JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

KUMMER

Sur les nombres complexes qui sont formés avec les nombres entiers réels et les racines de l'unité

Journal de mathématiques pures et appliquées 1re série, tome 12 (1847), p. 185-212.
<http://www.numdam.org/item?id=JMPA_1847_1_12__185_0>

SUR LES NOMBRES COMPLEXES

QUI SONT FORMÉS AVEC LES NOMBRES ENTIERS RÉELS

ET LES RACINES DE L'UNITÉ;

PAR M. KUMMER[*].

Numeri complexi, quos summus Gaussius primus in doctrinam numerorum introduxit, et quorum auxilio residuorum biquadraticorum theoriam absolvit, formam habent $a + b\sqrt{-1}$. Præter hos autem numeros complexos alii etiam innumeri fingi possunt, qui ad alia doctrinæ numerorum capita eodem modo pertineant, quo hoc genus simplicissimum numerorum complexorum præcipue ad residua quadratica et biquadratica referendum est. Inter hos præcipue notatu digni videntur numeri complexi altioribus unitatis radicibus, per numeros integros reales multiplicatis, compositi, qui doctrinæ de sectione circuli et de residuis potestatum altiorum inserviunt, et cum iis disciplinis tam arcte conjuncti sunt, ut ab ipsis quasi generentur. Quæ de iis numeris hactenus in publicum edita sunt summo geometræ Cl. Jacobi debentur, qui primus demonstravit quemlibet numerum primum formæ $m\lambda + 1$ in duos factores complexos ejus generis discerpi posse. Quod idem numerus primus p pluribus modis diversis in factores duos diffinditur, et quod producta certa ex iis factoribus formata per alios factores divisibiles fiunt, neque tamen hi ipsi factores cum illis compensari possunt, res maximi momenti, indicat hos factores non esse primos sed compositos. Ulteriorem factorum dissolutionem in factores primos Cl. Jacobi pro iis numeris perfecit, qui radices unitatis quintas, octavas et duodecimas continent, ejusque rei notitiam cum regia Academia litterarum Berolinensi communicavit. In hoc quæstionum genere etiam ea versantur, quæ vobis almæ Universitatis Albertinæ viris doctis illustrissimis tanquam magnæ meæ erga vos observantiæ et reverentiæ documentum, hac occasione solemni data, tradere audeo.

[*] C'est le Mémoire que nous avons annoncé à la page 136 : il a été imprimé pour la première fois, comme nous l'avons dit, en 1844, à Breslau, sous ce titre : *De numeris complexis, qui radicibus unitatis et numeris integris realibus constant*, et adressé par l'Université de Breslau à l'Université de Kœnigsberg, à l'occasion du troisième jubilé séculaire de cette dernière Université. Nous donnons ici le texte latin. Nous n'avons pas eu le temps d'en faire la traduction. (J. LIOUVILLE.)

§ 1.

Si α est radix quædam primitiva æquationis $\alpha^\lambda = 1$, quemlibet functionem rationalem integram radicis α, cujus omnes coefficientes numeri integri sint, numerum integrum complexum voco. Talis functio, æquationis $\alpha^\lambda = 1$ ope, statim ad gradum $\lambda - 1$ reducitur, itaque numerorum complexorum quos tractaturi sumus forma generalis est hæc

$$f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1};$$

numerum λ hic ubique numerum primum accipimus, qui est casus maximi momenti, et quasi fons a quo tota hæc doctrina derivatur. Inde rejecta radice $\alpha = 1$, quæ hac conditione est sola radix non primitiva, habemus æquationem

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

cujus ope ex repræsentatione numeri complexi $f(\alpha)$ unus terminus removeri potest, ex. gr. ultimus, quo facto numerus complexus respectu radicis α ad gradum $\lambda - 2$ deprimitur. Hanc autem reductionem, quæ summarum symetriam turbaret, in universum non adoptabimus, sed retentis omnibus terminis et coefficientibus a, a_1, a_2, etc., æquatione

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0$$

ita utemur, ut summa omnium coefficientium $a + a_1 + a_2 + \ldots + a_{\lambda-1}$ quodam modo in potestate nostra sit. Nam, *si coefficientes numeri complexi $f(\alpha)$ omnes eodem numero augentur vel minuuntur, hic ipse numerus $f(\alpha)$ non mutatur,* quia nihil accedit nisi multiplum formæ $1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1}$, quæ nihilo æqualis est. Vice versa, *duo numeri complexi æquales esse nequeunt nisi, coefficientibus omnibus eodem numero auctis vel minutis, alter prorsus idem fit atque alter.* Positis enim

$$f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1},$$
$$\varphi(\alpha) = b + b_1\alpha + b_2\alpha^2 + \ldots + b_{\lambda-1}\alpha^{\lambda-1},$$

si est $f(\alpha) = \varphi(\alpha)$, habemus

$$0 = a - b + (a_1 - b_1)\alpha + (a_2 - b_2)\alpha^2 + \ldots + (a_{\lambda-1} - b_{\lambda-1})\alpha^{\lambda-1}.$$

Hæc autem æquatio gradus $\lambda - 1$ idem valere debet atque æquatio

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

quia, si res aliter se haberet, ex utraque æquatione conjuncta alia æquatio gradus minoris prodiret, cujus coefficientes rationales essent, quod fieri non posse ex Gaussii disquisitionibus arithmeticis notum est. Itaque ex æqualitate numerorum $f(\alpha)$ et $\varphi(\alpha)$, sequitur

$$a - b = a_1 - b_1 = a_2 - b_2 = \ldots = a_{\lambda-1} - b_{\lambda-1}.$$

In numero complexo $f(\alpha)$ est α radix quædam æquationis

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

cujus ceteræ radices unius α potestates sunt: omnibus iis radicibus loco α in $f(\alpha)$ substitutis habemus $\lambda - 1$ numeros complexos $f(\alpha), f(\alpha^2), f(\alpha^3), \ldots, f(\alpha^{\lambda-1})$, quos *numeros conjunctos* appellabimus. Inter hos bini ad radices reciprocas pertinent, scilicet $f(\alpha^{\mu})$ et $f(\alpha^{-\mu})$, quos *numeros reciprocos* vocare convenit. Productum omnium numerorum conjunctorum tanquam functio invariabilis integra omnium radicum æquationis

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1} = 0,$$

semper est numerus realis integer, qui numeri complexi *norma* appellatur. Ex ipsa normæ definitione statim perspici possunt propositiones simplices: *numeros conjunctos eamdem normam habere,* et *normam producti æqualem esse producto ex normis singulorum factorum.* Numeri complexi $f(\alpha)$ normam, præeunte Cl. Lejeune-Dirichlet, præposita littera N designamus, ita ut sit

$$\mathrm{N} f(\alpha) = f(\alpha) f(\alpha^2) f(\alpha^3) \ldots f(\alpha^{\lambda-1});$$

unde hæ propositiones tali modo exhiberi possunt

$$\mathrm{N} f(\alpha^r) = \mathrm{N} f(\alpha) \quad \text{et} \quad \mathrm{N}[f(\alpha)\varphi(\alpha)] = \mathrm{N} f(\alpha) . \mathrm{N}\varphi(\alpha).$$

§ II.

Si omnes coefficientes numeri complexi $f(\alpha)$ pro indeterminatis habentur, et productum factorum omnium qui normam constituunt evolvitur, forma homogenea gradus $\lambda - 1$ et λ indeterminatorum prodit, quorum vero unus ex arbitrio eligi potest, ita ut $\lambda - 1$ numeri indeterminati remaneant. Omnes igitur disquisitiones de numeris complexis pro disquisitionibus de talibus formis gradus $\lambda - 1$ totidemque indeterminatorum haberi possunt. De formatione hujus formæ notare convenit eam pro æquatione haberi posse, quæ ex æquationibus duabus

$$0 = a + a_1 \alpha + a_2 \alpha^2 + \ldots + a_{\lambda-1} \alpha^{\lambda-1},$$

$$0 = 1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1},$$

quantitate α eliminata, efficitur, quam eamdem esse atque æquationem

$$f(\alpha) f(\alpha^2) \ldots f(\alpha^{\lambda-1}) = 0,$$

ex notissimis regulis algebraicis constat. Alio modo, norma tanquam denominator communis invenitur, quem systematis æquationum linearium incognitæ evolutæ habent. Quales denominatores Cl. Jacobi determinantium nomine ornavit et pluribus locis in-

geniosissime tractavit. Accipimus systema æquationum linearium hocce :

$$(A)\quad \begin{cases} a\,b + a_{\lambda-1}\,b_1 + a_{\lambda-2}\,b_2 + \ldots + a_1\,b_{\lambda-1} = c + m, \\ a_1 b + a\,b_1 + a_{\lambda-1}\,b_2 + \ldots + a_2\,b_{\lambda-1} = c_1 + m, \\ a_2 b + a_1 b_1 + a\,b_2 + \ldots + a_3\,b_{\lambda-1} = c_2 + m, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{\lambda-1}\,b + a_{\lambda-2}\,b_1 + a_{\lambda-3}\,b_2 + \ldots + a\,b_{\lambda-1} = c_{\lambda-1} + m, \end{cases}$$

cujus incognitæ sint $b,\ b_1,\ b_2,\ldots,\ b_{\lambda-1}$, easque æquationes secundum ordinem multiplicamus per $1,\ \alpha,\ \alpha^2,\ldots,\ \alpha^{\lambda-1}$, quo facto summa omnium facile in hanc formam redigitur

$$(a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1})\,(b + b_1\alpha + b_2\alpha^2 + \ldots + b_{\lambda-1}\alpha^{\lambda-1}) = c + c_1\alpha + c_2\alpha^2 + \ldots + c_{\lambda-1}\alpha^{\lambda-1};$$

inde positis

$$f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1},$$
$$\varphi(\alpha) = b + b_1\alpha + b_2\alpha^2 + \ldots + b_{\lambda-1}\alpha^{\lambda-1},$$
$$\psi(\alpha) = c + c_1\alpha + c_2\alpha^2 + \ldots + c_{\lambda-1}\alpha^{\lambda-1},$$

est

$$f(\alpha).\varphi(\alpha) = \psi(\alpha),$$

et utraque parte per $f(\alpha^2)f(\alpha^3)\ldots f(\alpha^{\lambda-1})$ multiplicata, fit

$$\varphi(\alpha).\mathrm{N}f(\alpha) = \psi(\alpha)f(\alpha^2)f(\alpha^3)\ldots f(\alpha^{\lambda-1}),$$

sive

$$\varphi(\alpha) = \frac{\psi(\alpha)f(\alpha^2)f(\alpha^3)\ldots f(\alpha^{\lambda-1})}{\mathrm{N}f(\alpha)},$$

ex quo apparet quantitatum $b,\ b_1,\ b_2,\ldots,\ b_{\lambda-1}$, quæ formulam $\varphi(\alpha)$ constituunt, denominatorem generalem esse normam $\mathrm{N}f(\alpha)$, uti contendimus.

