31.

De residuis cubicis disquisitiones nonnullae analyticae.

(Auct. *E. E. Kummer*, prof. math. Vratislaviae.)

Quum clarissimus *Gauss* disquisitiones suas arithmeticas edidisset, abhinc annos XLI, perpauci erant geometrae, qui profundissimas ejus cogitationes mathematicas mente capere possent, admirationes autem omnium effecerunt theoremata nova de divisionibus circuli geometrice perficiendis, exempli gratia in septendecim partes, quae omnibus patefecerat. Iis praesertim inventis clarissimis adducti geometrae in doctrinam numerorum, imprimis autem in opus illud Gaussianum, operam maximam impenderunt, sed paucis tantum successit inceptum, rei ipsius enim difficultas eo augetur, quod in hoc libro omnia ita inter se cohaerent, ut these aliqua omissa, ea quae sequuntur vix perspici possint. Sero tandem, quum in Germania litterae mathematicae magis effloruissent, nonnulli exstiterunt qui *Gaussii* disquisitiones non solum penitus intelligerent, sed ipsi inventis novis doctrinam numerorum ulterius promoverent. Inter quos prae ceteris duo viri summi commemorandi sunt *Jacobi* et *Lejeune Dirichlet*, quorum inventa et methodi cum iis quae nos hac dissertatione tractabimus arcte connexa sunt. Cl. *Jacobi* pro residuis cubicis primus invenit reciprocitatis legem simplicissimam, qua totius huius doctrinae summa continetur, et Cl. *Lejeune Dirichlet* analysin quantitatum continuarum ad doctrinam numerorum tam prospero successu applicavit, ut omnium admirationem sibi pararet et nomen suum celeberrimum redderet. Disquisitiones, quas hactenus in publicum edidit, praecipue in residuis et formis quadraticis versantur, ideoque a nostris, quae de residuis cubicis instituemus, alienae videntur esse; nihilominus tamen confitemur in omnibus fere nos illius vestigia secutos esse. Magna enim residuorum cubicorum analogia est cum residuis quadraticis, praecipue numerorum formae $4n+1$, multaque theoremata et methodi, quae pro hisce locum habent, mutatis mutandis ad illa transferri possunt. Nuper etiam audivimus a geometra quodam Gallico *Lebesque* commentationem de residuis cubicis conscriptam esse, anno 1837, quam vero comparare non potuimus, praeterea de hac re in *Crellii* diario adnotationes nonnullae exstant minoris momenti, quarum auctores sunt viri clarissimi *Clausen* et *Stern*.

§. 1.

Ante omnia notiones et propositiones nonnullae elementares de residuis cubicis nobis repetendae sunt, quibus disquisitiones nostrae nituntur. Quilibet numerus α, qui cubo alicui congruus est modulo p, numero primo formae $6n+1$, hujus numeri primi residuum cubicum appellatur, qui vero cubo congrui esse non possunt, appellantur nonresidua; sive si congruentia $x^3 \equiv k$, modulo p, radicem aliquam habet, est k residuum, si vero haec congruentia radicem nullam habet, est k nonresiduum numeri primi p. Quia numeri inter se congrui semper simul sunt residua, vel nonresidua, hic soli numeri modulo p minores considerandi sunt. Potestas $x^{\frac{1}{3}(p-1)}$ pro valoribus variis numeri x non nisi tria residua incongrua habet, quorum unum est unitas, alterum si ponitur $=f$, est tertium $\equiv f^2$ et $1+f+f^2 \equiv 0$. Eos numeros x, pro quibus est $x^{\frac{1}{3}(p-1)} \equiv 1$, per α, eos qui dant $x^{\frac{1}{3}(p-1)} \equiv f$, per β, et eos qui dant $x^{\frac{1}{3}(p-1)} \equiv f^2$ per γ designamus, quibus literis ubi opus erit indices addemus. Omnes numeri modulo p minores aequaliter inter has tres classes distributae inveniuntur, ita ut numerus ipsorum α sit $\frac{1}{3}(p-1)$, idemque numerus ipsorum β et γ. Si g est radix primitiva pro modulo p, residua potestatum $g^0, g^3, g^6, \dots g^{p-4}$ cum numeris $\alpha, \alpha_1, \alpha_2, \dots$ consentiunt, residua potestatum $g^1, g^4, g^7, \dots, g^{p-3}$ cum numeris $\beta, \beta_1, \beta_2, \dots$ et residua potestatum $g^2, g^5, g^8, \dots g^{p-2}$ cum numeris $\gamma, \gamma_1, \gamma_2, \dots$ In serie numerorum $\alpha, \alpha_1, \alpha_2, \dots$ reperiuntur etiam $p-\alpha, p-\alpha_1, p-\alpha_2, \dots$, qua de causa eos tantum numeros $\alpha, \alpha_1, \alpha_2, \dots$ cognovisse sufficit, qui minores sunt quam $\frac{1}{2}p$, cum quibus altera semissis simul data est, idem cadit in numeros $\beta, \beta_1, \beta_2, \dots$ nec non in numeros $\gamma, \gamma_1, \gamma_2, \dots$ Seriei $\alpha, \alpha_1, \alpha_2, \dots$ termini unitate aucti: $\alpha+1, \alpha_1+1, \alpha_2+1, \dots$ excepto ultimo, qui est p, cujus loco ponimus 1, omnes in aliqua serierum α, β, et γ reperiuntur, numerus eorum qui continentur in serie α sit a, eorum qui in serie β continentur $=b$, ceterorum qui in serie γ continentur $=c$. Numeri a, b, c hoc modo definiti satisfaciunt aequationibus duabus

$$a+b+c = \tfrac{1}{3}(p-1), \quad \text{et} \quad (6a-3b-3c-2)^2+27(c-b)^2 = 4p;$$

itaque posito $6a-3b-3c-2=t$, $c-b=u$, est $4p=t^2+27u^2$, et quum numerus $4p$ unico tantum modo in hanc formam redigi possit, t et u, neglectis signis $\pm$, omnino determinati sunt, signum numeri t eo determinatur, quod $t=6a-3b-3c-2$ esse debet numerus formae $3m+1$, sed signum numeri u hoc modo definiri nequit, quia nondum distinximus quaenam nonresiduorum cubicorum literis β et quae literis γ designandae sint; nam serie numerorum β permutata cum serie numerorum γ, signum numeri u simul mutatur. Hinc autem nos serierum $\beta, \beta_1, \beta_2, \ldots$ et $\gamma, \gamma_1, \gamma_2, \ldots$ distinctionem accuratam petimus, quas ita semper eligendas esse constituimus, ut $u = c - b$ sit numerus positivus. Summas tres, quae in theoria residuorum cubicorum maximi momenti sunt:

$$\Sigma \cos \frac{2\alpha\pi}{p} = y_1, \quad \Sigma \cos \frac{2\beta\pi}{p} = y_2, \quad \Sigma \cos \frac{2\gamma\pi}{p} = y_3,$$

cl. *Gauss* invenit radices esse aequationis cubicae

$$y^3 + y^2 - \tfrac{1}{3}(p-1)y - \tfrac{1}{27}(pt + 3p - 1) = 0;$$

nos autem in iis quae sequuntur illarum summarum loco accipiemus has:

$$\Sigma \cos \frac{2\alpha x^3 \pi}{p} = z_1, \quad \Sigma \cos \frac{2\beta x^3 \pi}{p} = z_2, \quad \Sigma \cos \frac{2\gamma x^3 \pi}{p} = z_3,$$

in quibus signa summatoria ad valores $x = 0, 1, 2, \ldots p-1$ referenda sunt. Hae summae z_1, z_2 et z_3 sunt radices aequationis simplicioris

$$1. \qquad z^3 = 3pz + pt,$$

et cum summis y_1, y_2, y_3 ita cohaerent, ut sit $z_1 = 1 + 3y_1$, $z_2 = 1 + 3y_2$, $z_3 = 1 + 3y_3$. Inde efficiuntur aequationes

$$2. \quad \begin{cases} z_1 + z_2 + z_3 = 0, \quad z_1 z_2 + z_2 z_3 + z_3 z_1 = -3p, \quad z_1 z_2 z_3 = pt, \\ z_1^2 + z_2^2 + z_3^2 = 6p, \quad z_1^3 + z_2^3 + z_3^3 = 3pt. \end{cases}$$

