frac{1}{2}\mathfrak{A}$, unde $pp + 2qq < \frac{5}{4}\mathfrak{A}\mathfrak{A}$, quotusque $< \frac{5}{4}\mathfrak{A}$, qui esset vel ipse numerus non $xx + 2yy$, vel factorem talem haberet \mathfrak{B} , qui cum etiam factor esset ipsius $pp + 2qq$, minimus talis numerus \mathfrak{B} assignari posset, divisor formae cujuspian $xx + 2yy$, quod cum fieri nequeat, numeri $pp + 2qq$ nullos habent divisores primos, qui non ipsi sint formae $xx + 2yy$.