CARL FRIEDRICH GAUSS

WERKE

ERSTER BAND

HERAUSGEGEBEN
VON DER
KÖNIGLICHEN GESELLSCHAFT DER WISSENSCHAFTEN
ZU
GÖTTINGEN
1863.

CARL FRIEDRICH GAUSS WERKE

BAND I.

CARL FRIEDRICH GAUSS

WERKE

ERSTER BAND

HERAUSGEGEBEN
VON DER
KÖNIGLICHEN GESELLSCHAFT DER WISSENSCHAFTEN
ZU
GÖTTINGEN
1863.

DISQUISITIONES

ARITHMETICAE

AUCTORE

D. CAROLO FRIDERICO GAUSS.

LIPSIAE

IN COMMISSIS APUD GERH. FLEISCHER JUN.

1801.

SERENISSIMO

PRINCIPI AC DOMINO

CAROLO GUILIELMO FERDINANDO

BRUNOVICENSIUM AC LUNEBURGENSIUM DUCI.

PRINCEPS SERENISSIME

Summae equidem felicitati mihi duco, quod Celsissimo nomini Tuo hoc opus inscribere mihi permittis, quod ut Tibi offeram sancto pietatis officio obstringor. Nisi enim Tua gratia, Serenissime princeps, introitum mihi ad scientias primum aperuisset, nisi perpetua Tua beneficia studia mea usque sustentavissent, scientiae mathematicae, ad quam vehementi semper amore delatus sum, totum me devovere non potuissem. Quin adeo eas ipsas meditationes, quarum partem hoc volumen exhibet, ut suscipere, per plures annos continuare literisque consignare liceret, Tua sola benignitas effecit, quae ut, ceterarum curarum expers, huic imprimis incumbere possem praestitit. Quas quum tandem in lucem emittere cuperem, Tua munificentia cuncta, quae editionem remorabantur, obstacula removit. Haec Tua tanta de me meisque conatibus merita gratissima potius mente tacitaque admiratione

revolvere, quam iustis dignisque laudibus celebrare possum. Namque non solum tali me muneri haud parem sentio, sed et neminem ignorare puto, solennem Tibi esse tam insignem liberalitatem in omnes qui ad optimas disciplinas excolendas conferre videntur, neque eas scientias, quae vulgo abstrusiores et a vitae communis utilitate remotiores creduntur, a patrocinio Tuo exclusas esse, quum Tu ipse intimum scientiarum omnium inter se et necessarium vinculum mente illa sapientissima omniumque quae ad humanae societatis prosperitatem augendam pertinent peritissima, penitus perspexeris. Quodsi Tu, Princeps Serenissime, hunc librum, et gratissimi in Te animi et laborum nobilissimae scientiae dicatorum testem, insigni illo favore, quo me tamdiu amplexus es, haud indignum iudicaveris, operam meam me non inutiliter collocasse, eiusque honoris, quem prae omnibus in votis habui, compotem me factum esse, mihi gratulabor

PRINCEPS SERENISSIME

Brunovici mense Julio 1801.

Celsitudinis Tuae servus addictissimus

C. F. Gauss.

PRAEFATIO.

Disquisitiones in hoc opere contentae ad eam Matheseos partem pertinent, quae circa numeros integros versatur, fractis plerumque, surdis semper exclusis. Analysis indeterminata quam vocant seu Diophantaea, quae ex infinitis solutionibus problemati indeterminato satisfacientibus eas seligere docet, quae per numeros integros aut saltem rationales absolvuntur (plerumque ea quoque conditione adiecta ut sint positivi) non est illa disciplina ipsa, sed potius pars eius valde specialis, ad eamque ita fere se habet, ut ars aequationes reducendi et solvendi (Algebra) ad universam Analysin. Nimirum quemadmodum ad *Analyseos* ditionem referuntur omnes quae circa quantitatum affectiones generales institui possunt disquisitiones: ita numeri integri (fractique quatenus per integros determinantur) objectum proprium Arithmeticae constituunt. Sed quum ea, quae Arithmetices nomine vulgo traduntur, vix ultra artem numerandi et calculandi (i. e. numeros per signa idonea e. g. secundum systema decadicum exhibendi, operationesque arithmeticas perficiendi) extendantur, adiectis nonnullis quae vel ad Arithmeticam omnino non pertinent (ut doctrina de logarithmis) vel saltem numeris integris non sunt propria sed ad omnes quantitates patent: e re esse videtur, duas Arithmeticae partes distinguere, illaque ad Arithmeticam elementarem referre, omnes autem disquisitiones generales de numerorum integrorum affectionibus propriis *Arithmeticae Sublimiori*, de qua sola hic sermo erit, vindicare.

Pertinent ad Arithmeticam Sublimiorem ea, quae Euclides in Elementis L. VII sqq. elegantia et rigore apud veteres consuetis tradidit: attamen ad prima initia huius scientiae limitantur. Diophanti opus celebre, quod totum problematis

indeterminatis dicatum est, multas quaestiones continet, quae propter difficultatem suam artificiorumque subtilitatem de auctoris ingenio et acumine existimationem haud mediocrem suscitant, praesertim si subsidiorum quibus illi uti licuit tenuitatem consideres. At quum haec problemata dexteritatem quandam potius scitamque tractationem, quam principia profundiora postulent, praetereaque nimis specialia sint raroque ad conclusiones generaliores deducant: hic liber ideo magis epocham in historia Matheseos constituere videtur, quod prima artis characteristicae et Algebrae vestigia sistit, quam quod Arithmeticam Sublimiorem inventis novis auxerit. Longe plurima recentioribus debentur, inter quos pauci quidem sed immortalis gloriae viri P. DE FERMAT, L. EULER, L. LA GRANGE, A. M. LE GENDRE (ut paucos alios praetream) introitum ad penetralia huius divinae scientiae aperuerunt, quantisque divitiis abundent patefecerunt. Quaenam vero inventa a singulis his geometris profecta sint, hic enarrare supersedeo, quum e praefationibus Additamentorum quibus ill. La Grange Euleri Algebram ditavit operisque mox memorandi ab ill. Le Gendre nuper editi cognosci possint, insuperque pleraque locis suis in his Disquisitionibus Arithmeticis laudentur.

Propositum huius operis, ad quod edendum iam annos abhinc quinque publice fidem dederam, id fuit, ut disquisitiones ex Arithmetica Sublimiori, quas partim ante id tempus partim postea institui, divulgarem. Ne quis vero miretur, scientiam hic a primis propemodum initiis repetitam, multasque disquisitiones hic denuo resumtas esse, quibus alii operam suam iam navarunt, monendum esse duxi, me, quum primum initio a. 1795 huic disquisitionum generi animum applicavi, omnium quae quidem a recentioribus in hac arena elaborata fuerint ignarum, omniumque subsidiorum per quae de his quidpiam comperire potuissem expertem fuisse. Scilicet in alio forte labore tunc occupatus, casu incidi in eximiam quandam veritatem arithmeticam (fuit autem ni fallor theorema art. 108), quam quum et per se pulcherrimam aestimarem et cum maioribus connexam esse suspicarer, summa qua potui contentione in id incubui, ut principia quibus inniteretur perspicerem, demonstrationemque rigorosam nanciscerer. Quod postquam tandem ex voto successisset, illecebris harum quaestionum ita fui implicatus, ut eas deserere non potuerim; quo pacto, dum alia semper ad alia viam sternebant, ea quae in quatuor primis Sectionibus huius operis traduntur ad maximam partem absoluta erant, antequam de aliorum geometrarum laboribus similibus quidquam vi-

dissem. Dein copia mihi facta, horum summorum ingeniorum scripta evolvendi, maiorem quidem partem meditationum mearum rebus dudum transactis impensam esse agnovi: sed eo alacrior, illorum vestigiis insistens, Arithmeticam ulterius excolere studui; ita variae disquisitiones institutae sunt, quarum partem Sectiones V, VI et VII tradunt. Postquam interiecto tempore consilium de fructibus vigiliarum in publicum edendis cepi: eo lubentius, quod plures optabant, mihi persuaderi passus sum, ne quid vel ex illis investigationibus prioribus supprimerem, quod tum temporis liber non habebatur, ex quo aliorum geometrarum labores de his rebus, in Academiarum Commentariis sparsi, edisci potuissent; quod multae ex illis omnino novae et pleraeque per methodos novas tractatae erant; denique quod omnes tum inter se tum cum disquisitionibus posterioribus tam arcto nexu cohaerebant, ut ne nova quidem satis commode explicari possent, nisi reliquis ab initio repetitis.

Prodiit interea opus egregium viri iam antea de Arithmetica Sublimiori magnopere meriti, *Le Gendre Essai d'une théorie des nombres, Paris a. VI*, in quo non modo omnia quae hactenus in hac scientia elaborata sunt diligenter collegit et in ordinem redegit, sed permulta insuper nova de suo adiecit. Quum hic liber serius ad manum mihi pervenerit, postquam maxima operis pars typis iam exscripta esset; nullibi, ubi rerum analogia occasionem dare potuisset, eius mentionem inicere licuit; de paucis tantummodo locis quaedam observationes in Additamentis adiungere necessarium videbatur, quas vir humanissimus et candidissimus benigne ut spero interpretabitur.

Inter impressionem huius operis, quae pluries interrupta variisque impedimentis usque in quartum annum protracta est, non modo eas investigationes, quas quidem iam antea susceperam, sed quarum promulgationem in aliud tempus differre constitueram, ne liber nimis magnus evaderet, ulterius continuavi, sed plures etiam alias novas aggressus sum. Plures quoque, quas ex eadem ratione leviter tantum attigi, quum tractatio uberior minus necessaria videretur (e. g. eae quae in artt. 37, 82 sqq. aliisque locis traduntur), postea resumtae sunt, disquisitionibusque generalioribus quae luce perdignae videntur locum dederunt (Conf. etiam quae in Additamentis de art. 306 dicuntur). Denique quum liber praesertim propter amplitudinem Sect. V in longe maius quam exspectaveram volumen excres-

ceret, plura quae ab initio ei destinata erant, interque ea totam Sectionem *octavam* (quae passim iam in hoc volumine commemoratur, atque tractationem generalem de congruentiis algebraicis cuiusvis gradus continet) resecare oportuit. Haec omnia, quae volumen huic aequale facile explebunt, publici iuris fient, quamprimum occasio aderit.

Quod, in pluribus quaestionibus difficilibus, demonstrationibus syntheticis usus sum, analysinque per quam erutae sunt suppressi, imprimis brevitatis studio tribuendum est, cui quantum fieri poterat consulere oportebat.

Theoria divisionis circuli, sive polygonorum regularium, quae in Sect. VII tractatur, *ipsa* quidem *per se* ad Arithmeticam non pertinet, attamen eius *principia* unice ex Arithmetica Sublimiori petenda sunt: quod forsan geometris tam inexspectatum erit, quantum veritates novas, quas ex hoc fonte haurire licuit, ipsis gratas fore spero.

Haec sunt, de quibus lectorem praemonere volui. De rebus ipsis non meum est iudicare. Nihil equidem magis opto, quam ut iis, quibus scientiarum incrementa cordi sunt, placeant, quae vel hactenus desiderata explent, vel aditum ad nova aperiunt.

DISQUISITIONES ARITHMETICAE.

SECTIO PRIMA

DE

NUMERORUM CONGRUENTIA IN GENERE.

Numeri congrui, moduli, residua et nonresidua.

1.

Si numerus a numerorum b, c differentiam metitur, b et c *secundum* a *congrui* dicuntur, sin minus, *incongrui*: ipsum a *modulum* appellamus. Uterque numerorum b, c priori in casu alterius *residuum*, in posteriori vero *nonresiduum* vocatur.

Hae notiones de omnibus numeris integris tam positivis quam negativis*) valent, neque vero ad fractos sunt extendendae. *E. g.* -9 et $+16$ secundum modulum 5 sunt congrui; -7 ipsius $+15$ secundum modulum 11 residuum, secundum modulum 3 vero nonresiduum. Ceterum quoniam cifram numerus quisque metitur, omnis numerus tamquam sibi ipsi congruus secundum modulum quemcunque est spectandus.

2.

Omnia numeri dati a residua secundum modulum m sub formula $a + km$ comprehenduntur, designante k numerum integrum indeterminatum. Propositionum quas post trademus faciliores nullo negotio hinc demonstrari possunt: sed istarum quidem veritatem aeque facile quivis intuendo poterit perspicere.

*) Modulus manifesto semper *absolute* i. e. sine omni signo est sumendus.

Numerorum congruentiam hoc signo, $\equiv$, in posterum denotabimus, modulum ubi opus erit in clausulis adiungentes. $-16 \equiv 9 \pmod 5$. $-7 \equiv 15 \pmod{11}$ *).

3.

THEOREMA. *Propositis m numeris integris successivis*

$$a,\ a+1,\ a+2\ \ldots.\ a+m-1$$

alioque A, illorum aliquis huic secundum modulum m congruus erit, et quidem unicus tantum.

Si enim $\frac{a-A}{m}$ integer, erit $a \equiv A$, sin fractus, sit integer proxime maior, (aut quando est negativus, proxime *minor*, si ad signum non respiciatur) $= k$, cadetque $A+km$ inter a et $a+m$, quare erit numerus quaesitus. Et manifestum est omnes quotientes $\frac{a-A}{m}$, $\frac{a+1-A}{m}$, $\frac{a+2-A}{m}$ etc. inter $k-1$ et $k+1$ sitos esse; quare plures quam unus integri esse nequeunt.

Residua minima.

4.

Quisque igitur numerus residuum habebit tum in hac serie, $0, 1, 2, \ldots m-1$, tum in hac, $0, -1, -2, \ldots -(m-1)$, quae *residua minima* dicemus, patetque, nisi 0 fuerit residuum, bina semper dari, *positivum* alterum, alterum *negativum*. Quae si magnitudine sunt inaequalia, alterum erit $< \frac{m}{2}$, sin secus utrumque $= \frac{m}{2}$, signi respectu non habito. Unde patet, quemvis numerum residuum habere moduli semissem non superans quod *absolute minimum* vocabitur.

E. g. -13 secundum modulum 5, habet residuum minimum positivum 2, quod simul est absolute minimum, -3 vero residuum minimum negativum; $+5$ secundum modulum 7 sui ipsius est residuum minimum positivum, -2 negativum, simulque absolute minimum.

Propositiones elementares de congruentiis.

5.

His notionibus stabilitis eas numerorum congruorum proprietates quae prima fronte se offerunt colligamus.

*) Hoc signum propter magnam analogiam quae inter aequalitatem atque congruentiam invenitur adoptavimus. Ob eandem caussam ill. Le Gendre in comment. infra saepius laudanda ipsum aequalitatis signum pro congruentia retinuit, quod nos ne ambiguitas oriatur imitari dubitavimus.

Qui numeri secundum modulum compositum sunt congrui, etiam secundum quemvis eius divisorem congrui.

Si plures numeri eidem numero secundum eundem modulum sunt congrui, inter se erunt congrui (secundum eundem modulum).

Haec modulorum identitas etiam in sequentibus est subintelligenda.

Numeri congrui residua minima habent eadem, incongrui diversa.

6.

Si habentur quotcunque numeri A, B, C etc. totidemque alii a, b, c etc. illis secundum modulum quemcunque congrui,

$$A \equiv a,\ B \equiv b \text{ etc.},\ \text{erit}\ A+B+C+ \text{ etc.} \equiv a+b+c+ \text{ etc.}$$

Si $A \equiv a$, $B \equiv b$, erit $A-B \equiv a-b$.

7.

Si $A \equiv a$, erit quoque $kA \equiv ka$.

Si k numerus positivus, hoc est tantummodo casus particularis propos. art. praec., ponendo ibi $A = B = C$ etc., $a = b = c$ etc. Si k negativus, erit $-k$ positivus, adeoque $-kA \equiv -ka$, unde $kA \equiv ka$.

Si $A \equiv a$, $B \equiv b$, erit $AB \equiv ab$. Namque $AB \equiv Ab \equiv ba$.

8.

Si habentur quotcunque numeri A, B, C etc. totidemque alii a, b, c etc. his congrui, $A \equiv a$, $B \equiv b$ etc., producta ex utrisque erunt congrua, ABC etc. $\equiv abc$ etc.

Ex artic. praec. $AB \equiv ab$, et ob eandem rationem $ABC \equiv abc$; eodemque modo quotcunque alii factores accedere possunt.

Si omnes numeri A, B, C etc. aequales assumuntur, nec non respondentes a, b, c etc., habetur hoc theorema: *Si $A \equiv a$ et k integer positivus, erit $A^k \equiv a^k$.*

9.

Sit X functio algebraica indeterminatae x, huius formae

$$Ax^\alpha + Bx^\beta + Cx^\gamma + \text{etc.}$$

designantibus A, B, C etc. numeros integros quoscunque; α, β, γ etc. vero integros non negativos. Tum si indeterminatae x valores secundum modulum quemcunque congrui tribuuntur, valores functionis X inde prodeuntes congrui erunt.

Sint f, g valores congrui ipsius x. Tum ex art. praec. $f^a \equiv g^a$ et $Af^a \equiv Ag^a$, eodemque modo $Bf^b \equiv Bg^b$ etc. Hinc

$$Af^a + Bf^b + Cf^c + \text{etc.} \equiv Ag^a + Bg^b + Cg^c + \text{etc.} \quad Q.\ E.\ D.$$

Ceterum facile intelligitur, quomodo hoc theorema ad functiones plurium indeterminatarum extendi possit.

10.

Quodsi igitur pro x omnes numeri integri consecutivi substituuntur, valoresque functionis X ad residua minima reducuntur, haec seriem constituent, in qua post intervallum m terminorum (designante m modulum) iidem termini iterum recurrunt; sive haec series ex *periodo* m terminorum infinities repetita, erit formata. Sit e. g. $X = x^3 - 8x + 6$ et $m = 5$; tum pro $x = 0, 1, 2, 3$ etc., valores ipsius X haec residua minima positiva suppeditant, 1, 4, 3, 4, 3, 1, 4 etc., ubi quina priora 1, 4, 3, 4, 3 in infinitum repetuntur; atque si series retro continuatur, i. e. ipsi x valores negativi tribuuntur, eadem periodus ordine terminorum inverso prodit: unde manifestum est, terminos alios quam qui hanc periodum constituant in tota serie locum habere non posse.

11.

In hoc igitur exemplo X neque $\equiv 0$, neque $\equiv 2 \pmod 5$ fieri potest, multoque minus $= 0$, aut $= 2$. Unde sequitur, aequationes $x^3 - 8x + 6 = 0$, et $x^3 - 8x + 4 = 0$ per numeros integros et proin, uti notum est, per numeros rationales solvi non posse. Generaliter perspicuum est, aequationem $X = 0$, quando X functio incognitae x, huius formae

$$x^n + Ax^{n-1} + Bx^{n-2} + \text{etc.} + N$$

A, B, C etc. integri, atque n integer positivus, (ad quam formam omnes aequationes algebraicas reduci posse constat) radicem rationalem nullam habere, si congruentiae $X \equiv 0$ secundum ullum modulum satisfieri nequeat. Sed hoc criterium, quod hic sponte se nobis obtulit, in Sect. VIII fusius pertractabitur. Poterit certe ex hoc specimine notiuncula qualiscunque de harum investigationum utilitate efformari.

Quaedam applicationes.

12.

Theorematibus in hoc capite traditis complura quae in arithmeticis doceri solent innituntur, e. g. regulae ad explorandam divisibilitatem numeri propositi per 9, 11 aut alios numeros. *Secundum modulum* 9 omnes numeri 10 potestates unitati sunt congruae: quare si numerus propositus habet formam $a + 10b + 100c + \text{etc.}$, idem residuum minimum secundum modulum 9 dabit, quod $a + b + c + \text{etc.}$ Hinc manifestum est, si figurae singulae numeri decadice expressi sine respectu loci quem occupant addantur, summam hanc numerumque propositum eadem residua minima praebere, adeoque hunc per 9 dividi posse, si illa per 9 sit divisibilis, et contra. Idem etiam de divisore 3 tenendum. Quoniam *secundum modulum* 11, $100 \equiv 1$ erit generaliter $10^{2k} \equiv 1$, $10^{2k+1} \equiv 10 \equiv -1$, et numerus formae $a + 10b + 100c + \text{etc.}$ secundum modulum 11 idem residuum minimum dabit quod $a - b + c$ etc.; unde regula nota protinus derivatur. Ex eodem principio omnia similia praecepta facile deducuntur.

Nec minus ex praecedentibus petenda est ratio regularum, quae ad verificationem operationum arithmeticarum vulgo commendantur. Scilicet si ex numeris datis alii per additionem, subtractionem, multiplicationem aut elevationem ad potestates sunt deducendi: substituuntur datorum loco residua ipsorum minima secundum modulum arbitrarium (vulgo 9 aut 11, quoniam in nostro systemate decadico secundum hos, uti modo ostendimus, residua tam facile possunt inveniri). Numeri hinc oriundi illis, qui ex numeris propositis deducti fuerunt, congrui esse debent; quod nisi eveniat, vitium in calculum irrepsisse concluditur.

Sed quum haec hisque similia abunde sint nota, diutius iis immorari superfluum foret.

SECTIO SECUNDA

DE

CONGRUENTIIS PRIMI GRADUS.

Theoremata praeliminaria de numeris primis, factoribus etc.

13.

THEOREMA. *Productum e duobus numeris positivis numero primo dato minoribus per hunc primum dividi nequit.*

Sit p primus, et a positivus $< p$; tum nullus numerus positivus b ipso p minor dabitur, ita ut sit $ab \equiv 0 \pmod{p}$.

Dem. Si quis neget, supponamus dari numeros b, c, d etc. omnes $< p$, ita ut $ab \equiv 0$, $ac \equiv 0$, $ad \equiv 0$ etc. (mod. p). Sit omnium minimus b, ita ut omnes numeri ipso b minores hac proprietate sint destituti. Manifesto erit $b > 1$: si enim $b = 1$, foret $ab = a < p$ (*hyp.*), adeoque per p non divisibilis. Quare p tamquam primus per b dividi non poterit, sed inter duo ipsius b multipla proxima mb et $(m+1)b$ cadet. Sit $p - mb = b'$, critque b' numerus positivus et $< b$. Iam quia supposuimus, $ab \equiv 0 \pmod{p}$, habebitur quoque $mab \equiv 0$ (art. 7), et hinc, subtrahendo ab $ap \equiv 0$, erit $a(p - mb) = ab' \equiv 0$; i. e. b' inter numeros b, c, d etc. referendus, licet minimo eorum b sit minor. *Q. E. A.*

14.

Si nec a nec b per numerum primum p dividi potest: etiam productum ab per p dividi non poterit.

Sint numerorum a, b, secundum modulum p residua minima positiva $\alpha, \vec{\alpha}$, quorum neutrum erit 0 (*hyp.*). Iam si esset $ab \equiv 0 \pmod{p}$, foret quoque, propter $ab \equiv \alpha\vec{\alpha}$, $\alpha\vec{\alpha} \equiv 0$, quod cum theoremate praec. consistere nequit.

Huius theorematis demonstratio iam ab Euclide tradita, *El.* VII. 32. Nos tamen omittere eam noluimus, tum quod recentiorum complures seu ratiocinia vaga pro demonstratione venditaverunt, seu theorema omnino praeterierunt, tum quod indoles methodi hic adhibitae, qua infra ad multo reconditiora enodanda utemur, e casu simpliciori facilius deprehendi poterit.

15.

Si nullus numerorum a, b, c, d etc. per numerum primum p dividi potest, etiam productum $abcd$ etc. per p dividi non poterit.

Secundum artic. praec. ab per p dividi nequit; ergo etiam abc; hinc $abcd$ etc.

16.

THEOREMA. *Numerus compositus quicunque unico tantum modo in factores primos resolvi potest.*

Dem. Quemvis numerum compositum in factores primos resolvi posse, ex elementis constat, sed pluribus modis diversis fieri hoc non posse perperam plerumque supponitur tacite. Fingamus numerum compositum A, qui sit $= a^{\alpha} b^{\beta} c^{\gamma}$ etc., designantibus a, b, c etc. numeros primos inaequales, alio adhuc modo in factores primos esse resolubilem. Primo manifestum est, in secundum hoc factorum systema alios primos quam a, b, c etc. ingredi non posse, quum quicunque alius primus numerum A ex his compositum metiri nequeat. Similiter etiam in secundo hoc factorum systemate nullus primorum a, b, c etc. deesse potest, quippe qui alias ipsum A non metiretur (art. praec.). Quare hae binae in factores resolutiones in eo tantummodo differre possunt, quod in altera aliquis primus pluries quam in altera habeatur. Sit talis primus p, qui in altera resolutione m, in altera vero n vicibus occurrat, sitque $m > n$: Iam deleatur ex utroque systemate factor p, n vicibus, quo fiet ut in altero adhuc $m - n$ vicibus remaneat, ex altero vero omnino abierit. I. e. numeri $\frac{A}{p^n}$ duae in factores resolutiones habentur, quarum altera a factore p prorsus libera, altera vero $m - n$ vicibus eum continet; contra ea quae modo demonstravimus.