Porro habentur sex aequationes, quarum ope quaelibet radicum z_1, z_2, z_3 rationaliter per aliam determinatur:

$$3. \quad \begin{cases} 3uz_2 = -z_1^2 + \tfrac{1}{2}(t - 3u)z_1 + 2p, \quad 3uz_3 = z_1^2 - \tfrac{1}{2}(t + 3u)z_1 - 2p, \\ 3uz_3 = -z_2^2 + \tfrac{1}{2}(t - 3u)z_2 + 2p, \quad 3uz_1 = z_2^2 - \tfrac{1}{2}(t + 3u)z_2 - 2p, \\ 3uz_1 = -z_3^2 + \tfrac{1}{2}(t - 3u)z_3 + 2p, \quad 3uz_2 = z_3^2 - \tfrac{1}{2}(t + 3u)z_3 - 2p; \end{cases}$$

quae binae per subtractionem conjunctae dant:

$$4. \quad \begin{cases} 3u(z_2 - z_3) = -2z_1^2 + tz_1 + 4p, \\ 3u(z_3 - z_1) = -2z_2^2 + tz_2 + 4p, \\ 3u(z_1 - z_2) = -2z_3^2 + tz_3 + 4p, \end{cases}$$

iisque multiplicatis, per faciles reductiones fit

$$5. \qquad (z_1 - z_2)(z_2 - z_3)(z_3 - z_1) = 27pu.$$

Aequatio cubica (1.) rite soluta dat radices tres:

$$z = -\sqrt{p}\cdot\sin\tfrac{1}{3}\nu - \sqrt{(3p)}\cos\tfrac{1}{3}\nu, \quad z = 2\sqrt{p}\cdot\sin\tfrac{1}{3}\nu, \quad z = -\sqrt{p}\cdot\sin\tfrac{1}{3}\nu + \sqrt{(3p)}\cos\tfrac{1}{3}\nu,$$

in quibus ν est arcus minimus cujus sinus $= \frac{-t}{2\sqrt{p}}$, qui intra limites $-\frac{1}{2}\pi$ et $+\frac{1}{2}\pi$ versatur. Inde concluditur harum radicum unam intra limites $-2\sqrt{p}$ et $-\sqrt{p}$, alteram intra limites $-\sqrt{p}$ et $+\sqrt{p}$, tertiam intra limites $+\sqrt{p}$ et $+2\sqrt{p}$ sitam esse, quae autem radicum definitarum z_1, z_2, z_3, ad hos singulos limites pertineat, quaestio est difficillima, de qua infra copiosius agemus.

§. 2.

In theoria residuorum quadraticorum summae serierum duarum $\Sigma\cos\frac{2ax^2\pi}{p}$ et $\Sigma\cos\frac{2bx^2\pi}{p}$, quae seriebus z_1, z_2 et z_3 respondent, facile adeo extenduntur, ut p sit numerus quicunque compositus; eandem summarum amplificationem in seriebus z_1, z_2 et z_3 perficiemus, unde magna earum differentia ab iis, quae ad residua quadratica pertinent, elucebit. Quum enim theoremata, quae de illis pro modulis primis inventa sunt, aucta etiam elegantia pro modulis compositis pronunciari possint, et res tota vertatur in residuis, quae numerus compositus p habeat, modulo 4: hic non ipsius numeri compositi, sed factorum ejus primorum formae lineares, et numerus factorum inter se aequalium summas determinant. Antequam vero de modulis quomodocunque compositis agemus, casum peculiarem absolvemus, quo modulus est potestas numeri primi, atque in eo seorsim considerabimus factores primos formarum $6r+1$ et $6r-1$, et praeterea numeros primos 2 et 3.

Si p est numerus primus formae $6r+1$, et n numerus integer unitate major, residua numerorum 1^3, 2^3, 3^3, 4^3, ... $(p^n-1)^3$, modulo p^n, separatis multiplis numeri p, omnia continentur forma $\alpha+\mu p$, ubi α quodvis residuum cubicum numeri p, et μ quemvis numerorum 0, 1, 2, 3, ... $(p^{n-1}-1)$ significat. Nam congruentiae $x^3\equiv A$, modulo p^n, satisfieri nequit, nisi sit $x^3\equiv A$, modulo p, sive, quod idem est, $A=\alpha+\mu p$, numerus autem residuorum cubicorum α est $\frac{1}{3}(p-1)$, et numerus omnium valorum numeri μ, qui formam $\alpha+\mu p$ modulo p^n minorem reddunt, est p^{n-1}, unde colligitur numerum omnium residuorum cubicorum, pro modulo p^n, majorem quam $\frac{1}{3}p^{n-1}(p-1)$ esse non posse. Praeterea notum est congruentiam $x^3\equiv A$, modulo p^n, plures quam tres radices incongruas non habere, qua re, quum terni numeri 1^3, 2^3, 3^3, ... $(p^n-1)^3$ idem residuum dare possint, neque plures, numerus omnium residuorum non minor esse potest tertia parte numerorum illorum, quae est $\frac{1}{3}p^{n-1}(p-1)$. Ex iis concluditur, omnes numeros, quos forma $\alpha+\mu p$ contineat, et praeter hos nullos, residua esse numerorum 1^3, 2^3, 3^3, ... $(p^n-1)^3$, modulo p^n, eaque residua singula ter inveniri. Multipla numeri p, quae series 0^3, 1^3, 2^3, 3^3, ... $(p^n-1)^3$ continet, sunt 0^3, $1^3\cdot p^3$, $3^3\cdot p^3$, ... $(p^{n-1}-1)^3p^3$, eorumque residua, modulo p^n, si n non majus quam 3, omnia sunt aequalia nihilo; si vero $n>3$, factore communi p^3 omisso, quaerenda sunt residua numerorum 0, 1^3, 2^3, 3^3, ... $(p^{n-1}-1)^3$, modulo p^{n-3}, quae esse residua numerorum 0, 1^3, 2^3, 3^3, ... $(p^{n-3}-1)^3$ toties iterata quot p^2 continet unitates, sponte apparet. Quibus positis, si $n > 3$ et m numerus arbitrarius ad p^n primus, summa quaesita tali modo exhiberi potest:

$$\Sigma \cos \frac{2m\varkappa^3 \pi}{p^n} = p^2 \Sigma \cos \frac{2m\lambda^3 \pi}{p^{n-3}} + 3 \Sigma\Sigma \cos \frac{2m(\alpha + \mu p)\pi}{p^n};$$

in qua formula signa summatoria hanc vim habent, ut literae $\varkappa$ tribuendi sint valores $0, 1, 2, \ldots. (p^n - 1)$, literae λ valores $0, 1, 2, \ldots. (p^{n-3} - 1)$, literae μ valores $0, 1, 2, 3, \ldots. (p^{n-1} - 1)$ et literae α valores omnium residuorum cubicorum numeri p. Consummatio secundum literam μ, quae per notas formulas trigonometricas facillime perficitur, summam dat zero, qua re haec aequationis pars tota evanescit, et formula efficitur simplicissima

$$6. \quad \Sigma \cos \frac{2m\varkappa^3 \pi}{p^n} = p^2 \Sigma \cos \frac{2m\lambda^3 \pi}{p^{n-3}}.$$

Inde pro quolibet numero n hujus seriei summa reducta est ad casus quibus $n = 1$, 2 et 3. Pro $n = 2$ et $n = 3$ ex iis, quae modo exposuimus, facile concluditur

$$\Sigma \cos \frac{2m\varkappa^3 \pi}{p^2} = p, \quad \Sigma \cos \frac{2m\varkappa^3 \pi}{p^3} = p^2,$$

itaque formula (6.) adhibita est generaliter

$$7. \quad \begin{cases} \Sigma \cos \dfrac{2m\varkappa^3 \pi}{p^n} = p^{\frac{1}{3}(2n-2)} \Sigma \cos \dfrac{2m\varkappa^3 \pi}{p}, & \text{si } n \equiv 1 \text{ modulo } 3, \\ \Sigma \cos \dfrac{2m\varkappa^3 \pi}{p^n} = p^{\frac{1}{3}(2n-1)}, & \text{si } n \equiv 2, \text{ modulo } 3, \\ \Sigma \cos \dfrac{2m\varkappa^3 \pi}{p^n} = p^{\frac{2}{3}n}, & \text{si } n \equiv 0, \text{ modulo } 3. \end{cases}$$

Deinde si q est numerus primus formae $6r - 1$, residua cuborum 1^3, 2^3, 3^3, $\ldots. (q^n - 1)^3$, omissis multiplis numeri q, eadem sunt ac numeri omnes minores quam q^n et ad q primi, cujus propositionis demonstrationem eo petimus, quod illorum cuborum duo x^3 et y^3 eadem residua dare non possunt. Posito enim $x^3 \equiv y^3$, esset $(x - y)(x^2 + xy + y^2) \equiv 0$, et quia forma $x^2 + xy + y^2$ factorem $q = 6r - 1$ habere non potest, esse deberet $x - y \equiv 0, \ldots.,$ modulo q^n, quod, quia x et y minores quam q^n supponuntur, nullo modo fieri potest. Facile inde concluditur, haec residua omnia forma $\nu + \mu q$ contineri, in qua $\nu = 1, 2, 3, \ldots. q^{n-1} - 1$. De residuis cuborum qui per q divisibiles sunt idem valet, quod supra de modulo p^n invenimus, scilicet, si n non > 3, haec residua, quorum numerus est q^{n-1} omnia nihilo aequalia sunt, si vero $n > 3$, factore communi q^3 omisso, residuis numerorum 0^3, 1^3, 2^3, 3^3, $\ldots.$ $(q^{n-3} - 1)^3$, totidem sumtis quot q^2 continet unitates. Itaque est simili modo ac supra:

$$\Sigma\cos\frac{2m\varkappa^3\pi}{q^n} = q^2\Sigma\cos\frac{2m\lambda^3\pi}{q^{n-1}} + \Sigma\Sigma\cos\frac{2m(\nu+\mu q)\pi}{q^n},$$

ubi $\varkappa = 0, 1, 2, 3, \ldots\ q^n-1$, $\lambda = 0, 1, 2, 3, \ldots\ q^{n-3}-1$, $\mu = 0, 1, 2, \ldots\ q^{n-1}-1$, $\nu = 1, 2, 3, \ldots\ q-1$. Consummatione secundum omnes valores literae μ perfecta, haec summa duplex evanescit, et prodit formula simplex

$$\Sigma\cos\frac{2m\varkappa^3\pi}{q^n} = q^2\Sigma\cos\frac{2m\lambda^3\pi}{q^{n-3}}.$$

