

etiam ad valores quosuis compositos ipsius n extendi posse: sed de his rebus quae altioris sunt indaginis hoc loco tacere earumque considerationem ad aliam occasionem nobis reservare oportet.

357. Sit aequatio m^{ta} gradus, cuius radices sunt m radices in periodo $(m, 1)$ contentae haec $x^m - ax^{m-1} + bx^{m-2} - \text{etc.} = 0$ siue $z = 0$, eritque $a = (m, 1)$, singulique reliqui coëfficientes b etc. sub forma tali $\mathcal{X} + \mathcal{B}(m, 1) + \mathcal{C}(m, g)$ comprehensi, ita ut \mathcal{X} , \mathcal{B} , \mathcal{C} sint integri (art. 348); denotandoque per z' functionem, in quam z transit, si pro $(m, 1)$ vbique substituitur (m, g) , pro (m, g) vero (m, gg) siue quod idem est $(m, 1)$, radices aequationis $z' = 0$ erunt radices in (m, g) contentae, productumque $zz' = \frac{x^n - 1}{x - 1} = X$. Potest itaque z ad formam talem $R + S(m, 1) + T(m, g)$ reduci, ubi R , S , T erunt functiones integrae ipsius x , quarum omnes coëfficientes etiam integri erunt; quo facto habebitur $z' = R + S(m, g) + T(m, 1)$. Hinc fit scribendo breuitatis causa p et q pro $(m, 1)$ et (m, g) resp., $2z = 2R + (S + T)(p + q) - (T - S)(p - q) = 2R - S - T - (T - S)(p - q)$ similiterque $2z' = 2R - S - T + (T - S)(p - q)$, vnde ponendo $2R - S - T = Y$, $T - S = Z$, fit $4X = YY - (p - q)^2 ZZ$, adeoque quum $(p - q)^2 = \pm n$, $4X = YY \mp nZZ$, signo superiori valente quando n est formae $4k + 1$, inferiori quando n formae $4k + 3$. Hoc est theorema, cuius demonstrationem supra (art. 124) polliciti sumus. Terminos duos summos functionis Y semper fieri

$2x^m + x^{m-1}$; summumque functionis Z , x^{m-1} facile perspicietur; coëfficientes reliqui autem, qui manifesto omnes erunt integri, variant pro diuersa indole numeri n , nec formulae analyticae generali subiici possunt.

Ex. Pro $n = 17$ aequatio cuius radices sunt octo adices in $(8, 1)$ contentae per praecepta art. 348 eruitur $x^8 - px^7 + (4 + p + 2q)x^6 - (4p + 3q)x^5 + (6 + 3p + 5q)x^4 - (4p + 3q)x^3 + (4 + p + 2q)xx - px + 1 = 0$, vnde $R = x^8 + 4x^5 + 6x^4 + 4xx + 1$, $S = -x^7 + x^6 - 4x^5 + 3x^4 - 4x^3 + xx - x$, $T = 2x^6 - 3x^5 + 5x^4 - 3x^3 + 2xx$, atque hinc $Y = 2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3 + 5xx + x + 2$, $Z = x^7 + x^6 + x^5 + 2x^4 + x^3 + xx + x$. Ecce adhuc alia quaedam exempla:

n	Y	Z
3	$2x + 1$	1
5	$2xx + x + 2$	x
7	$2x^3 + xx - x - 2$	$xx + x$
11	$2x^5 + x^4 - 2x^3 + 2xx - x - 2$	$x^4 + x$
13	$2x^6 + x^5 - 4x^4 - x^3 - 4xx + x + 2$	$x^5 + x^3 + x$
19	$2x^9 + x^8 - 4x^7 + 3x^6 + 5x^5 - 5x^4 - 3x^3 + 4xx - x - 2$	$x^8 - x^6 + x^5 + x^4 - x^3 + x$
23	$2x^{11} + x^{10} - 5x^9 - 8x^8 - 7x^7 - 4x^6 + 4x^5 + 7x^4 + 8x^3 + 5xx - x - 2$	$x^{10} + x^9 - x^7 - 2x^6 - 2x^5 - x^4 + xx + x$

358. Progredimur ad considerationem aequationum cubicarum, per quas in eo casu ubi n est formae $3k + 1$ tria aggregata $\frac{1}{3}(n - 1)$ terminorum complexum Ω componentia determinantur. Sit g radix primitiua quaecunque pro modulo n , atque $\frac{1}{3}(n - 1) = m$, qui erit integer par. Tunc tria aggregata e quibus Ω constat erunt $(m, 1)$, (m, g) , (m, gg) pro quibus resp. scribemus p , p' , p'' , patet que primum continere radices $[1]$, $[g^3]$, $[g^6]$... $[g^{n-4}]$, secundum has $[g]$, $[g^4]$... $[g^{n-3}]$, tertium has $[gg]$, $[g^7]$... $[g^{n-2}]$. Supponendo, aequationem quaesitam esse $x^3 - Axx + Bx - C = 0$, fit $A = p + p' + p''$, $B = pp' + p'p'' + pp''$, $C = pp'p''$, vnde protinus habetur $A = -1$. Sint residua minima positiua numerorum g^3 , g^6 ... g^{n-4} secundum modulum n ordine arbitrario haec \mathcal{A} , \mathcal{B} , \mathcal{C} etc., atque \mathcal{R} ipsorum complexus superadiecto numero 1; similiter sint \mathcal{A}' , \mathcal{B}' , \mathcal{C}' etc. residua minima numerorum g , g^4 , g^7 ... g^{n-3} , atque \mathcal{R}' illorum complexus; denique \mathcal{A}'' , \mathcal{B}'' , \mathcal{C}'' etc. residua minima ipsorum gg , g^7 , g^8 ... g^{n-2} et \mathcal{R}'' eorum complexus, vnde omnes numeri in \mathcal{R} , \mathcal{R}' , \mathcal{R}'' diuersi erunt et cum his $1, 2, 3 \dots n - 1$ conuenient. Ante omnia hic obseruandum est, numerum $n - 1$ necessario in \mathcal{R} reperiri, quippe quem esse residuum ipsius $g^{\frac{3}{2}m}$ facile perspicitur. Hinc facile quoque consequitur, duos numeros tales h , $n - h$ semper in eodem trium complexuum \mathcal{R} , \mathcal{R}' , \mathcal{R}'' reperiri, si enim alter est residuum potestatis g^λ , alter erit residuum potestatis $g^{\lambda + \frac{3}{2}m}$, aut huius $g^{\lambda - \frac{3}{2}m}$ si $\lambda > \frac{3}{2}m$. Denotemus hocce signo $(\mathcal{R}\mathcal{R})$ multitudinem nume-