17.

Si itaque numerus compositus A est productum ex B, C, D etc., patet, inter factores primos numerorum B, C, D etc. alios esse non posse, quam qui etiam sint inter factores numeri A, et quemvis horum factorum toties in B, C, D etc. coniunctim occurrere debere, quoties in A. Hinc colligitur criterium, utrum numerus B alium A metiatur, necne. Illud eveniet, si B neque alios factores primos, neque ullum pluries involvit, quam A; quarum conditionum si aliqua deficit, B ipsum A non metietur.

Facile hinc calculi combinationum auxilio derivari potest, si $A = a^\alpha b^\beta c^\gamma$ etc. designantibus ut supra a, b, c etc. numeros primos diversos, A habere

$$(\alpha+1)(\beta+1)(\gamma+1)\text{ etc.}$$

divisores diversos, inclusis etiam 1 et A.

18.

Si igitur $A = a^\alpha b^\beta c^\gamma$ etc., $K = k^\varkappa l^\lambda m^\mu$ etc., atque primi a, b, c etc., k, l, m etc. omnes diversi, patet A et K divisorem communem praeter 1 non habere, sive inter se esse primos.

Pluribus numeris A, B, C etc. propositis *maxima omnibus communis mensura* ita determinatur. Resolvantur omnes in suos factores primos, atque ex his excerpantur ii, qui omnibus numeris A, B, C etc. sunt communes (si tales non adsunt, nullus divisor erit omnibus communis). Tum quoties quisque horum factorum primorum in singulis A, B, C etc. continetur, sive *quot dimensiones* in singulis A, B, C etc. quisque habeat, adnotetur. Tandem singulis factoribus primis tribuantur dimensiones omnium quas in A, B, C etc. habent minimae, componaturque productum ex iis, quod erit mensura communis quaesita.

Quando vero numerorum A, B, C etc. *minimus communis dividuus* desideratur, ita procedendum. Colligantur omnes numeri primi, qui numerorum A, B, C etc. aliquem metiuntur, tribuatur cuivis dimensio omnium quas in numeris A, B, C etc. habet maxima, sicque ex omnibus productum confletur, quod erit dividuus quaesitus.

Ex. Sit $A = 504 = 2^3 3^2 7$; $B = 2880 = 2^6 3^2 5$; $C = 864 = 2^5 3^3$. Pro inveniendo divisore communi maximo habentur factores primi 2, 3, quibus dimensiones 3, 2 tribuendi; unde fiet $= 2^3 3^2 = 72$; dividuus vero communis minimus erit $2^6 3^3 5 . 7 = 60480$.

Demonstrationes propter facilitatem omittimus. Ceterum quomodo haec problemata solvenda sint, quando numerorum A, B, C etc. in factores resolutio non detur, ex elementis notum.

19.

Si numeri a, b, c etc. ad alium k sunt primi, etiam productum ex illis abc etc. ad k primum est.

Quia enim nulli numerorum a, b, c etc. factor primus cum k est communis productumque abc etc. alios factores primos habere nequit, quam qui sunt factores alicuius numerorum a, b, c etc., productum abc etc. etiam cum k factorem primum communem non habebit. Quare ex art. praec. k ad abc etc. primus.

Si numeri a, b, c etc. inter se sunt primi, aliumque k singuli metiuntur: etiam productum ex illis numerum k metietur.

Hoc aeque facile ex artt. 17, 18 derivatur. Sit enim quicunque producti abc etc. divisor primus p, quem contineat π vicibus, manifestumque est, aliquem numerorum a, b, c etc. eundem hunc divisorem p vicibus continere debere. Quare etiam k, quem hic numerus metitur, π vicibus divisorem p continet. Similiter de reliquis producti abc etc. divisoribus.

Hinc *si duo numeri m, n secundum plures modulos inter se primos a, b, c etc. sunt congrui, etiam secundum productum ex his congrui erunt.* Quum enim $m - n$ per singulos a, b, c etc. sit divisibilis, etiam per eorum productum dividi poterit.

Denique *si a ad b primus et ak per b divisibilis, erit etiam ak per b divisibilis.* Namque quoniam ak tam per a quam per b divisibilis, etiam per ab dividi poterit, i. e. $\frac{ak}{ab} = \frac{k}{b}$ erit integer.

20.

Quando $A = a^\alpha b^\beta c^\gamma$ etc., designantibus a, b, c etc. numeros primos inaequales, est potestas aliqua, puta $= k^n$: omnes exponentes α, β, γ etc. per n erunt divisibiles.

Numerus enim k alios factores primos quam a, b, c etc. non involvit. Contineat factorem a, α' vicibus, continebitque k^n sive A hunc factorem $n\alpha'$ vicibus; quare $n\alpha' = \alpha$, et $\frac{\alpha}{n}$ integer. Similiter $\frac{\beta}{n}$ etc. integros esse demonstratur.

21.

Quando a, b, c etc. sunt inter se primi, et productum abc etc. potestas aliqua, puta $= k^n$: singuli numeri a, b, c etc. similes potestates erunt.

Sit $a = l^\lambda m^\mu p^\pi$ etc., designantibus l, m, p etc. numeros primos diversos, quorum nullus per *hyp.* est factor numerorum b, c etc. Quare productum abc etc. factorem l implicabit λ vicibus, factorem m vero μ vicibus etc.: hinc (*art. praec.*) λ, μ, π etc. per n divisibiles adeoque

$$\sqrt[n]{a} = l^{\frac{\lambda}{n}} m^{\frac{\mu}{n}} p^{\frac{\pi}{n}} \text{ etc.}$$

integer. Similiter de reliquis b, c etc.

Haec de numeris primis praemittenda erant; iam ad ea quae finem nobis propositum propius attinent convertimur.

22.

Si numeri a, b per alium k divisibiles secundum modulum m ad k primum sunt congrui: $\frac{a}{k}$ et $\frac{b}{k}$ secundum eundem modulum congrui erunt.

Patet enim $a - b$ per k divisibilem fore, nec minus per m (*hyp.*); quare (*art.* 19) $\frac{a-b}{k}$ per m divisibilis erit, i.e. erit $\frac{a}{k} \equiv \frac{b}{k} \pmod{m}$.

Si autem reliquis manentibus m et k habent divisorem communem maximum e, erit $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{e}}$. Namque $\frac{k}{e}$ et $\frac{m}{e}$ inter se primi. At $a - b$ tam per k quam per m divisibilis adeoque etiam $\frac{a-b}{e}$ tam per $\frac{k}{e}$ quam per $\frac{m}{e}$, hinc per $\frac{km}{ee}$ i.e. $\frac{a-b}{k}$ per $\frac{m}{e}$, sive $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{e}}$.

23.

Si a ad m primus, et e, f numeri secundum modulum m incongrui: erunt etiam ae, af incongrui secundum m.

Hoc est tantum conversio theor. art. praec.

Hinc vero manifestum est, si a per omnes numeros integros a 0 usque ad $m - 1$ multiplicetur productaque secundum modulum m ad residua sua minima reducantur, haec omnia fore inaequalia. Et quum horum residuorum, quorum nullum $> m$, numerus sit m, totidemque dentur numeri a 0 usque ad $m - 1$, patet, nullum horum numerorum inter illa residua deesse posse.

24.

Expressio $ax + b$, denotantibus a, b numeros datos, x numerum indeterminatum seu variabilem, *secundum modulum m, ad a primum, cuivis numero dato congrua fieri potest.*

Sit numerus, cui congrua fieri debet, c, et residuum minimum positivum ipsius $c - b$ secundum modulum m, e. Ex art. praec. necessario datur valor ipsius $x < m$, talis; ut producti ax secundum modulum m residuum minimum fiat e; esto hic valor v, eritque $av \equiv e \equiv c - b$; unde $av + b \equiv c \pmod{m}$ *Q. E. F.*

25.

Expressionem duas quantitates congruas exhibentem ad instar aequationum, *congruentiam* vocamus; quae si incognitam implicat, *resolvi* dicitur, quando pro hac valor invenitur congruentiae satisfaciens (*radix*). Hinc porro intelligitur, quid sit *congruentia resolubilis et congruentia irresolubilis*. Tandem facile perspicitur similes distinctiones locum hic habere posse uti in aequationibus. Congruentiarum *transscendentium* infra exempla occurrent; *algebraicae* vero secundum dimensionem maximam incognitae in congruentias primi, secundi altiorumque *graduum* distribuuntur. Nec minus congruentiae plures proponi possunt plures incognitas involventes, de quarum *eliminatione* disquirendum.

Solutio congruentiarum primi gradus.

26.

Congruentia itaque primi gradus $ax + b \equiv c$ ex art. 24 semper resolubilis, quando modulus ad a est primus. Quodsi vero v fuerit valor idoneus ipsius x, sive radix congruentiae, palam est, omnes numeros, ipsi v secundum congruentiae propositae modulum congruos, etiam radices fore (art. 9). Neque minus facile perspicitur, omnes radices ipsi v congruos esse debere: si enim alia radix fuerit t, erit $av + b \equiv at + b$, unde $av \equiv at$, et hinc $v \equiv t$ (art. 22). Hinc colligitur congruentiam $x \equiv v \pmod{m}$ exhibere resolutionem completam congruentiae $ax + b \equiv c$.

Quia resolutiones congruentiae per valores ipsius x congruos per se sunt obviae, atque, hoc respectu, numeri congrui tamquam aequivalentes considerandi, tales congruentiae resolutiones pro una eademque habebimus. Quamobrem quum

nostra congruentia $ax + b \equiv c$ alias resolutiones non admittat, pronunciabimus, unico tantum modo eam esse resolubilem seu unam tantum radicem habere. Ita *e. g.* congruentia $6x + 5 \equiv 13 \pmod{11}$ alias radices non admittit, quam quae sunt $\equiv 5 \pmod{11}$. Haud perinde res se habet in congruentiis altiorum graduum, sive etiam in congruentiis primi gradus, ubi incognita per numerum est multiplicata, ad quem modulus non est primus.

27.

Superest, ut de invenienda resolutione ipsa congruentiae huiusmodi, quaedam adiiciamus. Primo observamus, congruentiam formae $ax + t \equiv u$, cuius modulum ad a primum supponimus, ab hac $ax \equiv \pm 1$ pendere: si enim huic satisfacit $x \equiv r$, illi satisfaciet $x \equiv \pm (u - t)\, r$. At congruentiae $ax \equiv \pm 1$, modulo per b designato, aequivalet aequatio indeterminata $ax = by \pm 1$, quae quomodo sit solvenda hoc quidem tempore abunde est notum; quare nobis sufficiet, calculi algorithmum huc transscripsisse.

Si quantitates A, B, C, D, E etc. ita ab his $\alpha, \beta, \gamma, \delta$ etc. pendent, ut habeatur

$$A = \alpha, \quad B = \beta A + 1, \quad C = \gamma B + A, \quad D = \delta C + B, \quad E = \varepsilon D + C \text{ etc.}$$

brevitatis gratia ita eas designamus,

$$A = [\alpha], \quad B = [\alpha, \beta], \quad C = [\alpha, \beta, \gamma], \quad D = [\alpha, \beta, \gamma, \delta] \text{ etc.}^*)$$

Iam proposita sit aequatio indeterminata $ax = by \pm 1$, ubi a, b positivi. Supponamus, id quod licet, a esse non $< b$. Tum ad instar algorithmi noti, secundum quem duorum numerorum divisor communis maximus investigatur, formentur per divisionem vulgarem aequationes,

$$a = \alpha b + c, \quad b = \beta c + d, \quad c = \gamma d + e \text{ etc.}$$

ita ut α, β, γ etc. c, d, e etc. sint integri positivi, et b, c, d, e continuo decrescentes, donec perveniatur ad $m = \mu n + 1$

*) Multo generalius haecce relatio considerari potest, quod negotium alia forsan occasione suscipiemus. Hic duas tantum propositiones adiicimus, quae usum suum in praesenti investigatione habent; scilicet,

1°. $[\alpha, \beta, \gamma \ldots, \lambda, \mu]\,[\beta, \gamma \ldots, \lambda] - [\alpha, \beta, \gamma \ldots \lambda]\,[\beta, \gamma, \ldots \lambda, \mu] = \pm 1$,

ubi signum superius accipiendum quando numerorum $\alpha, \beta, \gamma \ldots \lambda, \mu$ multitudo par, inferius quando impar.

2°. Numerorum α, β, γ etc. ordo inverti potest, $[\alpha, \beta, \gamma \ldots, \lambda, \mu] = [\mu, \lambda \ldots, \gamma, \beta, \alpha]$.

Demonstrationes quae non sunt difficiles hic supprimimus.

quod tandem evenire debere constat. Erit itaque

$$a = [n, \mu, \ldots \gamma, \beta, \alpha], \quad b = [n, \mu \ldots \gamma, \beta].$$

Tum fiat $x = [\mu, \ldots \gamma, \beta], \quad y = [\mu, \ldots \gamma, \beta, \alpha]$

eritque $ax = by + 1$, quando numerorum $\alpha, \beta, \gamma \ldots \mu, n$ multitudo est par aut $ax = by - 1$, quando est impar. *Q. E. F.*

28.

Resolutionem generalem huiusmodi aequationum indeterminatarum ill. Euler primus docuit, *Comment. Petrop.* T. VII. p. 46. Methodus qua usus est consistit in substitutione aliarum incognitarum loco ipsarum x, y, atque hoc quidem tempore satis est nota. Ill. La Grange paullo aliter rem aggressus est: scilicet ex theoria fractionum continuarum constat, si fractio $\frac{b}{a}$ in fractionem continuam

$$\cfrac{1}{\alpha + \cfrac{1}{\beta + \cfrac{1}{\gamma + \text{etc.} \cfrac{1}{\mu + \cfrac{x}{n}}}}}$$

convertatur, haecque deleta ultima sui parte $\frac{x}{n}$ in fractionem communem $\frac{x}{y}$ restituatur, fore $ax = by \pm 1$, siquidem fuerit a ad b primus. Ceterum ex utraque methodo idem algorithmus derivatur. Investigationes ill. La Grange exstant *Hist. de l'Ac. de Berlin Année* 1767 *p.* 175, et cum aliis in *Supplementis versioni gallicae Algebrae Eulerianae adiectis.*

29.

Congruentiae $ax + t \equiv u$ cuius modulus ad a non primus, facile ad casum praecedentem reducitur. Sit modulus m, maximusque numerorum a, m divisor communis δ. Primo patet quemvis valorem ipsius x congruentiae secundum modulum m satisfacientem eidem etiam secundum modulum δ satisfacere (art. 5). At semper $ax \equiv 0 \pmod{\delta}$, quoniam δ ipsum a metitur. Quare, nisi $t \equiv u \pmod{\delta}$ i. e. $t - u$ per δ divisibilis, congruentia proposita non est resolubilis.

Ponamus itaque $a = \delta e$, $m = \delta f$, $t - u = \delta k$, eritque e ad f primus. Tum vero congruentiae propositae $\delta ex + \delta k \equiv 0 \pmod{\delta f}$, aequivalebit haec $ex + k \equiv 0 \pmod{f}$, i. e. quicunque ipsius x valor huic satisfaciat, etiam illi satisfaciet et vice versa. Manifesto enim $ex + k$ per f dividi poterit, quando $\delta ex + \delta k$ per δf dividi potest, et vice versa. At congruentiam $ex + k \equiv 0 \pmod{f}$ supra solvere docuimus; unde simul patet, si v sit unus ex valoribus ipsius x, $x \equiv v \pmod{f}$ exhibere resolutionem completam congruentiae propositae.

30.

Quando modulus est compositus, nonnumquam praestat sequenti methodo uti.

Sit modulus $= mn$, atque congruentia proposita $ax \equiv b$. Solvatur primo congruentia haec secundum modulum m, ponamusque ei satisfieri, si $x \equiv v \pmod{\frac{m}{\delta}}$, designante δ divisorem communem maximum numerorum m, a. Iam manifestum est, quemvis valorem ipsius x congruentiae $ax \equiv b$ secundum modulum mn satisfacientem eidem etiam secundum modulum m satisfacere debere: adeoque in forma $v + \frac{m}{\delta} x'$ contineri, designante x' numerum indeterminatum, quamvis non vice versa omnes numeri in forma $v + \frac{m}{\delta} x'$ contenti congruentiae secundum mod. mn satisfaciant. Quomodo autem x' determinari debeat, ut $v + \frac{m}{\delta} x'$ fiat radix congruentiae $ax \equiv b \pmod{mn}$, ex solutione congruentiae $\frac{am}{\delta} x' + av \equiv b \pmod{mn}$ deduci potest, cui aequivalet haec $\frac{a}{\delta} x' \equiv \frac{b - av}{m} \pmod{n}$. Hinc colligitur solutionem congruentiae cuiuscunque primi gradus secundum modulum mn reduci posse ad solutionem duarum congruentiarum secundum modulum m et n. Facile autem perspicietur, si n iterum sit productum e duobus factoribus, solutionem congruentiae secundum modulum n pendere a solutione duarum congruentiarum quarum moduli sint illi factores. Generaliter solutio congruentiae secundum modulum compositum quemcumque pendet a solutione aliarum congruentiarum, quarum moduli sunt factores illius numeri; hi autem, si commodum esse videtur, ita semper accipi possunt, ut sint numeri primi.

Ex. Si congruentia $19x \equiv 1 \pmod{140}$ proponitur: solvatur primo secundum modulum 2, eritque $x \equiv 1 \pmod{2}$. Ponatur $x = 1 + 2x'$, fietque $38x' \equiv -18 \pmod{140}$ cui aequivalet $19x' \equiv -9 \pmod{70}$. Si haec

iterum secundum modulum 2 solvitur, fit $x' \equiv 1 \pmod{2}$, positoque $x' = 1 + 2x''$, fit $38x'' \equiv -28 \pmod{70}$ sive $19x'' \equiv -14 \pmod{35}$. Haec secundum 5 soluta dat $x'' \equiv 4 \pmod{5}$, substitutoque $x'' = 4 + 5x'''$, fit $95x''' \equiv -90 \pmod{35}$ sive $19x''' \equiv -18 \pmod{7}$. Ex hac tandem sequitur, $x''' \equiv 2 \pmod{7}$, positoque $x''' = 2 + 7x''''$ colligitur $x = 59 + 140x''''$; quare $x \equiv 59 \pmod{140}$ est solutio completa congruentiae propositae.

31.

Simili modo ut aequationis $ax = b$ radix per $\frac{b}{a}$ exprimitur, etiam congruentiae $ax \equiv b$ radicem quamcunque per $\frac{b}{a}$ designabimus, congruentiae modulum, distinctionis gratia, apponentes. Ita e. g. $\frac{1}{5} \pmod{12}$ denotat quemvis numerum, qui est $\equiv 11 \pmod{12}$ *). Generaliter ex praecedentibus patet, $\frac{a}{b} \pmod{c}$ nihil reale significare (aut si quis malit aliquid imaginarii), si a, c habeant divisorem communem, qui ipsum b non metiatur. At hoc casu excepto, expressio $\frac{b}{a} \pmod{c}$ semper valores reales habebit, et quidem infinitos: hi vero omnes secundum c erunt congrui quando a ad c primus, aut secundum $\frac{c}{\delta}$, quando δ numerorum c, a divisor communis maximus.

Hae expressiones similem fere habent algorithmum ut fractiones vulgares. Aliquot proprietates quae facile ex praecedentibus deduci possunt hic apponimus.

1. Si secundum modulum c, $a \equiv \alpha$, $b \equiv \beta$ expressiones $\frac{a}{b} \pmod{c}$ et $\frac{\alpha}{\beta} \pmod{c}$ sunt aequivalentes.
2. $\frac{a\delta}{b\delta} \pmod{c\delta}$ et $\frac{a}{b} \pmod{c}$ sunt aequivalentes.
3. $\frac{ak}{bk} \pmod{c}$ et $\frac{a}{b} \pmod{c}$ sunt aequivalentes quando k ad c est primus.

Multae aliae similes propositiones afferri possent: at quum nulli difficultati sint obnoxiae, neque ad sequentia adeo necessariae, ad alia properamus.

De inveniendo numero secundum modulos datos residuis datis congruo.

32.

Problema quod magnum in sequentibus usum habebit, *invenire omnes numeros, qui secundum modulos quotcunque datos residua data praebent*, facile ex praecedentibus solvi potest. Sint primo duo moduli A, B, secundum quos numerus

*) id quod ex analogia per $\frac{3.1}{4} \pmod{12}$ designari potest.

quaesitus, z, numeris a, b respective congruus esse debeat. Omnes itaque valores ipsius z sub forma $Ax + a$ continentur, ubi x est indeterminatus sed talis ut fiat $Ax + a \equiv b \pmod{B}$. Quodsi iam numerorum A, B divisor communis maximus est δ, resolutio completa huius congruentiae hanc habebit formam: $x \equiv v \pmod{\frac{B}{\delta}}$ sive quod eodem redit, $x = v + \frac{kB}{\delta}$, denotante k numerum integrum arbitrarium. Hinc formula $Av + a + \frac{kAB}{\delta}$ omnes ipsius z valores comprehendet, i. e. $z \equiv Av + a \pmod{\frac{AB}{\delta}}$, erit resolutio completa problematis. Si ad modulos A, B tertius accedit, C, secundum quem numerus quaesitus z debet esse $\equiv c$, manifesto eodem modo procedendum, quum binae priores conditiones in unicam iam sint conflatae. Scilicet si numerorum $\frac{AB}{\delta}, C$ divisor communis maximus $= \varepsilon$, atque congruentiae $\frac{AB}{\delta}x + Av + a \equiv c \pmod{C}$ resolutio: $x \equiv w \pmod{\frac{C}{\varepsilon}}$, problema per congruentiam $z \equiv \frac{ABw}{\delta} + Av + a \pmod{\frac{ABC}{\delta\varepsilon}}$ complete erit resolutum. Similiter procedendum, quotcunque moduli proponantur. Observari convenit $\frac{AB}{\delta}, \frac{ABC}{\delta\varepsilon}$ esse numerorum A, B; et A, B, C respective minimos communes dividuos, facileque inde perspicitur, quotcunque habeantur moduli A, B, C etc., si eorum minimus communis dividuus sit M, resolutionem completam hanc formam habere, $z \equiv r \pmod{M}$. Ceterum quando ulla congruentiarum auxiliarium est irresolubilis, problema impossibilitatem involvere concludendum est. Perspicuum vero, hoc evenire non posse, quando omnes numeri A, B, C etc. inter se sint primi.

Ex. Sint numeri A, B, C; a, b, c; 504, 35, 16; 17, — 4, 33; hic duae conditiones ut z sit $\equiv 17 \pmod{504}$ et $\equiv -4 \pmod{35}$ unicae, ut sit $\equiv 521 \pmod{2520}$ aequivalent; ex qua cum hac: $z \equiv 33 \pmod{16}$ coniuncta, prodeat $z \equiv 3041 \pmod{5040}$.

33.

Quando omnes numeri A, B, C etc. inter se sunt primi, constat, productum ex ipsis esse minimum omnibus communem dividuum. In quo casu manifestum est, omnes congruentias $z \equiv a \pmod{A}$; $z \equiv b \pmod{B}$ etc. unicae $z \equiv r \pmod{R}$ prorsus aequivalere, denotante R numerorum A, B, C etc. productum. Hinc vero vicissim sequitur, unicam conditionem $z \equiv r \pmod{R}$ in plures dissolvi posse, scilicet si R quomodocunque in factores inter se primos A, B, C etc. resolvitur, conditiones $z \equiv r \pmod{A}$, $z \equiv r \pmod{B}$, $z \equiv r \pmod{C}$, etc. propositum exhaurient. Haec observatio methodum nobis aperit

non modo impossibilitatem, si quam forte conditiones propositae implicent, statim detegendi, sed etiam calculum commodius atque concinnius instituendi.

34.

Sint ut supra conditiones propositae, ut sit $z \equiv a \pmod{A}$, $z \equiv b \pmod{B}$, $z \equiv c \pmod{C}$. Resolvantur omnes moduli in factores inter se primos, A in $A' A'' A'''$ etc.; B in $B' B'' B'''$ etc. etc. et quidem ita ut numeri A', A'' etc. B', B'' etc. etc. sint aut primi, aut primorum potestates. Si vero aliquis numerorum A, B, C etc. iam per se est primus, aut primi potestas, nulla resolutione in factores pro hocce opus est. Tum vero ex praecedentibus patescit, pro conditionibus propositis hasce substitui posse: $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, $z \equiv a \pmod{A'''}$ etc., $z \equiv b \pmod{B'}$, $z \equiv b \pmod{B''}$ etc. etc. Iam nisi omnes numeri A, B, C etc. fuerint inter se primi, ex. gr. si A ad B non primus, manifestum est, omnes divisores primos ipsorum A, B diversos esse non posse, sed inter factores A', A'', A''' etc. unum aut alterum esse debere, qui inter B', B'', B''' etc. aut aequalem aut multiplum aut submultiplum habeat. Si *primo* $A' = B'$, conditiones $z \equiv a \pmod{A'}$, $z \equiv b \pmod{B'}$ identicae esse debent, sive $a \equiv b \pmod{A' \text{ vel } B'}$, quare alterutra reiici poterit. Si vero non $a \equiv b \pmod{A'}$, problema impossibilitatem implicat. Si *secundo* B' multiplum ipsius A', conditio $z \equiv a \pmod{A'}$ in hac $z \equiv b \pmod{B'}$ contenta esse debet, sive haec $z \equiv b \pmod{A'}$ quae ex posteriori deducitur cum priori identica esse debet. Unde sequitur conditionem $z \equiv a \pmod{A'}$, nisi alteri repugnet (in quo casu problema impossibile) reiici posse. Quando omnes conditiones superfluae ita reiectae sunt, patet, omnes modulos ex his A', A'', A''' etc., B', B'', B''' etc. etc. remanentes inter se primos fore: tum igitur de problematis possibilitate certi esse et secundum praecepta ante data procedere possumus.