Quum norma sit forma aliqua gradus $\lambda - 1$ et $\lambda - 1$ indeterminatorum, statim quæstio oboritur de numeris qui hac forma repræsentari possint et qui non possint. Hanc autem quæstionem gravissimam, quæ sine dubio inter mysteria doctrinæ numerorum maxime recondita referenda est, hactenus non potuimus absolvere; sola hæc propositio elementaris ad hanc quæstionem spectans : *normam semper habere formam* $m\lambda + 1$, *vel* $m\lambda$, jam hoc loco, quasi in limine disquisitionum nostrarum, facile demonstrari potest. Quem ad finem adhibemus tres numeros complexos $f(\alpha)$, $\varphi(\alpha)$ et $\psi(\alpha)$, eosdem quibus modo usi sumus, quorum vero coefficientes omnes integri sint. Si est

$$f(\alpha).\varphi(\alpha) = \psi(\alpha),$$

inter coefficientes horum numerorum complexorum æquationes lineares (A) locum ha-

bere debent, iisque additis fit

$$(a + a_1 + a_2 + \ldots + a_{\lambda-1})(b + b_1 + b_2 + \ldots + b_{\lambda-1}) = c + c_1 + c_2 + \ldots + c_{\lambda-1} + \lambda m,$$

quæ æquatio in congruentiam pro modulo λ mutata docet : *summam coefficientium producti duorum numerorum complexorum producto e summis coefficientium utriusque factoris congruam esse, modulo* λ. Quæ propositio facillime ad productum quotcunque factorum extenditur. Norma semper est productum $\lambda - 1$ factorum complexorum, qui easdem coefficientium summas habent, pro ea igitur productum e summis coefficientium omnium factorum conflatum in potestatem exponentis $\lambda - 1$ abit, unde habemus

$$(a + a_1 + a_2 + \ldots + a_{\lambda-1})^{\lambda-1} \equiv \mathrm{N}f(\alpha) \pmod{\lambda},$$

itaque, per theorema Fermatianum,

$$\mathrm{N}f(\alpha) \equiv 1 \pmod{\lambda},$$

nisi forte sit

$$a + a_1 + a_2 + \ldots + a_{\lambda-1} \equiv 0 \pmod{\lambda},$$

qua conditione fit

$$\mathrm{N}f(\alpha) \equiv 0 \pmod{\lambda}.$$

§ III.

Normæ usus insignis est in divisione numerorum complexorum, quippe cujus auxilio divisor complexus semper in divisorem realem mutari potest. Posito enim

$$\mathrm{F}(\alpha) = f(\alpha^2) f(\alpha^3) \ldots f(\alpha^{\lambda-1})$$

fit

$$\frac{\varphi(\alpha)}{f(\alpha)} = \frac{\varphi(\alpha)\mathrm{F}(\alpha)}{\mathrm{N}f(\alpha)}.$$

Si $\varphi(\alpha)$ per $f(\alpha)$ divisibilis est, i. e. si hic quotiens numero integro complexo æqualis est, $\varphi(\alpha)\mathrm{F}(\alpha)$ per numerum integrum realem $\mathrm{N}f(\alpha)$ dividi possit necesse est, numerus autem complexus per numerum realem divisibilis non est, nisi coefficientes ejus singuli, per hunc numerum divisi, eadem residua habeant. Inde nacti sumus hoc criterium generale, quo dijudicari possit, utrum numerus complexus per alium numerum complexum divisibilis sit, an non : *Numerus complexus* $\varphi(\alpha)$ *per alium numerum* $f(\alpha)$ *divisibilis est, si in producto evoluto* $\varphi(\alpha) f(\alpha^2) f(\alpha^3) \ldots f(\alpha^{\lambda-1})$ *omnes coefficientes pro modulo* $\mathrm{N}f(\alpha)$ *congrui sunt, sin vero hi coefficientes non omnes congrui sunt,* $\varphi(\alpha)$ *certo non divisibilis est per* $f(\alpha)$.

Alio etiam modo numerorum complexorum divisio perfici potest, ita quidem, ut ad divisionem fonctionum rationalium integrarum revocetur. Altioribus enim potestatibus radicis α admissis, numerus $\varphi(\alpha)$ infinitis modis diversis representari potest, qui

omnes hac forma generali continentur

$$\varphi(\alpha) - (1 + \alpha + \alpha^2 + \ldots + \alpha^{\lambda-1})\,\psi(\alpha),$$

in qua $\psi(\alpha)$ functionem integram quamcunque designat, quæ pro fine singulorum problematum apte eligi poterit. Jam dico, *si* $\varphi(\alpha)$ *per* $f(\alpha)$ *divisibilis sit, huic numero* $\varphi(\alpha)$ *semper formam ejusmodi dari posse, ut pro quolibet valore quantitatis* α, *quæ tanquam variabilis spectanda est, divisio succedat et residuum relinquatur nullum.* Per hypothesin quotiens $\frac{\varphi(\alpha)}{f(\alpha)}$ æqualis est numero alicui complexo $\mathrm{F}(\alpha)$, itaque

$$\frac{\varphi(\alpha)}{f(\alpha)} = \mathrm{F}(\alpha), \quad \text{sive } \varphi(\alpha) = f(\alpha)\,\mathrm{F}(\alpha).$$

Jam signo α in x mutato, videmus functionem rationalem integram variabilis x, $\varphi(x) - f(x)\,\mathrm{F}(x)$ evanescere, si x cuilibet radici æquationis

$$1 + x + x^2 + \ldots + x^{\lambda-1} = 0$$

æqualis fit; hæc igitur functio integra factorem $1 + x + x^2 + \ldots + x^{\lambda-1}$ habeat necesse est: quare in hanc formam redigi potest

$$\varphi(x) - f(x)\,\mathrm{F}(x) = (1 + x + x^2 + \ldots + x^{\lambda-1})\,\psi(x),$$

ex qua theorema enuntiatum sponte manat.

§ IV.

Inter numeros complexos præcipue notatu digni sunt ii, quorum norma est unitas, quos omnes unitatum complexarum nomine designamus. Hæ unitates in doctrina numerorum complexorum easdem fere partes suscipiunt, quas æquationis Pellianæ

$$x^2 - \mathrm{D}y^2 = \pm 1$$

solutiones in doctrina formarum secundi gradus determinantis positivi agunt. Numerus harum unitatum, excepto solo casu $\lambda = 3$, semper infinitus est, et simili modo ut in solvenda æquatione Pelliana semper unitates quædam fundamentales dantur, ex quibus ad potestates evectis et inter se multiplicatis infinitus numerus aliarum unitatum deducitur. Simplicissimæ unitates sunt ± 1, $\pm\alpha$, $\pm\alpha^2$, ..., $\pm\alpha^{\lambda-1}$, quæ sponte se offerunt, præter has autem aliæ facile inveniuntur, ratione habita numeri complexi $1 + \alpha + \alpha^2 + \ldots + \alpha^{r-1}$, in quo r est numerus quilibet integer minor quam λ; hic numerus fractionis forma exhibetur hoc modo

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{r-1} = \frac{1 - \alpha^r}{1 - \alpha},$$

ejusque norma est

$$\frac{(1 - \alpha^r)(1 - \alpha^{2r})(1 - \alpha^{3r}) \ldots (1 - \alpha^{(\lambda-1)r})}{(1 - \alpha)(1 - \alpha^2)(1 - \alpha^3) \ldots (1 - \alpha^{\lambda-1})},$$

in qua, loco exponentium r, $2r$, $3r$, ..., $(\lambda-1)r$ residuis minimis modulo λ substitutis, singuli factores numeratoris iidem fiunt atque denominatoris, quæ igitur unitati æqualis est. Quum jam $1+\alpha+\alpha^2+\ldots+\alpha^{r-1}$ sit unitas, et norma producti æqualis producto e normis factorum composito, sequitur ut forma generalis

$$\pm\alpha^k(1+\alpha+\alpha^2+\ldots+\alpha^{r-1})^l(1+\alpha+\alpha^2+\ldots+\alpha^{s-1})^m(1+\alpha+\alpha^2+\ldots+\alpha^{t-1})^n\ldots,$$

pro omnibus numeris k, l, m, n,..., r, s, t,..., unitates complexas contineat. Numerus factorum diversorum, qui ad potestates evehendi et multiplicandi sunt, ut diversæ unitates obtineantur, itemque numeri r, s, t,..., pro singulis numeris λ accurate definiri possunt, quam vero disquisitionem hoc loco prætereuntes, unitatum proprietatem generalem demonstrabimus, qua in posterum utemur, scilicet : *unitates complexas non tam singularum radicum* 1, α, α^2,..., $\alpha^{\lambda-1}$, *quam periodorum ex binis earum*, $\alpha+\alpha^{\lambda-1}$, $\alpha^2+\alpha^{\lambda-2}$, *etc.*, *functiones lineares esse*, *si ad factorem accedentem* $\pm\alpha^k$ *non respiciatur*, sive *omnes unitates hanc formam habere*

$$\pm\alpha^k\left\{c+c_1(\alpha+\alpha^{\lambda-1})+c_2(\alpha^2+\alpha^{\lambda-2})+\ldots+c_{\frac{\lambda-1}{2}}\left(\alpha^{\frac{\lambda-1}{2}}+\alpha^{\frac{\lambda-1}{2}}\right)\right\}.$$

E producto

$$1=\varphi(\alpha)\,\varphi(\alpha^2)\,\varphi(\alpha^3)\ldots\varphi(\alpha^{\lambda-1})$$

factorum semissem ex arbitrio eligo, ita tamen ut reciproci in eadem semissi non insint, sed cujuslibet factoris reciprocus in altera semissi reperiatur. Horum factorum productum sit $\psi(\alpha)$, unde alterius semissis productum est $\psi(\alpha^{-1})$, et $\psi(\alpha)\,\psi(\alpha^{-1})=1$. Ponatur

$$\psi(\alpha)=a+a_1\alpha+a_2\alpha^2+\ldots+a_{\lambda-1}\alpha^{\lambda-1},$$

unde

$$\psi(\alpha^{-1})=a+a_1\alpha^{\lambda-1}+a_2\alpha^{\lambda-2}+\ldots+a_{\lambda-1}\alpha,$$

atque ex multiplicatione oriatur

$$\psi(\alpha)\,\psi(\alpha^{-1})=\mathrm{A}+\mathrm{A}_1\alpha+\mathrm{A}_2\alpha^2+\ldots+\mathrm{A}_{\lambda-1}\alpha^{\lambda-1},$$

erit

$$\mathrm{A}=a^2+a_1^2+a_2^2+\ldots+a_{\lambda-1}^2,$$

$$\mathrm{A}_1=aa_1+a_1a_2+a_2a_3+\ldots+a_{\lambda-1}a,$$

$$\mathrm{A}_2=aa_2+a_1a_3+a_2a_4+\ldots+a_{\lambda-1}a_1,$$

etc., etc.

