

rorum in seriei $1, 2, 3 \dots n - 1$ qui tum ipsi tum simul numeri proximi unitate maiores in \mathfrak{K} continentur; similiter sit $(\mathfrak{K}\mathfrak{K}')$ multitudo numerorum in eadem serie qui ipsi in \mathfrak{K} proxime sequentes vero in \mathfrak{K}' continentur, vnde simul significatio signorum $(\mathfrak{K}\mathfrak{K}'')$, $(\mathfrak{K}'\mathfrak{K})$, $(\mathfrak{K}'\mathfrak{K}')$, $(\mathfrak{K}'\mathfrak{K}'')$, $(\mathfrak{K}''\mathfrak{K})$, $(\mathfrak{K}''\mathfrak{K}')$, $(\mathfrak{K}''\mathfrak{K}'')$ sponte innotescet. Quo facto dico primo, fieri $(\mathfrak{K}\mathfrak{K}') = (\mathfrak{K}'\mathfrak{K})$. Supponendo enim, h, h', h'' etc. esse omnes numeros seriei $1, 2, 3 \dots n - 1$ qui ipsi in \mathfrak{K} proxime maiores $h + 1, h' + 1, h'' + 1$ etc. autem in \mathfrak{K}' continentur, et quorum ideo multitudo $= (\mathfrak{K}\mathfrak{K}')$, manifestum est omnes numeros $n - h - 1, n - h' - 1, n - h'' - 1$ etc. in \mathfrak{K}' contineri, proxime maiores vero $n - h, n - 1'$ etc. in \mathfrak{K} ; quare quum tales numeri omnino dentur $(\mathfrak{K}'\mathfrak{K})$, certo nequit esse $(\mathfrak{K}'\mathfrak{K}) < (\mathfrak{K}\mathfrak{K}')$, et perinde demonstratur, esse non posse $(\mathfrak{K}\mathfrak{K}') < (\mathfrak{K}'\mathfrak{K})$, quocirca hi numeri necessario aequales erunt. Prorsus eodem modo probatur $(\mathfrak{K}\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K})$, $(\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}')$. Secundo, quum necessario quemvis numerum ex \mathfrak{K} , maximo $n - 1$ excepto, sequi debeat proxime maior vel in \mathfrak{K} , vel in \mathfrak{K}' vel in \mathfrak{K}'' contentus, summa $(\mathfrak{K}\mathfrak{K}) + (\mathfrak{K}\mathfrak{K}') + (\mathfrak{K}\mathfrak{K}'')$ fiet aequalis multitudini omnium numerorum in \mathfrak{K} unitate deminutae puta $= m - 1$, et simili ratione erit $(\mathfrak{K}'\mathfrak{K}) + (\mathfrak{K}'\mathfrak{K}') + (\mathfrak{K}'\mathfrak{K}'') = (\mathfrak{K}''\mathfrak{K}) + (\mathfrak{K}''\mathfrak{K}') + (\mathfrak{K}''\mathfrak{K}'') = m$.

His ita praeparatis euoluimus per praecepta art. 345 productum pp' in $(m, \mathfrak{K}' + 1) + (m, \mathfrak{B}' + 1) + (m, \mathfrak{C}' + 1) + \text{etc.}$, quam expressionem facile perspicietur reduci ad $(\mathfrak{K}'\mathfrak{K})p + (\mathfrak{K}'\mathfrak{K}')p' + (\mathfrak{K}'\mathfrak{K}'')p''$, et quum per art. 345 I productum

