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 $d - b = \frac{n(a - c)}{n}$, 
unde $b = \frac{m(a + c)}{2m} - \frac{n(a - c)}{2n}$; hinc

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

ubi denominatoris factorem tollere nequirit. (*)

---

Caput XVI.

De divisoribus numerorum formae $xx + 2yy$.

571. Summis $x$ et $y$ inter se primis, vel ambo sunt impares, vel altertus tantum par, ergo vel $x$, vel $y$ erit par; ex quod tres resultant casus considerandì, qui cujusmodi numeros ratione paritatis et imparitatis praebent, 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 $xx = 8m + 1$ et $2yy = 2.4n$, 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 $xx + 2yy = 2(8n - 1)$, vel $xx + 2yy = 2(8n - 3)$.

574. Omnes ergo numeri in forma $xx + 2yy$ contenti, dum $x$ et $y$ sunt primi inter se, vel saltam non ambo pares, si fuerint impares, pertinabant 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, siclicit $2zz + yy$ 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 tali producta duplici modo in ista forma contineri.

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

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

L. Euleri Op. posthuma. T. J. 10
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 $aa + 2bb$ divisibles.

578. Si concedatur hoc modo omnes formulas $ffaa + 2ggbb$ per $aa + 2bb$ divisibles obtineri, ibi etiam continebitur casus $gg = ff$, seu $g = \mp f$, unde prodit
\[ \frac{pp - 2qq}{aa + 2bb} = \left( \frac{mm}{2} \right) \frac{(aa + 2bb) \pm 2mfa}{f} - ff = \left( \frac{m}{2} \right) (ma + 2mb)^2 + 2(m = na)^2. \]

579. Hoc autem, quod concedendum postulari, 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 quodcunque residuum quadratum $qq$ per $aa + 2bb$ divisiorem 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 $aegg$, sicque quadrata $pp$ et $aegg$ paria relinquant 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 $aa + 2bb$, necessae est sit $ff - gg$, idque 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 $A$, qui non sit formae $xx + 2yy$, dividii quaeat, 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 eodem $A, B, C, D$, 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 $pp + 2qq$ dividii quaeat per numerum $A$ 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 $A, B, C, D$, etc. numeros primos ex forma $xx + 2yy$ exclusos, et vidimus $pp + 2qq$ non esse posse $AA$, neque $AB$, neque $ABC$, quare certum est, inter factores primos numerorum $pp + 2qq$ vel nullum, vel duos ad minimum numeros $A, B$ contineris.

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

Si $\frac{axx - ayy}{aa + nbb} = \text{integro, erit} \quad \frac{bxx - ayy}{aa + nbb} = \text{int. et} \quad \frac{axx - nblhy}{aa + nbb} = \text{int.}$
586. Hinc autem nondum concludi potest, si unus factor, etiam si sit compositus, ipsius \(pp + 2qq\) fenerit formae \(xx + 2yy\), etiam alterum fore hujus formae. Demonstrandum restat numerum \(pp + 2qq\) non esse posse formae vel \(AB\), vel \(A^2B\), vel \(AB^2\), quod si esset, foret utique \(AB\) numerus hujus formae.

587. Visuri autem an \(pp + 2qq\) per numerum \(A\) non formae \(xx + 2yy\) dividique quaeat, quod si fieri posset, foret \(p < \frac{1}{2}A\) et \(q < \frac{1}{2}A\), unde \(pp + 2qq + \frac{2}{A}\), quotusque \(< \frac{1}{2}A\); qui esset vel ipse numerus non \(xx + 2yy\), vel factorin talem haberet \(B\), qui cum etiam factor esset ipsius \(pp + 2qq\), minimus talis numerus \(B\) assignari posset, divisor formae cujusiam \(xx + 2yy\), quod cum fieri nequeat, numeri \(pp + 2qq\) nulos habent divisores primos, qui non ipsi sint formae \(xx + 2yy\).