et summa coefficientium fit

$$\mathrm{A}+\mathrm{A}_1+\mathrm{A}_2+\ldots+\mathrm{A}_{\lambda-1}=(a+a_1+a_2+\ldots+a_{\lambda-1})^2;$$

præterea quum sit

$$\mathrm{A} + \mathrm{A}_1 \alpha + \mathrm{A}_2 \alpha^2 + \ldots + \mathrm{A}_{\lambda-1} \alpha^{\lambda-1} = 1,$$

erit

$$\mathrm{A}_1 = \mathrm{A}_2 = \mathrm{A}_3 = \ldots = \mathrm{A}_{\lambda-1} = m$$

et

$$\mathrm{A} = m + 1,$$

itaque

$$m\lambda + 1 = (a + a_1 + a_2 + \ldots + a_{\lambda-1})^2$$

et

$$\pm 1 \equiv a + a_1 + a_2 + \ldots + a_{\lambda-1} \pmod{\lambda};$$

horum coefficientium summa, quæ congrua est ± 1 modulo λ, etiam æqualis ± 1 accipi potest, quo facto fit $m = 0$, $\mathrm{A} = 1$, et quum A sit summa quadratorum positivorum integrorum

$$\mathrm{A} = a^2 + a_1^2 + a_2^2 + \ldots + a_{\lambda-1}^2,$$

unitati æqualis fieri non potest nisi unus numerorum a, a_1, a_2,..., unitati æqualis, ceteri nihilo æquales fiunt, habemus igitur

$$\psi(\alpha) = \pm \alpha^k.$$

Quum $\psi(\alpha)$ alteram factorum semissem normæ 1 contineat, hac sola conditione eligendam, ut factores reciproci non insint, semper plura producta $\psi(\alpha)$ erunt, quæ unitati simplici $\pm \alpha^k$ æqualia sint. Quorum productorum duo eligo, $\psi(\alpha)$ et $\psi_1(\alpha)$, quæ excepto uno factores ceteros omnes eosdem habeant, atque hic solus factor, quo $\psi(\alpha)$ differt a $\psi_1(\alpha)$, sit $\varphi(\alpha^\mu)$, unde factorquem $\psi_1(\alpha)$ continet, neque tamen $\psi(\alpha)$, erit $\varphi(\alpha^{-\mu})$. Inde, ex conjunctis æquationibus

$$\psi(\alpha) = \pm \alpha^k$$

et

$$\psi_1(\alpha) = \pm \alpha^h,$$

fit

$$\psi_1(\alpha) = \pm \alpha^{h-k} \psi(\alpha),$$

et factoribus communibus sublatis et posito

$$h - k = m,$$

est

$$\varphi(\alpha^{-\mu}) = \pm \alpha^m \varphi(\alpha^\mu);$$

quælibet igitur unitas complexa hoc proprium habet, ut a reciproca sua non differat

nisi adjecto factore qui ipse est unitas simplex. Facillime inde theorematis supra propositi veritas perspicitur.

Pro $\lambda = 3$, unitates omnes habere debent formam hanc :

$$\varphi(\alpha) = \pm \alpha^k [c + c_1(\alpha + \alpha^2)],$$

et quia $\alpha + \alpha^2 = -1$,

$$\varphi(\alpha) = \pm \alpha^k (c - c_1),$$

ex quo sequitur ut sit

$$c - c_1 = 1;$$

pro hoc igitur casu præter unitates simplices ± 1, $\pm \alpha$, $\pm \alpha^2$, aliæ non dantur.

Pro $\lambda = 5$, unitatum forma generalis hæc est

$$\varphi(\alpha) = \pm \alpha^k [c + c_1(\alpha + \alpha^4) + c_2(\alpha^2 + \alpha^3)],$$

quæ adhibita æquatione

$$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0,$$

et posito

$$c - c_2 = t, \quad c_1 - c_2 = u,$$

in hanc simpliciorem mutatur

$$\varphi(\alpha) = \pm \alpha^k [t + u(\alpha + \alpha^4)],$$

ex qua fit

$$\varphi(\alpha)\varphi(\alpha^2) = \alpha^{3k}(t^2 - tu - u^2),$$

itaque

$$t^2 - tu - u^2 = \pm 1.$$

Cognitæ hujus æquationis solutiones omnes continentur formis

$$t = \frac{\left(\frac{-1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{-1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}}, \quad u = \frac{\left(\frac{-1+\sqrt{5}}{2}\right)^{n} - \left(\frac{-1-\sqrt{5}}{2}\right)^{n}}{\sqrt{5}},$$

quæ, quia

$$\alpha + \alpha^4 = \frac{-1+\sqrt{5}}{2}, \quad \alpha^2 + \alpha^3 = \frac{-1-\sqrt{5}}{2},$$

etiam hoc modo repræsentari possunt

$$t = \frac{(\alpha+\alpha^4)^{n-1} - (\alpha^2+\alpha^3)^{n-1}}{\alpha+\alpha^4-\alpha^2-\alpha^3}, \quad u = \frac{(\alpha+\alpha^4)^{n} - (\alpha^2+\alpha^3)^{n}}{\alpha+\alpha^4-\alpha^2-\alpha^3};$$

per faciles transformationes ex iis fit

$$t + u(\alpha + \alpha^4) = (\alpha + \alpha^4)^n, \quad \varphi(\alpha) = \pm \alpha^k (\alpha + \alpha^4)^n,$$

itaque pro $\lambda = 5$, unitates complexæ omnes unius unitatis fundamentalis potestates existunt, quæ præterea unitatibus simplicibus formæ $\pm \alpha^k$ multiplicatæ esse possunt,

præter has autem aliæ non dantur. Pro majoribus numeris λ unitatum omnium indagatio multo difficilior est, et principia peculiaria poscit, quæ nos hactenus nondum satis perscrutati sumus. Eo magis hac quæstione nobis supersedendum videtur, quum compertum habeamus Cl. Lejeune-Dirichlet recentissimo tempore in Italia, ubi etiam nunc versatur, de iis unitatibus complexis theoremata fundamentalia elaborasse, quæ ut propediem in publicum edat cum desiderio exspectamus. Hic etiam adnotabo geometram juvenilem Leopoldum Kronecker, qui nunc Vratislaviæ litteris mathematicis studet, pro absolvendis iis unitatibus quæ ad numerum $\lambda = 7$ pertinent methodum subtilem invenisse, quæ ni fallor felici successu ad altiorum ordinum unitates pertractandas applicari poterit.

§ V.

Progredimur ad perscrutandos eos numeros complexos, quorum norma sit numerus primus p, ita ut habeatur

$$p = f(\alpha) f(\alpha^2) f(\alpha^3) \ldots f\left(\alpha^{\lambda-1}\right).$$

Numerus primus, qui tali modo in $\lambda - 1$ factores dissolvi potest, secundum theorema paragrapho tertia propositum, formam linearem $m\lambda + 1$ habere debet, nisi est ipse numerus $\lambda = p$, qui tali modo in $\lambda - 1$ factores dissolvitur

$$\lambda = (1 - \alpha)(1 - \alpha^2)(1 - \alpha^3) \ldots \left(1 - \alpha^{\lambda-1}\right).$$

Factores $f(\alpha)$, $f(\alpha^2)$, etc., *sunt numeri complexi primi qui, si unitates complexæ excluduntur, ulterius in factores dissolvi non possunt.* Nam si ponimus $f(\alpha)$ e factoribus $\varphi(\alpha).\psi(\alpha)$ constare, habemus

$$f(\alpha) = \varphi(\alpha).\psi(\alpha),$$

et

$$\mathrm{N}f(\alpha) = \mathrm{N}\varphi(\alpha).\mathrm{N}\psi(\alpha),$$

et quia $\mathrm{N}f(\alpha) = p$ est numerus primus, alter factorum realium integrorum $\mathrm{N}\varphi(\alpha)$ et $\mathrm{N}\psi(\alpha)$ unitati æqualis esse debet, itaque alter factorum $\varphi(\alpha)$ et $\psi(\alpha)$ erit unitas complexa, et $f(\alpha)$ numerus primus complexus. Porro demonstramus *hos factores* $f(\alpha)$, $f(\alpha^2)$, etc., *omnes inter se diversos esse.* Ex æqualitate duorum factorum

$$f(\alpha^\mu) = f(\alpha^\nu),$$

alia radice idonea loco α substituta, sequeretur

$$f(\alpha) = f(\alpha^n),$$

et repetita substitutione α^n loco α, esset

$$f(\alpha) = f(\alpha^n) = f\left(\alpha^{n^2}\right) = f\left(\alpha^{n^3}\right) = \ldots.$$

Jam si infima potestas numeri n, quæ unitati congrua sit modulo λ, est n^h, in producto

$\lambda - 1$ factorum numeri p erunt h factores æquales; alia deinde radice substituta, quæ inter radices α, α^n, α^{n^2}, etc., non invenitur, statim alios h factores æquales obtinemus, et ita porro, usque dum omnes factores exhausti sunt. Igitur ex æqualitate duorum factorum primum sequeretur ut p sit potestas h^{ta} producti eorum factorum complexorum qui inter se diversi sint. Radices α, α^n, α^{n^2}, etc., periodum h terminorum efficiunt, atque si functio rationalis integra $f(\alpha)$, loco α omnibus periodi radicibus substitutis, immutata manet, hanc ipsam omnium similium periodorum, itaque etiam unius earum, functionem rationalem integram esse constat. Ceteri factores diversi ab hoc non differre possunt, nisi quod ceterarum periodorum functiones sunt, et omnium factorum diversorum productum, tanquam functio invariabilis omnium periodorum similium, esse debet numerus integer realis. Hinc tandem sequeretur ut p esset potestas numeri realis et exponentis h, quod quum absurdum sit concludimus omnes illos factores primos complexos numeri p inter se diversos esse.

Si tali factore primo complexo numeri p tanquam modulo sive divisore utimur, simul productum ceterorum factorum

$$\mathrm{F}(\alpha) = f(\alpha^2) f(\alpha^3) \dots f(\alpha^{\lambda-1}),$$

cujus auxilio divisio per numerum complexum $f(\alpha)$ ad divisionem per numerum realem $\mathrm{N} f(\alpha)$ reducitur, magni momenti est, quam ob rem hujus producti proprietates principales præterire non possumus. Sit

$$p = f(\alpha)\,\mathrm{F}(\alpha),$$

et producto $\mathrm{F}(\alpha)$ per multiplicationem evoluto habeatur

$$\mathrm{F}(\alpha) = \mathrm{A} + \mathrm{A}_1\alpha + \mathrm{A}_2\alpha^2 + \dots + \mathrm{A}_{\lambda-1}\alpha^{\lambda-1},$$

unde etiam

$$\begin{aligned}
\mathrm{F}(\alpha^2) &= \mathrm{A} + \mathrm{A}_1\alpha^2 + \mathrm{A}_2\alpha^4 + \dots + \mathrm{A}_{\lambda-1}\alpha^{2\lambda-2},\\
\mathrm{F}(\alpha^3) &= \mathrm{A} + \mathrm{A}_1\alpha^3 + \mathrm{A}_2\alpha^6 + \dots + \mathrm{A}_{\lambda-1}\alpha^{3\lambda-3},\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
\mathrm{F}(\alpha^{\lambda-1}) &= \mathrm{A} + \mathrm{A}_1\alpha^{\lambda-1} + \mathrm{A}_2\alpha^{2\lambda-2} + \dots + \mathrm{A}_{\lambda-1}\alpha^{(\lambda-1)(\lambda-1)};
\end{aligned}$$

iis æquationibus secundum ordinem per α^{-n}, α^{-2n}, α^{-3n}, ..., $\alpha^{-(\lambda-1)n}$ multiplicatis et additione conjunctis, habemus