35.

Ex. Si ut supra esse debet $z \equiv 17 \pmod{504}$, $\equiv -4 \pmod{35}$, et $\equiv 33 \pmod{16}$; hae conditiones in sequentes resolvi possunt, $z \equiv 17 \pmod{8}$, $\equiv 17 \pmod{9}$, $\equiv 17 \pmod{7}$, $\equiv -4 \pmod{5}$, $\equiv -4 \pmod{7}$, $\equiv 33 \pmod{16}$. Ex his conditiones $z \equiv 17 \pmod{8}$, $z \equiv 17 \pmod{7}$ reiici possunt, quum prior in conditione $z \equiv 33 \pmod{16}$ contineatur, posterior vero cum hac $z \equiv -4 \pmod{7}$ sit identica; remanent itaque

$$z \equiv \begin{cases} 17 \pmod 9 \\ -4 \pmod 5 \\ -4 \pmod 7 \\ 33 \pmod{16} \end{cases} \quad \text{unde colligitur} \quad z \equiv 3041 \pmod{5040}.$$

Ceterum palam est, plerumque commodius fore, si de conditionibus remanentibus eae quae ex una eademque conditione evolutae erant seorsim recolligantur, quum hoc nullo negotio fieri possit; *e. g.* quando ex conditionibus $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$ etc. aliquae abiernnt: quae ex reliquis restituitur, haec erit, $z \equiv a$ secundum modulum qui est productum omnium modulorum ex A', A'', A''' etc. remanentium. Ita in nostro exemplo ex conditionibus $z \equiv -4 \pmod 5$, $z \equiv -4 \pmod 7$ ea ex qua ortae erant $z \equiv -4 \pmod{35}$ sponte restituitur. Porro hinc sequitur haud prorsus perinde esse, quaenam ex conditionibus superfluis reiiciantur, quantum ad calculi brevitatem: sed haec aliaque artificia practica, quae ex usu multo facilius quam ex praeceptis ediscuntur hic tradere non est instituti nostri.

36.

Quando omnes moduli A, B, C, D etc. inter se sunt primi, sequenti methodo saepius praestat uti. Determinetur numerus α secundum A unitati, secundum reliquorum modulorum productum vero cifrae congruus, sive sit α valor quicunque (plerumque praestat *minimum* accipere) expressionis $\frac{1}{BCD \text{ etc.}} \pmod A$, per BCD etc. multiplicatus (vid. art. 32); similiter sit $\mathfrak{b} \equiv 1 \pmod B$ et $\equiv 0 \pmod{ACD \text{ etc.}}$, $\gamma \equiv 1 \pmod C$ et $\equiv 0 \pmod{ABD \text{ etc.}}$, etc. Tunc si numerus z desideratur, qui secundum modulos A, B, C, D etc. numeris a, b, c, d etc. respective sit congruus, poni poterit

$$z \equiv \alpha a + \mathfrak{b} b + \gamma c + \mathfrak{d} d \text{ etc.} \pmod{ABCD \text{ etc.}}.$$

Manifesto enim, $\alpha a \equiv a \pmod A$; reliqua autem membra $\mathfrak{b} b$, γc etc. omnia $\equiv 0 \pmod A$: quare $z \equiv a \pmod A$. Similiter de reliquis modulis demonstratio adornatur. Haec solutio priori praeferenda, quando plura huiusmodi problemata sunt solvenda, pro quibus moduli A, B, C etc. valores suos retinent; tunc enim numeri $\alpha, \mathfrak{b}, \gamma$ etc., valores constantes nanciscuntur. Hoc usu venit in problemate chronologico ubi quaeritur, quotus in periodo Juliana sit annus, cuius indictio, numerus aureus, et cyclus solaris dantur. Hic $A = 15$, $B = 19$, $C = 28$; quare,

quum valor expressionis $\frac{1}{19 \cdot 28} \pmod{15}$, sive $\frac{1}{532} \pmod{15}$, sit 13, erit $\alpha = 6916$. Similiter pro $\mathfrak{b}$ invenitur 4200, et pro γ 4845, quare numerus quaesitus erit residuum minimum numeri $6916a + 4200b + 4845c$, denotantibus a indictionem, b numerum aureum, c cyclum solarem.

Congruentiae lineares quae plures incognitas implicant.

37.

Haec de congruentiis primi gradus unicam incognitam continentibus sufficiant. Superest ut de congruentiis agamus, in quibus plures incoguitae sunt permixtae. At quoniam hoc caput, si omni rigore singula exponere velimus, sine prolixitate absolvi non potest, propositumque hoc loco nobis non est, omnia exhaurire, sed ea tantum tradere, quae attentione digniora videantur: hic ad paucas observationes investigationem restringimus, uberiorem huius rei expositionem ad aliam occasionem nobis reservantes.

1) Simili modo, ut in aequationibus, perspicitur, etiam hic totidem congruentias haberi debere, quot sint incognitae determinandae.

2) Propositae sint igitur congruentiae

$$\begin{aligned} ax + by + cz \ldots &\equiv f \pmod m \quad \ldots \quad (A) \\ a'x + b'y + c'z \ldots &\equiv f' \quad \ldots \quad (A') \\ a''x + b''y + c''z \ldots &\equiv f'' \quad \ldots \quad (A'') \\ &\text{etc.} \end{aligned}$$

totidem numero, quot sunt incognitae x, y, z etc.

Iam determinentur numeri ξ, ξ', ξ'' etc. ita ut sit

$$\begin{aligned} b\xi + b'\xi' + b''\xi'' + \text{etc.} &= 0 \\ c\xi + c'\xi' + c''\xi'' + \text{etc.} &= 0 \\ &\text{etc.} \end{aligned}$$

et quidem ita ut omnes sint integri nullumque factorem communem habeant, quod fieri posse ex theoria aequationum linearium constat. Simili modo determinentur v, v', v'' etc., ζ, ζ', ζ'' etc. etc. ita ut sit

$$\begin{aligned} av + a'v' + a''v'' + \text{etc.} &= 0 \\ cv + c'v' + c''v'' + \text{etc.} &= 0 \\ &\text{etc.} \end{aligned}$$

$$a\zeta + a'\zeta' + a''\zeta'' + \text{etc.} \equiv 0$$
$$b\zeta + b'\zeta' + b''\zeta'' + \text{etc.} \equiv 0$$
$$\text{etc.} \quad \text{etc.}$$

3) Manifestum est si congruentiae A, A', A'' etc. per ξ, ξ', ξ'' etc., tum per v, v', v'', etc. etc. multiplicentur, tuncque addantur, has congruentias proventuras esse:

$$(a\xi + a'\xi' + a''\xi'' + \text{etc.})x \equiv f\zeta + f'\xi' + f''\xi'' + \text{etc.}$$
$$(bv + b'v' + b''v'' + \text{etc.})y \equiv fv + f'v' + f''v'' + \text{etc.}$$
$$(c\zeta + c'\zeta' + c''\zeta'' + \text{etc.})z \equiv f\zeta + f'\zeta' + f''\zeta'' + \text{etc.}$$
$$\text{etc.}$$

quas brevitatis gratia ita exhibemus:

$$\Sigma(a\xi)x \equiv \Sigma(f\xi), \quad \Sigma(bv)y \equiv \Sigma(fv), \quad \Sigma(c\zeta)z \equiv \Sigma(f\zeta) \quad \text{etc.}$$

4) Iam plures casus sunt distinguendi.

Primo quando omnes incognitarum coefficientes $\Sigma(a\xi)$, $\Sigma(av)$ etc. ad congruentiarum modulum m sunt primi, hae congruentiae secundum praecepta ante tradita solvi possunt, problematisque solutio completa per congruentias formae $x \equiv p \pmod m$, $y \equiv q \pmod m$ etc. exhibebitur*). *E.g.* Si proponuntur congruentiae

$$x + 3y + z \equiv 1, \quad 4x + y + 5z \equiv 7, \quad 2x + 2y + z \equiv 3 \pmod 8$$

invenietur $\xi = 9$, $\xi' = 1$, $\xi'' = -14$, unde fit $-15x \equiv -26$, quare $x \equiv 6 \pmod 8$; eodem modo invenitur $15y \equiv -4$, $15z \equiv 1$, et hinc $y \equiv 4$, $z \equiv 7 \pmod 8$.

5) *Secundo* quando non omnes coefficientes $\Sigma(a\xi)$, $\Sigma(bv)$ etc. ad modulum sunt primi, sint α, β, γ etc. divisores communes maximi ipsius m cum $\Sigma(a\xi)$, $\Sigma(bv)$, $\Sigma(c\zeta)$ etc. resp., patetque problema impossibile esse, nisi illi numeros $\Sigma(f\xi)$, $\Sigma(fv)$, $\Sigma(f\zeta)$ etc. resp. metiantur. Quando vero hae conditiones locum habent, congruentiae in (3) complete resolventur per tales $x \equiv p \pmod{\frac{m}{\alpha}}$, $y \equiv q \pmod{\frac{m}{\beta}}$, $z \equiv r \pmod{\frac{m}{\gamma}}$ etc., aut si mavis dabuntur α valores diversi ipsius x (i. e. secundum m incongrui puta $p, p + \frac{m}{\alpha} \ldots p + \frac{(\alpha-1)m}{\alpha}$),

*) Observare convenit hancce conclusionem demonstratione egere, quam autem hic supprimimus. Proprie enim nihil aliud ex analysi nostra sequitur, quam quod congruentiae propositae per alios incognitarum x, y etc. valores solvi nequeant: hos vero satisfacere non sequitur. Fieri enim posset ut nulla omnino solutio daretur. Similis paralogismus etiam in aequationum linearium explicatione plerumque committitur.

β valores diversi ipsius y etc., illis congruentiis satisfacientes: manifestoque omnes solutiones congruentiarum propositarum (si quae omnino dantur) inter illas reperientur. Attamen hanc conclusionem convertere non licet; nam plerumque non omnes combinationes omnium α valorum ipsius x cum omnibus ipsius y cum omnibus ipsius z etc. problemati satisfaciunt, sed quaedam tantum, quarum nexum per unam pluresve congruentias conditionales exhibere licet. At quum completa huius problematis resolutio ad sequentia non sit necessaria, hoc argumentum fusius hoc loco non exsequimur, exemploque ideam qualemcunque de eo dedisse sat habemus.

Propositae sint congruentiae

$$3x + 5y + z \equiv 4, \quad 2x + 3y + 2z \equiv 7, \quad 5x + y + 3z \equiv 6 \pmod{12}$$

Hic fiunt ξ, ξ', ξ''; v, v', v''; ζ, ζ', ζ''; resp. $\equiv 1, -2, 1$; $1, 1, -1$; $-13, 22, -1$, unde $4x \equiv -4, 7y \equiv 5, 28z \equiv 96$. Hinc prodeunt quatuor valores ipsius x puta $\equiv 2, 5, 8, 11$; unus valor ipsius y puta $\equiv 11$; quatuor valores ipsius z puta $\equiv 0, 3, 6, 9 \pmod{12}$. Iam ut sciamus, quasnam combinationes valorum ipsius x cum valoribus ipsius z adhibere liceat, substituimus in congruentiis propp. pro x, y, z resp. $2 + 3t, 11, 3u$, unde transeunt in has

$$57 + 9t + 3u \equiv 0, \quad 30 + 6t + 6u \equiv 0, \quad 15 + 15t + 9u \equiv 0 \pmod{12}$$

quibus facile intelligitur aequivalere has

$$19 + 3t + u \equiv 0, \quad 10 + 2t + 2u \equiv 0, \quad 5 + 5t + 3u \equiv 0 \pmod 4$$

Prima manifesto requirit ut sit $u \equiv t + 1 \pmod 4$, quo valore in reliquis substituto etiam his satisfieri invenitur. Hinc colligitur, valores ipsius x hos 2, 5, 8, 11 (qui prodeunt statuendo $t \equiv 0, 1, 2, 3$) necessario combinandos esse cum valoribus ipsius z his $z \equiv 3, 6, 9, 0$ resp., ita ut omnino quatuor solutiones habeantur

$$x \equiv 2, 5, 8, 11 \pmod{12}$$
$$y \equiv 11, 11, 11, 11$$
$$z \equiv 3, 6, 9, 0$$

* * *

His disquisitionibus, per quas sectionis propositum iam absolutum est, adhuc quasdam propositiones similibus principiis innixas adiungimus, quibus in sequentibus frequenter opus erit.

Theoremata varia.

38.

Problema. *Invenire, quot numeri positivi dentur numero positivo dato A minores simulque ad ipsum primi.*

Designemus brevitatis gratia multitudinem numerorum positivorum ad numerum datum primorum ipsoque minorum per praefixum characterem ϕ. Quaeritur itaque ϕA.

I. Quando A est primus, manifestum est omnes numeros ab 1 usque ad $A-1$ ad A primos esse; quare in hoc casu erit

$$\phi A = A - 1$$

II. Quando A est numeri primi potestas puta $= p^m$, omnes numeri per p divisibiles ad A non erunt primi, reliqui erunt. Quamobrem de $p^m - 1$ numeris hi sunt reiiciendi: $p, 2p, 3p \ldots (p^{m-1}-1)p$; remanent igitur $p^m - 1 - (p^{m-1}-1)$ sive $p^{m-1}(p-1)$. Hinc

$$\phi p^m = p^{m-1}(p-1)$$

III. Reliqui casus facile ad hos reducuntur ope sequentis propositionis: *Si A in factores M, N, P etc. inter se primos est resolutus, erit*

$$\phi A = \phi M . \phi N . \phi P \text{ etc.}$$

quae ita demonstratur. Sint numeri ad M primi ipsoque M minores m, m', m'' etc. quorum itaque multitudo $= \phi M$. Similiter sint numeri ad N, P etc. respective primi ipsisque minores n, n', n'' etc.; p, p', p'' etc. etc., quorum multitudo $\phi N, \phi P$ etc. Iam constat omnes numeros ad productum A primos etiam ad factores singulos M, N, P etc. primos fore et vice versa (art. 19); porro omnes numeros qui horum m, m', m'' etc. alicui sint congrui secundum modulum M ad M primos fore et vice versa, similiterque de N, P etc. Quaestio itaque huc reducta est: determinare quot dentur numeri infra A, qui secundum modulum M, alicui numerorum m, m', m'' etc. secundum N, alicui ex his n, n', n'' etc. etc. sint congrui. Sed ex art. 32 sequitur, omnes numeros, secundum singulos modulos M, N, P etc. residua determinata dantes, congruos secundum eorum productum A fore, adeoque infra A unicum tantum dari, secundum singulos M, N, P etc. residuis datis congruum. Quare numerus quaesitus aequalis erit numero combinationum singulorum numerorum m, m', m'' cum singulis n, n', n'' atque p, p', p'' etc. etc. Hunc vero esse $= \phi M . \phi N . \phi P$ etc. ex theoria combinationum constat. *Q. E. D.*

IV. Iam quomodo hoc ad casum de quo agimus applicandum sit facile intelligitur. Resolvatur A in factores suos primos sive reducatur ad formam $a^\alpha b^\beta c^\gamma$ etc. designantibus a, b, c etc. numeros primos diversos. Tum erit

$$\phi A = \phi a^\alpha . \phi b^\beta . \phi c^\gamma \text{ etc.} = a^{\alpha-1}(a-1)\, b^{\beta-1}(b-1)\, c^{\gamma-1}(c-1) \text{ etc.}$$

seu concinnius

$$\phi A = A \frac{a-1}{a} . \frac{b-1}{b} . \frac{c-1}{c} \text{ etc.}$$

Exempl. Sit $A = 60 = 2^2 . 3 . 5$, adeoque $\phi A = \frac{1}{2} . \frac{2}{3} . \frac{4}{5} . 60 = 16$. Numeri hi ad 60 primi sunt 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

Solutio prima huius problematis exstat in commentatione ill. Euleri, *theoremata arithmetica nova methodo demonstrata*, Comm. nov. Ac. Petrop. VIII p. 74. Demonstratio postea repetita est in alia diss. *Speculationes circa quasdam insignes proprietates numerorum*, Acta Petrop. VIII p. 17.

39.

Si characteris ϕ significatio ita determinatur, ut ϕA exprimat multitudinem numerorum ad A primorum ipsoque A *non maiorum*, perspicuum est $\phi 1$ fore non amplius $= 0$, sed $= 1$, in omnibus reliquis casibus nihil hinc immutari. Hancce definitionem adoptantes sequens habebimus theorema.

Si a, a', a'' etc. sunt omnes divisores ipsius A (unitate et ipso A non exclusis), erit

$$\phi a + \phi a' + \phi a'' + \text{etc.} = A$$

Ex. sit $A = 30$, tum erit $\phi 1 + \phi 2 + \phi 3 + \phi 5 + \phi 6 + \phi 10 + \phi 15 + \phi 30 = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$.

Demonstr. Multiplicentur omnes numeri ad a primi ipsoque a non maiores per $\frac{A}{a}$, similiter omnes ad a' primi per $\frac{A}{a'}$ etc., habebunturque $\phi a + \phi a'$

$+\phi a''+$ etc. numeri, omnes ipso A non maiores. At 1) omnes hi numeri erunt inaequales. Omnes enim eos qui ex *eodem* ipsius A divisore sint generati, inaequales fore, per se clarum. Si vero e divisoribus diversis M, N numerisque μ, ν ad istos respective primis aequales prodiissent, i. e. si esset $\frac{A}{M}\mu = \frac{A}{N}\nu$, sequeretur $\mu N = \nu M$. Ponatur $M > N$ (id quod licet). Quoniam M ad μ est primus, atque numerum μN metitur, etiam ipsum N metietur, maior minorem. *Q. E. A.*

2) inter hos numeros, omnes hi $1, 2, 3 \ldots A$ invenientur. Sit numerus quicunque ipsum A non superans t, maxima numerorum A, t communis mensura δ eritque $\frac{A}{\delta}$ divisor ipsius A, ad quem $\frac{t}{\delta}$ primus. Manifesto hinc numerus t inter eos invenietur qui ex divisore $\frac{A}{\delta}$ prodierunt.

3) Hinc colligitur horum numerorum multitudinem esse A, quare

$$\phi a + \phi a' + \phi a'' + \text{etc.} = A. \quad Q.\ E.\ D.$$

40.

Si maximus numerorum A, B, C, D etc. divisor communis $= \mu$; numeri a, b, c, d etc. ita determinari possunt, ut sit

$$aA + bB + cC + \text{etc.} = \mu.$$

Dem. Consideremus primo duos tantum numeros A, B, sitque horum divisor maximus communis $= \lambda$. Tum congruentia $Ax \equiv \lambda \pmod{B}$ erit resolubilis (art. 30). Sit radix $= \alpha$, ponaturque $\frac{\lambda - A\alpha}{B} = \overline{\alpha}$. Tum erit $\alpha A + \overline{\alpha} B = \lambda$, uti desiderabatur.

Accedente numero tertio C, sit maximus divisor communis numerorum λ, C. $= \lambda'$, eritque hic simul maximus divisor communis numerorum A, B, C*). Determinentur numeri k, γ ita ut sit $k\lambda + \gamma C = \lambda'$, eritque $k\alpha A + k\overline{\alpha} B + \gamma C = \lambda'$.

Accedente numero quarto D, ponatur maximus divisor communis numerorum λ', D (quem simul esse maximum divisorem communem numerorum A, B, C, D facile perspicitur) $= \lambda''$, fiatque $k'\lambda' + \delta D = \lambda''$. Tum erit $kk'\alpha A + kk'\overline{\alpha} B + k'\gamma C + \delta D = \lambda''$.

*) Metietur enim manifesto λ' omnes A, B, C. Si vero non esset divisor communis *maximus*: maximus foret maior quam λ'. Iam quoniam hic divisor maximus metitur ipsos A, B, C, metietur etiam ipsum $k\alpha A + k\overline{\alpha} B + \gamma C$ i. e. ipsum λ', maior minorem. *Q. E. A.* — Facilius adhuc hoc ex art. 18 deduci potest.

Simili modo procedi potest, quotcunque alii numeri accedant.

Si itaque numeri A, B, C, D etc. divisorem communem non habent, patet fieri posse

$$aA + bB + cC + \text{etc.} = 1$$

41.

Si p est numerus primus atque habentur p res, inter quas quotcunque aequales esse possunt, modo non omnes sint aequales: numerus permutationum harum rerum per p erit divisibilis.

Ex. Quinque res A, A, A, B, B decem modis diversis possunt transponi.

Demonstratio huius theorematis facile quidem ex nota permutationum theoria peti potest. Si enim inter has res sunt primo a aequales nempe $= A$, tum b aequales nempe $= B$, tum c aequales nempe $= C$ etc. (ubi numeri a, b, c etc. etiam unitatem designare possunt), ita ut habeatur

$$a + b + c + \text{etc.} = p$$

numerus permutationum erit

$$= \frac{1.2.3.\ldots.p}{1.2.3\ldots a.1.2\ldots b.1.2\ldots c \text{ etc.}}$$

Iam per se clarum est, huius fractionis numeratorem per denominatorem divisibilem esse, quoniam numerus permutationum debet esse integer: at numerator per p divisibilis est, denominator vero, qui ex factoribus ipso p minoribus est compositus, per p non divisibilis (art. 15). Quare numerus permutationum per p erit divisibilis (art. 19).

Speramus tamen fore quibus etiam sequens demonstratio haud ingrata sit futura.

Quando in duabus permutationibus rerum e quibus compositae sunt ordo in eo tantum discrepat, ut ea res quae in altera primum locum occupat, aliam sedem in altera teneat, reliquae autem eodem in utraque ordine progrediuntur, eamque quae in altera ultima est, ea quae est prima, in altera excipit; *permutationes similes* vocemus*). Ita in ex. nostro permutationes $ABAAB$ et $ABABA$ similes erunt, quoniam res quae in priori primum secundum etc. locum occupant, in posteriori loco tertio quarto etc. eodem ordine sunt collocatae.

*) Si permutationes similes in circulum scriptae esse concipiuntur ita ut ultima res primae fiat contigua, nulla omnino erit discrepantia, quoniam nullus locus primus aut ultimus vocari poterit.

Iam quoniam quaeque permutatio ex p rebus constat, patet cuivis $p-1$ similes adinveniri posse, si ea res quae prima fuerat, ad secundum, tertium etc. locum promoveatur. Quarum si nullae identicae esse possunt manifestum est, omnium permutationum numerum per p divisibilem evadere, quippe qui p vicibus maior sit quam numerus omnium permutationum dissimilium. Supponamus igitur duas permutationes

$$PQ\ldots TV\ldots YZ; \qquad V\ldots YZPQ\ldots T$$

quarum altera ex altera per terminorum promotionem orta sit, identicas esse sive $P=V$ etc. Sit terminus P qui in priori est primus, $n+1^{\text{tus}}$ in posteriori. Erit igitur in serie posteriori terminus $n+1^{\text{tus}}$ aequalis primo, $n+2^{\text{tus}}$ secundo etc. unde $2n+1^{\text{tus}}$ rursus primo aequalis evadet, eademque ratione $3n+1^{\text{tus}}$ etc.; generaliterque terminus $kn+m^{\text{tus}}$ m^{to} (ubi quando $kn+m$ ipsum p superat, aut series $V\ldots YZPQ\ldots T$ semper ab initio repeti concipienda est, aut a $kn+m$ multiplum ipsius p proxime minus rescindendum). Quamobrem si k ita determinatur, ut fiat $kn\equiv 1 \pmod p$, quod fieri potest quia p primus, sequitur generaliter terminum m^{tum} $m+1^{\text{to}}$ aequalem esse, sive quemvis terminum sequenti, *i. e.* omnes terminos aequales esse contra hypothesin.

42.