$p'p''$ ex illo oriatur, substituendo pro $(m, 1)$, (m, g) , (m, gg) resp. (m, g) , (m, gg) , (mg^3) i. e. pro p , p' , p'' resp. p' , p'' , p , fiet $p'p'' = (\mathfrak{R}'\mathfrak{R})p' + (\mathfrak{R}'\mathfrak{R}')p'' + (\mathfrak{R}'\mathfrak{R}'')p$, et prorsus simili modo $p''p = (\mathfrak{R}'\mathfrak{R})p'' + (\mathfrak{R}'\mathfrak{R}')p + (\mathfrak{R}'\mathfrak{R}'')p'$. Hinc protinus sequitur primo $B = m(p + p' + p'') = m$, secundo quum simili ratione, vt antea pp' euolutum est, etiam pp'' ad $(\mathfrak{R}''\mathfrak{R})p + (\mathfrak{R}''\mathfrak{R}')p' + (\mathfrak{R}''\mathfrak{R}'')p''$ reducatur, atque haec expressio cum praecedente identica esse debeat, necessario erit $(\mathfrak{R}''\mathfrak{R}) = (\mathfrak{R}'\mathfrak{R}')$ et $(\mathfrak{R}''\mathfrak{R}'') = (\mathfrak{R}'\mathfrak{R})$. Hinc colligitur, statuendo $(\mathfrak{R}'\mathfrak{R}'') = (\mathfrak{R}''\mathfrak{R}') = a$, $(\mathfrak{R}''\mathfrak{R}'') = (\mathfrak{R}'\mathfrak{R}) = (\mathfrak{R}\mathfrak{R}') = b$, $(\mathfrak{R}'\mathfrak{R}') = (\mathfrak{R}''\mathfrak{R}) = (\mathfrak{R}\mathfrak{R}'') = c$, fieri $m - 1 = (\mathfrak{R}\mathfrak{R}) + (\mathfrak{R}\mathfrak{R}') + (\mathfrak{R}\mathfrak{R}'') = (\mathfrak{R}\mathfrak{R}) + b + c$, atque $a + b + c = m$, vnde $(\mathfrak{R}\mathfrak{R}) = a - 1$, ita vt illae nouem quantitates incognitae ad tres, a , b , c siue potius propter aequationem $a + b + c = m$ ad duas reductae sint. Denique patet, quadratum pp euolui in $(m, 1 + 1) + (m, 2 + 1) + (m, 3 + 1) + (m, 4 + 1) + \text{etc.}$; inter partes huius expressionis reperietur (m, n) quae reducitur ad $(m, 0)$ siue ad m , reliquas vero facile perspicietur reduci ad $(\mathfrak{R}\mathfrak{R})p + (\mathfrak{R}\mathfrak{R}')p' + (\mathfrak{R}\mathfrak{R}'')p''$, vnde habetur $pp = m + (a - 1)p + bp' + cp''$.

Hoc itaque modo per disquisitiones praecedentes quatuor hasce reductiones nacti sumus:

$$\begin{aligned} pp &= m + (a - 1)p + bp' + cp'' \\ pp' &= bp + cp' + ap'' \\ pp'' &= cp + ap' + bp'' \\ p'p'' &= ap + bp' + cp'' \end{aligned}$$

vbi inter tres incognitas a, b, c aequatio conditionalis $a + b + c = m \dots$ (I) intercedit, insuperque certum est ipsas esse numeros integros. Hinc colligitur $C = p \times p'p'' = app + bpp' + cpp'' = am + (aa + bb + cc - a)p + (ab + bc + ac)p' + (ab + bc + ac)p''$. At quum $pp'p''$ sit functio inuariabilis aggregatorum p, p', p'' , coëfficientes per quos haec in expr. praec. multiplicata sunt necessario aequales erunt (art. 350), vnde habetur aequatio noua $aa + bb + cc - a = ab + bc + ac \dots$ (II), atque hinc $C = am + (ab + bc + ac)(p + p' + p'')$, siue (propter I, et $p + p' + p'' = -1$), $C = aa - bc \dots$ (III). Iam etsi C hic a tribus incognitis pendeat, inter quas duae tantum aequationes habentur, tamen hae, adiumento conditionis ex qua a, b, c sunt integri, ad plenam determinationem ipsius C sufficiunt. Quod vt ostendamus, aequationem II ita exhibemus $12a + 12b + 12c + 4 = 36aa + 36bb + 36cc - 36ab - 36ac - 36bc - 24a + 12b + 12c + 4$; pars prior, per I, fit $= 12m + 4 = 4n$; posterior vero reducitur ad $(6a - 3b - 3c - 2)^2 + 27(b - c)^2$, aut scribendo k pro $2a - b - c$, ad $(3k - 2)^2 + 27(b - c)^2$. Hinc patet, numerum $4n$ (i. e. generaliter quadruplum cuiuslibet primi formae $3n + 1$) per formam $xx + 27yy$ repraesentari posse, quod quidem sine difficultate e theoria generali formarum binariarum deduci potest, attamen satis mirum est, talem discriptionem cum valoribus ipsarum a, b, c cohaerere. At numerus $4n$ semper vnico tantum modo in quadratum et quadratum 27^{plex} discerpi potest,