$$\alpha^{-n}\mathrm{F}(\alpha) + \alpha^{-2n}\mathrm{F}(\alpha^2) + \dots + \alpha^{-(\lambda-1)n}\mathrm{F}(\alpha^{\lambda-1}) = \lambda\mathrm{A}_n - (\mathrm{A} + \mathrm{A}_1 + \mathrm{A}_2 + \dots + \mathrm{A}_{\lambda-1}),$$

inde mutando n in $n-1$, et subtrahendo,

$$\alpha^{-n}(1-\alpha)\mathrm{F}(\alpha) + \alpha^{-2n}(1-\alpha^2)\mathrm{F}(\alpha^2) + \dots + \alpha^{-(\lambda-1)n}\mathrm{F}(\alpha^{\lambda-1}) = \lambda(\mathrm{A}_n - \mathrm{A}_{n-1});$$

ex hac forma, denuo mutato n in $n+1$ et $n+2$, prodeunt similes formæ pro

$\lambda(A_{n+1} - A_n)$ et $\lambda(A_{n+2} - A_{n+1})$, quibus inter se multiplicatis formetur evolutio formæ

$$\lambda^2 (A_{n-1} - A_n)^2 - \lambda^2 (A_{n+2} - A_{n+1})(A_n - A_{n-1}).$$

Facile perspicitur in hac evolutione quadrata numerorum complexorum $F(\alpha)$, $F(\alpha^2)$, etc., non reperiri, sed sola producta binorum diversorum, quæ factores $f(\alpha)f(\alpha^2)f(\alpha^3)\dots f(\alpha^{\lambda-1})$ omnes simul, ideoque factorem realem p continent. Quum igitur p sit factor communis omnium terminorum hujus formulæ evolutæ, factore λ^2 omisso, habemus congruentiam

$$(A_{n+1} - A_n)^2 \equiv (A_{n+2} - A_{n+1})(A_n - A_{n-1}) \pmod{p},$$

quæ etiam hoc modo repræsentari potest

$$\frac{A_{n+1} - A_n}{A_{n+2} - A_{n+1}} \equiv \frac{A_n - A_{n-1}}{A_{n+1} - A_n} \pmod{p};$$

posito igitur

$$\frac{A_{n+1} - A_n}{A_{n+2} - A_{n+1}} \equiv \xi \pmod{p},$$

videmus numerum ξ pro omnibus diversis numeris n eumdem manere. Hanc congruentiam si hoc modo scribimus

$$A_{n+1}\xi - A_n \equiv A_{n+2}\xi - A_{n+1} \pmod{p},$$

videmus etiam

$$A_{n+1}\xi - A_n \equiv \eta \pmod{p}$$

pro omnibus diversis numeris n non variari, itaque habemus congruentias

$$(A) \quad \begin{cases} A\xi - A_{\lambda-1} \equiv \eta, \\ A_1\xi - A \equiv \eta, \\ A_2\xi - A_1 \equiv \eta \pmod{p}, \\ \dots\dots\dots\dots \\ A_{\lambda-1}\xi - A_{\lambda-2} \equiv \eta. \end{cases}$$

Aliud etiam systema congruentiarum, quibus coefficientes producti $F(\alpha)$ satisfacere debent, facile e congruentia

$$A_{n+1}\xi - A_n \equiv A_{n+2}\xi - A_{n+1} \pmod{p}$$

deducitur:

$$(B) \quad \begin{cases} A_{\lambda-1} - A \equiv (A - A_1)\xi, \\ A_{\lambda-2} - A_{\lambda-1} \equiv (A - A_1)\xi^2, \\ A_{\lambda-3} - A_{\lambda-2} \equiv (A - A_1)\xi^3, \\ \dots\dots\dots\dots\dots\dots \\ A_1 - A_2 \equiv (A - A_1)\xi^{\lambda-1}, \end{cases}$$

quibus additis, omisso factore $A - A_1$, qui nihilo congruus esse non potest, sequitur ut ξ sit una $\lambda - 1$ radicum realium congruentiæ

$$1 + \xi + \xi^2 + \xi^3 + \ldots + \xi^{\lambda-1} \equiv 0 \pmod{p}.$$

§ VI.

Singulis congruentiis (A) paragraphi antecedentis secundum ordinem quo scriptæ sunt factoribus $1, \alpha, \alpha^2, \ldots, \alpha^{\lambda-1}$ multiplicatis, earum summa facile in hanc formam redigitur :

$$\xi - \alpha)(A + A_1\alpha + A_2\alpha^2 + \ldots + A_{\lambda-1}\alpha^{\lambda-1} \equiv 0 \pmod{p},$$

sive

$$(\xi - \alpha) F(\alpha) \equiv 0 \pmod{p},$$

et factore communi $F(\alpha)$ e modulo $p = f(\alpha)F(\alpha)$ et ex ipsa congruentia sublato habemus

$$\xi - \alpha \equiv 0 \pmod{f(\alpha)}$$

unde elucet etiam pro quolibet numero complexo $\varphi(\alpha)$ semper esse

$$\varphi(\alpha) \equiv \varphi(\xi) \pmod{f(\alpha)};$$

itaque nacti sumus theorema insigne : *Pro modulo complexo $f(\alpha)$, cujus norma est numerus primus, omnes numeri complexi realibus numeris congrui sunt.* Hoc theorema omnibus congruentiis numerorum complexorum, quarum modulus normam habet numerum primum, viam patefacit, quam vero patefactam hic statim relinquimus.

E congruentia

$$\alpha \equiv \xi \pmod{f(\alpha)}$$

sequitur

$$f(\alpha) \equiv f(\xi) \pmod{f(\alpha)},$$

itaque

$$f(\xi) \equiv 0 \pmod{f(\alpha)};$$

numerus autem integer realis $f(\xi)$, qui factorem $f(\alpha)$ continet, omnes etiam factores huic conjunctos, ideoque factorem p continere debet, unde concludimus eam esse indolem factorum complexorum numeri p, ut certa radice congruentiæ

$$1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0 \pmod{p},$$

loco α substituta, horum factorum unus per p divisibilis fiat. Præterea adnotamus pro quolibet numero ξ unum, non plures, factorum $f(\xi)$, $f(\xi^2)$, $f(\xi^3)$, etc., per p divisibilem esse ; si enim simul esset

$$f(\xi) \equiv 0 \quad \text{et} \quad f(\xi^r) \equiv 0 \pmod{p},$$

per congruentiam

$$\xi \equiv \alpha \pmod{f(\alpha)}$$

etiam esse deberet

$$f(\alpha^r) \equiv 0 \pmod{f(\alpha)},$$

duo igitur factores $f(\alpha)$ et $f(\alpha^r)$ æquales esse deberent, quod fieri non posse supra demonstravimus. Quum radices congruentiæ

$$1+\xi+\xi^2+\ldots+\xi^{\lambda-1}\equiv 0 \pmod{p}$$

omnes tanquam potestates unius radicis repræsentari possint, alia quacunque radice loco ξ substituta, alium etiam factorem producti $f(\xi).f(\xi^2).f(\xi^3)\ldots f(\xi^{\lambda-1})$ per p divisibilem fieri patet, *singuli igitur* $\lambda-1$ *factores* $f(\alpha), f(\alpha^2)\ldots f(\alpha^{\lambda-1})$, *cum singulis* $\lambda-1$ *radicibus congruentiæ*

$$1+\xi+\xi^2+\ldots+\xi^{\lambda-1}\equiv 0,$$

ita conjuncti sunt, ut pro certa radice ξ *certus etiam illorum factorum, si* ξ *loco* α *substituitur, per p divisibilis fiat, idemque sit divisor numeri* $\xi-\alpha$.

Jam eo pervenimus ut quæstionem gravissimam absolvere possimus : utrum plures numeri complexi eamdem normam, quæ numerus primus est, habere possint an non, sive an idem numerus primus p, pluribus modis diversis in $\lambda-1$ factores primos complexos dissolvi possit. Fingamus duos numeros complexos $f(\alpha)$ et $\varphi(\alpha)$ eamdem normam p, numerum primum, habere, ita ut sit

$$p=f(\alpha)f(\alpha^2)f(\alpha^3)\ldots f(\alpha^{\lambda-1}),$$
$$p=\psi(\alpha)\psi(\alpha^2)\psi(\alpha^3)\ldots\psi(\alpha^{\lambda-1}).$$

Quum singuli factores horum productorum ad singulas radices congruentiæ

$$1+\xi+\xi^2+\ldots+\xi^{\lambda-1}\equiv 0 \pmod{p}$$

pertineant, alterius producti factores ita dispositos accipiamus, ut $\psi(\alpha)$ et $f(\alpha)$ ad eamdem radicem ξ pertineant, quo facto uterque etiam erit divisor numeri $\xi-\alpha$, atque

$$\psi(\xi)\equiv 0, \quad f(\xi)\equiv 0 \pmod{p}.$$

Inde positis

$$\psi(\alpha)=c+c_1\alpha+c_2\alpha^2+\ldots+c_{\lambda-1}\alpha^{\lambda-1},$$
$$F(\alpha)=f(\alpha^2)f(\alpha^3)\ldots f(\alpha^{\lambda-1})=A+A_1\alpha+A_2\alpha^2+\ldots+A_{\lambda-1}\alpha^{\lambda-1},$$

et

$$\psi(\alpha).F(\alpha)=C+C_1\alpha+C_2\alpha^2+\ldots+C_{\lambda-1}\alpha^{\lambda-1}.$$

hoc producto per multiplicationem evoluto habemus :

$$C=Ac+A_{\lambda-1}c_1+A_{\lambda-2}c_2+\ldots+A_1c_{\lambda-1},$$
$$C_1=A_1c+Ac_1+A_{\lambda-1}c_2+\ldots+A_2c_{\lambda-1},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$C_{\lambda-1}=A_{\lambda-1}c+A_{\lambda-2}c_1+A_{\lambda-3}c_2+\ldots+Ac_{\lambda-1},$$

et si harum æquationum binæ contiguæ subtrahuntur :

$$C - C_1 = (A - A_1)c + (A_{\lambda-1} - A)c_1 + (A_{\lambda-2} - A_{\lambda-1})c_2 + \ldots + (A_1 - A_2)c_{\lambda-1},$$

$$C_1 - C_2 = (A_1 - A_2)c + (A - A_1)c_1 + (A_{\lambda-1} - A)c_2 + \ldots + (A_2 - A_3)c_{\lambda-1},$$

. . . . . .

$$C_{\lambda-2} - C_{\lambda-1} = (A_{\lambda-2} - A_{\lambda-1})c + (A_{\lambda-3} - A_{\lambda-2})c_1 + (A_{\lambda-1} - A_{\lambda-3})c_2 + \ldots + (A_{\lambda-1} - A)c_{\lambda-1}$$

quæ per congruentias (B), § V, mutantur in

$$C - C_1 \equiv (A - A_1)(c + c_1\xi + c_2\xi^2 + \ldots + c_{\lambda-1}\xi^{\lambda-1}),$$

$$C_1 - C_2 \equiv (A_1 - A_2)(c + c_1\xi + c_2\xi^2 + \ldots + c_{\lambda-1}\xi^{\lambda-1}),$$

. . . . . .