Denique, quum sit

$$\Sigma\cos\frac{2m\varkappa^3\pi}{q} = 0, \quad \Sigma\cos\frac{2m\varkappa^3\pi}{q^2} = q, \quad \Sigma\cos\frac{2m\varkappa^3\pi}{q^3} = q^2,$$

est generaliter:

$$8. \quad \begin{cases} \Sigma\cos\dfrac{2m\varkappa^3\pi}{q^n} = 0, & \text{si } n\equiv 1, \text{ modulo } 3, \\ \Sigma\cos\dfrac{2m\varkappa^3\pi}{q^n} = q^{\frac{1}{3}(2n-1)}, & \text{si } n\equiv 2, \text{ modulo } 3, \\ \Sigma\cos\dfrac{2m\varkappa^3\pi}{q^n} = q^{\frac{2}{3}n}, & \text{si } n\equiv 0, \text{ modulo } 3. \end{cases}$$

Eaedem summae valent etiam pro $q=2$, neque alia huius rei est demonstratio, nisi quod forma x^2+xy+y^2 hic tanquam summa trium numerorum imparium factorem $q=2$ habere non potest.

Denique pro modulo 3^n residua cuborum per 3 non divisibilium 1^3, 2^3, 4^3, 5^3, ... $(3^n-1)^3$ formam habent $9\mu\pm1$; nam si horum cuborum aliquis accipitur x^3, x habet formam $3r\pm1$, et congruentia $x^3\equiv A$, modulo 3^n, dat $27r^3+27r^2+9r\pm1\equiv A$, ergo A divisum per 9, residuum dat ±1, uti contendimus. Porro congruentia $x^3\equiv y^3$ habet tres radices incongruas, terna igitur residua numerorum 1^3, 2^3, 4^3, ... $(3^n-1)^3$ inter se aequalia sunt, et numerus inaequalium est $2\cdot3^{n-2}$, qui, quum sit numerus omnium numerorum formae $9\mu\pm1$, modulo 3^n minorum, concluditur hos omnes in residuis illis reperiri. Cuborum per 3 divisibilium 0, $1^3\cdot3^3$, $2^3\cdot3^3$, $3^3\cdot3^3$, ... $(3^{n-1}-1)^3\cdot3^3$ residua, factore communi 3^3 omisso, non alia sunt ac residua cuborum 0, 1^3, 2^3, 3^3, ... $(3^{n-3}-1)^3$, quae novies iterantur, unde sequitur

$$\Sigma\cos\frac{2m\varkappa^3\pi}{3^n} = 9\Sigma\cos\frac{2m\lambda^3\pi}{3^{n-3}} + 3\Sigma\cos\frac{2m(9\mu\pm1)\pi}{3^n},$$

ubi $\varkappa = 0, 1, 2, \ldots (3^n-1)$, $\lambda = 0, 1, 2, \ldots 3^{n-3}-1$, $\mu = 0, 1, 2, \ldots 3^{n-2}-1$, et m est numerus arbitrarius factorem 3 non complectens. Etiam hoc casu terminus tertius, consummatione secundum valores literae μ peracta, evanescit, unde fit:

$$\Sigma\cos\frac{2m\varkappa^3\pi}{3^n} = 9\Sigma\cos\frac{2m\lambda^3\pi}{3^{n-3}},$$

et quia summa quaesita pro $n=1$, $n=2$ et $n=3$ facile invenitur

$$\Sigma\cos\frac{2m\varkappa^3\pi}{3}=0,\quad \Sigma\cos\frac{2m\varkappa^3\pi}{9}=3\left(1+2\cos\frac{2m\pi}{9}\right),\quad \Sigma\cos\frac{2m\varkappa^3\pi}{27}=9,$$

habemus generaliter:

$$9.\quad \begin{cases} \Sigma\cos\dfrac{2m\varkappa^3\pi}{3^n}=0, & \text{si } n\equiv 1, \text{ modulo } 3,\\[2mm] \Sigma\cos\dfrac{2m\varkappa^3\pi}{3^n}=3^{\frac{1}{3}(2n-1)}\left(1+2\cos\dfrac{2m\pi}{9}\right), & \text{si } n\equiv 2, \text{ modulo } 3,\\[2mm] \Sigma\cos\dfrac{2m\varkappa^3\pi}{3^n}=3^{\frac{2}{3}n}, & \text{si } n\equiv 0, \text{ modulo } 3. \end{cases}$$

Casibus iis specialibus absolutis, seriei propositae summa pro modulis quomodocunque compositis facile invenitur, theorematis ope quod in hac aequatione continetur:

$$10.\qquad \Sigma\cos\frac{2mQ^2\varkappa^3\pi}{P}\cdot\Sigma\cos\frac{2mP^2\lambda^3\pi}{Q}=\Sigma\cos\frac{2m\mu^3\pi}{PQ},$$

in qua summae extendendae sunt ad numeros $\varkappa=0,1,2,3,\ldots. P-1$; $\lambda=0,1,2,3,\ldots. Q-1$; $\mu=0,1,2,3,\ldots. PQ-1$, et literae P, Q, m numeros quoscunque inter se primos designant. Primum observamus seriem $\Sigma\cos\frac{2m\varkappa^3\pi}{P}$ eandem esse ac $\Sigma e^{\frac{2m\varkappa^3\pi\sqrt{-1}}{P}}$, cujus pars imaginaria per se evanescit, qua de causa in seriebus illis cosinuum loco quantitatibus exponentialibus imaginariis uti licet. Inde per multiplicationem simplicem habemus

$$\Sigma e^{\frac{2mQ^2\varkappa^3\pi\sqrt{-1}}{P}}\cdot\Sigma e^{\frac{2mP^2\lambda^3\pi\sqrt{-1}}{Q}}=\Sigma\Sigma e^{\frac{2m(Q^3\varkappa^3+P^3\lambda^3)\pi\sqrt{-1}}{PQ}},$$

adjecto factore $e^{6m\varkappa\lambda(Q\varkappa+P\lambda)\pi\sqrt{-1}}$, qui est $=1$, haec summa duplex induit formam

$$\Sigma\Sigma e^{\frac{2m(Q\varkappa+P\lambda)^3\pi\sqrt{-1}}{PQ}}.$$

Formula $Q\varkappa+P\lambda$ valores congruos, modulo PQ, non habet. Si enim esset $Q\varkappa+P\lambda\equiv Q\varkappa^1+P\lambda^1$, modulo PQ, inde sequeretur $Q(\varkappa-\varkappa^1)+P(\lambda-\lambda^1)\equiv 0$, et quum P et Q per hypothesin sint inter se primi, haec congruentia subsistere nequit, nisi $\varkappa-\varkappa^1\equiv 0$, modulo P, et $\lambda-\lambda^1\equiv 0$, modulo Q, quod, quia $\varkappa$ et $\varkappa^1$ sunt minores quam P et inaequales, λ et λ^1 minores quam Q et inaequales, absurdum est. Praeterea patet, numerum omnium valorum formae $Q\varkappa+P\lambda$ esse PQ, unde sequitur ut, multiplis moduli PQ omissis, hi valores consentiant cum numeris $0, 1, 2, 3, \ldots. PQ-1$. Inde ista summa duplex in simplicem mutatur, partibusque imaginariis, quarum altera alteram tollit, rejectis, provenit aequatio supra allata. Jam si $R=2^\alpha\cdot 3^\beta\cdot p^\gamma\cdot \overset{1}{p}{}^{\gamma'}\ldots. q^\delta\cdot \overset{1}{q}{}^{\delta'}\ldots.$ est numerus quomodocunque compositus, in quo p, $\overset{1}{p}$, ... designant numeros primos formae $6m+1$ et q, $\overset{1}{q}$, ... numeros primos formae $6r-1$, summa $\Sigma\cos\frac{2m\varkappa^3\pi}{R}$, per hoc theorema in productum tot summarum diffinditur, quot R factores habet inter se primos, scilicet

$$11.\quad \Sigma\cos\frac{2m\varkappa^3\pi}{R}=\Sigma\cos\frac{2ma\varkappa^3\pi}{2^\alpha}\cdot\Sigma\cos\frac{2mb\varkappa^3\pi}{3^\beta}\cdot\Sigma\cos\frac{2mc\varkappa^3\pi}{p^\gamma}\cdot\Sigma\cos\frac{2m\overset{1}{c}\varkappa^3\pi}{\overset{1}{p}{}^{\overset{1}{\gamma}}}\cdots$$
$$\cdots\Sigma\cos\frac{2md\varkappa^3\pi}{q^\delta}\cdot\Sigma\cos\frac{2m\overset{1}{d}\varkappa^3\pi}{\overset{1}{q}{}^{\overset{1}{\delta}}}\cdots;$$