Si coefficientes $A, B, C\ldots N$; $a, b, c\ldots n$ *duarum functionum formae*

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} \ldots + N \quad (P)$$
$$x^\mu + ax^{\mu-1} + bx^{\mu-2} + cx^{\mu-3} \ldots + n \quad (Q)$$

omnes sunt rationales, neque vero omnes integri, productumque ex (P) *et* (Q)

$$= x^{m+\mu} + \mathfrak{A}x^{m+\mu-1} + \mathfrak{B}x^{m+\mu-2} + \text{etc.} + \mathfrak{Z}$$

omnes coefficientes $\mathfrak{A}, \mathfrak{B}\ldots\mathfrak{Z}$ *integri esse nequeunt.*

Demonstr. Exprimantur omnes fractiones in coefficientibus A, B etc. a, b etc. per numeros quam minimos, eligaturque ad libitum numerus primus p, qui aliquem aut plures ex denominatoribus harum fractionum metiatur. Ponamus, id quod licet, p metiri denominatorem alicuius coefficientis fracti in (P), patetque si (Q) per p dividatur, etiam in $\frac{(Q)}{p}$ dari ad minimum unum coefficientem fractum cuius denominator implicet factorem p (puta coefficientem primum $\frac{1}{p}$).

Iam facile perspicitur, in (P) datum iri terminum unum, fractum, cuius denominator involvat *plures* dimensiones ipsius p quam denominatores omnium similium praecedentium, et *non pauciores* quam denominatores omnium sequentium; sit hic terminus $= Gx^\vartheta$, et multitudo dimensionum ipsius p in denominatore ipsius G, $= t$. Similis terminus dabitur in $\frac{(Q)}{p}$ qui sit $= \Gamma x^\gamma$ et multitudo dimensionum ipsius p in denominatore ipsius Γ, $= \tau$. Manifesto hic erit $t+\tau$ ad minimum $=2$. His ita praeparatis, terminus $x^{\vartheta+\gamma}$ producti ex (P) et (Q) coefficientem habebit fractum, cuius denominator $t+\tau-1$ dimensiones ipsius p involvet, id quod ita demonstratur.

Sint termini qui in (P) terminum Gx^ϑ praecedunt, $'Gx^{\vartheta+1}$, $''Gx^{\vartheta+2}$ etc. sequentes vero $G'x^{\vartheta-1}$, $G''x^{\vartheta-2}$ etc.; similiterque in $\frac{(Q)}{p}$ praecedant terminum Γx^γ termini $'\Gamma x^{\gamma+1}$, $''\Gamma x^{\gamma+2}$ etc. sequantur autem termini $\Gamma' x^{\gamma-1}$, $\Gamma'' x^{\gamma-2}$ etc. Tum constat in producto ex (P), $\frac{(Q)}{p}$ coefficientem termini $x^{\vartheta+\gamma}$ fore

$$= G\Gamma + {}'G\Gamma + {}''G\Gamma + \text{etc.}$$
$$+ {}'\Gamma G' + {}''\Gamma G'' + \text{etc.}$$

Pars $G\Gamma$ erit fractio quae si per numeros quam minimos exprimitur in denominatore $t+\tau$ dimensiones ipsius p involvit, reliquae autem partes si sunt fractae, in denominatore pauciores dimensiones numeri p implicabunt, quoniam omnes sunt producta e binis factoribus quorum alter non plures quam t, alter vero pauciores quam τ dimensiones ipsius p implicat; vel alter non plures quam τ, alterque pauciores quam t. Hinc $G\Gamma$ erit formae $\frac{e}{fp^{t+\tau}}$ reliquarum vero summa formae $\frac{e'}{f'p^{t+\tau-\delta}}$ ubi δ positivus et e, f, f' a factore p liberi: quare omnium summa erit $= \frac{ef'+e'fp^\delta}{ff'p^{t+\tau}}$ cuius numerator per p non divisibilis, adeoque denominator per nullam reductionem pauciores dimensiones quam $t+\tau$ obtinere potest. Hinc coefficiens termini $x^{\vartheta+\gamma}$ in producto ex (P), (Q) erit

$$= \frac{ef'+e'fp^\delta}{ff'p^{t+\tau-1}}$$

i. e. fractio cuius denominator $t+\tau-1$ dimensiones ipsius p implicat. *Q. E. D.*

43.

Congruentia m^{ti} gradus

$$Ax^m + Bx^{m-1} + Cx^{m-2} + etc. + Mx + N \equiv 0$$

cuius modulus est numerus primus p, ipsum A non metiens, pluribus quam m modis diversis solvi non potest, sive plures quam m radices secundum p incongruas non habet (Vid. artt. 25, 26).

Si quis neget, ponamus dari congruentias diversorum graduum m, n etc. quae plures quam m, n etc. radices habeant, sitque minimus gradus m, ita ut omnes similes congruentiae inferiorum graduum theoremati nostro sint consentaneae. Quod quum de primo gradu iam supra sit demonstratum (art. 26), manifestum est, m fore aut $= 2$ aut maiorem. Admittet itaque congruentia

$$Ax^m + Bx^{m-1} + \text{etc.} + Mx + N \equiv 0$$

saltem $m+1$ radices, quae sint $x \equiv \alpha, x \equiv \vec{6}, x \equiv \gamma$ etc., ponamusque id quod licet omnes numeros $\alpha, \vec{6}, \gamma$ etc. esse positivos et minores quam p, omniumque minimum α. Iam in congruentia proposita substituatur pro x, $y + \alpha$, transeatque inde in hanc

$$A'y^m + B'y^{m-1} + C'y^{m-2} \ldots + My + N \equiv 0$$

Tum manifestum est, huic congruentiae satisfieri, si ponatur $y \equiv 0$, aut $\equiv \vec{6} - \alpha$, aut $\equiv \gamma - \alpha$ etc., quae radices omnes erunt diversae, numerusque earum $= m+1$. At ex eo quod $y \equiv 0$ est radix, sequitur, N' per p divisibilem fore. Quare etiam haec expressio

$$y(A'y^{m-1} + B'y^{m-2} + \text{etc.} + M') \text{ fiet } \equiv 0 \pmod{p},$$

si ipsi y unus ex m valoribus $\vec{6} - \alpha, \gamma - \alpha$ etc. tribuitur, qui omnes sunt > 0 et $< p$, adeoque in omnibus hisce casibus etiam

$$A'y^{m-1} + B'y^{m-2} + \text{etc.} + M' \text{ fiet } \equiv 0 \text{ (art. 22)}$$

i. e. congruentia $$A'y^{m-1} + B'y^{m-2} + \text{etc.} + M' \equiv 0$$

quae est gradus $m-1^{ti}$, m radices habet et proin theoremati nostro adversatur (patet enim facile, A' fore $= A$, adeoque per p non divisibilem, uti requiritur) licet supposuerimus, omnes congruentias inferioris gradus quam m^{ti}, theoremati consentire. *Q. E. A.*

44.

Quamvis hic supposuerimus, modulum p non metiri coefficientem termini summi, tamen theorema ad hunc casum non restringitur. Si enim primus coefficiens sive etiam aliqui sequentium per p divisibiles essent, hi termini tuto reiici possent, congruentiaque tandem ad inferiorem graduum deprimeretur, ubi coefficiens primus per p non amplius foret divisibilis, siquidem non omnes coefficientes per p dividi possunt; in quo casu congruentia foret identica atque incognita prorsus indeterminata.

Theorema hoc primum ab ill. La Grange propositum atque demonstratum est (*Mém. de l'Ac. de Berlin, Année* 1768 *p.* 192). Exstat etiam in dissert. ill. Le Gendre, *Recherches d'Analyse indéterminée, Hist. de l'Acad. de Paris* 1785 *p.* 466. Ill. Euler in *Nov. Comm. Ac. Petr.* XVIII *p.* 93 demonstravit congruentiam $x^n - 1 \equiv 0$ plures quam n radices diversas habere non posse. Quae quamvis sit particularis, tamen methodus qua vir summus usus est omnibus congruentiis facile adaptari potest. Casum adhuc magis limitatum iam antea absolverat, *Comm. nov. Ac. Petr.* V *p.* 6, sed haec methodus generaliter adhiberi nequit. Infra Sect. VIII alio adhuc modo theorema demonstrabimus; at quantumvis diversae primo aspectu omnes hae methodi videri possint, periti qui comparare eas voluerint facile certiores fient omnes eidem principio superstructas esse. Ceterum quum hoc theorema hic tantum tamquam lemma sit considerandum, neque completa expositio huc pertineat: de modulis compositis seorsim agere supersedemus.

SECTIO TERTIA

DE

RESIDUIS POTESTATUM.

Residua terminorum progressionis geometricae ab unitate incipientis constituunt seriem periodicam.

45.

THEOREMA. *In omni progressione geometrica* $1, a, aa, a^3$ *etc. praeter primum* 1, *alius adhuc datur terminus* a^t, *secundum modulum* p *ad* a *primum unitati congruus, cuius exponens* $t < p$.

Demonstr. Quoniam modulus p ad a, adeoque ad quamvis ipsius a potestatem est primus, nullus progressionis terminus erit $\equiv 0 \pmod{p}$, sed quivis alicui ex his numeris $1, 2, 3 \ldots p-1$ congruus. Quorum multitudo quum sit $p-1$, manifestum est, si plures quam $p-1$ progressionis termini considerentur, omnes residua minima diversa habere non posse. Quocirca inter terminos $1, a, aa, a^3 \ldots a^{p-1}$ bini ad minimum congrui invenientur. Sit itaque $a^m \equiv a^n$ et $m > n$, fietque dividendo per a^n, $a^{m-n} \equiv 1$ (art. 22) ubi $m-n < p$, et > 0. *Q. E. D.*

Ex. In progressione 2, 4, 8 etc. terminus primus qui secundum modulum 13 unitati est congruus, invenitur $2^{12} = 4096$. At secundum modulum 23 in eadem progressione fit $2^{11} = 2048 \equiv 1$. Similiter numeri 5 potestas sexta, 15625, unitati congrua secundum modulum 7, quinta vero, 3125, secundum 11. In aliis igitur casibus potestas exponentis minoris quam $p-1$ unitati congrua evadit, in aliis contra usque ad potestatem $p-1^{\text{tam}}$ ascendere necesse est.

46.

Quando progressio ultra terminum qui unitati est congruus continuatur, eadem quae ab initio habebantur residua prodeunt iterum. Scilicet si $a^t \equiv 1$. erit $a^{t+1} \equiv a$, $a^{t+2} \equiv aa$ etc. donec ad terminum a^{2t} perveniatur, cuius residuum minimum iterum erit $\equiv 1$, atque residuorum *periodum* denuo inchoat. Habetur itaque periodus t residua comprehendens, quae simulac finita est ab initio semper repetitur; neque alia residua quam quae in hac periodo continentur in tota progressione occurrere possunt. Generaliter erit $a^{mt} \equiv 1$, et $a^{mt+n} \equiv a^n$, id quod per designationem nostram ita exhibetur:

Si $r \equiv \rho \pmod{t}$, *erit* $a^r \equiv a^\rho \pmod{p}$.

47.

Petitur ex hoc theoremate compendium potestatum quantumvis magno exponente affectarum residua expedite inveniendi, simulac potestas unitati congrua innotescat. Si *ex. gr.* residuum e divisione potestatis 3^{1000} per 13 oriundum quaeritur, erit propter $3^3 \equiv 1 \pmod{13}$, $t \equiv 3$; quare quum sit $1000 \equiv 1 \pmod{3}$, erit $3^{1000} \equiv 3 \pmod{13}$.

48.

Quando a^t est *infima* potestas unitati congrua (praeter $a^0 = 1$, ad quem casum hic non respicimus), illi t termini, residuorum periodum constituentes omnes erunt diversi, uti ex demonstratione art. 45 nullo negotio perspicitur. Tum autem propositio art. 46 converti potest; scilicet si $a^m \equiv a^n \pmod{p}$, erit $m \equiv n \pmod{t}$. Si enim m, n secundum modulum t incongrui essent, residua eorum minima μ, ν diversa forent. At $a^m \equiv a^\mu$, $a^n \equiv a^\nu$, quare $a^\mu \equiv a^\nu$ *i. e.* non omnes potestates infra a^t incongruae forent contra hypoth.

Si itaque $a^k \equiv 1 \pmod{p}$, erit $k \equiv 0 \pmod{t}$ *i. e.* k per t divisibilis.

Hactenus de modulis quibuscunque si modo ad a sint primi diximus. Iam modulos qui sunt numeri absolute primi seorsim consideremus atque huic fundamento investigationem generaliorem postea superstruamus.

Considerantur primo moduli qui sunt numeri primi.

49.

THEOREMA. *Si p est numerus primus ipsum a non metiens, atque a^t infima ipsius a potestas secundum modulum p unitati congrua, exponens t aut erit $= p-1$ aut pars aliquota huius numeri.*

Conferantur exempla art. 15.

Demonstr. Quum iam ostensum sit, t esse aut $= p-1$, aut $< p-1$, superest, ut in posteriori casu t semper ipsius $p-1$ partem aliquotam esse evincatur.

I. Colligantur residua minima positiva omnium horum terminorum $1, a, aa \ldots a^{t-1}$, quae per $\alpha, \alpha', \alpha''$ etc. designentur, ita ut sit $\alpha = 1, \alpha' \equiv a, \alpha'' \equiv aa$ etc. Perspicuum est, haec omnia fore diversa, si enim duo termini a^m, a^n eadem praeberent, foret (supponendo $m > n$) $a^{m-n} \equiv 1$ atque $m - n < t$, *Q. E. A.* quum nulla inferior potestas quam a^t unitati sit congrua (*hyp.*). Porro omnes $\alpha, \alpha', \alpha''$ etc. in serie numerorum $1, 2, 3 \ldots p-1$ continentur, quam tamen non exhaurient, quum $t < p-1$. Complexum omnium $\alpha, \alpha', \alpha''$ etc. per (A) designabimus. Comprehendet igitur (A) terminos t.

II. Accipiatur numerus quicunque ϑ ex his $1, 2, 3 \ldots p-1$, qui in (A) desit. Multiplicetur ϑ per omnes $\alpha, \alpha', \alpha''$ etc., sintque residua minima inde oriunda $\vartheta, \vartheta', \vartheta''$ etc., quorum numerus etiam erit t. At haec residua tum inter se quam ab omnibus $\alpha, \alpha', \alpha''$ etc. erunt diversa. Si enim *prior* assertio falsa esset, haberetur $\vartheta a^m \equiv \vartheta a^n$ adeoque dividendo per ϑ, $a^m \equiv a^n$, contra ea quae modo demonstravimus; si vero *posterior*, haberetur $\vartheta a^m \equiv a^n$, unde, quando $m < n$, $\vartheta \equiv a^{n-m}$ *i. e.* ϑ alicui ex his $\alpha, \alpha', \alpha''$ etc. congruus contra hyp.; quando vero $m > n$, sequitur multiplicando per a^{t-m}, $\vartheta a^t \equiv a^{t+n-m}$, sive propter $a^t \equiv 1$, $\vartheta \equiv a^{t+n-m}$, quae est eadem absurditas. Designetur complexus omnium $\vartheta, \vartheta', \vartheta''$ etc. quorum multitudo $= t$, per (B), habebunturque iam $2t$ numeri ex his $1, 2, 3 \ldots p-1$. Quodsi igitur (A) et (B) omnes hos numeros complectuntur, fit $\frac{p-1}{2} = t$, adeoque theorema demonstratum.

III. Si vero aliqui adhuc deficiunt, sit horum aliquis γ. Per hunc multiplicentur omnes $\alpha, \alpha', \alpha''$ etc., productorumque residua minima sint $\gamma, \gamma', \gamma''$ etc.: omnium complexus per (C) designetur. (C) igitur comprehendet t numeros ex his $1, 2, 3 \ldots p-1$, qui omnes tum inter se quam a numeris in (A) et (B)

contentis erunt diversi. Assertiones priores eodem modo demonstrantur ut in II, tertia ita. Si esset $\gamma a^m \equiv \vartheta a^n$, fieret $\gamma \equiv \vartheta a^{n-m}$, aut $\equiv \vartheta a^{t+n-m}$ prout $m < n$, aut $> n$, in utroque casu γ alicui ex (B) congrua contra hyp. Habentur igitur $3t$ numeri ex his $1, 2, 3 \ldots p-1$, atque si nulli amplius desunt, fiet $t = \frac{p-1}{3}$, adeoque theorema erit demonstratum.

IV. Si vero etiamnum aliqui desunt, eodem modo ad quartum numerorum complexum (D) progrediendum erit etc. Patet vero quoniam numerorum $1, 2, 3 \ldots p-1$ multitudo est finita, tandem eam exhaustum iri, adeoque multiplum ipsius t fore: quare t erit pars aliquota numeri $p-1$. *Q. E. D.*

Fermatii Theorema.

50.

Quum igitur $\frac{p-1}{t}$ sit integer, sequitur evehendo utramque partem congruentiae $a^t \equiv 1$ ad potestatem exponentis $\frac{p-1}{t}$, $a^{p-1} \equiv 1$, *sive* $a^{p-1} - 1$ *semper per p divisibilis est, quando p est primus ipsum a non metiens.*

Theorema hoc quod tum propter elegantiam tum propter eximiam utilitatem omni attentione dignum, ab inventore *theorema Fermatianum* appellari solet. Vid. *Fermatii Opera Mathem. Tolosae* 1679 *fol. p.* 163. Demonstrationem inventor non adiecit, quam tamen in potestate sua esse professus est. Ill. Euler primus demonstrationem publici iuris fecit in diss. cui titulus *Theorematum quorundam ad numeros primos spectantium demonstratio, Comm. Acad. Petrop. T.* VIII*). Innititur ista evolutioni potestatis $(a+1)^p$, ubi ex coefficientium forma facillime deducitur $(a+1)^p - a^p - 1$ semper per p fore divisibilem, adeoque $(a+1)^p - (a+1)$ per p divisibilem fore, quando $a^p - a$ per p sit divisibilis. Iam quia $1^p - 1$ semper per p divisibilis est, etiam $2^p - 2$ semper erit; hinc etiam $3^p - 3$ etc., generaliterque $a^p - a$. Quodsi itaque p ipsum a non metitur, etiam $a^{p-1} - 1$ per p divisibilis erit. Haec sufficient ad methodi indolem declarandam. Clar. Lambert similem demonstrationem tradidit in *Actis Erudit.* 1769

*) In comment. anteriore vir summus ad scopum nondum pervenerat. *Comm. Petr. T.* VI *p.* 196. — In controversia famosa inter Maupertuis et König, a principio actionis minimae orta, sed mox ad res heterogeneas egressa, König in manibus se habere dixit autographum Leibnitianum, in quo demonstratio huius theorematis cum Euleriana prorsus consentiens contineatur. *Appel au public. p.* 196. Licet vero fidem huic testimonio denegare nolimus, certe Leibnitius inventum suum numquam publicavit. Conf. *Hist. de l'Ac. de Prusse, A.* 1750 *p.* 530.

p. 109. Quia vero evolutio potestatis binomii a theoria numerorum satis aliena esse videbatur, aliam demonstrationem ill. Euler investigavit quae exstat *Comment. nov. Petr.* T. VII p. 70, atque cum ea quam nos art. praec. exposuimus prorsus convenit. In sequentibus adhuc aliae quaedam se nobis offerent. Hoc loco unam superaddere liceat, quae similibus principiis innititur, uti prima ill. Euleri. Propositio sequens, cuius casus tantum particularis est theorema nostrum, etiam ad alias investigationes infra adhibebitur.

51.

Polynomii $a+b+c+$ *etc. potestas* p^{ta} *secundum modulum* p *est*

$$\equiv a^p+b^p+c^p+\text{etc.}$$

siquidem p *est numerus primus.*

Demonstr. Constat potestatem p^{tam} polynomii $a+b+c+$ etc. esse compositam e partibus formae $\varkappa a^\alpha b^\beta c^\gamma$ etc. ubi $\alpha+\beta+\gamma$ etc. $=p$, et $\varkappa$ designat, quot modis p res, quarum α, β, γ etc. respective sunt $=a, b, c$ etc. permutari possint. At supra art. 41 ostendimus, hunc numerum semper esse per p divisibilem, nisi omnes res sint aequales, *i. e.* nisi aliquis numerorum α, β, γ etc. sit $=p$ reliqui vero $=0$. Unde sequitur omnes ipsius $(a+b+c+\text{etc.})^p$ partes, praeter has a^p, b^p, c^p etc., per p divisibiles esse; quae igitur quando de congruentia secundum modulum p agitur, tuto omitti poterunt, fietque

$$(a+b+c+\text{etc.})^p \equiv a^p+b^p+c^p+\text{etc.} \quad Q.\ E.\ D.$$

Quodsi iam omnes quantitates a, b, c etc. $=1$ ponuntur, numerusque earum $=k$, fiet $k^p \equiv k$ uti in art. praec.

Quot numeris respondeant periodi, in quibus terminorum multitudo est divisor datus numeri $p-1$.

52.

Quoniam igitur alii numeri quam qui sunt divisores ipsius $p-1$ nequeunt esse exponentes potestatum infimarum ad quas evecti numeri aliqui unitati congrui fiunt, quaestio sese offert, num omnes ipsius $p-1$ divisores ad hoc sint idonei, atque, quando omnes numeri per p non divisibiles secundum exponentem infimae suae potestatis unitati congruae classificentur, quot ad singulos exponentes sint perventuri. Ubi statim observare convenit, sufficere, si omnes numeri

positivi ab 1 usque ad $p-1$ considerentur; manifestum enim est, numeros congruos ad eandem potestatem elevari debere, quo unitati fiant congruae, adeoque numerum quemcunque ad eundem exponentem esse referendum ad quem residuum suum minimum positivum. Quocirca in id nobis erit incumbendum, ut quomodo hoc respectu numeri $1, 2, 3, \ldots p-1$ inter singulos factores numeri $p-1$ distribuendi sint eruamus. Brevitatis gratia, si d est unus e divisoribus numeri $p-1$ (ad quos etiam 1 et $p-1$ referendi), per ψd designabimus multitudinem numerorum positivorum ipso p minorum quorum potestas d^{ta} est infima unitati congrua.

53.

Quo facilius haec disquisitio intelligi possit, exemplum apponimus. Pro $p=19$ distribuentur numeri $1, 2, 3 \ldots 18$ inter divisores numeri 18 hoc modo:

1	1.
2	18.
3	7, 11.
6	8, 12.
9	4, 5, 6, 9, 16, 17.
18	2, 3, 10, 13, 14, 15.

In hoc igitur casu fit $\psi 1=1, \psi 2=1, \psi 3=2, \psi 6=2, \psi 9=6, \psi 18=6$. Ubi exigua attentio docet, totidem ad quemvis exponentem pertinere, quot dentur numeri hoc non maiores ad ipsumque primi, sive esse in hoc certe casu, retento signo art. 39, $\psi d=\phi d$. Hanc autem observationem generaliter veram esse ita demonstramus.

I. Si numerus aliquis habetur, a, ad exponentem d *pertinens* (*i. e.* cuius potestas d^{ta} unitati congrua, omnes inferiores incongruae), omnes huius potestates $aa, a^3, a^4, \ldots a^d$ sive ipsarum residua minima proprietatem priorem etiam possidebunt (ut potestas ipsarum d^{ta} unitati sit congrua) et quum hoc ita etiam exprimi possit, residua minima numerorum $a, aa, a^3 \ldots a^d$ (quae omnia sunt diversa) esse radices congruentiae $x^d \equiv 1$, haec autem plures quam d radices diversas habere nequeat, manifestum est, praeter numerorum $a, aa, a^3 \ldots a^d$ residua minima alios numeros inter 1 et $p-1$ incl. non dari quorum potestates ex-

ponentis d congruae sint unitati. Hinc patet omnes numeros ad exponentem d pertinentes inter residua minima numerorum $a, aa, a^3 \ldots a^d$ reperiri. Quales vero sint, quantaque eorum multitudo, ita definitur. Si k est numerus ad d primus, omnes potestates ipsius a^k, quarum exponentes $< d$, unitati non erunt congrui: esto enim $\frac{1}{k} \pmod d \equiv m$ (vid. art. 31) eritque $a^{km} \equiv a$; quare si potestas e^{ta} ipsius a^k unitati esset congrua atque $e < d$, foret etiam $a^{kme} \equiv 1$ et hinc $a^e \equiv 1$ contra hyp. Hinc manifestum est, residuum minimum ipsius a^k ad exponentem d pertinere. Si vero k divisorem aliquem, δ, cum d communem habet, ipsius a^k residuum minimum ad exponentem d non pertinet; quoniam tum potestas $\frac{d}{\delta}^{\text{ta}}$ iam unitati fit congrua (erit enim $\frac{kd}{\delta}$ per d divisibilis, sive $\equiv 0 \pmod d$ adeoque $a^{\frac{kd}{\delta}} \equiv 1$). Hinc colligitur, totidem numeros ad exponentem d pertinere quot numerorum $1, 2, 3 \ldots d$ ad d sint primi. At memorem esse oportet, hanc conclusionem innixam esse suppositioni, unum numerum a iam haberi ad exponentem d pertinentem. Quamobrem dubium remanet, fierine possit ut ad aliquem exponentem nullus omnino numerus pertineat; conclusioque eo limitatur ut ψd sit vel $= 0$ vel $= \phi d$.