$$C_{\lambda-2} - C_{\lambda-1} \equiv (A_{\lambda-2} - A_{\lambda-1})(c + c_1\xi + c_2\xi^2 + \ldots + c_{\lambda-1}\xi^{\lambda-1}),$$

et quum sit

$$\psi(\xi) = c + c_1\xi + c_2\xi^2 + \ldots + c_{\lambda-1}\xi^{\lambda-1} \equiv 0 \pmod{p},$$

habemus

$$C \equiv C_1 \equiv C_2 \equiv \ldots \equiv C_{\lambda-1} \pmod{p},$$

unde sequitur ut productum $\psi(\alpha)\,F(\alpha)$ per p divisibile sit ; itaque ponere licet

$$\psi(\alpha).F(\alpha) = p\,\varphi(\alpha),$$

et quum sit $p = f(\alpha)F(\alpha)$, factore communi $F(\alpha)$ sublato habemus

$$\psi(\alpha) = f(\alpha)\varphi(\alpha),$$

unde etiam

$$N\psi(\alpha) = N f(\alpha)\,N\varphi(\alpha),$$

et quia $N f(\alpha) = N\psi(\alpha) = p$, hoc factore omisso est

$$N\varphi(\alpha) = 1;$$

ergo $\varphi(\alpha)$ est unitas complexa, atque habemus theorema : *Omnes numeri complexi ejusdem normæ, quæ numerus primus est, non inter se differunt nisi unitatibus complexis, quibus multiplicatæ esse possunt.* Ad diversitatem numerorum conjunctorum, quæ obvia est, hic non respicimus. Idem theorema etiam hoc modo enuntiari potest : *Si numerus primus realis aliquo modo in* $\lambda - 1$ *factores complexos dissolvi potest, idem semper infinitis aliis modis tanquam productum* $\lambda - 1$ *factorum complexorum repræsentari potest, qui vero e factoribus unius repræsentationis unitatum complexarum ope, omnes eruuntur.*

§ VII.

Facile inveniuntur numeri complexi, quorum normæ factorem p, numerum primum formæ $m\lambda + 1$, implicant. Nam *si* ξ *est radix aliqua congruentiæ*

$$1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0 \pmod{p},$$

et si coefficientes numeri complexi

$$\psi(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1}$$

congruentiæ

$$a + a_1\xi + a_2\xi^2 + \ldots + a_{\lambda-1}\xi^{\lambda-1} \equiv 0$$

satisfaciunt, semper est

$$\mathrm{N}\psi(\alpha) \equiv 0 \pmod{p}.$$

Etenim, si ponimus

$$a_1(\xi - \alpha) + a_2(\xi^2 - \alpha^2) + a_3(\xi^3 - \alpha^3) + \ldots + a_{\lambda-1}(\xi^{\lambda-1} - \alpha^{\lambda-1}) = p\mathrm{P} - \psi(\alpha),$$

et si alteri parti hujus æquationis forma datur $(\xi - \alpha)\varphi(\alpha)$, est

$$\psi(\alpha) = p\mathrm{P} - (\xi - \alpha)\varphi(\alpha),$$

cujus numeri complexi normam factorem p habere patet siquidem, quod posuimus, norma numeri $\xi - \alpha$, i. e. $1 + \xi + \xi^2 + \ldots \xi^{\lambda-1}$, per p divisibilis est.

Hujus theorematis ope *omnes* numeros complexos inveniri, quorum normæ factorem p habeant, inde apparet, quod theorema inversum etiam valet, scilicet : *Si norma numeri complexi*

$$\psi(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1},$$

factorem p implicat, semper datur radix aliqua ξ *congruentiæ*

$$1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0 \pmod{p},$$

quæ numerum

$$\psi(\xi) = a + a_1\xi + a_2\xi^2 + \ldots + a_{\lambda-1}\xi^{\lambda-1}$$

per p divisibilem reddat. Consideremus hanc functionem rationalem integram variabilis x :

$$\psi(x)\,\psi(x^2)\,\psi(x^3)\ldots\psi(x^{\lambda-1}) - \mathrm{N}\psi(\alpha),$$

quæ quum manifesto evanescat pro

$$x = \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{\lambda-1},$$

factorem $1 + x + x^2 + \ldots + x^{\lambda-1}$ habere debet, eamque ob causam, si x radici alicui congruentiæ

$$1 + x + x^2 + \ldots + x^{\lambda-1} \equiv 0 \pmod{p}$$

æqualis ponitur, per p divisibilis est ; inde si hujus congruentiæ radicem aliquam, uti supra fecimus, littera ξ denotamus, semper unus factorum producti $\psi(\xi)\psi(\xi^2)\psi(\xi^3)\dots\psi(\xi^{\lambda-1})$ per p divisibilis esse debet. Præterea, quia omnes radices illius congruentiæ unius radicis ξ potestates sunt, sponte apparet pro alia radice ξ alium etiam factorem hujus producti per p divisibilem fieri, itaque pro quolibet factore certa quædam radix ξ exstare debet, qua substituta nihilo congruus reddatur.

§ VIII.

Postquam demonstravimus quo modo infinitus numerus complexorum numerorum omnium inveniatur, quorum normæ factorem p habeant, quærendum nobis videtur an semper inter hos numeros complexos exstent quarum norma sit ipse numerus p, sive, quod idem est, an quilibet numerus primus p formæ $m\lambda + 1$ in $\lambda - 1$ factores primos conjunctos diffindi possit. Ad hunc finem ponamus esse

$$p = f(\alpha) f(\alpha^2) f(\alpha^3) \dots f(\alpha^{\lambda-1}),$$

et videamus quæ inde pro numero p sequantur. Hujus producti factores secundum radices unitatis α, α^2, α^3, ..., $\alpha^{\lambda-1}$, quas continent in periodos dividamus. Productum factorum eorum qui ad eamdem periodum pertinent, ex notis Cl. Gaussii theorematis, erit functio rationalis integra linearis omnium periodorum similium. Jam si $\lambda - 1$ factoribus e et f constat, et e periodi f terminorum accipiuntur, quas Gaussii signis designamus $(f, 1)$, (f, g), (f, g^2), ..., (f, g^{e-1}), productum eorum factorum, qui eamdem periodum constituunt hanc formam habet

$$b + b_1 (f, 1) + b_2 (f, g) + \dots + b_e (f, g^{e-1}),$$

et simili modo producta factorum qui cæteras periodos conficiunt

$$b + b_1 (f, g) + b_2 (f, g^2) + \dots + b_e (f, 1),$$
$$b + b_1 (f, g^2) + b_2 (f, g^3) + \dots + b_e (f, g),$$
$$\text{etc.} \qquad\qquad \text{etc.};$$

quarum omnium productum quum sit functio invariabilis (symetrica) omnium periodorum, ab iis periodis liberum est, et formam certam gradus e et $e + 1$ indeterminatorum b, b_1, b_2, ..., b_e efficit, qui facile ad e indeterminatos numeros reducuntur. Igitur si e, e', e'', ... sunt divisores numeri $\lambda - 1$, numerus p repræsentari debet per formam certam gradus e et e indeterminatorum, idemque per formam gradus e' et e' indeterminatorum, etc. Hoc autem pro certis numeris p et λ fieri non posse facillime intelligitur ex forma secundi gradus et duorum indeterminatorum, quam p habere debet, si in $\lambda - 1$ factores primos complexos diffindi potest ; duæ enim periodi, quarum altera ad residua quadratica, altera ad non residua pertinet, valores habent $\frac{-1 + \sqrt{\pm\lambda}}{2}$ et $\frac{-1 - \sqrt{\pm\lambda}}{2}$, inde productum ex altera semissi factorum complexorum numeri p

compositum hanc formam habebit $\frac{a \pm b\sqrt{\pm\lambda}}{2}$, et ipse numerus p habebit formam $p = \frac{a^2 \mp \lambda b^2}{4}$, seu $4p = a^2 \mp \lambda b^2$, quam numeri formæ $m\lambda + 1$ non semper patiuntur, siquidem præter formam principalem aliæ quoque formæ non æquivalentes secundi gradus, determinantis $\mp\lambda$, locum habent. Simili modo etiam altiorum graduum formæ impedimento esse possunt, quominus numerus p in $\lambda - 1$ factores primos complexos dissolvi queat.

Quia numeri primi reales formæ $m\lambda + 1$ non semper tanquam producta $\lambda - 1$ factorum complexorum repræsentari possunt, multis etiam numerorum integrorum realium proprietatibus simplicibus numeri complexi carent. Pro iis generaliter non valet propositio fundamentalis ut quilibet numerus sit productum factorum complexorum simplicium, qui neglectis unitatibus complexis semper iidem sint, re enim vera nonnunquam idem numerus compositus pluribus modis diversis in factores simplices complexos diffindi potest. Eadem res etiam hoc modo enuntiari potest : Si numerus complexus per alium numerum complexum ita dividi potest, ut quotiens sit integer complexus, factores simplices divisoris non ubique cum factoribus simplicibus dividendi compensari possunt. Quod ut demonstremus denuo numerum ξ cognitæ illius congruentiæ radicem in auxilium vocamus, quæ hoc modo in factores dissolvitur :

$$(\xi - \alpha)(\xi - \alpha^2)\dots(\xi - \alpha^{\lambda-1}) \equiv 0 \pmod{p}.$$

Jam si factores divisoris p cum factoribus dividendi tollerentur, p cum aliquo factorum $\xi - \alpha$, $\xi - \alpha^2$, etc., factorem communem haberet, ideoque etiam cum singulo quoque. Sit $f(\alpha)$ hic factor communis numerorum p et $\xi - \alpha$, $f(\alpha^2)$ erit factor communis numerorum p et $\xi - \alpha^2$, et ita porro ; omnes igitur numeri complexi conjuncti $f(\alpha), f(\alpha^2)\dots f(\alpha^{\lambda-1})$, factores essent numeri p, omnesque inter se diversi, quia $\xi - \alpha$, $\xi - \alpha^2$, etc., non possunt factores communes habere nisi eos quorum norma sit 1 vel λ, scilicet $\alpha - \alpha^2$, $\alpha - \alpha^3$, etc. Inde sequeretur ut quilibet numerus primus $p = m\lambda + 1$ esset productum $\lambda - 1$ factorum complexorum conjunctorum, quod in universum non pro omnibus valoribus numerorum p et λ valere supra demonstravimus. Maxime dolendum videtur, quod hæc numerorum realium virtus, ut in factores primos dissolvi possint, qui pro eodem numero semper iidem sint, non eadem est numerorum complexorum, quæ si esset, tota hæc doctrina, quæ magnis adhuc difficultatibus laborat, facile absolvi et ad finem perduci posset. Eam ipsam ob causam numeri complexi, quos hic tractamus, imperfecti esse videntur, et dubium inde oriri posset, utrum hi numeri complexis ceteris qui fingi possint præferendi, an alii quærendi essent, qui in hac re fundamentali analogiam cum numeris integris realibus servarent. Attamen hi numeri complexi, qui unitatis radicibus et numeris integris realibus componuntur, non ex arbitrio facti sunt, sed ex ipsa doctrina numerorum procreati, atque ipsorum ea ratio est, ut in doctrina sectionis circuli et residuorum potestatum altiorum ulterius promovenda iis carere nullo modo possimus.