in qua formula brevitatis causa scriptum est $\left(\frac{R}{2^\alpha}\right)^2=a$, $\left(\frac{R}{3^\beta}\right)^2=b$, $\left(\frac{R}{p^\gamma}\right)^2=c$, etc. easque summas singulas, quarum moduli sunt numerorum primorum potestates, supra invenimus. Indoles igitur summae $\Sigma\cos\frac{2m\varkappa^3\pi}{R}$ maxime a residuis pendet quae factorum primorum numeri R exponentes, α, β, γ, $\overset{1}{\gamma}$, ... δ, $\overset{1}{\delta}$, ... dant modulo 3. Nam si quis numerorum α, β, δ, $\overset{1}{\delta}$, ... habet formam $3r+1$, semper est $\Sigma\cos\frac{2m\varkappa^3\pi}{R}=0$; si vero exponentium α, β, γ, $\overset{1}{\gamma}$, ... δ, $\overset{1}{\delta}$, ... nullus habet formam $3r+1$, haec summa aequatur numero integro C, numeri R divisori, cui, si $\beta=3r+2$, praeterae adjicendus est factor $1+2\cos\frac{2m\pi}{9}$; denique si qui numerorum γ, $\overset{1}{\gamma}$, ... habent formam $3r+1$, exempli causa ipsi duo numeri γ et $\overset{1}{\gamma}$, haec summa numero illi integro C aequatur, multiplicato per summas $\Sigma\cos\frac{2m\varkappa^3\pi}{\overset{1}{p}}\cdot\Sigma\cos\frac{2m\varkappa^3\pi}{p}$. Posito $R=42375500=2^2\cdot3^3\cdot5^3\cdot7^4\cdot13$, est:

$$\Sigma\cos\frac{2m\varkappa^3\pi}{R}=22050\,\Sigma\cos\frac{6m\varkappa^3\pi}{7}\cdot\Sigma\cos\frac{4m\varkappa^3\pi}{13};$$

posito $R=1000=2^3\cdot5^3$ est

$$\Sigma\cos\frac{2m\varkappa^3\pi}{1000}=100.$$

§. 3.

Notissimum est signum $\left(\frac{m}{p}\right)$ a Cl. *Legendre* residuis quadraticis adhibitum, et propter eximiam elegantiam, quam formulae describendae ideo accipiunt, postea ab omnibus fere geometris receptum, quod statuitur $=+1$ vel $=-1$, prout m est residuum vel nonresiduum quadraticum numeri primi p. Idem signum etiam residuis cubicis maximam utilitatem affert; pro iis vero $\left(\frac{m}{p}\right)$ non radici quadraticae, sed radici cubicae unitatis aequale statuendum est, ita ut sit $\left(\frac{m}{p}\right)=1$, si m est residuum cubicum, sive si m est aliquis numerorum $\alpha, \alpha_1, \alpha_2, \ldots$; porro sit $\left(\frac{m}{p}\right)=\frac{-1+\sqrt{-3}}{2}$, si m est aliquis numerorum $\beta, \beta_1, \beta_2, \ldots$; denique sit $\left(\frac{m}{p}\right)=\frac{-1-\sqrt{-3}}{2}$, si m est inter numeros $\gamma, \gamma_1, \gamma_2, \ldots$. Haec significationis amplificatio Clo. ***Jacobi*** debetur, qui in literis de circuli sectionibus earumque applicationibus ad doctrinam numerorum, regiae litterarum academiae Berolinensi mense octobri anni 1837 traditis, hujus signi ope residuorum cubicorum legem reciprocitatis forma simplicissima exhibuit. Pro hoc signo valent aequationes fundamentales:

$$12.\qquad \left(\frac{m}{p}\right)\cdot\left(\frac{n}{p}\right)=\left(\frac{mn}{p}\right),\quad \left(\frac{p-m}{p}\right)=\left(\frac{m}{p}\right),\quad \left(\frac{m+\varkappa p}{p}\right)=\left(\frac{m}{p}\right);$$

casu quo $m=\varkappa p$ est multiplum numeri p, signo $\left(\frac{m}{p}\right)$ valorem zero tribuimus. Jam nobis problema, cui disquisitiones ulteriores maxime innituntur, solvendum proponimus:

Data summa seriei

$$\varphi(v) = A_1\cos v+A_2\cos 2v+A_3\cos 3v+A_4\cos 4v+\ldots\ldots$$

invenire hujus seriei summam:

$$\left(\frac{1}{p}\right)A_1+\left(\frac{2}{p}\right)A_2+\left(\frac{3}{p}\right)A_3+\left(\frac{4}{p}\right)A_4+\ldots\ldots$$

Quem in finem consideremus summam $\Sigma\left(\frac{m\varkappa}{p}\right)^2\cos\frac{2m\varkappa\pi}{p}$ pro $\varkappa=0,1,2,\ldots.(p-1)$, quae, casibus, quibus $m\varkappa$ ad seriem numerorum α vel β vel γ pertinet, separatis, in has tres dilabitur:

$$\Sigma\left(\frac{m\varkappa}{p}\right)^2\cos\frac{2m\varkappa\pi}{p} = \Sigma\cos\frac{2\alpha\pi}{p}+\frac{-1-\sqrt{-3}}{2}\Sigma\cos\frac{2\beta\pi}{p}+\frac{-1+\sqrt{-3}}{2}\Sigma\cos\frac{2\gamma\pi}{p}.$$

Dehinc radicem cubicam unitatis $\frac{-1+\sqrt{-3}}{2}$ nos ubique litera h designabimus, unde sequitur ut alteri radici imaginariae $\frac{-1-\sqrt{-3}}{2}$ signum h^2 tribuendum sit. Summas singulas, quas haec formula continet, supra literis y_1, y_2, y_3 designavimus, earumque loco has novas $z_1=1+3y_1$, $z_2=1+3y_2$, $z_3=1+3y_3$ substituimus, quibus signis adhibitis haec formula simpliciorem formam accipit:

$$13.\qquad 3\Sigma\left(\frac{m\varkappa}{p}\right)^2\cos\frac{2m\varkappa\pi}{p} = z_1+h^2z_2+hz_3,$$

quia $\left(\frac{m\varkappa}{p}\right)^2 = \left(\frac{m}{p}\right)^2 \cdot \left(\frac{\varkappa}{p}\right)^2$ et $\left(\frac{m}{p}\right)^3 = 1$; multiplicando per $\left(\frac{m}{p}\right)$ habemus

$$14.\quad 3\Sigma\left(\frac{\varkappa}{p}\right)^2 \cos\frac{2m\varkappa\pi}{p} = \left(\frac{m}{p}\right)(z_1 + h^2 z_2 + h z_3);\ \varkappa = 0, 1, 2, \ldots (p-1).$$

Hujus summae termini bini, ab initio et a fine aeque distantes, aequales sunt, quibus binis in unum conjunctis, est

$$15.\quad 6\Sigma\left(\frac{\varkappa}{p}\right)^2 \cos\frac{2m\varkappa\pi}{p} = \left(\frac{m}{p}\right)(z_1 + h^2 z_2 + h z_3);\ \varkappa = 0, 1, 2, \ldots \tfrac{1}{2}(p-1).$$

Jam si in aequatione

$$\varphi(v) = A_1 \cos v + A_2 \cos 2v + A_3 \cos 3v + A_4 \cos 4v,$$

quae intra limites $v = 0$ et $v = 2\pi$ valere debet, $v = \frac{2\varkappa\pi}{p}$ ponitur, per $3\cdot\left(\frac{\varkappa}{p}\right)^2$ multiplicatur et summae formantur pro $\varkappa = 1, 2, 3, \ldots p-1$, per formulam (14.) fit

$$16.\quad 3\Sigma\left(\frac{\varkappa}{p}\right)^2 \varphi\left(\frac{2\varkappa\pi}{p}\right) = (z_1 + h^2 z_2 + h z_3)\left(\left(\frac{1}{p}\right)A_1 + \left(\frac{2}{p}\right)A_2 + \left(\frac{3}{p}\right)A_3 + \ldots\right)$$

pro $\varkappa = 1, 2, 3, 4, \ldots (p-1)$. Simili modo, si aequatio

$$\varphi(v) = A \cos v + A_2 \cos 2v + A_3 \cos 3v + \ldots$$

intra limites $v = 0$ et $v = \pi$ valet, ex formula (15.) deducitur

$$17.\quad 6\Sigma\left(\frac{\varkappa}{p}\right)^2 \varphi\left(\frac{2\varkappa\pi}{p}\right) = (z_1 + h^2 z_2 + h z_3)\left(\left(\frac{1}{p}\right)A_1 + \left(\frac{2}{p}\right)A_2 + \left(\frac{3}{p}\right)A_3 + \ldots\right)$$

pro $\varkappa = 1, 2, 3, \ldots \frac{1}{2}(p-1)$, eaeque formulae (16. et 17.) problematis propositi solutionem continent.

§. 4.