54.

II. Iam sint omnes divisores numeri $p-1$ hi: d, d', d'' etc. eritque, quia omnes numeri $1, 2, 3 \ldots p-1$ inter hos sunt distributi,

$$\psi d + \psi d' + \psi d'' + \text{etc.} = p - 1$$

At in art. 40 demonstravimus esse

$$\phi d + \phi d' + \phi d'' + \text{etc.} = p - 1$$

atque ex art. praec. sequitur ψd ipsi ϕd aut aequalem aut ipso minorem esse, maiorem esse non posse, similiterque de $\psi d'$ et $\phi d'$, etc. Si itaque aliquis terminus ex his $\psi d, \psi d', \psi d''$ etc. termino respondente ex his $\phi d, \phi d', \phi d''$, esset minor (sive etiam plures) illorum summa summae horum aequalis esse non posset. Unde tandem concludimus ψd *ipsi* ϕd *semper esse aequalem*, adeoque a magnitudine ipsius $p-1$ non pendere.

55.

Maximam autem attentionem meretur casus particularis propositionis praecedentis scilicet *semper dari numeros quorum nulla potestas inferior quam* $p-1^{ta}$ *unitati congrua*, et quidem totidem inter 1 et $p-1$ quot infra $p-1$ sint numeri ad $p-1$ primi. Cuius theorematis demonstratio quum minime tam obvia sit quam primo aspectu videri possit, propter theorematis dignitatem liceat aliam adhuc adiicere a praecedente aliquantum diversam, quandoquidem methodorum diversitas ad res obscuriores illustrandas plurimum conferre solet. Resolvatur $p-1$ in factores suos primos fiatque $p-1 = a^\alpha b^\beta c^\gamma$ etc., designantibus a, b, c etc. numeros primos inaequales. Tum theorematis demonstrationem per sequentia absolvemus:

I. Semper inveniri posse numerum A (aut plures) ad exponentem a^α pertinentem, similiterque numeros B, C etc. ad exponentes b^β, c^γ etc., respective pertinentes.

II. Productum ex omnibus numeris A, B, C etc. (sive huius producti residuum minimum) ad exponentem $p-1$ pertinere. Haec autem ita demonstramus.

I. Sit g numerus aliquis ex his $1, 2, 3 \ldots p-1$, congruentiae $x^{\frac{p-1}{a}} \equiv 1 \pmod p$, *non* satisfaciens, omnes enim hi numeri congruentiae huic, cuius gradus $< p-1$, satisfacere nequeunt. Tum dico si potestas $\frac{p-1}{a^\alpha}^{\text{ta}}$ ipsius g ponatur $\equiv h$, hunc numerum, sive eius residuum minimum ad exponentem a^α pertinere.

Namque patet potestatem $a^{\alpha\,\text{tam}}$ ipsius h congruam fore potestati $p-1^{\text{tae}}$ ipsius g *i. e.* unitati, potestas vero $a^{\alpha-1\,\text{ta}}$ ipsius h congrua erit potestati $\frac{p-1}{a}^{\text{tae}}$ ipsius g, *i. e.* unitati erit incongrua, multoque minus potestates $a^{\alpha-2}, a^{\alpha-3\,\text{tae}}$ etc. ipsius h unitati congruae esse possunt. At exponens infimae potestatis ipsius h, unitati congruae, sive exponens ad quam pertinet h, numerum a^α metiri debet (art. 48). Quare quum a^α per alios numeros divisibilis non sit quam per se ipsum, atque per inferiores ipsius a potestates, necessario a^α erit exponens ad quem h pertinet. *Q. E. D.* Per similem methodum demonstratur, dari numeros ad exponentes b^β, c^γ etc. pertinentes.

II. Si supponimus, productum ex omnibus A, B, C etc. non ad exponentem $p-1$, sed ad minorem t pertinere, t ipsum $p-1$ metietur (art. 48), sive erit $\frac{p-1}{t}$ integer unitate maior. Facile autem perspicitur, hunc quotientem vel esse unum e numeris primis a, b, c etc. vel saltem per aliquem eorum divisibilem (art. 17), *ex. gr.* per a, de reliquis enim simile est ratiocinium.

Metietur itaque t ipsum $\frac{p-1}{a}$; quare productum ABC etc. etiam ad potestatem $\frac{p-1}{a}^{\text{tam}}$ elevatum unitati erit congruum (art. 46). Sed perspicuum est singulos B, C, etc. (exemto ipso A) ad potestatem $\frac{p-1}{a}^{\text{tam}}$ elevatos unitati congruos fieri, quum exponentes b^β, c^γ etc. ad quos singuli pertinent ipsum $\frac{p-1}{a}$ metiantur. Hinc erit

$$A^{\frac{p-1}{a}} \cdot B^{\frac{p-1}{a}} \cdot C^{\frac{p-1}{a}} \text{ etc.} \equiv A^{\frac{p-1}{a}} \equiv 1.$$

Unde sequitur exponentem ad quem A pertinet ipsum $\frac{p-1}{a}$ metiri debere (art. 48), *i. e.* $\frac{p-1}{a^{\alpha+1}}$ esse integrum; at $\frac{p-1}{a^{\alpha+1}} = \frac{b^\beta c^\gamma \text{ etc.}}{a}$ integer esse nequit (art 15). Unde tandem concludere oportet, suppositionem nostram consistere non posse, *i. e.* productum ABC etc. revera ad exponentem $p-1$ pertinere. *Q. E. D.*

Demonstratio posterior priori aliquantulum prolixior esse videtur, prior contra posteriori minus directa.

56.

Hoc theorema insigne exemplum suppeditat, quanta circumspectione in theoria numerorum saepenumero opus sit, ne, quae non sunt, pro certis assumamus. Celeb. Lambert in diss. iam supra laudata *Acta Erudit.* 1769 *p.* 127 huius propositionis mentionem facit sed demonstrationis ne necessitatem quidem attigit. Nemo vero demonstrationem tentavit praeter summum Eulerum, *Comment. nov. Ac. Petrop. T.* XVIII ad annum 1773, *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia* p. 85 seqq. vid. imprimis art. 37 ubi de demonstrationis necessitate fusius locutus est. At demonstratio quam Vir sagacissimus exhibuit duos defectus habet. Alterum quod art. 31 et sqq. tacite supponit, congruentiam $x^n \equiv 1$ (translatis ratiociniis illic adhibitis in nostra signa) revera n radices diversas habere, quamquam ante nihil aliud fuerit demonstratum quam quod *plures* habere nequeat; alterum, quod formulam art. 34 per inductionem tantummodo deduxit.

Radices primitivae, bases, indices.

57.

Numeros ad exponentem $p-1$ pertinentes *radices primitivas* cum ill. Eulero vocabimus. Si igitur a est radix primitiva, potestatum $a, aa, a^3 \ldots a^{p-1}$

residua minima omnia erunt diversa; unde facile deducitur, inter haec omnes numeros $1, 2, 3, \ldots p-1$, qui totidem sunt multitudine quot illa residua minima, reperiri debere, *i. e.* quemvis numerum per p non divisibilem potestati alicui ipsius a congruum esse. Insignis haec proprietas permagnae est utilitatis, operationesque arithmeticas, ad congruentias pertinentes, haud parum sublevare potest, simili fere modo, ut logarithmorum introductio operationes arithmeticae vulgaris. Radicem aliquam primitivam, a, ad lubitum pro *basi* adoptabimus, ad quam omnes numeros per p non divisibiles referemus, et si fuerit $a^e \equiv b \pmod{p}$, e ipsius b *indicem* vocabimus. *Ex. gr.* si pro modulo 19, radix primitiva 2 pro basi assumatur respondebunt

numeris 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12. 13. 14. 15. 16. 17. 18.
indices 0. 1. 13. 2. 16. 14. 6. 3. 8. 17. 12. 15. 5. 7. 11. 4. 10. 9.

Ceterum patet, manente basi, cuique numero plures indices convenire, sed hos omnes secundum modulum $p-1$ fore congruos; quamobrem quoties de indicibus sermo erit, qui secundum modulum $p-1$ sunt congrui pro aequivalentibus habebuntur, simili modo uti numeri ipsi, quando secundum modulum p sunt congrui, tamquam aequivalentes spectantur.

Algorithmus indicum.

58.

Theoremata ad indices pertinentia prorsus analoga sunt iis quae ad logarithmos spectant.

Index producti e quotcunque factoribus conflati congruus est summae indicum singulorum factorum secundum modulum $p-1$.

Index potestatis numeri alicuius congruus est producto ex indice numeri dati in exponentem potestatis, secundum mod. $p-1$.

Demonstrationes propter facilitatem omittimus.

Hinc perspicitur si tabulam construere velimus ex qua omnium numerorum indices pro modulis diversis desumi possint, ex hac tum omnes numeros modulo maiores, tum omnes compositos omitti posse. Specimen huius modi tabulae ad calcem operis huius adiectum est, *Tab.* I, ubi in prima columna verticali positi sunt numeri primi primorumque potestates a 3 usque ad 97, qui tamquam moduli sunt spectandi, iuxta hos singulos numeri pro basi assumti; tum sequuntur indices numerorum primorum successivorum, quorum quini semper per parvulum in-

tervallum sunt disiuncti, eodemque ordine supra dispositi sunt numeri primi; ita ut quis index numero primo dato secundum modulum datum respondeat, facile tutoque inveniri possit.

Ita *ex. gr.* si $p=67$, index numeri 60, assumto 12 pro basi erit

$$\equiv 2\,\mathrm{Ind.}\,2+\mathrm{Ind.}\,3+\mathrm{Ind.}\,5 \pmod{66} \equiv 58+9+39 \equiv 40$$

59.

Index valoris cuiuscunque expressionis $\frac{a}{b}$ *(mod.* p*.), (art.* 31*) congruus est secundum modulum* $p-1$ *differentiae indicum numeratoris* a *et denominatoris* b*, siquidem numeri* a, b *per* p *non sunt divisibiles.*

Sit enim valor quicunque c: critque $bc \equiv a \pmod{p}$; hinc

$$\mathrm{Ind.}\,b+\mathrm{Ind.}\,c \equiv \mathrm{Ind.}\,a \pmod{p-1}$$

adeoque

$$\mathrm{Ind.}\,c \equiv \mathrm{Ind.}\,a-\mathrm{Ind.}\,b$$

Si itaque tabula habetur, ex qua index cuique numero respondens pro quovis modulo primo, aliaque ex qua numerus ad indicem datum pertinens derivari possit, omnes congruentiae primi gradus facillimo negotio solvi poterunt, quoniam omnes reduci possunt ad tales, quarum modulus est numerus primus (art. 30). *E.g.* proposita congruentia

$$29x+7 \equiv 0 \pmod{47} \text{ erit } x \equiv \tfrac{-7}{29} \pmod{47}$$

Hinc $\mathrm{Ind.}\,x \equiv \mathrm{Ind.}\,-7-\mathrm{Ind.}\,29 \equiv \mathrm{Ind.}\,40-\mathrm{Ind.}\,29 \equiv 15-43 \equiv 18 \pmod{46}$

At numerus cuius index 18 invenitur 3. Quare $x \equiv 3 \pmod{47}$. — Tabulam secundam quidem non adiecimus: at huius vice alia defungi poterit uti Sect. VI ostendemus.

De radicibus congruentiae $x^n \equiv A$.

60.

Simili modo ut art. 31 radices congruentiarum primi gradus designavimus, in sequentibus etiam congruentiarum purarum altiorum graduum radices per signum exhibebimus. Uti scilicet $\sqrt[n]{A}$ nihil aliud significat quam radicem aequationis $x^n = A$, ita apposito modulo per $\sqrt[n]{A} \pmod{p}$ denotabitur radix quaecunque congruentiae $x^n \equiv A \pmod{p}$. Hanc expressionem $\sqrt[n]{A} \pmod{p}$ tot valores habere dicemus, quot habet secundum p incongruos, omnes enim qui secundum p

sunt congrui tamquam aequivalentes spectandi (art. 26). Caeterum patet, si A, B secundum p fuerint congrui, expressiones $\sqrt[n]{A}$, $\sqrt[n]{B} \pmod{p}$ aequivalentes fore.

Iam si ponitur $\sqrt[n]{A} \equiv x \pmod{p}$, erit $n\,\mathrm{Ind.}\,x \equiv \mathrm{Ind.}\,A \pmod{p-1}$. Ex hac congruentia deducuntur ad praecepta sectionis praec. valores ipsius $\mathrm{Ind.}\,x$ atque ex his valores respondentes ipsius x. Facile vero perspicitur x habere totidem valores, quot radices congruentia $n\,\mathrm{Ind.}\,x \equiv \mathrm{Ind.}\,A \pmod{p-1}$. Manifesto igitur $\sqrt[n]{A}$ unum tantummodo valorem habebit quando n ad $p-1$ est primus; quando vero numeri $n, p-1$ divisorem communem habent δ, atque hic est maximus, $\mathrm{Ind.}\,x$ habebit δ valores incongruos secundum $p-1$, adeoque $\sqrt[n]{A}$ totidem valores incongruos secundum p, siquidem $\mathrm{Ind.}\,A$ per δ est divisibilis. Qua conditione deficiente $\sqrt[n]{A}$ nullum valorem realem habebit.

Exemplum. Quaeruntur valores expressionis $\sqrt[5]{11} \pmod{19}$. Solvi itaque debet congruentia $15\,\mathrm{Ind.}\,x \equiv \mathrm{Ind.}\,11 \equiv 6 \pmod{18}$, invenienturque tres valores ipsius $\mathrm{Ind.}\,x \equiv 4, 10, 16 \pmod{18}$. His vero respondent valores ipsius x, 6, 9, 4.

61.

Quantumvis expedita sit methodus haec quando tabulae necessariae adsunt, debemus tamen non oblivisci, indirectam eam esse. Operae igitur pretium erit inquirere quantum methodi directae polleant: trademusque hic ea quae ex praecedentibus hauriri possunt: alia, quae considerationes reconditiores postulant, ad sectionem VIII reservantes. Initium facimus a casu simplicissimo, ubi $A=1$, sive ubi radices congruentiae $x^n \equiv 1 \pmod{p}$ quaeruntur. Hic itaque, assumta radice quacunque primitiva pro basi, debet esse $n\,\mathrm{Ind.}\,x \equiv 0 \pmod{p-1}$. Quae congruentia, quando n ad $p-1$ est primus, unam tantummodo radicem habebit, scilicet $\mathrm{Ind.}\,x \equiv 0 \pmod{p-1}$; quare *in hocce casu* $\sqrt[n]{1} \pmod{p}$ unicum valorem habet, scilicet $\equiv 1$. Quando autem numeri $n, p-1$ habent divisorem communem (maximum) δ, congruentiae $n\,\mathrm{Ind.}\,x \equiv 0 \pmod{p-1}$ solutio completa erit $\mathrm{Ind.}\,x \equiv 0 \pmod{\frac{p-1}{\delta}}$ (V. art. 29), *i. e.* $\mathrm{Ind.}\,x$ secundum modulum $p-1$ alicui ex his numeris

$$0, \frac{p-1}{\delta}, \frac{2(p-1)}{\delta}, \frac{3(p-1)}{\delta}, \ldots \frac{(\delta-1)(p-1)}{\delta}$$

congruus esse debebit, sive δ valores secundum modulum $p-1$ incongruos habebit; quare etiam x in hocce casu δ valores diversos (secundum modulum

p incongruos) habebit. Hinc perspicitur, expressionem $\sqrt[\delta]{1}$ etiam δ valores diversos habere, quorum indices cum ante allatis prorsus conveniant. Quocirca expressio $\sqrt[\delta]{1} \pmod p$ huic $\sqrt[n]{1} \pmod p$ omnino aequivalet, *i. e.* congruentia $x^\delta \equiv 1 \pmod p$ easdem radices habet quas haec, $x^n \equiv 1 \pmod p$. Prior autem inferioris erit gradus siquidem δ et n sunt inaequales.

Ex. $\sqrt[3]{1} \pmod{19}$ tres habet valores, quia 3 maxima numerorum 15, 18 mensura communis, hique simul erunt valores expressionis $\sqrt[6]{1} \pmod{19}$. Sunt autem hi 1, 7, 11.

62.

Per hanc igitur reductionem id lucramur ut alias congruentias formae $x^n \equiv 1$ solvere non sit opus, quam ubi n numeri $p-1$ est divisor. Infra vero ostendemus, congruentias huius formae semper ulterius adhuc deprimi posse, licet praecedentia ad hoc non sufficiant. Unum tamen casum iam hic absolvere possumus scilicet ubi $n=2$. Manifesto enim valores expressionis $\sqrt[2]{1}$ erunt $+1$ et -1 quia plures quam duos habere nequit, hique $+1$ et -1 semper sunt incongrui nisi modulus sit $=2$, in quo casu $\sqrt[2]{1}$ unum tantum valorem habere posse, per se clarum. Hinc sequitur, $+1$ et -1 etiam fore valores expressionis $\sqrt[2m]{1}$ quando m ad $\frac{p-1}{2}$ sit primus. Hoc semper eveniet, quoties modulus est eius indolis ut $\frac{p-1}{2}$ fiat numerus absolute primus (nisi forte $p-1=2m$ in quo casu omnes numeri $1, 2, 3 \ldots p-1$ sunt radices) *ex. gr.* quando $p=3, 5, 7, 11, 23, 47, 59, 83, 107$ etc. Tamquam corollarium hic annotetur, indicem ipsius -1 semper esse $\equiv \frac{p-1}{2} \pmod{p-1}$, quaecunque radix primitiva pro basi accipiatur. Namque $2 \operatorname{Ind}.(-1) \equiv 0 \pmod{p-1}$. Quare $\operatorname{Ind}.(-1)$ erit vel $\equiv 0$, vel $\equiv \frac{p-1}{2} \pmod{p-1}$: 0 vero semper index ipsius $+1$, atque $+1$ et -1 semper indices diversos habere debent (praeter casum $p=2$ ad quem hic respicere operae non est pretium).

63.

Ostendimus art. 60 expressionem $\sqrt[\delta]{A} \pmod p$ habere δ valores diversos, aut omnino nullum, si fuerit δ divisor communis maximus numerorum $n, p-1$. Iam uti modo docuimus $\sqrt[n]{A}$ et $\sqrt[\delta]{A}$ aequivalentes esse, si fuerit $A \equiv 1$, generalius probabimus, expressionem $\sqrt[n]{A}$ semper ad aliam $\sqrt[\delta]{B}$ reduci posse cui aequivaleat. Illius enim valore quocunque denotato per x erit $x^n \equiv A$; iam

sit t valor quicunque expressionis $\frac{z}{n} \pmod{p-1}$, quam valores reales habere ex art. 31 perspicuum; eritque $x^{tn} \equiv A^t$ at $x^{tn} \equiv x^\delta$ propter $tn \equiv \delta \pmod{p-1}$. Quare $x^\delta \equiv A^t$ adeoque quicunque ipsius $\sqrt[n]{A}$ valor erit etiam valor ipsius $\sqrt[\delta]{A^t}$. Quoties igitur $\sqrt[n]{A}$ valores reales habet, expressioni $\sqrt[\delta]{A^t}$ prorsus aequivalens erit, quoniam illa neque alios habet quam haec neque pauciores, licet quando $\sqrt[n]{A}$ nullum valorem realem habet, fieri tamen possit ut $\sqrt[\delta]{A^t}$ valores reales habeat.

Ex. Si valores expressionis $\sqrt[6]{2} \pmod{31}$ quaeruntur, erit numerorum 21 et 30 divisor communis maximus 3, expressionisque $\frac{3}{21} \pmod{30}$ valor aliquis 3, quare si $\sqrt[6]{2}$ valores reales habet, huic expressioni $\sqrt[2]{2^3}$ sive $\sqrt[2]{8}$ aequivalebit, invenieturque revera, posterioris expressionis valores qui sunt 2, 10, 19 etiam priori satisfacere.

64.

Ne autem hanc operationem incassum suscepisse periclitemur, regulam investigare oportet, per quam statim diiudicari possit utrum $\sqrt[n]{A}$ valores reales admittat necne. Quodsi tabula indicum habetur, res in promtu est; namque ex art. 60 manifestum est, valores reales dari, si ipsius A index, radice quacunque primitiva pro basi accepta, per δ sit divisibilis, sin vero minus, non dari. Attamen hoc etiam absque tali tabula inveniri potest. Posito enim indice ipsius $A = k$, si hic fuerit per δ divisibilis, erit $\frac{k(p-1)}{\delta}$ per $p-1$ divisibilis et vice versa. Atqui numeri $A^{\frac{p-1}{\delta}}$ index erit $\frac{k(p-1)}{\delta}$. Quare si $\sqrt[n]{A} \pmod p$ habet valores reales, $A^{\frac{p-1}{\delta}}$ unitati congruus erit, sin minus, incongruus. Ita in exemplo art. praec. habetur $2^{30} = 1024 \equiv 1 \pmod{31}$, unde concluditur $\sqrt[6]{2}$ $\pmod{31}$ valores reales habere. Similiter certiores hinc fimus, $\sqrt{-1} \pmod p$ semper valores binos reales habere, quando p sit formae $4m+1$, nullum vero, quando p sit formae $4m+3$; propter $(-1)^{2m} = 1$ et $(-1)^{2m+1} = -1$. Elegans hoc theorema, quod vulgo ita profertur: *Si p est numerus primus formae $4m+1$, inveniri potest quadratum aa, ita ut $aa+1$ per p fiat divisibilis; si vero p est formae $4m-1$, tale quadratum non datur*, hoc modo demonstratum est ab ill. Eulero, *Comm. nov. Acad. Petrop.* T. XVIII p. 112 ad annum 1773. Demonstrationem aliam iam multo ante dederat, *Comm. nov.* T. V p. 5 qui prodiit a. 1760. In dissert. priori, *Comm. nov.* T. IV p. 25, rem nondum

perfecerat. Postea etiam ill. La Grange theorematis demonstrationem tradidit, *Nouveaux Mém. de l'Ac. de Berlin A.* 1775 *p.* 342. Aliam adhuc demonstrationem in sectione sequenti ubi proprie de hoc argumento agendum erit, dabimus.

65.

Postquam omnes expressiones $\sqrt[n]{A} \pmod{p}$ ad tales reducere docuimus, ubi n divisor numeri $p-1$, criteriumque nacti sumus utrum valores reales admittat, necne, tales expressiones $\sqrt[n]{A} \pmod{p}$ ubi n ipsius $p-1$ est divisor accuratius considerabimus. Primo ostendemus, quam relationem valores singuli expressionis inter se habeant, tum artificia quaedam trademus, quorum auxilio unus valor expressionis saepenumero inveniri possit.

Primo, quando $A \equiv 1$, atque r aliquis ex n valoribus expressionis $\sqrt[n]{1} \pmod{p}$, sive $r^n \equiv 1 \pmod{p}$, omnes etiam ipsius r potestates erunt valores istius expressionis; horum autem totidem erunt diversi quot unitates habet exponens ad quem r pertinet (art. 48). Quodsi igitur r est valor ad exponentem n pertinens, potestates ipsius r hae $r, r^2, r^3 \ldots r^n$ (ubi loco ultimae *unitas* substitui potest) omnes expressionis $\sqrt[n]{1} \pmod{p}$ valores involvent. Qualia autem subsidia exstent ad tales valores inveniendos qui ad exponentem n pertineant, in Sect. VIII fusius explicabimus.

Secundo. Quando A unitati est incongruus, unusque valor expressionis $\sqrt[n]{A} \pmod{p}$ notus, qui sit z, reliqui hoc modo inde deducuntur. Sint valores expressionis $\sqrt[n]{1}$ hi

$$1, r, r^2 \ldots r^{n-1}$$

(uti modo ostendimus), eruntque omnes expr. $\sqrt[n]{A}$ valores hi

$$z, zr, zr^2 \ldots zr^{n-1}$$

namque omnes hos congruentiae $x^n \equiv A$ satisfacere inde manifestum quod, posito quocunque eorum $\equiv zr^k$, potestas ipsius n^{ta}, $z^n r^{nk}$, propter $r^n \equiv 1$ et $z^n \equiv A$, ipsi A fit congrua; omnes diversos esse ex art. 23 facile intelligitur; plures autem valores quam hos quorum numerus est n, expressio $\sqrt[n]{A}$ habere nequit. Ita *ex. gr.* si alter expressionis $\sqrt[n]{A}$ valor est z, alter erit $-z$. Deni-

que hinc concludendum omnes valores expr. $\sqrt[n]{A}$ inveniri non posse, nisi simul omnes valores expr. $\sqrt[n]{1}$ constent.

66.