§ IX.

Quum numerorum primorum formæ $m\lambda + 1$ alii in $\lambda - 1$ factores complexos discerpi possint, alii non possint, e re est ut inveniatur qui et quales sint ii numeri λ et p, pro quibus talis repræsentatio locum habet, atque ut pro iis qui minorem tantum numerum factorum primorum habent, horum factorum numerus et forma propria indagetur, quod vero problema ulterioribus virorum doctorum perscrutationibus relinquendum est. Ipse ut hanc rem accuratius cognoscerem, et ut exemplis docerer, omnium numerorum primorum infra mille, qui formas habent

$$5m+1,\ 7m+1,\ 11m+1,\ 13m+1,\ 17m+1,\ 19m+1 \text{ et } 23m+1$$

factores primos computavi, et methodos quibus usus sum, et ipsos factores primos computatos hoc loco in publicum edam.

Altera methodus factore communi duorum numerorum complexorum inveniendo nititur, quod problema simili modo solvendum est atque pro numeris integris realibus. Si $\varphi(\alpha)$ et $f(\alpha)$ sunt numeri complexi quorum factor communis maximus investigandus est, et $\mathrm{N}\varphi(\alpha) > \mathrm{N}f(\alpha)$, a numero fracto $\frac{\varphi(\alpha)}{f(\alpha)}$ numerum certum integrum subtraho $\psi(\alpha)$, quem siquidem fieri potest ita eligo, ut norma residui sit minor unitate, sive

$$\mathrm{N}\left(\frac{\varphi(\alpha)}{f(\alpha)} - \psi(\alpha)\right) < 1.$$

Ut hoc efficiatur, evolvo productum

$$\mathrm{F}(\alpha) = f(\alpha^2) f(\alpha^3) \ldots f(\alpha^{\lambda-1}),$$

ejusque auxilio etiam productum

$$\varphi(\alpha)\,\mathrm{F}(\alpha) = \mathrm{C} + \mathrm{C}_1\alpha + \mathrm{C}_2\alpha^2 + \ldots + \mathrm{C}_{\lambda-1}\alpha^{\lambda-1};$$

porro accipio

$$\psi(\alpha) = c + c_1\alpha + c_2\alpha^2 + \ldots + c_{\lambda-1}\alpha^{\lambda-1},$$

et simpliciter scribo n, loco $\mathrm{N}f(\alpha)$. Inde erit

$$\frac{\varphi(\alpha)}{f(\alpha)} - \psi(\alpha) = \frac{\varphi(\alpha)\,\mathrm{F}(\alpha)}{n} - \psi(\alpha),$$

et posito

$$\frac{\varphi(\alpha)\,\mathrm{F}(\alpha)}{n} - \psi(\alpha) = k + k_1\alpha + k_2\alpha^2 + \ldots + k_{\lambda-1}\alpha^{\lambda-1},$$

erit

$$k = \frac{\mathrm{C}}{n} - c, \quad k_1 = \frac{\mathrm{C}_1}{n} - c_1, \quad k_2 = \frac{\mathrm{C}_2}{n} - c_2, \quad \text{etc.}$$

Jam numeros c, c_1, c_2, etc., ita eligo ut integri maximi sint, qui singulis fractionibus

$\frac{C}{n}, \frac{C_1}{n}, \frac{C_2}{n}$, etc., contineantur, quo facto numeri k, k_1, k_2, etc., omnes erunt positivi et minores unitate. Certo talis numeri complexi $k + k_1\alpha + k_2\alpha^2 + \ldots + k_{\lambda-1}\alpha^{\lambda-1}$, norma parva erit; sed semper eam unitate minorem fore nondum liquet, neque etiam semper res ita se habet. Hoc autem loco nobis notandum est numeros k, k_1, k_2, etc., iis conditionibus quas posuimus nondum plane determinatos esse, omnibus enim coefficientibus C, C_1, C_2, etc., eodem numero auctis, $\varphi(\alpha).F(\alpha)$ non mutatur, sed numeri integri maximi, qui fractionibus $\frac{C}{n}, \frac{C_1}{n}, \frac{C_2}{n}$, etc., insunt, revera mutari possunt. Nam si numeros C, C_1, C_2, etc., omnes æqualiter crescentes accipimus, numeri k, k_1, k_2, etc., omnes eodem modo crescent, usque dum maximus eorum unitatem superaverit, quo facto unitate minuendus est, et subito omnium minimus fit. Eadem mutatione repetita patet in universum obtineri λ numeros complexos $k + k_1\alpha + k_2\alpha^2 + \ldots + k_{\lambda-1}\alpha^{\lambda-1}$, quorum normæ diversæ sint. Jam si vel omnium harum normarum nulla unitate minor existet, methodus nostra nos deficit, hunc autem defectum non methodo vicio dandum, sed rei ipsius natura necessarium esse, infra demonstrabitur. Si vero, quod fere semper evenire solet, talis norma unitate minor fit, habemus

$$\mathrm{N}\left[\frac{\varphi(\alpha)}{f(\alpha)} - \psi(\alpha)\right] < 1, \quad \text{ideoque} \quad \mathrm{N}[\varphi(\alpha) - f(\alpha)\,\psi(\alpha)] < \mathrm{N}f(\alpha).$$

Posito $\varphi(\alpha) - f(\alpha)\,\psi(\alpha) = \mathrm{R}(\alpha)$, patet factorem maximum communem numerorum $\varphi(\alpha)$ et $f(\alpha)$ eumdem esse numerorum $f(\alpha)$ et $\mathrm{R}(\alpha)$; unde indagatio factoris communis eo reducta est, ut aliorum duorum numerorum, quorum normæ minores sunt, factor communis quærendus sit. Itaque, hac methodo repetita, nisi forte casus ille adversus evenit, quem supra commemoravimus, tandem ad duos numeros pervenimus, quorum alter factor alterius, ideoque hic ipse factor communis est quem quærimus; cujus norma si unitas est, numeri illi sunt inter se primi.

Facile hæc methodus ad factores primos numeri $p = m\lambda + 1$ indagandos applicari potest, siquidem p revera est productum $\lambda - 1$ factorum conjunctorum. Quem ad finem quæratur radix aliqua ξ congruentiæ

$$1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0 \pmod{p},$$

quæ si p in $\lambda - 1$ factores conjunctos diffindi potest, semper talis est, ut $\xi - \alpha$ et p factorem complexum communem habeant. Hic igitur, secundum methodum traditam inventus, erit factor simplex complexus numeri p. Supra vidimus pro certis numeris p et λ talem factorem communem numerorum $\xi - \alpha$ et p non adesse, quamvis norma numeri $\xi - \alpha$ per p divisibilis sit; porro si per methodum traditam numeri complexi normarum minorum quæruntur, patet eorum omnium normas per p divisibiles esse, quam ob rem nullo modo ad normam unitatem pervenire possumus; semper igitur factor communis ab unitate diversus inveniretur, etiam ubi talem factorem non adesse demonstravimus, nisi in omnibus iis calculis eveniret ut norma istius nu-

meri complexi fracti $k + k_1\alpha + k_2\alpha^2 + \ldots + k_{\lambda-1}\alpha^{\lambda-1}$ minor unitate fieri non posset, qua conditione methodus nostra ad finem propositum perducere non potest.

Altera methodus minus quidem directa tamen multo faciliori negotio factores primos complexos numeri $p = m\lambda + 1$ præbet. In hac omnes congruentiæ

$$1 + \xi + \xi^2 + \ldots + \xi^{\lambda-1} \equiv 0 \pmod{p},$$

radices ξ, ξ^2, ξ^3, etc., in usum vocamus, quibus e canone arithmetico a Cl. Jacobi edito depromptis, sive alio modo inventis, solutiones congruentiæ

$$a + a_1\xi + a_2\xi^2 + \ldots + a_{\lambda-1}\xi^{\lambda-1} \equiv 0 \pmod{p}$$

quærimus, ex quovis systemate numerorum a, a_1, a_2, ..., $a_{\lambda-1}$, qui huic congruentiæ satisfaciunt numerum complexum $f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1}$ componimus, et ex omnibus iis numeris, quarum normæ per theorema supra demonstratum, § VII, factorem p habent, eam eligimus quæ simplicissima sit, et normam quam minimam habere videatur, quæ jam ipsa computanda est, ut appareat utrum revera ipsi numero p an multiplo ejus æquælis sit. Si eveniret hanc normam non esse ipsum p, sed ejus multiplum e numeris complexis quarum normæ per p divisibiles sunt alius quærendus et examinandus esset, et ita porro. Si vero horum numerorum complexorum nullus ipsam normam p habet, hic numerus primus p iis adnumerandus est, qui $\lambda - 1$ factoribus complexis conjunctis non sunt compositi.

§ X.

Antequam ipsos numerorum primorum realium factores primos complexos quos invenimus litteris consignamus pauca de iis præmittere convenit. Pro $\lambda = 5, 7, 11, 13, 17$ et 19, omnes numeros primos formæ $m\lambda + 1$ in primo mille contentos in $\lambda - 1$ factores dissolvimus: primus numerus λ, pro quo hoc genus factorum primorum non semper datur, est numerus $\lambda = 23$; inter octo enim numeros primos formæ $23m + 1$, qui minores sunt quàm mille, tres sunt qui viginti duobus factoribus primis constant, reliquos autem quinque, qui quum formam quadraticam $4p = a^2 + 23b^2$ non patiantur, in viginti duo factores conjunctos dissolvi non possunt, in undecim factores primos complexos discerpere nobis contigit. Tales numeri eumdem characterem habere videntur ac numeri primi qui non sunt formæ $m\lambda + 1$, quos de hac nostra commentatione exclusimus, hi omnes habent minorem numerum factorum complexorum primorum, qui non tam radicum singularum æquationis $\alpha = 1$ quam periodorum functiones lineares sunt. Simili enim modo horum quinque numerorum primorum factores primi complexi, quos invenimus, periodos binarum radicum continent. Quibus præmissis ipsos factores inventos tradimus.

(1) Si $\lambda = 5$, et α radix æquationis $\alpha^5 = 1$.