Formularum generalium usum exemplis nonnullis illustraturi primum faciamus

$$\varphi(v) = \cos v + \frac{\cos 3v}{3^2} + \frac{\cos 5v}{5^2} + \ldots,$$

cujus seriei summa intra limites $v = 0$ et $v = \pi$ est $\varphi(v) = -\frac{1}{4}\pi v + \frac{1}{8}\pi^2$, quibus in formula (17.) substitutis, est

$$6\Sigma\left(\frac{\varkappa}{p}\right)^2\left(\frac{\pi^2}{8} - \frac{\pi^2\varkappa}{2p}\right) = (z_1 + h^2 z_2 + h z_3)\left(\left(\frac{1}{p}\right) + \left(\frac{3}{p}\right)\frac{1}{3^2} + \left(\frac{5}{p}\right)\frac{1}{5^2} + \ldots\right)$$

pro $\varkappa = 0, 1, 2, 3, \ldots \frac{1}{2}(p-1)$. Separatis casibus, quibus $\left(\frac{\varkappa}{p}\right) = 1$, $\left(\frac{\varkappa}{p}\right) = h$ et $\left(\frac{\varkappa}{p}\right) = h^2$, fit:

$$18.\quad -\frac{3\pi^2}{p}(\Sigma\alpha + h^2\Sigma\beta + h\Sigma\gamma) = (z_1 + h^2 z_2 + h z_3)\left(\left(\frac{1}{p}\right) + \left(\frac{3}{p}\right)\frac{1}{3^2} + \left(\frac{5}{p}\right)\frac{1}{5^2} + \ldots\right)$$

signaque summarum ad omnes valores numerorum α, β, γ, minores quam $\frac{1}{2}p$ extendenda sunt. Simili modo etiam haec series infinita in tres series singulas dilabitur. Posito enim

$$\Sigma\frac{1}{\alpha^2}=A,\quad \Sigma\frac{1}{\beta^2}=B,\quad \Sigma\frac{1}{\gamma^2}=C,$$

ubi summarum signa ad omnes valores impares numerorum α, β, γ in infinitum sunt extendenda, fit

$$\left(\frac{1}{p}\right)+\left(\frac{3}{p}\right)\frac{1}{3^2}+\left(\frac{5}{p}\right)\frac{1}{5^2}+\dots = A+hB+h^2C,$$

ideoque est

$$19.\qquad \frac{-3\pi^2}{p}(\Sigma\alpha+h^2\Sigma\beta+h\Sigma\gamma) = (z_1+h^2z_2+hz_3)(A+hB+h^2C).$$

Formulae quae sequuntur multo simpliciores fiunt, si loco ipsarum summarum $\Sigma\alpha$, $\Sigma\beta$, $\Sigma\gamma$ earum differentiis a valore medio arithmetico utimur, quas literis m_1, m_2 et m_3 designabimus. Ponimus igitur

$$\tfrac{1}{3}(\Sigma\beta+\Sigma\gamma-2\Sigma\alpha)=m_1,\ \tfrac{1}{3}(\Sigma\alpha+\Sigma\gamma-2\Sigma\beta)=m_2,\ \tfrac{1}{3}(\Sigma\alpha+\Sigma\beta-2\Sigma\gamma)=m_3,$$

sive, quia est $\Sigma\alpha+\Sigma\beta+\Sigma\gamma = 1+2+3+\dots+\frac{1}{2}(p-1) = \frac{1}{8}(p^2-1)$:

$$\tfrac{1}{24}(p^2-1)-\Sigma\alpha=m_1,\ \tfrac{1}{24}(p^2-1)-\Sigma\beta=m_2,\ \tfrac{1}{24}(p^2-1)-\Sigma\gamma=m_3.$$

Numeri m_1, m_2, m_3, quos integros esse patet, ita comparati sunt, ut eorum summa nihilo aequalis sit, sive $m_1+m_2+m_3=0$, iisque summarum $\Sigma\alpha$, $\Sigma\beta$, $\Sigma\gamma$ loco substitutis, formula (19.) hanc formam accipit:

$$20.\qquad \frac{3\pi^2}{p}(m_1+h^2m_2+hm_3) = (z_1+h^2z_2+hz_3)(A+hB+h^2C).$$

Quia h est forma imaginaria, haec aequatio duas reales complectitur, quibus, si adduntur aequationes $m_1+m_2+m_3=0$, $A+B+C=\frac{\pi^2(p^2-1)}{8p^2}$ et $z_1+z_2+z_3=0$, hae aequationes reales triplici modo exhiberi possunt, prout m_1, m_2, m_3, vel A, B, C, vel z_1, z_2, z_3 pro incognitis habentur. Inde prodeunt aequationes elegantes:

$$21.\qquad \begin{cases} \dfrac{3\pi^2}{p}m_1 = Az_1+Bz_2+Cz_3, \\[2mm] \dfrac{3\pi^2}{p}m_2 = Az_2+Bz_3+Cz_1, \\[2mm] \dfrac{3\pi^2}{p}m_3 = Az_3+Bz_1+Cz_2, \end{cases}$$

$$22.\quad \begin{cases} A = \dfrac{\pi^2(p^2-1)}{24p^2} + \dfrac{\pi^2}{3p^2}(m_1 z_1 + m_2 z_2 + m_3 z_3), \\ B = \dfrac{\pi^2(p^2-1)}{24p^2} + \dfrac{\pi^2}{3p^2}(m_1 z_2 + m_2 z_3 + m_3 z_1), \\ C = \dfrac{\pi^2(p^2-1)}{24p^2} + \dfrac{\pi^2}{3p^2}(m_1 z_3 + m_2 z_1 + m_3 z_2), \end{cases}$$

$$23.\quad \begin{cases} z_1 = \dfrac{2p^2(Am_1+Bm_3+Cm_2)}{\pi^2(m_1^2+m_2^2+m_3^2)} = \dfrac{-2p((A-B)m_3+(A-C)m_2)}{\pi(m_1^2+m_2^2+m_3^2)}, \\ z_2 = \dfrac{2p^2(Am_2+Bm_1+Cm_3)}{\pi^2(m_1^2+m_2^2+m_3^2)} = \dfrac{-2p((A-B)m_1+(A-C)m_3)}{\pi(m_1^2+m_2^2+m_3^2)}, \\ z_3 = \dfrac{2p^2(Am_3+Bm_2+Cm_1)}{\pi^2(m_1^2+m_2^2+m_3^2)} = \dfrac{-2p((A-B)m_2+(A-C)m_1)}{\pi(m_1^2+m_2^2+m_3^2)}. \end{cases}$$

His etiam differentias binarum quantitatum z_1, z_2 et z_3 adjungimus, quae consilio nostro inservient:

$$24.\quad \begin{cases} z_1 - z_2 = \dfrac{2p^2((A-2B+C)m_1-(A-2C+B)m_2)}{\pi^2(m_1^2+m_2^2+m_3^2)}, \\ z_2 - z_3 = \dfrac{2p^2((A-2B+C)m_2-(A-2C+B)m_3)}{\pi^2(m_1^2+m_2^2+m_3^2)}, \\ z_3 - z_1 = \dfrac{2p^2((A-2B+C)m_3-(A-2C+B)m_1)}{\pi^2(m_1^2+m_2^2+m_3^2)}. \end{cases}$$

Jam si praeter numeros m_1, m_2, m_3, etiam series infinitae A, B, C cognitae essent, per aequationes (23.) valores quantitatum z_1, z_2, z_3 accurate determinari possent; in quaestione vero praesenti sufficit cognovisse $A-B$, $A-C$, $A-2B+C$, $A-2C+B$ omnes esse positivos, quod inde sequitur ut sit $A = 1 + \frac{1}{\alpha_1^2} + \frac{1}{\alpha_2^2} + \dots$, ergo $A > 1$ et $A+B+C < \frac{1}{8}\pi^2 < \frac{5}{4}$, itaque $B+C < \frac{1}{4}$, nec non $B < \frac{1}{4}$, et $C < \frac{1}{4}$. Numerorum m_1, m_2, m_3, quorum summa est nihilo aequalis, unus est absolute maximus, reliqui duo minores eadem signa habent, opposita signo maximi. Ponamus primo, m_1 esse numerum maximum, eumque positivum, unde m_2 et m_3 minores et negativi, hinc per aequationes (23.) et (24.) est z_1 positivum, $z_1 - z_2$ positivum et $z_1 - z_3$ positivum, itaque z_1 est aequationis illius cubicae radix maxima positiva, quae intra limites $+2\sqrt{p}$ et $+\sqrt{p}$ sita est. Simili modo, si m_1 est numerus absolute maximus, sed negativus, m_2 et m_3 erunt positivi, et per aequationes (23.) et (24.) z_1, $z_1 - z_2$, $z_1 - z_3$ omnes erunt negativi; unde concluditur z_1 esse radicem minimam aequationis cubicae, quae intra limites $-\sqrt{p}$ et $-2\sqrt{p}$ sita est. Pro numero absolute maximo m_2 habemus eodem modo, si m_2 est positivus, z_2 intra limites $+2\sqrt{p}$ et $+\sqrt{p}$, si vero m_2 est negativus, z_2 intra limites