Secundum quod nobis proposueramus fuit docere, in quo casu unus expressionis $\sqrt[n]{A} \pmod{p}$ valor (ubi n supponitur esse divisor ipsius $p-1$) directe inveniri possit. Hoc evenit quando aliquis valor potestati alicui ipsius A congruus evadit, qui casus quum haud raro occurrat, aliquantum huic rei immorari

≡A^k et $A \equiv z^n$
petur, ita ut sit
alet ista, ut sit
(art. 46, 48). Ut
rimus. Hoc in
habent, nullus

videamus quo-
cile intelligitur,
ales habeat, uti
tum $y^{p-1} \equiv 1$,
tiae ad potesta-
bilis (art. 48).
≡1 etiam secun-
k congruentiae
odulum t, qui
erebatur inven-
factores primi
emur numerum
s factoribus pri-
. pervenimus ut
eoque etiam ip-
solvitur (quod

fieri potest quia n ad $\frac{p-1}{nq}$ primus), valor ipsius k etiam secundum modulum

perfecerat. Postea etiam ill. La Grange theorematis demonstrationem tradidit. *Nouveaux Mém. de l'Ac. de Berlin A.* 1775 *p.* 342. Aliam adhuc demonstrationem in sectione sequenti ubi proprie de hoc argumento agendum erit, dabimus.

65.

Postquam omnes expressiones $\sqrt[n]{A} \pmod{p}$ ad tales reducere docuimus, ubi n divisor numeri $p-1$, criteriumque nacti sumus utrum valores reales admittat, necne, tales expressiones $\sqrt[n]{A} \pmod{p}$ ubi n ipsius $p-1$ est divisor accuratius considerabi

sionis inter se

lor expressioni

Primo, q

$(\mathrm{mod}.p)$, sive

istius expressio

nens ad quem

n pertinens,

stitui potest) o

subsidia exster

in Sect. VIII f

Secundo,

$\sqrt[n]{A} \pmod{p}$ no

expressionis $\sqrt[n]{}$

(uti modo oste

namque omnes

sito quocunque

$\equiv A$, ipsi A

res autem valor

quit. Ita *ex. gr.* si alter expressionis $\sqrt[n]{A}$ valor est z, alter erit $-z$. Deni-

que hinc concludendum omnes valores expr. $\sqrt[n]{A}$ inveniri non posse, nisi simul omnes valores expr. $\sqrt[n]{1}$ constent.

66.

Secundum quod nobis proposueramus fuit docere, in quo casu unus expressionis $\sqrt[n]{A} \pmod{p}$ valor (ubi n supponitur esse divisor ipsius $p-1$) directe inveniri possit. Hoc evenit quando aliquis valor potestati alicui ipsius A congruus evadit, qui casus quum haud raro occurrat, aliquantum huic rei immorari non superfluum erit. Sit talis valor, *si quis datur* z, sive $z \equiv A^k$ et $A \equiv z^n \pmod{p}$. Hinc colligitur $A \equiv A^{kn}$; quare si numerus k habetur, ita ut sit $A \equiv A^{kn}$, A^k erit valor quaesitus. At huic conditioni aequivalet ista, ut sit $1 \equiv kn \pmod{t}$, designante t exponentem ad quem pertinet A (art. 46, 48). Ut vero haec congruentia possibilis sit, requiritur, ut sit n ad t primus. Hoc in casu erit $k \equiv \frac{1}{n} \pmod{t}$; si vero t et n divisorem communem habent, nullus valor z potestati ipsius A congruus esse potest.

67.

Quum autem ad hanc solutionem ipsum t novisse oporteat, videamus quomodo procedere possimus, si hunc numerum ignoremus. Primo facile intelligitur, t ipsum $\frac{p-1}{n}$ metiri debere, siquidem $\sqrt[n]{A} \pmod{p}$ valores reales habeat, uti hic semper supponimus. Sit enim quicunque valor y, eritque tum $y^{p-1} \equiv 1$, tum $y^n \equiv A \pmod{p}$; quare elevando partes posterioris congruentiae ad potestatem $\frac{p-1}{n}^{\text{tam}}$, fiet $A^{\frac{p-1}{n}} \equiv 1$; adeoque $\frac{p-1}{n}$ per t divisibilis (art. 48). Iam si $\frac{p-1}{n}$ ad n est primus, congruentia art. praec. $kn \equiv 1$ etiam secundum modulum $\frac{p-1}{n}$ solvi poterit, manifestoque valor ipsius k congruentiae secundum modulum hunc satisfaciens eidem etiam secundum modulum t, qui ipsum $\frac{p-1}{n}$ metitur, satisfaciet (art. 5). Tum igitur quod quaerebatur inventum. Si vero $\frac{p-1}{n}$ ad n non est primus, omnes ipsius $\frac{p-1}{n}$ factores primi qui simul ipsum n metiuntur ex $\frac{p-1}{n}$ eiiciantur. Hinc nanciscemur numerum $\frac{p-1}{nq}$, ad n primum, designante q productum ex omnibus illis factoribus primis, quos eiecimus. Quodsi iam conditio ad quam in artic. praec. pervenimus ut t ad n sit primus locum habet, t etiam ad q erit primus adeoque etiam ipsum $\frac{p-1}{nq}$ metietur. Quare si congruentia $kn \equiv 1 \pmod{\frac{p-1}{nq}}$ solvitur (quod fieri potest quia n ad $\frac{p-1}{nq}$ primus), valor ipsius k etiam secundum modulum

t congruentiae satisfaciet, id quod quaerebatur. Totum hoc artificium in eo versatur, ut numerus eruatur qui ipsius t, quem ignoramus, vice fungi possit. Attamen probe meminisse oportet, nos quando $\frac{p-1}{n}$ ad n non est primus, supposuisse conditionem art. praec. locum habere, quae si deficit omnes conclusiones erroneae erunt; atque si regulas datas temere sequendo pro z valor invenitur, cuius potestas n^{ta} ipsi A non sit congrua, indicio hoc est, conditionem deficere adeoque methodum hanc omnino adhiberi non posse.

68.

Sed in hocce etiam casu saepe prodesse potest, hunc laborem suscepisse; operaeque pretium est, quomodo hic valor falsus ad veros sese habeat investigare. Supponamus itaque numeros k, z rite esse determinatos sed z^n non esse $\equiv A$ (mod. p). Tum si modo valores expressionis $\sqrt[n]{\frac{A}{z^n}}$ (mod. p) determinari possint, hos singulos per z multiplicando valores ipsius $\sqrt[n]{A}$ obtinebimus. Si enim x est valor aliquis ipsius $\sqrt[n]{\frac{A}{z^n}}$: erit $(xz)^n \equiv A$. Sed expressio $\sqrt[n]{\frac{A}{z^n}}$ eatenus hac $\sqrt[n]{A}$ simplicior, quod $\frac{A}{z^n}$ (mod. p) ad exponentem minorem plerumque pertinet quam A. Scilicet si numerorum t, q divisor communis maximus est d, $\frac{A}{z^n}$ (mod. p) ad exponentem d pertinebit, id quod ita demonstratur. Substituto pro z valore, fit $\frac{A}{z^n} \equiv \frac{1}{A^{kn-1}}$ (mod. p). At $kn-1$ per $\frac{p-1}{nq}$ divisibilis (art. praec.), $\frac{p-1}{n}$ vero per t (ibid.) sive $\frac{p-1}{nd}$ per $\frac{t}{d}$. Atqui $\frac{t}{d}$ ad $\frac{q}{d}$ est primus (*hyp.*), quare etiam $\frac{p-1}{nd}$ per $\frac{tq}{dd}$ sive $\frac{p-1}{nq}$ per $\frac{t}{d}$; adeoque etiam $kn-1$ per $\frac{t}{d}$ et $(kn-1)d$ per t erit divisibilis. Hinc $A^{(kn-1)d} \equiv 1$ (mod. p). Unde facile deducitur, $\frac{A}{z^n}$ ad potestatem d^{tam} evectum unitati congruum fieri. Quod vero $\frac{A}{z^n}$ ad exponentem minorem quam d pertinere non possit facile quidem demonstrari potest, sed quoniam ad finem nostrum non requiritur, huic rei non immoramur. Certi igitur esse possumus, $\frac{A}{z^n}$ (mod. p) semper ad minorem exponentem pertinere quam A, unico excepto casu, scilicet quando t ipsum q metitur, adeoque $d=t$.

Sed quid iuvat, quod $\frac{A}{z^n}$ ad minorem exponentem pertinet quam A? Plures numeri dantur qui possunt esse A quam qui possunt esse $\frac{A}{z^n}$, et quando secundum eundem modulum plures huiusmodi expressiones $\sqrt[n]{A}$ evolvere occasio est, id lucramur ut plures ex eodem fonte haurire possimus. Ita *ex. gr.* semper unicum saltem valorem expressionis $\sqrt[n]{A}$ (mod. 29) determinare in potestate erit,

si modo expressionis $\sqrt[n]{-1}$ (mod. 29) valores (qui sunt ± 12) innotuerint. Facile enim ex art. praec. perspicitur, huiusmodi expressionum unum valorem semper directe determinari posse, quando t impar, et d fieri $=2$ quando t par; praeter -1 autem nullus numerus ad exponentem 2 pertinet.

Exempla. Quaeritur $\sqrt[3]{31}$ (mod. 37). Hic $p-1=36$, $n=3$, $\frac{p-1}{3}=12$, adeoque $q=3$; debet igitur esse $3k \equiv 1$ (mod. 4) quod obtinetur ponendo $k=3$. Hinc $z \equiv 31^3$ (mod. 37) $\equiv 6$, inveniturque revera $6^3 \equiv 31$ (mod. 37). Si valores expressionis $\sqrt[3]{1}$ (mod. 37) sunt noti, etiam reliqui expr. $\sqrt[3]{6}$ valores determinari possunt. Sunt vero illi 1, 10, 26, per quos multiplicando ipsum 6, prodeunt reliqui $\equiv 23$ et 8.

Si autem quaeritur valor expr. $\sqrt[3]{3}$ (mod. 37), erit $n=2$, $\frac{p-1}{n}=18$; adeoque $q=2$. Hinc debet esse $2k \equiv 1$ (mod. 9), unde fit $k \equiv 5$ (mod. 9). Quare $z \equiv 3^5 \equiv 21$ (mod. 37); at 21^2 non $\equiv 3$, sed $\equiv 34$; est autem $\frac{3}{34}$ (mod. 37) $\equiv -1$, atque $\sqrt{-1}$ (mod. 37) $\equiv \pm 6$; unde obtinentur valores veri $\pm 6.21 \equiv \pm 15$.

Haec fere sunt, quae hic de talium expressionum evolutione tradere licuit. Palam est methodos directas satis prolixas saepe evasuras: at hoc incommodum tantum non omnibus methodis directis in numerorum theoria incumbit: neque ideo negligendum censuimus, quantum hic praestare valeant ostendere. Etiam hic observare convenit, artificia particularia quae exercitato haud raro se offerunt sigillatim explicare, non esse instituti nostri.

Nexus indicum in systematibus diversis.

69.

Revertimur nunc ad radices quas diximus primitivas. Ostendimus, radice primitiva quacunque pro basi assumta omnes numeros, quorum indices ad $p-1$ primi, etiam fore radices primitivas, nullosque praeter hos: unde simul radicum primitivarum multitudo sponte innotescit. V. art. 53. Quaenam autem radicem primitivam pro basi adoptare velimus, in genere arbitrio nostro relinquitur; unde intelligitur, etiam hic, ut in calculo logarithmico, plura quasi systemata dari posse *).

*) In eo autem differunt, quod in logarithmis systematum numerus est infinitus, hic vero tantus, quantus numerus radicum primitivarum. Manifesto enim bases congruae idem systema generant.

quae quo vinculo connexa sint videamus. Sint a, b duae radices primitivae, aliusque numerus m, atque, quando a pro basi assumitur, index numeri $b \equiv \delta$, numeri m vero index $\equiv \mu \pmod{p-1}$; quando autem b pro basi assumitur, index numeri $a \equiv \alpha$, numeri m vero $\equiv \nu \pmod{p-1}$. Tum erit $\alpha\delta \equiv 1 \pmod{p-1}$; namque $a^{\xi} \equiv b$, quare $a^{\alpha\xi} \equiv b^{\alpha} \equiv a \pmod{p}$, (*hyp.*), hinc $\alpha\delta \equiv 1 \pmod{p-1}$. Per simile ratiocinium invenitur $\nu \equiv \alpha\mu$, atque $\mu \equiv \delta\nu \pmod{p-1}$. Si igitur tabella indicum pro basi a constructa habetur, facile in aliam converti potest, ubi b basis. Si enim pro basi a ipsius b index est $\equiv \delta$, pro basi b ipsius a index erit $\equiv \frac{1}{\delta} \pmod{p-1}$, multiplicandoque per hunc numerum omnes tabellae indices, habebuntur omnes indices pro basi b.

70.

Quamvis autem plures indices numero dato contingere possint, aliis aliisque radicibus primitivis pro basi acceptis, omnes tamen in eo convenient, quod omnes eundem divisorem maximum cum $p-1$ communem habebunt. Si enim pro basi a, index numeri dati est m, pro basi b vero n, atque divisores maximi his cum $p-1$ communes μ, ν supponuntur esse inaequales, alter erit maior, *ex. gr.* $\mu > \nu$, adeoque μ ipsum n non metietur. At designato indice ipsius a, quando b pro basi assumitur, per α, erit (art. praec.) $n \equiv \alpha m \pmod{p-1}$ adeoque μ etiam ipsum n metietur. *Q. E. A.*

Hunc divisorem maximum indicibus numeri dati, ipsique $p-1$ communem, a basi non pendere, etiam inde perspicuum, quod aequalis est ipsi $\frac{p-1}{t}$, designante t exponentem ad quem numerus, de cuius indicibus agitur, pertinet. Si enim index pro basi quacunque est k, erit t minimus numerus per quem k multiplicatus ipsius $p-1$ multiplum evadit (excepta cifra) vid. artt. 48, 58, sive minimus valor expressionis $\frac{0}{k} \pmod{p-1}$ praeter cifram; hunc autem aequalem esse divisori maximo communi numerorum k et $p-1$ ex art. 29 nullo negotio derivatur.

71.

Porro facile demonstratur, basin ita semper accipere licere, ut numerus ad exponentem t pertinens indicem quemlibet datum nansiscatur, cuius quidem maximus divisor cum $p-1$ communis $= \frac{p-1}{t}$. Designemus hunc brevitatis gratia per d, sitque index propositus $\equiv dm$, numerique propositi quando quaelibet

radix primitiva a pro basi accipitur, index $\equiv dn$, eruntque m, n ad $\frac{p-1}{d}$ sive ad t primi. Tum si ε est valor expressionis $\frac{dn}{dm} \pmod{p-1}$, simulque ad $p-1$ primus, erit a^{ε} radix primitiva, qua pro basi accepta numerus propositus indicem dm adipiscetur (erit enim $a^{\varepsilon dm} \equiv a^{dn} \equiv$ numero proposito), id quod desiderabatur. Sed expressionem $\frac{dn}{dm} \pmod{p-1}$ valores ad $p-1$ primos admittere, ita probatur. Aequivalet illa expressio huic: $\frac{n}{m} \pmod{\frac{p-1}{d}}$ sive $\frac{n}{m} \pmod{t}$ vid. art. 31, 2, eruntque omnes eius valores ad t primi; si enim aliquis valor e divisorem cum t communem haberet, hic divisor etiam ipsum me metiri deberet, adeoque etiam ipsum n, cui me secundum t congruus, contra hypoth., ex qua n ad t primus. Quando igitur omnes divisores primi ipsius $p-1$ etiam ipsum t metiuntur, *omnes* expr. $\frac{n}{m} \pmod{t}$ valores ad $p-1$ primi erunt multitudoque eorum $= d$; quando autem $p-1$ alios adhuc divisores primos, f, g, h etc. implicat, ipsum t non metientes, ponatur valor quicunque expr. $\frac{n}{m} \pmod{t} \equiv e$. Tum autem quia omnes t, f, g, h etc. inter se primi, inveniri potest numerus ε, qui secundum t ipsi e, secundum f, g, h etc. vero numeris quibuscunque ad hos respective primis fiat congruus (art. 32). Talis itaque numerus per nullum factorem primum ipsius $p-1$ divisibilis adeoque ad $p-1$ primus erit, uti desiderabatur. Tandem haud difficile ex combinationum theoria deducitur, talium valorum multitudinem fore $= \frac{p-1}{t} \cdot \frac{f-1}{f} \cdot \frac{g-1}{g} \cdot \frac{h-1}{h} \cdot \text{etc.}$; sed ne digressio haec in nimiam molem excrescat, demonstrationem, quum ad institutum nostrum non sit adeo necessaria, omittimus.

Bases usibus peculiaribus accommodatae.

72.

Quamvis in genere prorsus arbitrarium sit, quaenam radix primitiva pro basi adoptetur, interdum tamen bases aliae prae aliis commoda quaedam peculiaria praebere possunt. In tabula I semper numerum 10 pro basi assumsimus, quando fuit radix primitiva; alioquin basin ita semper determinavimus ut numeri 10 index evaserit quam minimus, *i. e.* $= \frac{p-1}{t}$ denotante t exponentem ad quem 10 pertinuit. Quid vero hinc lucremur, in Sect. VI ostendemus ubi eadem tabula ad alios adhuc usus adhibebitur. Sed quoniam etiam hic aliquid arbitrarii remanere potest, ut ex art. praec. apparet, ut aliquid certi statueremus, ex omnibus radicibus primitivis quaesitum praestantibus *minimam* semper pro basi elegimus. Ita pro $p = 73$, ubi $t = 8$ atque $d = 9$, a^{ε} habet $\frac{72.2}{8.3}$ *i. e.* 6 valores, qui sunt 5, 14, 20, 28, 39, 40. Assumsimus itaque minimum 5 pro basi.

Methodus radices primitivas assignandi.

73.

Methodi radices primitivas inveniendi maximam partem tentando inniuntur. Si quis ea quae art. 55 docuimus cum iis quae infra de solutione congruentiae $x^n \equiv 1$ trademus confert, omnia fere, quae per methodos directas effici possunt, habebit. III. Euler confitetur, *Opusc. Analyt.* T. I. p. 152, maxime difficile videri, hos numeros assignare, eorumque indolem ad profundissima numerorum mysteria esse referendam. At tentando satis expedite sequenti modo determinari possunt. Exercitatus operationis prolixitati per multifaria artificia particularia succurrere sciet: haec vero per usum multo citius quam per praecepta ediscuntur.

1°. Assumatur ad libitum numerus ad p (ita semper modulum designamus) primus, a, (plerumque ad calculi brevitatem conducit, si quam minimum accipimus, *ex. gr.* numerum 2) determineturque eius periodus (art. 46), *i. e.* residua minima ipsius potestatum, donec ad potestatem a^t perveniatur, cuius residuum minimum sit 1 *). Iam si fuerit $t = p-1$, a est radix primitiva.

2°. Si vero $t < p-1$, accipiatur alius numerus b in periodo ipsius a non contentus, investigeturque simili modo huius periodus. Designato exponente ad quem b pertinet per u, facile perspicitur u neque ipsi t aequalem neque ipsius partem aliquotam esse posse, in utroque enim casu fieret $b^t \equiv 1$, quod esse nequit, quum periodus ipsius a omnes numeros amplectatur, quorum potestas exponentis t unitati congrua (art. 53). Quodsi u fuerit $= p-1$, erit b radix primitiva; si vero u non quidem $= p-1$, sed tamen multiplum ipsius t, id lucrati sumus, ut numerus constet ad exponentem maiorem pertinens, adeoque scopo nostro, qui est invenire numerum ad exponentem *maximum* pertinentem, propiores iam simus. Si vero u neque $= p-1$, neque ipsius t multiplum, tamen numerum invenire possumus ad exponentem ipsis t, u maiorem pertinentem, nempe ad exponentem minimo dividuo communi numerorum t, u aequalem. Sit hic $= y$, resolvaturque y ita in duos factores inter se primos, m, n, ut alter ipsum t, alter ipsum u metiatur †). Tum fiat potestas $\frac{t}{m}$ ta ipsius a, $\equiv A$, potestas $\frac{u}{n}$ ta ipsius b, $\equiv B \pmod p$, eritque productum AB numerus ad exponentem n pertinens; facile enim intelligitur, A ad exponentem m, B ad exponentem n pertinere; adeoque productum AB ad mn pertinebit, quia m, n inter se sunt primi, id quod prorsus eodem modo uti in art. 55, II processimus probari poterit.

3°. Iam si $y = p-1$, AB erit radix primitiva; sin minus, simili modo ut antea alius numerus adhibendus erit, in periodo ipsius AB non occurrens; eritque hic aut radix primitiva, aut pertinebit ad exponentem ipso y maiorem, aut certe ipsius auxilio (uti ante) numerus ad exponentem ipso y maiorem pertinens inveniri poterit. Quum igitur numeri qui per repetitionem huius operationis prodeunt, ad exponentes continuo crescentes pertineant, manifestum est tandem numerum inventum iri, qui ad exponentem *maximum* pertineat, *i. e.* radicem primam, *q. e. f.*

*) Quisquis sponte perspiciet, non opus esse has potestates ipsas novisse, quum cuiusvis residuum minimum facile ex residuo minimo potestatis praecedentis obtineri possit.

†) Quomodo hoc fieri possit ex art. 15 haud difficulter derivatur. Resolvatur y in factores tales, qui sint aut numeri primi diversi aut numerorum primorum diversorum potestates. Horum quisque alterutrum numerorum t, u metietur (sive etiam utrumque). Adscribantur singuli aut numero t aut numero u, prout illum aut hunc metiuntur; quando aliquis utrumque metitur, arbitrarium est, cui adscribatur; productum ex iis qui ipsi t adscripti sunt, sit $= m$, productum e reliquis $= n$, facileque perspicietur m ipsum t, n ipsum u metiri, atque esse $mn = y$.

74.

Per exemplum praecepta haec clariora fient. Sit $p = 73$, pro quo radix primitiva quaeratur. Tentemus primo numerum 2, cuius periodus prodit haec:

1. 2. 4. 8. 16. 32. 64. 55. 37. 1 etc.
0. 1. 2. 3. 4. 5. 6. 7. 8. 9 etc.

Quum igitur iam potestas exponentis 9 unitati congrua fiat, 2 non est radix primitiva. Tentetur alius numerus in periodo ipsius 2 non occurrens *ex. gr.* 3, cuius periodus est haec:

1. 3. 9. 27. 8. 24. 72. 70. 64. 46. 65. 49. 1 etc.
0. 1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12 etc.

Quare neque 3 est radix primitiva. Exponentium autem ad quos 2, 3 pertinent, *i. e.* numerorum 9, 12) dividuus communis minimus est 36, qui in factores 9 et 4 ad praecepta art. praec. resolvitur. Evehendus itaque 2 ad potestatem exponentis $\frac{36}{9}$, *i. e.* numerus 2 ipse retinendus; 3 autem ad potestatem exponentis 3: productum ex his est 54, quod itaque ad exponentem 36 pertinebit. Si denique ipsius 54 periodus computatur numerusque in hac non contentus *ex. gr.* 5 denuo tentatur, hunc esse radicem primitivam, reperietur.

Theoremata varia de periodis et radicibus primitivis.

75.

Antequam hoc argumentum deseramus, propositiones quasdam trademus, quae ob simplicitatem suam attentione haud indignae videntur.

Productum ex omnibus terminis periodi numeri cuiusvis est $\equiv 1$, *quando ipsorum multitudo, sive exponens ad quem numerus pertinet, est impar, et* $\equiv -1$, *quando ille exponens est par.*

Ex. Pro modulo 13 periodus numeri 5 constat ex his terminis 1, 5, 12, 8 quorum productum $480 \equiv -1 \pmod{13}$.

Secundum eundem modulum periodus numeri 3 constat e terminis 1, 3, 9 quorum productum $27 \equiv 1 \pmod{13}$.

Demonstr. Sit exponens, ad quem numerus pertinet, t, atque index numeri, $\frac{p-1}{t}$, id quod si basis rite determinatur semper fieri potest (art. 71). Tum index producti ex omnibus periodi terminis erit

$$\equiv (1+2+3+\text{etc.}+t-1)\frac{p-1}{t} = \frac{(t-1)(p-1)}{2}$$

i. e. $\equiv 0 \pmod{p-1}$, quando t impar, et $\equiv \frac{p-1}{2}$, quando t par; hinc in priori casu productum illud $\equiv 1 \pmod{p}$; in posteriori vero $\equiv -1 \pmod{p}$, (art. 62). *Q. E. D.*

76.