$11 = N(2+\alpha)$
$31 = N(2-\alpha)$
$41 = N(3+2\alpha+\alpha^2)$
$61 = N(3+\alpha)$
$71 = N(3-\alpha+\alpha^2)$
$101 = N(3+\alpha-\alpha^2)$
$131 = N(3+\alpha-\alpha^4)$
$151 = N(3+2\alpha-\alpha^4)$
$181 = N(4+3\alpha)$
$191 = N(4+\alpha+2\alpha^2)$
$211 = N(3-2\alpha)$
$241 = N(4-\alpha+\alpha^2)$
$251 = N(5+2\alpha+\alpha^4)$
$271 = N(3-3\alpha+\alpha^2)$
$281 = N(4+\alpha-\alpha^2)$
$311 = N(3+2\alpha+2\alpha^2+\alpha^4)$
$331 = N(4-2\alpha+\alpha^2)$
$401 = N(4+3\alpha-\alpha^4)$
$421 = N(5+2\alpha+2\alpha^2)$
$431 = N(4-2\alpha-\alpha^4)$
$461 = N(4-\alpha-\alpha^2)$
$491 = N(5+3\alpha+\alpha^3)$
$521 = N(5+\alpha)$
$541 = N(3-3\alpha-\alpha^2)$
$571 = N(6+5\alpha+3\alpha^2)$
$601 = N(5+2\alpha-\alpha^2)$
$631 = N(4-2\alpha-\alpha^3)$
$641 = N(5+3\alpha+4\alpha^2)$
$661 = N(5+\alpha-\alpha^2+3\alpha^3)$
$691 = N(3-3\alpha-2\alpha^2)$
$701 = N(4-\alpha-2\alpha^2+\alpha^3)$
$751 = N(6+4\alpha+3\alpha^2)$
$761 = N(5-2\alpha+\alpha^2)$
$811 = N(3-3\alpha-2\alpha^2+\alpha^3)$
$821 = N(4-\alpha-2\alpha^2+2\alpha^3)$
$881 = N(6+2\alpha+\alpha^2)$
$911 = N(5+\alpha^2-2\alpha^4)$
$941 = N(4+3\alpha-3\alpha^2-\alpha^3)$
$971 = N(5-2\alpha-\alpha^4)$
$991 = N(6+\alpha+\alpha^3)$

(2) Si $\lambda = 7$, et α est radix æquationis $\alpha^7 = 1$.

$29 = N(1+\alpha-\alpha^2)$
$43 = N(2+\alpha)$
$71 = N(2+\alpha+\alpha^3)$
$113 = N(2-\alpha+\alpha^5)$
$127 = N(2-\alpha)$
$197 = N(3+\alpha+\alpha^5+\alpha^6)$
$211 = N(3+\alpha+2\alpha^2)$
$239 = N(3+2\alpha+2\alpha^2+\alpha^3)$
$281 = N(2-\alpha-2\alpha^3)$
$337 = N(2+\alpha-\alpha^2-\alpha^4)$
$379 = N(3+2\alpha+\alpha^2)$
$421 = N(3+\alpha+\alpha^2)$
$449 = N(2+\alpha-\alpha^3-\alpha^6)$
$463 = N(3+2\alpha)$
$491 = N(3+\alpha+\alpha^3-\alpha^5)$
$547 = N(3+\alpha)$
$617 = N(2+\alpha+\alpha^2-\alpha^5)$
$631 = N(2+2\alpha-\alpha^2+\alpha^3+\alpha^6)$

$659 = N(2 + 2\alpha - \alpha^2 + \alpha^5)$
$673 = N(4 + 3\alpha + 2\alpha^2 + \alpha^4 + 2\alpha^6)$
$701 = N(3 + \alpha + \alpha^4 - \alpha^5 + \alpha^6)$
$743 = N(3 + 2\alpha - \alpha^3 - \alpha^4)$
$757 = N(3 + 2\alpha + \alpha^3)$
$827 = N(2 + 2\alpha - \alpha^4 - \alpha^6)$
$883 = N(2 - \alpha^2 - 2\alpha^3 - \alpha^5)$
$911 = N(3 + 2\alpha - \alpha^3 + \alpha^4)$
$953 = N(3 + \alpha - \alpha^2 - \alpha^3)$
$967 = N(2 + 2\alpha - \alpha^3 + 2\alpha^5)$

(3) Si $\lambda = 11$, et α est radix æquationis $\alpha^{11} = 1$.

$23 = N(1 + \alpha + \alpha^9)$
$67 = N(1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5)$
$89 = N(1 + \alpha + \alpha^4 + \alpha^6)$
$199 = N(1 + \alpha - \alpha^2)$
$331 = N(1 - \alpha + \alpha^3 + \alpha^5)$
$353 = N(1 + \alpha + \alpha^3 + \alpha^4 - \alpha^7)$
$397 = N(1 + \alpha + \alpha^6 - \alpha^7)$
$419 = N(1 + \alpha - \alpha^2 + \alpha^3)$
$463 = N(1 - \alpha - \alpha^2 + \alpha^5 + \alpha^6)$
$617 = N(2 + \alpha + \alpha^3 + \alpha^{10})$
$661 = N(1 + \alpha - \alpha^2 + \alpha^4 - \alpha^5)$
$683 = N(2 + \alpha)$
$727 = N(1 + \alpha + \alpha^3 - \alpha^5 - \alpha^9)$
$859 = N(1 + \alpha + \alpha^2 + \alpha^3 + \alpha^7 - \alpha^8)$
$881 = N(1 + \alpha + \alpha^2 + \alpha^3 - \alpha^4 - \alpha^7 - \alpha^9)$
$947 = N(2 + \alpha^3 - \alpha^4 - \alpha^6)$
$991 = N(2 + \alpha + \alpha^3)$

(4) Si $\lambda = 13$, et α est radix æquationis $\alpha^{13} = 1$.

$53 = N(1 + \alpha + \alpha^3)$
$79 = N(1 - \alpha + \alpha^{10})$
$131 = N(1 - \alpha + \alpha^{11})$
$157 = N(1 + \alpha + \alpha^2 + \alpha^5)$
$313 = N(1 - \alpha + \alpha^3 + \alpha^6)$
$443 = N(1 + \alpha - \alpha^3 + \alpha^8)$
$521 = N(1 + \alpha - \alpha^{12})$
$547 = N(1 - \alpha - \alpha^2 + \alpha^3 + \alpha^4)$
$599 = N(1 + \alpha - \alpha^2 + \alpha^5 + \alpha^{11})$
$677 = N(1 - \alpha - \alpha^4 + \alpha^6 + \alpha^9)$
$959 = N(1 + \alpha - \alpha^2 - \alpha^5 + \alpha^7)$
$911 = N(1 + \alpha^3 + \alpha^5 - \alpha^7 - \alpha^{11})$
$937 = N(1 + \alpha^3 - \alpha^7 + \alpha^8 - \alpha^{10})$

(5) Si $\lambda = 17$, et α est radix æquationis $\alpha^{17} = 1$.

$103 = N(1 + \alpha^2 + \alpha^9)$
$137 = N(1 + \alpha - \alpha^3)$
$239 = N(1 + \alpha + \alpha^3)$
$307 = N(1 - \alpha + \alpha^7)$
$409 = N(1 - \alpha^3 + \alpha^8)$
$443 = N(1 + \alpha + \alpha^2 + \alpha^3 - \alpha^{15})$
$613 = N(1 + \alpha^2 - \alpha^3)$
$647 = N(1 + \alpha + \alpha^{13} + \alpha^{15})$
$919 = N(1 + \alpha + \alpha^3 + \alpha^5 + \alpha^6)$
$953 = N(1 + \alpha + \alpha^6 - \alpha^{13})$

(6) Si $\lambda = 19$, et α est radix æquationis $\alpha^{19} = 1$.

$$191 = N(1 + \alpha + \alpha^{16}) \qquad 457 = N(1 + \alpha + \alpha^{9})$$
$$229 = N(1 - \alpha - \alpha^{5}) \qquad 571 = N(1 + \alpha + \alpha^{2} + \alpha^{7} - \alpha^{5})$$
$$419 = N(1 - \alpha - \alpha^{7}) \qquad 647 = N(1 - \alpha^{2} + \alpha^{9})$$
$$761 = N(1 - \alpha^{2} + \alpha^{12})$$

(7) Si $\lambda = 23$, et α est radix æquationis $\alpha^{23} = 1$.

$$599 = N(1 + \alpha^{15} - \alpha^{16}) \qquad 691 = N(1 + \alpha + \alpha^{5})$$
$$829 = N(1 + \alpha^{11} + \alpha^{20})$$

Reliqui numeri primi formæ $23m + 1$ infra mille undecim factoribus primis constant, habet

$$47 \text{ factorem } \alpha^{10} + \alpha^{13} + \alpha^{8} + \alpha^{15} + \alpha^{7} + \alpha^{16}$$
$$139 \quad » \quad \alpha^{10} + \alpha^{13} + \alpha^{8} + \alpha^{15} + \alpha^{4} + \alpha^{19}$$
$$277 \quad » \quad 2 + \alpha + \alpha^{22} + \alpha^{7} + \alpha^{15}$$
$$461 \quad » \quad \alpha + \alpha^{22} + \alpha^{10} + \alpha^{12} + \alpha^{8} + \alpha^{15} + \alpha^{3} + \alpha^{11}$$
$$967 \quad » \quad 2 + \alpha^{11} + \alpha^{12} + \alpha^{5} + \alpha^{17}.$$

§ XI.

Quæ de numeris complexis et de eorum factoribus primis commentati sumus ad doctrinam de sectione circuli felicissimo successu applicari possunt. In hac enim doctrina tales numeri complexi eorumque producta maximi momenti sunt, quorum vera indoles in luce clarissima ponitur si in factores primos diffinduntur.

Sit p numerus primus realis formæ $m\lambda + 1$, α radix imaginaria æquationis $\alpha^{\lambda} = 1$, g radix primitiva numeri primi p, et

$$(\alpha, x) = x + \alpha x^{g} + \alpha^{2} x^{g^{2}} + \ldots + \alpha^{p-2} x^{g^{p-2}}.$$

Totius fere doctrinæ de circuli sectione caput est formæ hujus (α, x) potestas exponentis λ, quæ a radice x non pendet, sed radicis α functio rationalis integra est, ideoque numerus complexus ejus generis quod supra tractavimus. Ipsa hæc formula (α, x), quam Cl. Lagrange primus adhibuit, proprietatibus insignibus gaudet, quarum maximas Cl. Jacobi primus invenit

$$(\alpha, x)(\alpha^{-1}, x) = p,$$

$$\frac{(\alpha^{m}, x)(\alpha^{n}, x)}{(\alpha^{m+n}, x)} = \psi(\alpha) = A + A_{1}\alpha + A_{2}\alpha^{2} + \ldots + A_{\lambda-1}\alpha^{\lambda-1},$$

numerus complexus $\psi(\alpha)$ ita semper comparatus est, ut sit

$$\psi(\alpha)\,\psi(\alpha^{-1}) = p.$$

Inde positis

$$\begin{aligned}
(\alpha,x)\ (\alpha,\ x) &= \psi_1(\alpha)\ (\alpha^2,x),\\
(\alpha,x)\ (\alpha^2,x) &= \psi_2(\alpha)\ (\alpha^3,x),\\
(\alpha,x)\ (\alpha^3,x) &= \psi_3(\alpha)\ (\alpha^4,x),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
(\alpha,x)\ (\alpha^{\lambda-2},\ x) &= \psi_{\lambda-2}(\alpha)\ (\alpha^{\lambda-1},\ x),
\end{aligned}$$

iisque æquationibus inter se multiplicatis, adhibita formula

$$(\alpha,\ x)\,(\alpha^{-1},\ x) = p,$$

fit

$$(\alpha,\ x)^{\lambda} = p\cdot\psi_1(\alpha)\,\psi_2(\alpha)\cdots\psi_{\lambda-1}(\alpha).$$