$-\sqrt{p}$ et $-2\sqrt{p}$; denique pro numero absolute maximo m_3 est z_3 intra limites $+2\sqrt{p}$ et $\sqrt{p}$, si m_3 est positivus, et z_3 intra limites $-\sqrt{p}$ et $-2\sqrt{p}$, si m_3 est negativus. Semper igitur una radicum z_1, z_2, z_3 omnino determinata est per numeros m_1, m_2, m_3 et quia per unam radicem reliquae rationaliter expressae sunt, omnes jam determinatae sunt. Ceterum notandum est, ad reliquarum duarum radicum limites definiendos non opus esse aequationibus (3.), sed hanc quaestionem facillime per aequationem (5.) absolvi. In universum enim sex modi dantur quibus singulae tres radices z_1, z_2, z_3 ad tria intervalla $-2\sqrt{p}$ et $-\sqrt{p}$, $-\sqrt{p}$ et $+\sqrt{p}$, $+\sqrt{p}$ et $+2\sqrt{p}$ pertinere possunt. Quum vero per aequationem (5.) $(z_1-z_2)(z_2-z_3)(z_3-z_1) = 27pu$ sit, et u numerus positivus, haec intervalla, quae singulis radicibus respondent, ita eligi debent, ut $(z_1-z_2)(z_2-z_3)(z_3-z_1)$ sit quantitas positiva, unde fit ut tres casus rejiciendi sint, et soli tres sequentes locum habere possint:
z_1 intra lim. $-2\sqrt{p}$ et $-\sqrt{p}$, z_2 intra lim. $-\sqrt{p}$ et $+\sqrt{p}$, z_3 intra lim. $+\sqrt{p}$ et $+2\sqrt{p}$,
z_1 intra lim. $-\sqrt{p}$ et $+\sqrt{p}$, z_2 intra lim. $+\sqrt{p}$ et $+2\sqrt{p}$, z_3 intra lim. $-2\sqrt{p}$ et $-\sqrt{p}$,
z_1 intra lim. $+\sqrt{p}$ et $+2\sqrt{p}$, z_2 intra lim. $-2\sqrt{p}$ et $-\sqrt{p}$, z_3 intra lim. $-\sqrt{p}$ et $+\sqrt{p}$.

Hoc modo aequationis illius radices singulae accurate determinatae sunt; sed haec problematis solutio non ea est, quae peritis ab omni parte satisfacere possit; nam hoc desideratur, ut ex ispsius numeri primi p indole dijudicari possit, ad quae intervalla radices z_1, z_2, z_3 referendae sint, neque vero ex indole numerorum m_1, m_2, m_3, qui pro dato numero p non sine labore computantur. Hunc calculum numerorum m_1, m_2, m_3, pro omnibus numeris primis formae $6n+1$ usque ad 499, ope tabularum canonis arithmetici a Clo. ***Jacobi*** editi perfecimus et per methodum modo traditam ex iis invenimus esse I°, z_1 intra limites $-2\sqrt{p}$ et $-\sqrt{p}$ pro numeris primis $p = 97$, 139, 151, 199, 211, 331, 433. II°, z_1 intra limites $-\sqrt{p}$ et $+\sqrt{p}$ pro numeris primis $p = 13$, 19, 37, 61, 109, 157, 193, 241, 283, 367, 373, 379, 397, 487. III°, z_1 intra limites $+\sqrt{p}$ et $+2\sqrt{p}$ pro numeris primis $p = 7$, 31, 43, 67, 73, 79, 103, 127, 163, 181, 223, 229, 271, 277, 307, 313, 337, 349, 409, 421, 439, 457, 463, 499. Omnes numeri primi, formae $6n+1$, talimodo in tres classes dividuntur, atque ex 45 numeris primis infra 500 ad classem primam pertinent 7, ad classem secundam 14, ed ad classem tertiam 24, quorum numerorum ratio proxime exprimitur per 1:2:3; nec improbabile est, eandem rationem etiam pro majore numero semper servatum iri. Quum doctrinae numerorum historia multis exemplis doceat, veritates arithmeticas per inductionem inventas et tum demum demonstratas esse, nos talem inductionem pro his tribus classibus numerorum primorum dignoscendis multis modis tentavimus, sed hactenus frustra criterium quaesivimus, quo alicujus classis numeri a reliquis numeris primis formae $6n+1$ discerni possint.

§. 5.

Ex aequationibus supra allatis (20—23) etiam numerorum m_1, m_2, m_3, et serierum infinitarum A, B, C proprietates nonnullas deducemus. Trium aequationum (21.) quadrata addita, adhibitis aequationibus $z_1^2+z_2^2+z_3^2=6p$ et $z_1z_2+z_2z_3+z_3z_1=-3p$, dant

$$25. \quad \frac{3\pi^4}{2p^3}(m_1^2+m_2^2+m_3^2) = A^2+B^2+C^2-AB-BC-CA.$$

Quantitas $A^2+B^2+C^2-AB-BC-CA$, quam breviter litera δ designabimus, limitibus arctis circumscripta est, quos facillime per repraesentationem hujus quantitatis δ in forma producti infiniti invenimus. Quem in finem litera r designamus omnes numeros primos impares, qui sunt residua cubica numeri p, et litera n omnes numeros primos impares, qui sunt nonresidua cubica ejusdem numeri p. Inde, per principia, quae jam summus **Eulerus** in introductione in analysin infinitorum exposuit, concluditur

$$\Pi\frac{1}{1-\frac{1}{r^2}}\,\Pi\frac{1}{1-\left(\frac{n}{p}\right)\frac{1}{n^2}} = 1+\left(\frac{3}{p}\right)\frac{1}{3^2}+\left(\frac{5}{p}\right)\frac{1}{5^2}+\left(\frac{7}{p}\right)\frac{1}{7^2}+\ldots,$$

$$\Pi\frac{1}{1-\frac{1}{r^2}}\,\Pi\frac{1}{1-\left(\frac{n}{p}\right)^2\frac{1}{n^2}} = 1+\left(\frac{3}{p}\right)^2\frac{1}{3^2}+\left(\frac{5}{p}\right)^2\frac{1}{5^2}+\left(\frac{7}{p}\right)^2\frac{1}{7^2}+\ldots.$$

Harum serierum altera est $A+hB+h^2C$, altera $A+h^2B+hC$, earumque productum est δ; itaque, duabus iis formulis inter se multiplicatis, habemus

$$\Pi\frac{1}{1-\frac{2}{r^2}+\frac{1}{r^4}}\,\Pi\frac{1}{1+\frac{1}{n^2}+\frac{1}{n^4}} = \delta.$$

Praeterea est

$$\Pi\frac{1}{1-\frac{1}{r^2}}\,\Pi\frac{1}{1-\frac{1}{n^2}} = 1+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\ldots = \frac{\pi^2}{8}\left(1-\frac{1}{p^2}\right),$$

$$\Pi\frac{1}{1-\frac{1}{r^6}}\,\Pi\frac{1}{1-\frac{1}{n^6}} = 1+\frac{1}{3^6}+\frac{1}{5^6}+\frac{1}{7^6}+\ldots = \frac{\pi^6}{960}\left(1-\frac{1}{p^6}\right),$$

earumque aequationum altera per alteram divisa:

$$\Pi\frac{1}{1+\frac{1}{r^2}+\frac{1}{r^4}}\,\Pi\frac{1}{1+\frac{1}{n^2}+\frac{1}{n^4}} = \frac{\pi^4}{120}\left(1+\frac{1}{p^2}+\frac{1}{p^4}\right).$$

Per hanc aequationem nonresidua ex repraesentatione quantitatis δ tolli possunt, unde provenit

$$26. \quad \delta = \frac{\pi^4}{120}\left(1+\frac{1}{p^2}+\frac{1}{p^4}\right)\Pi\left(\frac{1+\frac{1}{r^2}+\frac{1}{r^4}}{1-\frac{2}{r^2}+\frac{1}{r^4}}\right);$$

simili modo δ per nonresidua n exprimitur

$$27. \quad \delta = \frac{\pi^4}{64}\left(1-\frac{1}{p^2}\right)^2\Pi\left(\frac{1-\frac{2}{n^2}+\frac{1}{n^4}}{1+\frac{1}{n^2}+\frac{1}{n^4}}\right).$$

Horum productorum infinitorum alterum est majus unitate, alterum minus unitate; qua de causa est $\delta > \frac{\pi^4}{120}\left(1+\frac{1}{p^2}+\frac{1}{p^4}\right) > \frac{\pi^4}{120}$, et $\delta < \frac{\pi^4}{64}\left(1-\frac{1}{p^2}\right)^2 < \frac{\pi^4}{64}$; limites igitur, intra quos δ continetur, sunt $\frac{\pi^4}{120}$ et $\frac{\pi^4}{64}$, et limites summae quadratorum $m_1^2+m_2^2+m_3^2$ sunt

$$28. \quad m_1^2+m_2^2+m_3^2 > \frac{p^3}{180}, \quad m_1^2+m_2^2+m_3^2 < \frac{p^3}{96}.$$

Hinc facile deducuntur limites, quos maximus numerorum m_1, m_2, m_3, quem m_1 esse accipimus, excedere nequit. Est enim $m_1+m_2+m_3=0$, itaque $m_1^2+m_2^2+m_3^2 = 2(m_1^2+m_1m_2+m_2^2)$; porro m_2 habet signum contrarium signo numeri m_1, qua re m_1m_2 est negativum; nec non est $m_1m_2+m_2^2 = -m_2m_3$ quantitas negativa, unde sequitur ut sit $m_1^2+m_2^2+m_3^2 < 2m_1^2$; valorem autem minimum formula $m_1^2+m_1m_2+m_2^2$ obtinet pro $m_2 = -\frac{1}{2}m_1$, unde habemus $m_1^2+m_2^2+m_3^2 > \frac{3}{2}m_1^2$. Quibus cum formulis (28.) comparatis, est

$$2m_1^2 > \frac{p^3}{180} \quad \text{et} \quad \tfrac{3}{2}m_1^2 < \frac{p^3}{96},$$

$$\pm m_1 > \frac{p\sqrt{p}}{6\sqrt{10}} \quad \text{et} \quad \pm m_1 < \frac{p\sqrt{p}}{12}.$$

§. 6.