Si numerus iste in theor. praecedente est radix primitiva, eius periodus omnes numeros $1, 2, 3, \ldots p-1$ comprehendet, quorum productum itaque semper $\equiv -1$ (namque $p-1$ semper par, unico casu $p=2$ excepto in quo -1 et $+1$ aequivalent). Theorema hoc elegans quod ita enunciari solet: *productum ex omnibus numeris numero primo dato minoribus, unitate auctum per hunc primum est divisibile*, primum a cel. Waring est prolatum armigeroque Wilson adscriptum, *Meditt. algebr. Ed. 3. p. 380.* Sed neuter demonstrare potuit, et cel. Waring fatetur demonstrationem eo difficiliorem videri, quod nulla *notatio* fingi possit, quae numerum primum exprimat. — At nostro quidem iudicio huiusmodi veritates ex notionibus potius quam ex notationibus hauriri debebant. Postea ill. La Grange demonstrationem dedit, *Nouv. Mém. de l'Ac. de Berlin*, 1771. Innititur ea consi-

derationi coefficientium ex evolutione producti

$$x+1.x+2.x+3\ldots x+p-1$$

oriundorum. Scilicet posito hoc producto

$$\equiv x^{p-1}+Ax^{p-2}+Bx^{p-3}+\text{etc.}+Mx+N$$

coefficientes A, B etc. M per p erunt divisibiles, N vero erit $= 1.2.3\ldots p-1$. Iam pro $x=1$, productum per p divisibile; tunc autem erit $\equiv 1+N \pmod{p}$; quare necessario $1+N$ per p dividi poterit.

Denique ill. Euler in *Opusc. analyt. T. I. p. 329* demonstrationem dedit, cum ea quam nos hic exposuimus conspirantem. Quodsi tales viri theorema hoc meditationibus suis non indignum censuerunt, non improbatum iri speramus, si aliam adhuc demonstrationem apponimus.

77.

Quando secundum modulum p, productum duorum numerorum a, b unitati est congruum, numeros a, b cum ill. Euler *socios* vocemus. Tum secundum sect. praec. quivis numerus positivus ipso p minor socium habebit positivum ipso p minorem et quidem unicum. Facile autem probari potest ex numeris $1, 2, 3\ldots p-1$; 1 et $p-1$ esse unicos qui sibi ipsis sint socii: numeri enim sibi ipsis socii, radices erunt congruentiae $xx \equiv 1$; quae quoniam est secundi gradus plures quam duas radices, *i. e.* alias quam 1 et $p-1$ habere nequit. Abiectis itaque his numerorum reliquorum $2, 3\ldots p-2$ bini semper erunt associati; quare productum ex ipsis erit $\equiv 1$ adeoque productum ex omnibus $1, 2, 3\ldots p-1$, $\equiv p-1$ sive $\equiv -1$. *Q. E. D.*

Ex. gr. pro $p=13$ numeri $2, 3, 4\ldots 11$ ita associantur: 2 cum 7; 3 cum 9; 4 cum 10; 5 cum 8; 6 cum 11; scilicet $2.7 \equiv 1$; $3.9 \equiv 1$ etc. Hinc $2.3.4\ldots 11 \equiv 1$; adeoque $1.2.3\ldots 12 \equiv -1$.

78.

Potest autem theorema Wilsonianum generalius sic proponi. *Productum ex omnibus numeris, numero* ***quocunque*** *dato A minoribus simulque ad ipsum primis, congruum est secundum A, unitati vel negative vel positive sumtae.* Negative sumenda est unitas, quando A est formae p^m, aut huiusce $2p^m$, designante p nume-

rum primum a 2 diversum, insuperque quando $A=4$; positive autem in omnibus casibus reliquis. Theorema, quale a cel. Wilson est prolatum, sub casu priori continetur. — *Ex. gr.* pro $A=15$ productum e numeris 1, 2, 4, 7, 8, 11, 13, 14 est $\equiv 1 \pmod{15}$. Demonstrationem brevitatis gratia non adiungimus: observamus tantum, eam simili modo perfici posse ut in art. praec., excepto quod congruentia $xx \equiv 1$ plures quam duas radices habere potest, quae considerationes quasdam peculiares postulant. Posset etiam demonstratio ex consideratione indicum peti, similiter ut in art. 75, si ea quae mox de modulis non primis trademus conferantur.

79.

Revertimur ad enumerationem aliarum propositionum (art. 75).

Summa omnium terminorum periodi numeri cuiusvis est $\equiv 0$, uti in ex. art. 75, $1+5+12+8=26\equiv 0 \pmod{13}$.

Dem. Numerus de cuius periodo agitur, sit $=a$, atque exponens ad quem pertinet, $=t$, eritque summa terminorum omnium periodi,

$$\equiv 1+a+aa+a^3+\text{etc.}+a^{t-1}\equiv\frac{a^t-1}{a-1}\pmod{p}$$

At $a^t-1\equiv 0$: quare summa haec semper erit $\equiv 0$ (art. 22), nisi forte $a-1$ per p sit divisibilis, sive $a\equiv 1$; hunc igitur casum excipere oportet, si vel unum terminum *periodum* vocare velimus.

80.

Productum ex omnibus radicibus primitivis est $\equiv 1$, excepto unico casu, $p=3$; tum enim una tantum datur radix primitiva, 2.

Demonstr. Si radix primitiva quaecunque pro basi assumitur, indices radicum omnium primitivarum erunt numeri ad $p-1$ primi simulque ipso minores. At horum numerorum summa, *i. e.* index producti ex omnibus radicibus primitivis, est $\equiv 0 \pmod{p-1}$ adeoque productum $\equiv 1 \pmod{p}$; facile enim perspicitur, si k fuerit numerus ad $p-1$ primus, etiam $p-1-k$ ad $p-1$ primum fore adeoque binos numeros ad $p-1$ primos summam constituere per $p-1$ divisibilem; (k autem ipsi $p-1-k$ numquam aequalis esse potest, praeter casum $p-1=2$, sive $p=3$, quem excepimus; manifesto enim $\frac{p-1}{2}$ in omnibus reliquis casibus ad $p-1$ non est primus).

81.

Summa omnium radicum primitivarum est aut $\equiv 0$ (quando $p-1$ per *quadratum* aliquod est divisibilis), *aut* $\equiv \pm 1 \pmod{p}$, (quando $p-1$ est productum e numeris primis inaequalibus; quorum multitudo si est par signum positivum, si vero impar, negativum sumendum).

Ex. 1° pro $p=13$, habentur radices primitivae 2, 6, 7, 11, quarum summa $26\equiv 0 \pmod{13}$.

2° pro $p=11$, radices primitivae sunt 2, 6, 7, 8 quarum summa $23\equiv +1 \pmod{11}$.

3° pro $p=31$, radices primitivae sunt 3, 11, 12, 13, 17, 21, 22, 24, quarum summa, $123\equiv -1 \pmod{31}$.

Demonstr. Supra demonstravimus (art. 55, II), si $p-1$ fuerit $=a^\alpha b^\beta c^\gamma$ etc. (designantibus a, b, c etc. numeros primos inaequales) atque A, B, C etc. numeri quicunque ad exponentes $a^\alpha, b^\beta, c^\gamma$ etc. respective pertinentes, omnia producta ABC etc. exhibere radices primitivas. Facile vero etiam demonstrari potest, quamvis radicem primitivam per huiusmodi productum exhiberi posse et quidem unico tantum modo *).

Unde sequitur haec producta loco ipsarum radicum primitivarum accipi posse. At quoniam in his productis omnes valores ipsius A cum omnibus ipsius B etc. combinari oportet, omnium horum productorum summa aequalis est producto ex summa omnium valorum ipsius A, in summam omnium valorum ipsius B, in summam omnium valorum ipsius C etc. uti ex doctrina combinationum notum est. Designentur omnes valores ipsorum A; B etc., per A, A', A'' etc.; B, B', B'' etc. etc., eritque summa omnium radicum primitivarum

$$\equiv (A+A'+\text{etc.})\,(B+B'+\text{etc.})\,\text{etc.}$$

Iam dico, si exponens α fuerit $=1$, summam $A+A'+A''+$etc. fore $\equiv -1 \pmod{p}$, si vero α fuerit >1, summam hanc fore $\equiv 0$, similiterque de reliquis δ, γ etc. Simulac haec erunt demonstrata, theorematis nostri veritas mani-

*) Determinentur scilicet numeri α, β, γ, etc. ita, ut sit $\alpha\equiv 1 \pmod{a^\alpha}$ et $\equiv 0 \pmod{b^\beta c^\gamma}$ etc.); $\beta\equiv 1 \pmod{b^\beta}$ et $\equiv 0 \pmod{a^\alpha c^\gamma}$ etc.) etc. (vid. art. 32), unde fiet $\alpha+\beta+\gamma+$ etc. $\equiv 1 \pmod{p-1}$, (art. 19). Iam si radix primitiva quaecunque, r, per productum ABC etc. exhiberi debet accipiatur $A\equiv r^\alpha$, $B\equiv r^\beta$, $C\equiv r^\gamma$ etc., atque pertinebunt A ad exponentem a^α, B ad exponentem b^β etc.; productumque ex omnibus A, B, C etc. erit $\equiv r \pmod{p}$; denique facile perspicitur A, B, C etc. alio modo determinari non posse.

festa erit. Quando enim $p-1$ per quadratum aliquod divisibilis est, aliquis exponentium α, β, γ etc. unitatem superabit, adeoque aliquis factorum, quorum producto congrua est summa omnium radicum primitivarum, erit $\equiv 0$, et proin etiam productum ipsum: quando vero $p-1$ per nullum quadratum dividi potest, omnes exponentes α, β, γ etc. erunt $=1$, unde summa omnium radicum primitivarum congrua erit producto ex tot factoribus, quorum quisque $\equiv -1$, quot habentur numeri a, b, c etc., adeoque erit $\equiv \pm 1$, prout horum numerorum multitudo par vel impar. Illa autem ita probantur.

1°. Quando $\alpha = 1$ atque A numerus ad exponentem a pertinens, reliqui numeri ad hunc exponentem pertinentes erunt $A^2, A^3, \ldots A^{a-1}$. At

$$1 + A + A^2 + A^3 \ldots + A^{a-1}$$

est summa periodi completae, adeoque $\equiv 0$ (art. 79), quare

$$A + A^2 + A^3 \ldots + A^{a-1} \equiv -1$$

2°. Quando autem $\alpha > 1$, atque A numerus ad exponentem a^2 pertinens, reliqui numeri ad hunc exponentem pertinentes habebuntur, si ex his $A^2, A^3, A^4 \ldots A^{a^2-1}$ reiiciuntur A^a, A^{2a}, A^{3a} etc., vid art. 53; quare summa eorum erit

$$\equiv 1 + A + A^2 \ldots + A^{a^2-1} - (1 + A^a + A^{2a} \ldots + A^{a^2-a})$$

i. e. congrua differentiae duarum periodorum, adeoque $\equiv 0$. *Q. E. D.*

De modulis qui sunt numerorum primorum potestates.

82.

Omnia quae hactenus exposuimus innituntur suppositioni, modulum esse numerum primum. Superest ut eum quoque casum consideremus, ubi pro modulo assumitur numerus compositus. Attamen quum hic neque proprietates tam elegantes eniteant, quam in casu priori, neque ad eas inveniendas artificiis subtilibus sit opus, sed potius omnia fere per solam principiorum praecedentium applicationem erui possint, omnes minutias hic exhaurire superfluum atque taediosum foret. Breviter itaque quae huic casui cum priori sint communia quaeque propria exponemus.

83.

Propositiones artt. 45—48 generaliter iam sunt demonstratae. At prop. art. 49 ita immutari debet:

Si f designat, quot numeri dentur ad m primi simul ipso m minores, i. e. si $f = \phi m$ (art. 38): exponens t infimae potestatis numeri dati a ad m primi, quae secundum modulum m unitati est congrua, vel erit $= f$ vel pars aliquota huius numeri.

Demonstratio prop. art. 49 etiam pro hoc casu valere potest, si modo ubique loco ipsius p, m, loco ipsius $p-1$, f, et loco numerorum $1, 2, 3, \ldots p-1$, numeri ad m primi simulque ipso m minores substituantur. Huc itaque lectorem ablegamus. Ceterum demonstrationes reliquae de quibus illic locuti sumus (artt. 50, 51) non sine multis ambagibus ad hunc casum applicari possunt. — At respectu propositionum sequentium, art. 52 sqq. magna differentia incipit inter modulos, qui numerorum primorum sunt potestates, eosque, qui per plures numeros primos dividi possunt. Seorsim itaque modulos prioris generis comtemplabimur.

84.

Si modulus $m = p^n$, designante p numerum primum, erit $f = p^{n-1}(p-1)$ (art. 38). Iam si disquisitiones in artt. 53, 54 contentae ad hunc casum applicantur, mutatis mutandis uti in art. praec. praescripsimus, invenietur, omnia quae ibi demonstrata sunt etiam pro hoc casu locum habere, si modo ante probatum esset, congruentiam formae $x^t - 1 \equiv 0 \pmod{p^n}$ plures quam t radices diversas habere non posse. Pro modulo primo hanc veritatem ex propositione generaliori art. 43 deduximus, quae autem in omni sua extensione de modulis primis tantummodo valet, neque adeo ad hunc casum applicanda. Attamen propositionem pro hoc casu particulari veram esse per methodum singularem demonstrabimus. Infra (sect. VIII) idem facilius invenire docebimus.

85.

Demonstrandum proponimus nobis hoc theorema:

Si numerorum t et $p^{n-1}(p-1)$ divisor communis maximus est e, congruentia $x^t \equiv 1 \pmod{p^n}$ habebit e radices diversas.

Sit $e = kp^\nu$ ita ut k factorem p non involvat, adeoque numerum $p-1$

metiatur. Tum congruentia $x^t \equiv 1$ secundum modulum p habebit k radices diversas, quibus per A, B, C etc. designatis, radix quaecunque eiusdem congruentiae secundum modulum p^n, congrua esse debet secundum modulum p alicui numerorum A, B, C etc. Iam demonstrabimus, congruentiam $x^t \equiv 1 \pmod{p^m}$ habere p^ν radices ipsi A, totidem ipsi B etc. congruas secundum modulum p. Quo facto omnium radicum numerus erit kp^ν sive e, uti diximus. Illam vero demonstrationem ita adornabimus, ut *primo* ostendamus, si α fuerit radix ipsi A secundum modulum p congrua, etiam

$$\alpha + p^{m-\nu},\ \alpha + 2p^{m-\nu},\ \alpha + 3p^{m-\nu}, \ldots \alpha + (p^\nu - 1)\, p^{m-\nu}$$

fore radices; *secundo*, numeros ipsi A secundum modulum p congruos alios quam qui in forma $\alpha + hp^{m-\nu}$ sint comprehensi (denotante h integrum quemcunque), radices esse non posse: unde manifesto p^ν radices diversae habebuntur, et non plures: atque idem etiam de radicibus, quae singulis B, C etc. sunt congruae, locum habebit: *tertio* docebimus, quomodo semper radix, ipsi A secundum p congrua, inveniri possit.

86.

Theorema. *Si uti in art. praec. t est numerus per p^ν, neque vero per $p^{\nu+1}$ divisibilis, erit*

$$(\alpha + hp^m)^t - \alpha^t \equiv 0 \,(mod.\, p^{m+\nu}),\ at \equiv \alpha^{t-1} hp^m t \,(mod.\, p^{m+\nu+1})$$

Theorematis pars posterior locum non habet, quando $p = 2$ simulque $\mu = 1$.

Demonstratio huius theorematis ex evolutione potestatis binomii peti posset, si ostenderetur omnes terminos post secundum per $p^{\mu+\nu+1}$ divisibiles esse. Sed quoniam consideratio denominatorum coefficientium in aliquot ambages deducit, methodum sequentem praeferimus.

Ponamus *primo* $\mu > 1$ atque $\nu = 1$, eritque propter

$$x^t - y^t = (x-y)(x^{t-1} + x^{t-2}y + x^{t-3}y^2 + \text{etc.} + y^{t-1})$$

$$(\alpha + hp^m)^t - \alpha^t = hp^\mu \left((\alpha + hp^m)^{t-1} + (\alpha + hp^m)^{t-2}\alpha + \text{etc.} + \alpha^{t-1}\right)$$

At est

$$\alpha + hp^\mu \equiv \alpha \,(\text{mod.}\, p^2)$$

quare quisque terminus $(\alpha + hp^m)^{t-1}$, $(\alpha + hp^m)^{t-2}\alpha$ etc. erit $\equiv \alpha^{t-1} \,(\text{mod.}\, p^2)$, adeoque omnium summa $\equiv t\alpha^{t-1} \,(\text{mod.}\, p^2)$ sive formae $t\alpha^{t-1} + Vp^2$ denotante V numerum quemcunque. Hinc $(\alpha + hp^m)^t - \alpha^t$ erit formae

$$\alpha^{t-1} hp^\mu t + Vhp^{\mu+2},\ i.e. \equiv \alpha^{t-1} hp^\mu t \,(\text{mod.}\, p^{\mu+2}) \text{ et } \equiv 0 \,(\text{mod.}\, p^{\mu+1}).$$

Pro hoc itaque casu theorema est demonstratum.

Iam si theorema pro aliis ipsius ν valoribus verum non esset, manente etiamnum $\mu > 1$, limes aliquis necessario daretur, usque ad quem theorema semper verum foret, ultra vero falsum. Sit minimus valor ipsius ν, pro quo falsum est $= \varrho$, unde facile perspicitur, si t per $p^{\varrho-1}$ non autem per p^ϱ fuerit divisibilis, theorema adhuc verum esse, at si loco ipsius t substituatur tp, falsum. Habemus itaque

$$(\alpha + hp^m)^t \equiv \alpha^t + \alpha^{t-1} hp^\mu t \,(\text{mod.}\, p^{\mu+\varrho}) \text{ sive } = \alpha^t + \alpha^{t-1} hp^\mu t + up^{\mu+\varrho}$$

denotante u numerum integrum. At quia pro $\nu = 1$ theorema iam est demonstratum, erit

$$(\alpha^t + \alpha^{t-1} hp^\mu t + up^{\mu+\varrho})^p \equiv \alpha^{tp} + \alpha^{tp-1} hp^{\mu+1} t + \alpha^{tp-t} up^{\mu+\varrho+1} \,(\text{mod.}\, p^{\mu+\varrho+1})$$

adeoque etiam

$$(\alpha + hp^m)^{tp} \equiv \alpha^{tp} + \alpha^{tp-1} hp^\mu tp \,(\text{mod.}\, p^{\mu+\varrho+1})$$

i.e. theorema etiam verum, si loco ipsius t substituitur tp, *i.e.* etiam pro $\nu = \varrho$, contra hypothesin. Unde manifestum pro omnibus ipsius ν valoribus theorema verum esse.

87.

Superest casus ubi $\mu = 1$. Per methodum prorsus similem ei qua in art. praec. usi sumus, sine adiumento theorematis binomialis demonstrari potest, esse

$$\begin{aligned} (\alpha + hp)^{t-1} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-1)hp \pmod{p^2} \\ \alpha(\alpha + hp)^{t-2} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-2)hp \\ \alpha\alpha(\alpha + hp)^{t-3} &\equiv \alpha^{t-1} + \alpha^{t-2}(t-3)hp \\ &\text{etc.} \end{aligned}$$

unde aggregatum erit (quia partium multitudo $= t$)

$$\equiv t\alpha^{t-1}+\tfrac{(t-1)t}{2}\alpha^{t-2}hp \pmod{p^3}$$

At quoniam t per p divisibilis, etiam $\frac{(t-1)t}{2}$ per p divisibilis erit in omnibus casibus excepto eo ubi $p=2$ de quo iam in art. praec. monuimus. In reliquis autem casibus erit $\frac{(t-1)t}{2}\alpha^{t-2}hp\equiv 0 \pmod{p^2}$, adeoque etiam illud aggregatum $\equiv t\alpha^{t-1} \pmod{p^2}$ ut in art. praec. In reliquis demonstratio hic eodem modo procedit ut istic.

Colligimus igitur generaliter unico casu $p=2$ excepto, esse

$$(\alpha+hp^n)^t \equiv \alpha^t \pmod{p^{n+\nu}}$$

et $(\alpha+hp^n)^t$ *non* $\equiv \alpha^t$ pro quovis modulo qui sit altior potestas ipsius p, quam haec $p^{n+\nu}$, quoties quidem h per p non est divisibilis, atque p^ν potestas suprema ipsius p quae numerum t dividit.

Hinc protinus derivantur propositiones 1. et 2. quas art. 85 demonstrandas nobis proposueramus: scilicet

primo, si $\alpha^t\equiv 1$, erit etiam $(\alpha+hp^{n-\nu})^t\equiv 1 \pmod{p^n}$;

secundo si numerus aliquis α' ipsi A adeoque etiam ipsi α secundum modulum p congruus, neque vero huic secundum modulum $p^{n-\nu}$, congruentiae $x^t\equiv 1 \pmod{p^n}$ satisfaceret, ponamus α' esse $=\alpha+lp^\lambda$, ita ut l per p non sit divisibilis, eritque $\lambda<n-\nu$, tunc autem $(\alpha+lp^\lambda)^t$ secundum modulum $p^{\lambda+\nu}$ ipsi α^t congruus erit, non autem secundum modulum p^n, quae est altior potestas, quare α' radix congruentiae $x^t\equiv 1$ esse nequit.

88.

Tertium vero fuit radicem aliquam congruentiae $x^t\equiv 1 \pmod{p^n}$, ipsi A congruam, invenire. Ostendemus hic tantummodo quomodo hoc fieri possit, si iam radix eiusdem congruentiae secundum modulum p^{n-1} innotuerit; manifesto hoc sufficit, quum a modulo p pro quo A est radix, ad modulum p^2, sicque deinceps ad omnes potestates consecutivas progredi possimus.

Esto itaque α radix congruentiae $x^t\equiv 1 \pmod{p^{n-1}}$ quaeriturque radix eiusdem congruentiae secundum modulum p^n, ponatur haec $=\alpha+hp^{n-\nu-1}$, quam formam eam habere debere ex art. praec. sequitur (casum ubi $\nu=n-1$ postea seorsim considerabimus: maior vero quam $n-1$, ν esse nequit). Debet itaque esse

$$(\alpha+hp^{n-\nu-1})^t \equiv 1 \pmod{p^{n-1}}$$

At
$$(\alpha+hp^{n-\nu-1})^t \equiv \alpha^t+\alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}$$

Si itaque h ita determinatur, ut fiat $1\equiv\alpha^t+\alpha^{t-1}htp^{n-\nu-1} \pmod{p^n}$; sive (quia per hyp. $1\equiv\alpha^t \pmod{p^{n-1}}$ atque t per p^ν divisibilis) ita ut fiat $\frac{\alpha^t-1}{p^{n-1}}+\alpha^{t-1}h\frac{t}{p^\nu}$ per p divisibilis, quaesito satisfactum erit. Hoc autem semper fieri posse ex Sect. praec. manifestum, quum t per altiorem ipsius p potestatem quam p^ν dividi non posse hic supponamus, adeoque $\alpha^{t-1}\frac{t}{p^\nu}$ ad p sit primus.

Si vero $\nu=n-1$ *i. e.* t per p^{n-1} sive etiam per altiorem ipsius p potestatem divisibilis, quivis valor A congruentiae $x^t\equiv 1$ secundum modulum p satisfaciens eidem etiam secundum modulum p^n satisfaciet. Sit enim $t=p^{n-1}\tau$, eritque $t\equiv\tau \pmod{p-1}$: quare quoniam $A^t\equiv 1 \pmod{p}$ erit etiam $A^\tau\equiv 1 \pmod{p}$. Ponatur itaque $A^\tau=1+hp$ eritque $A^t=(1+hp)^{p^{n-1}}\equiv 1 \pmod{p^n}$ art. 87.

89.

Omnia quae art. 57 sqq. adiumento theorematis, congruentiam $x^t\equiv 1$ plures quam t radices diversas non habere eruimus, etiam pro modulo qui est numeri primi potestas locum habent, et si *radices primitivae* vocantur numeri, qui ad exponentem $p^{n-1}(p-1)$ pertinent, sive in quorum periodis omnes numeri per p non divisibiles inveniuntur, etiam hic radices primitivae exstabunt. Omnia autem quae supra de indicibus eorumque usu tradidimus, necnon de solutione congruentiae $x^t\equiv 1$, ad hunc quoque casum applicari possunt. Quae quum nulli difficultati obnoxia sint omnia ex integro repetere superfluum foret. Praeterea radices congruentiae $x^t\equiv 1$ secundum modulum p^n e radicibus eiusdem congruentiae secundum p deducere docuimus. Sed de eo casu ubi potestas aliqua numeri 2 est modulus, quia supra exceptus fuit, aliqua adhuc sunt adiicienda.

Moduli qui sunt potestates binarii.

90.

Si potestas aliqua numeri 2, altior quam secunda, puta 2^n pro modulo accipitur, numeri cuiusvis imparis potestas exponentis 2^{n-2}, unitati est congrua.

Ex. gr. $3^8 = 6561 \equiv 1 \pmod{32}$.

Quivis enim numerus impar vel sub forma $1+4h$, vel sub hac $-1+4h$ comprehenditur: unde propositio protinus sequitur (theor. art. 86).