Numeri integri complexi, quibus hoc productum constat, $\psi_1(\alpha)$, $\psi_2(\alpha)$, etc., a se invicem ita pendent, ut quamvis non singuli, tamen productum omnium per unum eorum exprimi possit. Tali autem reductione non indigemus, si pro numeris complexis p, $\psi_1(\alpha)$, $\psi_2(\alpha)$, etc., qui compositi sunt, eorum factores primos adhibemus, quo facto repræsentatio formæ $(\alpha,\ x)^{\lambda}$ solos factores primos conjunctos numeri p continebit. Disquisitionem nostram ad tales numeros primos p restringentes, qui in $\lambda-1$ factores complexos conjunctos diffindi possunt, habemus

$$p = f(\alpha)\,f(\alpha^2)\,f(\alpha^3)\cdots f(\alpha^{\lambda-1}):$$

etiam numeri complexi $\psi_1(\alpha)$, $\psi_2(\alpha)$, etc., alios factores primos habere non possunt nisi eos qui in p reperiuntur; est enim, pro quolibet numero r, $\psi_r(\alpha)\,\psi_r(\alpha^{-1}) = p$, et supra, § VI, demonstravimus numerum p, neglectis unitatibus complexis, quibus factores affecti esse possunt, pluribus modis diversis in $\lambda-1$ factores primos dissolvi non posse. Quilibet igitur numerorum $\psi_r(\alpha)$ est productum alterius semissis factorum $f(\alpha)$, $f(\alpha^2)$, etc., et unitas complexa, quæ factor accedere potest, si per $\varphi(\alpha)$ designatur, conditioni $\varphi(\alpha)\,\varphi(\alpha^{-1}) = 1$ satisfacere, ideoque secundum ea quæ § IV invenimus, simplex unitas $\pm\alpha^{\varkappa}$ esse debet. Inde loco factorum compositorum factoribus simplicibus substitutis, hanc formam habemus:

$$(\alpha,x)^{\lambda} = \pm\alpha^{\varkappa} f^{m_1}(\alpha)\,f^{m_2}(\alpha^2)\,f^{m_3}(\alpha^3)\cdots f^{m_{\lambda-1}}(\alpha^{\lambda-1}),$$

in qua m_1, m_2, m_3, etc., sunt exponentes integri positivi, quos jam determinaturi sumus. Primum adhibita formula simplici

$$(\alpha,x)\,(\alpha^{-1},x) = p = f(\alpha)\,f(\alpha^2)\,f(\alpha^3)\cdots f(\alpha^{\lambda-1}),$$

sponte elucet esse

$$m_1 + m_{\lambda-1} = \lambda,\quad m_2 + m_{\lambda-2} = \lambda,\quad \text{etc.},$$

i. e. summam binorum exponentium, ab initio et a fine æque distantium, constantem esse et numero λ æqualem ; unde sequitur ut omnes hi exponentes numero λ minores sint. Deinde per formulam generaliorem

$$\frac{(\alpha, x)\,(\alpha^r, x)}{(\alpha^{r+1}, x)} = \psi_r(\alpha),$$

fit

$$\frac{f^{m_1}(\alpha)\,f^{m_2}(\alpha^2)\ldots f^{m_{\lambda-1}}(\alpha^{\lambda-1})\,.\,f^{m_1}(\alpha^r)\,f^{m_2}(\alpha^{2r})\ldots f^{m_{\lambda-1}}(\alpha^{r\lambda-r})}{f^{m_1}(\alpha^{r+1})\,f^{m_2}(\alpha^{2r+2})\ldots f^{m_{\lambda-1}}\left(\alpha^{(\lambda-1)(r+1)}\right)} = [\psi_r(\alpha)]^{\wedge},$$

et quia quotiens talium numerorum complexorum, quorum norma est numerus primus, non potest integer esse, nisi singuli factores denominatoris cum factoribus numeratoris compensantur, et quia hic quotiens potestati $\lambda^{\text{tæ}}$ numeri complexi æqualis est, singulis tribus potestatibus numeri primi $f(\alpha^k)$ in unam conjunctis, facile colligitur pro quolibet numero k esse debere

$$m_k + m_\mu - m_\nu \equiv 0, \quad \text{si } \mu \equiv \frac{k}{r}, \quad \nu \equiv \frac{k}{r+1} \pmod{\lambda};$$

inde, posito

$$km_k \equiv n_k, \quad \text{sive } m_k \equiv \frac{n_k}{k} \pmod{\lambda},$$

fit

$$m_\mu \equiv \frac{n_\mu}{\mu} \equiv \frac{rn_\mu}{k} \quad \text{et } m_\nu \equiv \frac{n_\nu}{\nu} \equiv \frac{(r+1)\,n_\nu}{k} \pmod{\lambda},$$

iisque substitutis, congruentia

$$m_k + m_\mu - m_\nu \equiv 0$$

mutatur in

$$\frac{n_k}{k} + \frac{r.n_k}{k} - \frac{(r+1)\,n_\nu}{k} \equiv 0 \pmod{\lambda},$$

unde posito $k = 1$, habemus

$$n_1 + rm_\mu - (r+1)\,n_\nu \equiv 0, \quad \text{si } \mu \equiv \frac{1}{r} \quad \text{et } \nu \equiv \frac{1}{r+1} \pmod{\lambda}.$$

Jam si primum facimus $r = 1$, fit n_1 æquale numero n cujus index congruus est $\frac{1}{2}$; deinde, posito $r = 2$, idem æqualis invenitur numero n cujus index congruus est $\frac{1}{3}$: tum, posito $r = 3$, etiam n cujus index $\frac{1}{4}$ illis æqualis invenitur, et ita porro ; numeri autem fracti $\frac{1}{1}$, $\frac{1}{2}$, $\frac{1}{3}$, etc., omnibus numeris integris 1, 2, 3, etc., etsi alio ordine, congrui sunt, modulo λ ; itaque numeri n pro omnibus indicibus diversis iidem sunt et indices omitti possunt, quo facto habemus

$$m_k \equiv \frac{n}{k} \pmod{\lambda},$$

quæ determinatio revera congruentiæ

$$m + m_{\mu} - m_{\nu} \equiv 0,$$

pro quolibet valore numerorum k et r satisfacit. Inde habemus theorema insigne: *Si $f(\alpha)$ est factor primus complexus numeri p, cujus norma est ipse numerus p, est*

$$(C \qquad (\alpha, x)^{\lambda} = \pm \alpha^{x} f^{m_1}(\alpha) f^{m_2}(\alpha^2) f^{m_3}(\alpha^3) \dots f^{m_{\lambda-1}}(\alpha^{\lambda-1}),$$

et exponentes m_1, m_2, m_3, etc., ita determinantur ut sint numeri minimi positivi, qui per exponentes potestatum radicis α, ad quos pertinent, multiplicati omnes eidem numero congrui fiant pro modulo λ. Numerus primus complexus $f(\alpha)$, alia radice imaginaria æquationis $\alpha^{\lambda} = 1$ accepta, etiam signo $f(\alpha^r)$ designari potest, in quo r est numerus integer arbitrarius, quem si ita eligimus ut sit $nr \equiv 1 \pmod{\lambda}$ exponentes m_1, m_2, m_3, etc., non jam per congruentiam $m_k \equiv \frac{n}{k}$, sed per hanc simpliciorem $m_k \equiv \frac{1}{k} \pmod{\lambda}$ determinatur; præterea, quum omnes debeant esse minores quam λ, nihil amplius indeterminati relictum est nisi radix α, quæ ex omnibus æquationis $\alpha^{\lambda} = 1$ radicibus imaginariis eligenda sit, et unitas simplex $\pm \alpha^{x}$ qua hoc productum multiplicatum sit. Inde formæ (α, x) repræsentatio, quæ sectionis circuli caput est, pro omnibus iis numeris p, qui in $\lambda - 1$ factores complexos conjunctos diffindi possunt, ad simplicitatem maximam perducta est. Omnes enim difficultates et calculi longiores eo revocati sunt, ut numeri $p = m\lambda + 1$ factores primi complexi inveniantur, quod methodorum supra traditarum ope facile perficitur. Quum numerus $f(\alpha)$, cujus norma est p, siquidem revera talis numerus datur, non plane determinatus sit, sed semper infinite multis modis diversis exhiberi possit, dubium inde oriri posset, quisnam omnium horum numerorum accipiendus sit, nisi productum illud hac virtute gauderet, ut pro omnibus iis diversis numeris semper idem sit. Facile hoc theorematum paragraphi quartæ auxilio demonstratur; nam si $f(\alpha)$ est aliquis numerorum quorum norma est p, ceteros omnes demonstravimus hac forma contineri $f(\alpha)\varphi(\alpha)$, in qua $\varphi(\alpha)$ est unitas complexa: inde, si $f(\alpha)\varphi(\alpha)$ loco $f(\alpha)$ in formula (C) substituitur, accedit factor

$$\varphi^{m_1}(\alpha)\varphi^{m_2}(\alpha^2)\varphi^{m_3}(\alpha^3)\dots\varphi^{m_{\lambda-1}}(\alpha^{\lambda-1}) = \Phi(\alpha),$$

Hac unitate $\Phi(\alpha)$ cum reciproca $\Phi(\alpha^{-1})$ multiplicata, quia

$$m_1 + m_{\lambda-1} = \lambda, \quad m_2 + m_{\lambda-2} = \lambda, \quad \text{etc.},$$

fit

$$\Phi(\alpha)\Phi(\alpha^{-1}) = \left[\varphi(\alpha)\varphi(\alpha^2)\varphi(\alpha^3)\dots\varphi(\alpha^{\lambda-1})\right]^{\lambda} = 1;$$

unitas autem complexa, quæ per reciprocam suam multiplicata unitatem realem efficit, simplici unitati $\pm \alpha^{x}$ æqualis est; itaque quum sit $\Phi(\alpha) = \pm \alpha^{x}$ videmus solam mutationem levem quam, substitutis aliis numeris complexis $f(\alpha)$ æquationi $Nf(\alpha) = p$ sa-

tisfacientibus, formula (C) pati possit, eam esse, ut loco factoris α' alia quæcunque radix æquationis $\alpha^{\lambda} = 1$ substituenda sit.

Ut methodi in hac paragrapho explicatæ indolem veram melius cognoscamus, ad eam respiciamus qua Cl. Gauss usus est in sectione septima disquisitionum arithmeticarum, § CCCLVIII, ubi casum $\lambda = 3$ ingeniosissime pertractavit. Hic totam rem eo reduxit ut numerus $4p$ in formam $t^2 + 27u^2$ redigatur, et quum eo pervenisset, problema ab omni parte absolutum esse censuit. Simili modo secundum methodum nostram numerus p in formam certam gradus $\lambda - 1$, totidemque indeterminatorum redigi debet, quo facto difficultates omnes sublatæ sunt. Quum enim norma sit forma certa gradus $\lambda - 1$ et $\lambda - 1$ indeterminatorum, talem factorem primum complexum numeri p invenire idem est, atque hunc numerum in formam dictam redigere. Si omnes numeri primi p formæ $m\lambda + 1$ in hanc formam redigi possent, sive, quod idem est, si in $\lambda - 1$ factores complexos conjunctos discerpi possent, totius doctrinæ de circuli sectione pars major confecta esset; quum vero non omnes numeri p repræsentationem per formam illam patiantur, restat ut etiam pro iis forma propria expressionis $(\alpha, x)^{\lambda}$ inveniatur. Hæc autem res maximis difficultatibus obnoxia est, quæ ut superentur magno etiam virorum doctorum labore opus erit.