Series A, B, C hoc proprium habent, ut aequationis cubicae radices sint, cujus coëfficientes, si radices A, B et C per $\frac{p^2}{\pi^2}$ multiplicatae accipiuntur, omnes sunt numeri integri. Formam autem simplicissimam haec aequatio habet, si quantitates

$$\frac{p^2}{\pi^2}A - \frac{p^2-1}{24} = \xi_1, \quad \frac{p^2}{\pi^2}B - \frac{p^2-1}{24} = \xi_2, \quad \frac{p^2}{\pi^2}C - \frac{p^2-1}{24} = \xi_3$$

pro radicibus accipiuntur, quarum summa est nihilo aequalis. Aequationem quaesitam ex formula (20.) deducemus, lemmatis hujus facile demonstrandi auxilio:

Si a, b, c quantitates quascunque designant, quarum summa est nihilo aequalis, et h est radix imaginaria aequationis $h^3=1$, est

$$(a+h^2b+hc)^3 = \tfrac{1}{2}\cdot 27abc+\tfrac{1}{2}\cdot 3\sqrt{-3}(a-b)(b-c)(c-a),$$
$$(a+h^2b+hc)(a+hb+h^2c) = -3(ab+bc+ca).$$

Formula (20.), si loco quantitatum A, B et C novae ξ_1, ξ_2 et ξ_3 introducuntur, hanc formam accipit:

$$3p(m_1+h^2m_2+hm_3) = (z_1+h^2z_2+hz_3)(\xi_1+h\xi_2+h^2\xi_3),$$

et utraque parte per $(z_1+hz_2+h^2z_3)$ multiplicata, fit

$$29. \qquad (z_1+hz_2+h^2z_3)(m_1+h^2m_2+hm_3) = 3(\xi_1+h\xi_2+h^2\xi_3).$$

Mutato h in h^2, unde h^2 mutatur in $h^4=h$, haec aequatio cum priori multiplicata dat

$$30. \qquad p(m_1m_2+m_2m_3+m_3m_1) = \xi_1\xi_2+\xi_2\xi_3+\xi_3\xi_1.$$

Porro per lemma supra propositum est

$$(m_1+h^2m_2+hm_3)^3 = \tfrac{1}{2}\cdot 27m_1m_2m_3+\tfrac{1}{2}\cdot 3\sqrt{-3}(m_1-m_2)(m_2-m_3)(m_3-m_1),$$
$$(\xi_1+h\xi_2+h^2\xi_3)^3 = \tfrac{1}{2}\cdot 27\xi_1\xi_2\xi_3-\tfrac{1}{2}\cdot 3\sqrt{-3}(\xi_1-\xi_2)(\xi_2-\xi_3)(\xi_3-\xi_1),$$
$$(z_1+hz_2+h^2z_3)^3 = \tfrac{1}{2}\cdot 27p(t-3u\sqrt{-3}),$$

unde aequationis (29.) utraque parte ad tertiam potestatem elevata, efficitur

$$\tfrac{1}{2}p(t-3u\sqrt{-3})(\tfrac{1}{2}\cdot 27m_1m_2m_3+\tfrac{1}{2}\cdot 3\sqrt{-3}(m_1-m_2)(m_2-m_3)(m_3-m_1))$$
$$= \tfrac{1}{2}.27\xi_1\xi_2\xi_3-\tfrac{1}{2}\cdot 3\sqrt{-3}(\xi_1-\xi_2)(\xi_2-\xi_3)(\xi_3-\xi_1);$$

quae aequatio, partibus realibus et imaginariis separatis, in has duas dilabitur:

$$\xi_1\xi_2\xi_3 = \tfrac{1}{2}p(tm_1m_2m_3+u(m_1-m_2)(m_2-m_3)(m_3-m_1)),$$
$$(\xi_1-\xi_2)(\xi_2-\xi_3)(\xi_3-\xi_1) = \tfrac{1}{2}p(27um_1m_2m_3-t(m_1-m_2)(m_2-m_3)(m_3-m_1)).$$

Quantitatibus $\xi_1+\xi_2+\xi_3$, $\xi_1\xi_2+\xi_2\xi_3+\xi_3\xi_1$, $\xi_1\xi_2\xi_3$ inventis, statim formatur aequatio cubica

$$31. \quad x^3+p(m_1m_2+m_2m_3+m_3m_1)x-\tfrac{1}{2}p(tm_1m_2m_3+u(m_1-m_2)(m_2-m_3)(m_3-m_1)) = 0,$$

cujus radices sunt $x=\frac{p^2}{\pi^2}A-\frac{p^2-1}{24}$, $x=\frac{p^2}{\pi^2}B-\frac{p^2-1}{24}$, $x=\frac{p^2}{\pi^2}C-\frac{p^2-1}{24}$.

Per formulam generalem (17.) serierum infinitarum A, B et C summae notatu dignae iuveniuntur, statuendo

$$\varphi(v) = \cos 8v+2\cos 16v+3\cos 24v+\ldots+\tfrac{1}{2}(p-1)\cdot\cos 4(p-1)v,$$

cujus seriei summa est

$$\varphi(v) = \frac{p+1}{4}\cdot\frac{\sin 4pv}{\sin 4v}-\tfrac{1}{2}\left(\frac{\sin 2(p+1)v}{\sin 4v}\right)^2,$$

quae, posito $v = \frac{2\varkappa\pi}{p}$, dat

$$\varphi\left(\frac{2\varkappa\pi}{p}\right) = -\tfrac{1}{8}\sec^2\frac{4\varkappa\pi}{p},$$

quibus in formula (17.) substitutis, habemus

$$-\tfrac{3}{4}\Sigma\left(\frac{\varkappa}{\pi}\right)^2\sec^2\frac{4\varkappa\pi}{p}$$

$$= (z_1 + h^2 z_2 + h z_3)\left(\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right)\cdot 2 + \left(\frac{3}{p}\right)\cdot 3 + \ldots + \left(\frac{\frac{1}{2}(p-1)}{p}\right)\tfrac{1}{2}(p-1)\right);$$

sejunctis casibus, quibus $\left(\frac{\varkappa}{p}\right) = 1 \cdot \left(\frac{\varkappa}{p}\right) = h$ et $\left(\frac{\varkappa}{p}\right) = h^2$, haec formula hoc modo repraesentari potest:

$$-\tfrac{3}{4}\left(\Sigma\sec^2\frac{4\varkappa\pi}{p} + h^2\Sigma\sec^2\frac{4\varkappa\pi}{p} + h\Sigma\sec^2\frac{4\varkappa\pi}{p}\right)$$
$$= (z_1 + h^2 z_2 + h z_3)(\Sigma\alpha + h\Sigma\beta + h^2\Sigma\gamma).$$

Substituto valore formulae $\Sigma\alpha + h\Sigma\beta + h^2\Sigma\gamma$, quem aequatio (19.) praebet, in qua h mutandum est cum h^2, haec formula transit in hanc:

$$\Sigma\sec^2\frac{4\alpha\pi}{p} + h^2\Sigma\sec^2\frac{4\beta\pi}{p} + h\Sigma\sec^2\frac{4\gamma\pi}{p} = \frac{4p^2}{\pi^2}(A + h^2 B + hC),$$

quae, conjuncta cum aequatione facile demonstranda

$$\Sigma\sec^2\frac{4\alpha\pi}{p} + \Sigma\sec^2\frac{4\beta\pi}{p} + \Sigma\sec^2\frac{4\gamma\pi}{p} = \frac{4p^2}{\pi^2}(A + B + C),$$

in has aequationes simplices dilabitur:

$$32. \quad A = \frac{\pi^2}{4p^2}\Sigma\sec^2\frac{4\alpha\pi}{p}, \quad B = \frac{\pi^2}{4p^2}\Sigma\sec^2\frac{4\beta\pi}{p}, \quad C = \frac{\pi^2}{4p^2}\Sigma\sec^2\frac{4\gamma\pi}{p}.$$

§. 7.

