

residuum autem omnium formae $20n + 13$, vel $20n + 17$. Et quoniam qui quis numerus primus, praeter 2 et 5 (quorum residuum ± 5), in aliqua harum formarum continetur $20n + 1$, 3, 7, 9, 11, 13, 17, 19, patet, de omnibus iam iudicium ferri posse, exceptis iis qui sint formae $20n + 1$, vel formae $20n + 9$.

123. Ex inductione facile deprehenditur, $+ 5$ et $- 5$ esse residua omnium numerorum primorum formae $20n + 1$, vel $20 + 9$. Quod si hoc generaliter verum est, lex elegans habebitur, $+ 5$ esse residuum omnium numerorum primorum qui ipsius 5 sint residua, (hi enim in alterutra formarum $5n + 1$ vel $5n + 4$ siue in aliqua harum, $20n + 1$, 9, 11, 19, continentur, de quarum tertia et quarta illud iam ostensum est) non-residuum vero omnium numerorum qui ipsius 5 sint non-residua, ut iam supra demonstrauimus. Clarum autem est, hoc theorema sufficere, ad diiudicandum, vtrum $+ 5$ (eoque ipso, $- 5$, si tamquam productum ex $+ 5$ et $- 1$ consideretur) numeri cuiuscunque dati residuum sit an non-residuum. Denique obseruetur huius theorematis cum illo quod art. 120 de residuo $- 3$ exposuimus analogia.

At verificatio illius inductionis non adeo facilis. Quando numerus primus formae $20n + 1$, siue generalius formae $5n + 1$ proponebitur, res simili modo absolui potest, vt in artt. 114, 119. Sit scilicet numerus quicunque pro modulo $5n + 1$ ad exponentem 5 pertinens a , quales dari ex sect. praec. manifestum, erit-

que $a^5 \equiv 1$, siue $(a - 1)(a^4 + a^3 + a^2 + a + 1) \equiv 0$ (mod. $5n + 1$). At quia nequit esse $a \equiv 1$, neque adeo $a - 1 \equiv 0$; necessario erit $a^4 + a^3 + a^2 + a + 1 \equiv 0$. Quare etiam $4(a^4 + a^3 + a^2 + a + 1) = (2aa + a + 2)^2 - 5a^2$ erit $\equiv 0$ i. e. $5a^2$ erit residuum ipsius $5n + 1$, adeoque etiam 5, quia a^2 est residuum per $5n + 1$ non diuisibile (a enim per $5n + 1$ non diuisibilis propter $a^5 \equiv 1$). Q. E. D.

At casus, vbi numerus primus formae $5n + 4$ proponitur, subtiliora artifacia postulat. Quoniam vero propositiones quarum ope negotium absolvitur in sequentibus generalius tractabuntur, hic breuiter tantum eas attingimus.

I. Si p est numerus primus atque b non-residuum quadraticum datum ipsius p , valor expressionis (A)...
$$\frac{(x + \sqrt{b})^{p+1} - (x - \sqrt{b})^{p+1}}{\sqrt{b}}$$

(ex qua euoluta irrationalitatem abire facile perspicitur), semper per p diuisibilis erit, quicunque numerus pro x assumatur. Patet enim ex inspectione coefficientium qui ex euolutione ipsius A obtinentur, omnes terminos a secundo vsque ad penultimum (incl.) per p diuisibles fore, adeoque esse $A \equiv 2(p + 1)(x^p + xb^{\frac{p-1}{2}})$, (mod. p). At quoniam b ipsius p non-residuum est, erit $b^{\frac{p-1}{2}} \equiv -1$ (mod. p), (art. 106); x^p autem semper est $\equiv x$ (sect. praec.) vnde fit $A \equiv 0$. Q. E. D.

II. In congruentia $A \equiv 0$ (mod. p), indeterminata x habet p dimensiones, omnesque

numeri 0, 1, 2... $p - 1$ illius radices erunt. Iam ponatur e esse diuisorem ipsius $p + 1$, eritque expressio $\frac{(x + \sqrt{b})^e - (x - \sqrt{b})^e}{\sqrt{b}}$

(quam per B designamus) si euoluitur, ab irrationalitate libera, indeterminata x in ipsae $e - 1$ dimensiones habebit, constatque ex analyseos primis elementis, A per B (indefinite) esse diuisibilem. Iam dico $e - 1$ valores ipsius x dari, quibus in B substitutis, B per p diuisibilis euadat. Ponatur enim $A = BC$, habebitque x in C dimensiones $p - e + 1$, adeoque congruentia $C \equiv 0$ (mod. p) non plures quam $p - e + 1$ radices. Vnde facile patet, omnes reliquos numeros ex his 0, 1, 2, 3... $p - 1$, quorum multitudo $= e - 1$, congruentiae $B \equiv 0$ radices fore.

III. Iam ponatur p esse formae $5n + 4$, $e = 5$, b non-residuum ipsius p , atque numerum a ita determinatum, ut sit $\frac{(a + \sqrt{b})^5 - (a - \sqrt{b})^5}{\sqrt{b}}$ per p diuisibilis.

At illa expressio fit $= 10a^4 + 20aab + 2bb = 2((b + 5aa)^2 - 20a^4)$. Erit igitur etiam $(b + 5aa)^2 - 20a^4$ per p diuisibilis i. e. $20a^4$ residuum ipsius p ; at quoniam $4a^4$ residuum est per p non diuisibile (facile enim intelligitur, a per p diuidi non posse), etiam 5 residuum ipsius p erit. Q. E. D.

Hinc patet theorema in initio huius articuli prolatum generaliter verum esse. —