Summae numerorum α, β, γ, qui minores sunt quam $\frac{1}{2}p$, scilicet $\Sigma\alpha$, $\Sigma\beta$, $\Sigma\gamma$, si numerus p magnus est, non sine multo labore computantur; singulae enim $\frac{1}{2}(p-1)$ terminis constant. Hic autem per applicationem singularem methodi generalis in §. 3. expositae, formulas simplices inveniemus, quibus hae summae ad similes summas reducuntur, qui eos tantum numeros α, β et γ continent, qui sunt minores quam $\frac{1}{4}p$, qua re hic labor dimidio minuitur. Ad hunc finem adhibemus seriem infinitam

$$\varphi(v) = \cos v + \frac{\cos 2v}{2^2} + \frac{\cos 3v}{3^2} + \frac{\cos 5v}{5^2} + \frac{\cos 6v}{6^2} + \ldots,$$

in qua omnes termini desunt, quorum denominatores sunt multipla numeri 4.

Cujus seriei summa est:

$$\varphi(v) = \frac{-3\pi v}{8} + \frac{5\pi^2}{32}, \text{ si } v \text{ est intra limites } 0 \text{ et } \tfrac{1}{2}\pi,$$

$$\varphi(v) = \frac{-\pi v}{8} + \frac{\pi^2}{32}, \text{ si } v \text{ est intra limites } \tfrac{1}{2}\pi \text{ et } \pi;$$

est igitur

$$\varphi\left(\frac{2\varkappa\pi}{p}\right) = \frac{-3\pi^2\varkappa}{4} + \frac{5\pi^2}{32}, \text{ si } \varkappa \text{ est intra limites } 0 \text{ et } \tfrac{1}{4}p,$$

$$\varphi\left(\frac{2\varkappa\pi}{p}\right) = \frac{-\pi^2\varkappa}{4} + \frac{\pi^2}{32}, \text{ si } \varkappa \text{ est intra limites } \tfrac{1}{4}p \text{ et } \tfrac{1}{2}p,$$

quibus in formula generali (17.) substitutis, habemus

$$33. \quad 6\pi^2\Sigma\left(\frac{\varkappa}{p}\right)^2\left(\frac{-3\varkappa}{4p} + \frac{5}{32}\right) + 6\pi^2\Sigma\left(\frac{\varkappa}{p}\right)^2\left(\frac{-\varkappa}{4p} + \frac{1}{32}\right) +$$
$$= (z_1 + h^2 z_2 + h z_3)\left(\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right)\frac{1}{2^2} + \left(\frac{3}{p}\right)\frac{1}{3^2} + \left(\frac{5}{p}\right)\frac{1}{5^2} + \dots\right),$$

in qua formula signum summae alterum ad omnes numeros integros $\varkappa$ extendendum est, qui intra limites 0 et $\frac{1}{4}p$, alterum autem ad eos qui intra limites $\frac{1}{4}p$ et $\frac{1}{2}p$ jacent. Altera pars hujus aequationis facile in hanc formam redigitur:

$$(z_1 + h^2 z_2 + h z_3)\left(1 + \left(\frac{2}{p}\right)\frac{1}{4}\right)\left(\left(\frac{1}{p}\right) + \left(\frac{3}{p}\right)\frac{1}{3^2} + \left(\frac{5}{p}\right)\frac{1}{5^2} + \left(\frac{7}{p}\right)\frac{1}{7^2} + \dots\right),$$

quae per formulam (18.) transformatur in hanc:

$$-\frac{3\pi^2}{p}\left(1 + \left(\frac{2}{p}\right)\frac{1}{4}\right)(\Sigma\alpha + h^2\Sigma\beta + h\Sigma\gamma).$$

Etiam in altera parte formulae (33.) sejungendi sunt valores literae $\varkappa$, pro quibus $\left(\frac{\varkappa}{p}\right) = 1$, $\left(\frac{\varkappa}{p}\right) = h$ et $\left(\frac{\varkappa}{p}\right) = h^2$. Quem in finem per characterem $\Sigma_1\alpha$ designamus summam eorum numerorum α, qui sunt minores quam $\frac{1}{4}p$, et per $\Sigma_2\alpha$ summam eorum, qui intra limites $\frac{1}{4}p$ et $\frac{1}{2}p$ reperiuntur, unde etiam signorum $\Sigma_1\beta$, $\Sigma_2\beta$, $\Sigma_1\gamma$ et $\Sigma_2\gamma$ vis perspicua est. Praeterea sit λ numerus terminorum summae $\Sigma_1\alpha$, λ_1 numerus terminorum summae $\Sigma_2\alpha$, et eodem modo sint μ et μ_1, ν et ν_1 numeri terminorum quos summae $\Sigma_1\beta$ et $\Sigma_2\beta$, $\Sigma_1\gamma$ et $\Sigma_2\gamma$ habent. Quibus positis formula (33.) hanc formam accipit:

$$\left(-\tfrac{3}{2}\Sigma_1\alpha + \frac{5\lambda p}{16} - \tfrac{1}{2}\Sigma_2\alpha + \frac{\lambda_1 p}{16}\right) + h^2\left(-\tfrac{3}{2}\Sigma_1\beta + \frac{5\mu p}{16} - \tfrac{1}{2}\Sigma_2\beta + \frac{\mu_1 p}{16}\right)$$
$$+ h\left(-\tfrac{3}{2}\Sigma_1\gamma + \frac{5\nu p}{16} - \tfrac{1}{2}\Sigma_2\gamma + \frac{\nu_1 p}{16}\right) = -\left(1 + \left(\frac{2}{p}\right)\frac{1}{4}\right)(\Sigma\alpha + h^2\Sigma\beta + h\Sigma\gamma).$$

Haec formula multo simplicior redditur per aequationes

$$\Sigma_1\alpha + \Sigma_2\alpha = \Sigma\alpha, \quad \Sigma_1\beta + \Sigma_2\beta = \Sigma\beta, \quad \Sigma_1\gamma + \Sigma_2\gamma = \Sigma\gamma,$$
$$\lambda + \lambda_1 = \tfrac{1}{6}(p-1), \quad \mu + \mu_1 = \tfrac{1}{6}(p-1), \quad \nu + \nu_1 = \tfrac{1}{6}(p-1),$$

quorum auxilio fit:

$$(4\Sigma_1\alpha - p\lambda) + h^2(4\Sigma_1\beta - p\mu) + h(4\Sigma_1\gamma - p\nu) = \left(2 + \left(\frac{2}{p}\right)\right)(\Sigma\alpha + h^2\Sigma\beta + h\Sigma\gamma).$$

Haec aequatio, unitatis radicem cubicam imaginariam h involvens, duas aequationes reales continet, quae cum aequatione $\Sigma\alpha + \Sigma\beta + \Sigma\gamma = \frac{1}{8}(p^2 - 1)$ conjunctae ad determinandas singulas quantitates $\Sigma\alpha$, $\Sigma\beta$ et $\Sigma\gamma$ sufficiunt. In hac re tres casus distinguendi sunt: primus quo $\left(\frac{2}{p}\right) = 1$, secundus quo $\left(\frac{2}{p}\right) = h$ et tertius quo $\left(\frac{2}{p}\right) = h^2$, pro quibus singulis calculi indicati sine ulla difficultate perficiuntur, quibus igitur perscribendis supersedebimus. Summae autem hae sunt:

I. Si $\left(\frac{2}{p}\right) = 1$, sive si 2 est residuum cubicum:

$$\begin{aligned}
3\Sigma\alpha &= 4\Sigma_1\alpha - p\lambda + \tfrac{1}{6}p(p-1),\\
3\Sigma\beta &= 4\Sigma_1\beta - p\mu + \tfrac{1}{6}p(p-1),\\
3\Sigma\gamma &= 4\Sigma_1\gamma - p\nu + \tfrac{1}{6}p(p-1).
\end{aligned}$$

II. Si $\left(\frac{2}{p}\right) = h$, sive si 2 in serie numerorm β reperitur:

$$\begin{aligned}
3\Sigma\alpha &= 4\Sigma_1\alpha - 4\Sigma_1\beta - p\lambda + p\mu + \tfrac{1}{8}(p^2-1),\\
3\Sigma\beta &= 4\Sigma_1\beta - 4\Sigma_1\gamma - p\mu + p\nu + \tfrac{1}{8}(p^2-1),\\
3\Sigma\gamma &= 4\Sigma_1\gamma - 4\Sigma_1\alpha - p\nu + p\lambda + \tfrac{1}{8}(p^2-1).
\end{aligned}$$

III. Si $\left(\frac{2}{p}\right) = h^2$, sive si 2 in serie numerorum γ reperitur:

$$\begin{aligned}
3\Sigma\alpha &= 4\Sigma_1\alpha - 4\Sigma_1\gamma - p\lambda + p\nu + \tfrac{1}{8}(p^2-1),\\
3\Sigma\beta &= 4\Sigma_1\beta - 4\Sigma_1\alpha - p\mu + p\lambda + \tfrac{1}{8}(p^2-1),\\
3\Sigma\gamma &= 4\Sigma_1\gamma - 4\Sigma_1\beta - p\nu + p\mu + \tfrac{1}{8}(p^2-1).
\end{aligned}$$

Eaedem formulae etiam per methodos directas, in doctrina numerorum usitatas, demonstrari possunt, sed hic earum deductionem methodo analytica tradere placuit, qua primum a nobis inventae sunt. Hae autem disquisitiones, quas de residuis cubicis instituimus, tanquam specimina sufficiant.