Quoniam igitur exponens ad quem quicunque numerus impar secundum modulum 2^n pertinet, divisor ipsius 2^{n-2} esse debet, quivis ad aliquem horum numerum pertinebit $1, 2, 4, 8, \ldots 2^{n-2}$, ad quemnam vero pertineat ita facile diindicatur. Sit numerus propositus $= 4h \pm 1$, atque exponens maximae potestatis numeri 2, quae ipsum h metitur, $= m$ (qui etiam $= 0$ esse potest, quando scilicet h est impar); tum exponens ad quem numerus propositus pertinet, erit $= 2^{n-m-2}$, siquidem $n > m+2$; si autem $n =$ vel $< m+2$, numerus propositus est $\equiv \pm 1$ adeoque vel ad exponentem 1 vel ad exponentem 2 pertinebit. Numerum enim formae $\pm 1 + 2^{m+2}k$, (quae huic aequivalet, $4h \pm 1$) ad potestatem exponentis 2^{n-m-2} elevatum unitati secundum modulum 2^n congruum fieri, ad potestatem autem exponentis, qui est inferior numeri 2 potestas, incongruum, ex art. 86 nullo negotio deducitur. Numerus itaque quicunque formae $8k+3$ vel $8k+5$ ad exponentem 2^{n-2} pertinebit.

91.

Hinc patet eo sensu quo supra expressionem accepimus, *radices primitivas* hic non dari, nullos scilicet numeros, quorum periodus omnes numeros modulo minores ad ipsumque primos amplectatur. Attamen facile perspicitur, analogon hic haberi. Invenitur enim, numeri formae $8k+3$ potestatem exponentis imparis semper esse formae $8k+3$, potestatem autem exponentis paris, semper formae $8k+1$; nulla igitur potestas formae $8k+5$ aut $8k+7$ esse potest. Quare quum periodus numeri formae $8k+3$, ex 2^{n-2} terminis diversis constet, quorum quisque aut formae $8k+3$ aut huius $8k+1$, neque plures huiusmodi numeri modulo minores dentur quam 2^{n-2}, manifesto quivis numerus formae $8k+1$ vel $8k+3$ congruus est secundum modulum 2^n potestati alicui numeri cujuscunque formae $8k+3$. Simili modo ostendi potest periodum numeri formae $8k+5$ comprehendere omnes numeros formarum $8k+1$ et $8k+5$. Si igitur numerus formae $8k+5$ pro basi assumitur, omnes numeri formae $8k+1$ et $8k+5$, positive, omnesque formae $8k+3$ et $8k+7$, negative sumti, indices reales nanciscentur, et quidem hic indices secundum 2^{n-2} congrui pro aequivalentibus sunt habendi. Hoc modo tabula nostra I intelligenda, ubi pro modulis 16, 32 et 64

(namque pro modulo 8 nulla tabula necessaria erit) semper numerum 5 pro basi accepimus. *Ex. gr.* numero 19 qui est formae $8n+3$ adeoque *negative* sumendus, respondet pro modulo 64 index 7, id quod significat esse $5^7 \equiv -19 \pmod{64}$. Numeris autem formarum $8n+1$, $8n+5$ negative, atque numeris formarum $8n+3$, $8n+7$ positive acceptis, indices quasi imaginarii tribuendi forent. Quos introducendo calculus indicum ad algorithmum perquam simplicem reduci potest. Sed quoniam, si haec ad omnem rigorem exponere vellemus, nimis longe evagari oporteret, hoc negotium ad aliam occasionem nobis reservamus, quando forsan fusius quantitatum imaginarium theoriam, quae nostro quidem iudicio a nemine hactenus ad notiones claras est reducta, pertractare suscipiemus. Periti hunc algorithmum facile ipsi eruent: qui minus sunt exercitati, perinde tamen tabula hac uti poterunt, ut ii qui recentiorum commenta de *logarithmis* imaginariis ignorant, logarithmis utuntur, si quidem principia supra stabilita probe tenuerint.

Moduli e pluribus primis compositi.

92.

Secundum modulum e pluribus primis compositum tantum non omnia quae ad residua potestatum pertinent ex theoria congruentiarum generali deduci possunt; quia vero infra congruentias quascunque secundum modulum e pluribus primis compositum ad congruentias, quarum modulus est primus aut primi potestas, reducere fusius docebimus, non est quod huic rei multum hic immoremur. Observamus tantum, bellissimam proprietatem, quae pro reliquis modulis locum habeat, quod scilicet semper exstent numeri quorum periodus omnes numeros ad modulum primos complectatur, hic deficere, excepto unico casu, quando scilicet modulus est duplum numeri primi, aut potestatis numeri primi. Si enim modulus m redigitur ad formam $A^a B^b C^c$ etc. designantibus A, B, C etc. numeros primos diversos, praeterea $A^{a-1}(A-1)$ designatur per α, $B^{b-1}(B-1)$ per $\mathfrak{b}$ etc. denique z est numerus ad m primus; erit $z^\alpha \equiv 1 \pmod{A^a}$, $z^\mathfrak{b} \equiv 1 \pmod{B^b}$ etc. Quodsi igitur μ est minimus numerorum $\alpha, \mathfrak{b}, \gamma$ etc. dividuus communis, erit $z^\mu \equiv 1$ secundum omnes modulos A^a, B^b etc. adeoque etiam secundum m, cui illorum productum est aequale. At excepto casu ubi m est duplum numeri primi aut potestatis numeri primi, numerorum $\alpha, \mathfrak{b}, \gamma$ etc. dividuus communis minimus, ipsorum producto est minor (quoniam numeri $\alpha, \mathfrak{b}, \gamma$ etc. inter se primi esse nequeunt sed certe divisorem 2 communem habent). Nullius itaque numeri

periodus tot terminos comprehendere potest, quot dantur numeri ad modulum primi ipsoque minores, quia horum numerus producto ex α, δ, γ etc. est aequalis. Ita *ex. gr.* pro $m = 1001$ cuiusvis numeri ad m primi potestas exponentis 60 unitati est congrua, quia 60 est dividuus communis numerorum 6, 10, 12. — Casus autem ubi modulus est duplum numeri primi aut duplum potestatis numeri primi illi ubi est primus aut primi potestas prorsus est similis.

93.

Scriptorum in quibus alii geometrae de argumento in hac sectione pertractato egerunt, iam passim mentio est facta. Eos tamen qui quaedam fusius, quam nobis brevitas permisit, explicata desiderant, ablegamus imprimis ad sequentes ill. Euleri commentationes, ob perspicuitatem qua vir summus prae omnibus semper excelluit, maxime commendabiles.

Theoremata circa residua ex divisione potestatum relicta Comm. nov. Petr. T. VII *p.* 49 sqq.

Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia. Ibid. T. XVIII *p.* 85 sqq.

Adiungi his possunt *Opusculorum analyt. T.* I, *dissertt.* 5 et 8.

SECTIO QUARTA

DE

CONGRUENTIIS SECUNDI GRADUS.

Residua et non-residua quadratica.

94.

THEOREMA. *Numero quocunque m pro modulo accepto, ex numeris* $0, 1, 2, 3 \ldots m-1$, *plures quam* $\frac{1}{2}m+1$ *quando m est par, sive plures quam* $\frac{1}{2}m+\frac{1}{2}$, *quando m est impar quadrato congrui fieri non possunt.*

Dem. Quoniam numerorum congruorum quadrata sunt congrua; quivis numerus, qui ulli quadrato congruus fieri potest, etiam quadrato alicui cuius radix $< m$ congruus erit. Sufficit itaque residua minima quadratorum $0, 1, 4, 9 \ldots (m-1)^2$ considerare. At facile perspicitur, esse $(m-1)^2 \equiv 1$, $(m-2)^2 \equiv 2^2$, $(m-3)^2 \equiv 3^2$ etc. Hinc etiam, quando m est par, quadratorum $(\frac{1}{2}m-1)^2$ et $(\frac{1}{2}m+1)^2$, $(\frac{1}{2}m-2)^2$ et $(\frac{1}{2}m+2)^2$ etc. residua minima eadem erunt: quando vero m est impar, quadrata $(\frac{1}{2}m-\frac{1}{2})^2$ et $(\frac{1}{2}m+\frac{1}{2})^2$, $(\frac{1}{2}m-\frac{3}{2})^2$ et $(\frac{1}{2}m+\frac{3}{2})^2$ etc. erunt congrua. Unde palam est, alios numeros, quam qui alicui ex quadratis $0, 1, 4, 9 \ldots (\frac{1}{2}m)^2$ congrui sint, quadrato congruos fieri non posse, quando m par; quando vero impar, quemvis numerum, qui ulli quadrato sit congruus, alicui ex his $0, 1, 4, 9 \ldots (\frac{1}{2}m-\frac{1}{2})^2$ necessario congruum esse. Quare dabuntur ad summum in priori casu $\frac{1}{2}m+1$ residua minima diversa, in posteriori $\frac{1}{2}m+\frac{1}{2}$. *Q. E. D.*

Exemplum. Secundum modulum 13 quadratorum numerorum $0, 1, 2, 3 \ldots 6$ residua minima inveniuntur $0, 1, 4, 9, 3, 12, 10$, post haec vero eadem

ordine inverso recurrunt 10, 12, 3 etc. Quare numerus quisque, nulli ex istis residuis congruus, sive qui alicui ex his est congruus, 2, 5, 6, 7, 8, 11, nulli quadrato congruus esse potest.

Secundum modulum 15 haec inveniuntur residua 0, 1, 4, 9, 1, 10, 6, 4 post quae eadem ordine inverso recurrunt. Hic igitur numerus residuorum, quae quadrato congrua fieri possunt, minor adhuc est quam $\frac{1}{2}m+\frac{1}{2}$, quum sint 0, 1, 4, 6, 9, 10. Numeri autem 2, 3, 5, 7, 8, 11, 12, 13, 14 et qui horum alicui sunt congrui, nulli quadrato secundum mod. 15 congrui fieri possunt.

95.

Hinc colligitur, pro quovis modulo omnes numeros in duas classes distingui posse, quarum altera contineat numeros, qui quadrato alicui congrui fieri possint, altera eos qui non possint. Illos appellabimus *residua quadratica numeri istius quem pro modulo accepimus**), hos vero *ipsius non-residua quadratica*, sive etiam, quoties ambiguitas nulla inde oriri potest, simpliciter *residua* et *non-residua*. Ceterum palam est sufficere, si omnes numeri $0, 1, 2 \ldots m-1$ in classes redacti sint: numeri enim congrui ad eandem classem erunt referendi.

Etiam in hac disquisitione a modulis primis initium faciemus, quod itaque subintelligendum erit, etiamsi expressis verbis non moneatur. Numerus primus 2 autem excludendus, sive numeri primi *impares* tantum considerandi.

Quoties modulus est numerus primus, multitudo residuorum ipso minorum multitudini non-residuorum aequalis.

96.

Numero primo p pro modulo accepto, numerorum $1, 2, 3 \ldots p-1$ semissis erunt residua quadratica, reliqui non-residua, i. e. dabuntur $\frac{1}{2}(p-1)$ residua totidemque non-residua.

Facile enim probatur, omnia quadrata $1, 4, 9 \ldots \frac{1}{4}(p-1)^2$ esse incongrua. Scilicet si fieri posset $rr \equiv r'r' \pmod{p}$ atque numeri r, r' inaequales et non maiores quam $\frac{1}{2}(p-1)$ posito $r > r'$ i. q. licet, fieret $(r-r')(r+r')$ positivus et

*) Proprie quidem hic casu secundo alio sensu utimur, quam hucusque fecimus. Dicere scilicet oporteret, r esse residuum quadrati aa secundum modulum m quando $r \equiv aa \pmod{m}$; at brevitatis gratia in hac sectione semper r *ipsius* m residuum quadraticum vocamus neque hinc ulla ambiguitas metuenda. Expressionem enim, *residuum*, quando idem significat quod numerus congruus, abhinc non adhibebimus, nisi forte de residuis *minimis* sermo sit, ubi nullum dubium esse potest.

per p divisibilis. At uterque factor $r-r'$, et $r+r'$ ipso p est minor, quare suppositio consistere nequit (art. 13). Habentur itaque $\frac{1}{2}(p-1)$ residua quadratica inter hos numeros $1, 2, 3 \ldots p-1$ contenta; plura vero inter ipsos esse nequeunt quia accedente residuo 0 prodeunt $\frac{1}{2}(p+1)$, quem numerum omnium residuorum multitudo superare nequit. Quare reliqui numeri erunt non-residua horumque multitudo $= \frac{1}{2}(p-1)$.

Quum cifra semper sit residuum, hanc numerosque per modulum divisibiles ab investigationibus his excludimus, quia hic casus per se est clarus, theorematumque concinnitatem tantum turbaret. Ex eadem caussa etiam modulum 2 exclusimus.

97.

Quum plura quae in hac Sect. exponemus etiam ex principiis Sect. praec. derivari possint, neque inutile sit, eandem veritatem per methodos diversas perscrutari, hunc nexum ostendemus. Facile vero intelligitur, omnes numeros quadrato congruos, indices *pares* habere, eos contra, qui quadrato nullo modo congrui fieri possint, impares. Quia vero $p-1$ est numerus par, tot indices pares erunt quot impares, scilicet $\frac{1}{2}(p-1)$, totidemque tum residua tum non-residua dabuntur.

Exempla. Pro modulis sunt residua

3 . . . . . 1.
5 . . . . . 1, 4.
7 . . . . . 1, 2, 4.
11 . . . . . 1, 3, 4, 5, 9.
13 . . . . . 1, 3, 4, 9, 10, 12.
17 . . . . . 1, 2, 4, 8, 9, 13, 15, 16.

etc.

reliqui vero numeri his modulis minores, non-residua.

Quaestio, utrum numerus compositus residuum numeri primi dati sit an non-residuum, ab indole factorum pendet.

98.

Theorema. *Productum e duobus residuis quadraticis numeri primi p, est residuum; productum e residuo in non-residuum, est non-residuum; denique productum e duobus non-residuis, residuum.*

Demonstr. I. Sint A, B residua e quadratis aa, bb oriunda sive $A \equiv aa$, $B \equiv bb$, eritque productum AB quadrato numeri ab congruum *i. e.* residuum.

II. Quando A est residuum, puta $\equiv aa$, B vero non-residuum, AB erit non-residuum. Ponatur enim si fieri potest $AB \equiv kk$, sitque valor expressionis $\frac{k}{a} (\mathrm{mod}.p) \equiv b$; erit itaque $aaB \equiv aabb$, unde $B \equiv bb$, *i. e.* B residuum contra hyp.

Aliter. Multiplicentur omnes numeri qui inter hos $1, 2, 3 \ldots . p-1$ sunt residua (quorum multitudo $= \frac{1}{2}(p-1)$), per A omniaque producta erunt residua quadratica, et quidem erunt omnia incongrua. Iam si non-residuum B per A multiplicatur, productum nulli productorum quae iam habentur congruum erit; quare si residuum esset, haberentur $\frac{1}{2}(p+1)$ residua incongrua inter quae nondum est residuum 0, contra art. 96.

III. Sint A, B non-residua. Multiplicentur omnes numeri qui inter hos $1, 2, 3 \ldots . p-1$ sunt residua per A, habebunturque $\frac{1}{2}(p-1)$ non-residua inter se incongrua (II); iam productum AB nulli illorum congruum esse potest, quodsi igitur esset non-residuum, haberentur $\frac{1}{2}(p+1)$ non-residua inter se incongrua, contra art. 96. Quare productum etc. *Q. E. D.*

Facilius adhuc haec theoremata e principiis sect. praec. derivantur. Quia enim residuorum indices semper sunt pares, non-residuorum vero impares, index producti e duobus residuis vel non-residuis erit par, adeoque productum ipsum, residuum. Contra index producti e residuo in non-residuum erit impar adeoque productum ipsum non-residuum.

Utraque demonstrandi methodus etiam pro his theorematibus adhiberi potest: *Expressionis* $\frac{a}{b} (mod.p)$ *valor erit residuum, quando numeri* a, b *simul sunt residua, vel simul non-residua; contra autem erit non-residuum, quando numerorum* a, b *alter est residuum alter non-residuum.* Possunt etiam ex conversione theorr. praecc. obtineri.

99.

Generaliter, productum ex quotcunque factoribus est residuum tum quando omnes sunt residua, tum quando non-residuorum, quae inter eos occurrunt, multitudo est par; quando vero multitudo non-residuorum quae inter factores reperiuntur est impar, productum erit non-residuum. Facile itaque diiudicari potest,

utrum numerus compositus sit residuum necne, si modo quid sint singuli ipsius factores constet. Quamobrem in tabula II numeros primos tantummodo recepimus. Oeconomia huius tabulae haec est. In margine positi sunt moduli *), in facie vero numeri primi successivi; quando ex his aliquis fuit residuum moduli alicuius, in spatio utrique respondente lineola collocata est, quando vero numerus primus fuit non-residuum moduli, spatium respondens vacuum mansit.

De modulis, qui sunt numeri compositi.

100.

Antequam ad difficiliora progrediamur, quaedam de modulis non primis adiicienda sunt.

Si numeri primi p, potestas aliqua p^n pro modulo assumitur (ubi p non esse 2 supponimus), omnium numerorum per p non divisibilium moduloque minorum altera semissis erunt residua, altera non-residua, *i. e.* utrorumque multitudo $= \frac{1}{2}(p-1)p^{n-1}$.

Si enim r est residuum: quadrato alicui congruus erit, cuius radix moduli dimidium non superat, vid. art. 94. Iam facile perspicitur, dari $\frac{1}{2}(p-1)p^{n-1}$ numeros per p non divisibiles modulique semisse minoribus; superest itaque ut demonstretur, omnium horum numerorum quadrata incongrua esse, sive residua quadratica diversa suppeditare. Quodsi duorum numerorum a, b per p non divisibilium modulique semisse minorum quadrata essent congrua, foret $aa - bb$ sive $(a-b)(a+b)$ per p^n divisibilis (posito i. q. licet $a > b$). Hoc vero fieri non potest, nisi *vel* alter numerorum $a-b$. $a+b$ per p^n fuerit divisibilis, quod fieri nequit, quoniam uterque $< p^n$, *vel* alter per p^m alter vero per p^{n-m}, *i. e.* uterque per p. Sed etiam hoc fieri nequit. Manifesto enim etiam summa et differentia $2a$ et $2b$ per p foret divisibilis adeoque etiam a et b contra hyp. — Hinc tandem colligitur inter numeros per p non divisibiles moduloque minores $\frac{1}{2}(p-1)p^n$ residua dari, reliquos quorum multitudo aeque magna, esse non-residua *Q. E. D.* — Potest etiam theorema hoc ex consideratione indicum derivari simili modo ut art. 97.

101.

Quivis numerus per p *non divisibilis, qui ipsius* p *est residuum, erit residuum*

*) Quomodo etiam modulis compositis carere possimus mox docebimus.

etiam ipsius p^n; qui vero ipsius p est non-residuum, etiam ipsius p^n non-residuum erit.

Pars posterior huius propositionis per se est manifesta. Si itaque prior falsa esset, inter numeros ipso p^n minores simulque per p non divisibiles plures forent residua ipsius p quam ipsius p^n; *i. e.* plures quam $\frac{1}{2}p^{n-1}(p-1)$. Nullo vero negotio perspici poterit, multitudinem residuorum numeri p inter illos numeros esse praecise $=\frac{1}{2}p^{n-1}(p-1)$.

Aeque facile est, quadratum reipsa invenire, quod secundum modulum p^n residuo dato sit congruum, si quadratum huic residuo secundum modulum p congruum habetur.

Scilicet si quadratum habetur, aa, quod residuo dato A secundum modulum p^μ est congruum, deducitur inde quadratum ipsi A secundum modulum p^ν congruum (ubi $\nu > \mu$ et $=$ vel $< 2\mu$ supponitur) sequenti modo. Ponatur radix quadrati quaesiti $=\pm a + xp^\mu$, quam formam eam habere debere facile perspicitur; debetque esse $aa \pm 2axp^\mu + xxp^{2\mu} \equiv A \pmod{p^\nu}$ sive propter $2\mu > \nu$, $A - aa \equiv \pm 2axp^\mu \pmod{p^\nu}$. Sit $A - aa = p^\mu d$, eritque x valor expressionis $\pm\frac{d}{2a} \pmod{p^{\nu-\mu}}$, quae huic $\pm\frac{A-aa}{2ap^\mu} \pmod{p^\nu}$ aequivalet.

Dato igitur quadrato ipsi A secundum p congruo, deducitur inde quadratum ipsi A secundum modulum p^2 congruum; hinc ad modulum p^4, hinc ad p^8 etc. ascendi poterit.

Ex. Proposito residuo 6, quod secundum modulum 5 quadrato 1 congruum, invenitur quadratum 9^2 cui secundum 25 est congruum, 16^2 cui secundum 125 congruum etc.

102.

Quod vero attinet ad numeros per p divisibiles, patet, eorum quadrata per pp fore divisibilia, adeoque omnes numeros per p quidem divisibiles, neque vero per pp, ipsius p^n fore non residua. Generaliter vero, si proponitur numerus $p^k A$ ubi A per p non est divisibilis, hi casus erunt distinguendi:

1) Quando $k = $ vel $> n$, erit $p^k A \equiv 0 \pmod{p^n}$; *i. e.* residuum.

2) Quando $k < n$ atque impar, erit $p^k A$ non-residuum.

Si enim esset $p^k A = p^{2\varkappa+1} A \equiv ss \pmod{p^n}$, ss per $p^{2\varkappa+1}$ divisibilis esset, id quod aliter fieri nequit, quam si fuerit s per $p^{\varkappa+1}$ divisibilis. Tunc vero ss

etiam per $p^{2\varkappa+2}$ divisibilis, adeoque etiam (quia $2\varkappa+2$ certo non maior quam n) $p^k A$ *i. e.* $p^{2\varkappa+1}A$; sive A per p, contra hyp.

3) Quando $k < n$ atque par. Tum $p^k A$ erit residuum vel non-residuum ipsius p^n, prout A est residuum vel non-residuum ipsius p. Quando enim A est residuum ipsius p, erit etiam residuum ipsius p^{n-k}. Posito autem $A \equiv aa \pmod{p^{n-k}}$ erit $Ap^k \equiv aap^k \pmod{p^n}$, aap^k vero est quadratum. Quando autem A est non-residuum ipsius p, $p^k A$ residuum ipsius p^n esse nequit. Ponatur enim $p^k A \equiv aa \pmod{p^n}$, eritque necessario aa per p^k divisibilis. Quoties erit quadratum cui A secundum modulum p^{n-k} adeoque etiam secundum modulum p congruus, *i. e.* A erit residuum ipsius p contra hyp.

103.

Quoniam casum $p = 2$ exclusimus, de hoc adhuc quaedam dicenda. Quando numerus 2 est modulus, numerus quicunque erit residuum, non-residua nulla erunt. Quando vero 4 est modulus, omnes numeri impares formae $4k+1$ erunt residua, omnes vero formae $4k+3$ non-residua. Tandem quando 8 aut altior potestas numeri 2 est modulus, omnes numeri impares formae $8k+1$ erunt residua, reliqui vero, seu ii qui sunt formarum $8k+3$, $8k+5$, $8k+7$, erunt non-residua. Pars posterior huius propositionis inde clara, quod quadratum cuiusvis numeri imparis, sive sit formae $4k+1$, sive formae $4k-1$, fit formae $8k+1$. Priorem ita probamus.

1) Si duorum numerorum vel summa vel differentia per 2^{n-1} est divisibilis, numerorum quadrata erunt congrua secundum modulum 2^n. Si enim alter ponitur $= a$, erit alter formae $2^{n-1}h \pm a$, cuius quadratum invenitur $\equiv aa \pmod{2^n}$.

2) Quivis numerus impar, qui ipsius 2^n est residuum quadraticum, congruus erit quadrato alicui, cuius radix est numerus impar et $< 2^{n-2}$. Sit enim quadratum quodcunque, cui numerus ille congruus, $\alpha\alpha$ atque numerus $a \equiv \pm\alpha \pmod{2^{n-1}}$ ita ut α moduli semissem non superet (art. 4), eritque $aa \equiv \alpha\alpha$. Quare etiam numerus propositus erit $\equiv \alpha\alpha$. Manifesto vero tum a tum α erunt impares atque $\alpha < 2^{n-2}$.

3) Omnium numerorum imparium ipso 2^{n-2} minorum quadrata secundum 2^n incongrua erunt. Sint enim duo tales numeri r et s, quorum quadrata si secundum 2^n essent congrua, foret $(r-s)(r+s)$ per 2^n divisibilis (posito $r > s$). Facile vero perspicitur numeros $r-s$, $r+s$ simul per 4 divisibiles esse non

posse, quare si alter tantummodo per 2 est divisibilis, alter, ut productum per 2^n divisibilis fieret, per 2^{n-1} divisibilis esse deberet. *Q. E. A.* quoniam uterque $< 2^{n-2}$.

4) Quodsi denique haec quadrata ad *residua* sua *minima positiva* reducuntur, habebuntur 2^{n-3} residua quadratica diversa modulo minora*), quorum quodvis erit formae $8k+1$. Sed quum praecise 2^{n-3} numeri formae $8k+1$ modulo minores exstent, necessario hi omnes inter illa residua reperientur. *Q. E. D.*

Ut quadratum numero dato formae $8k+1$ secundum modulum 2^n congruum inveniatur, methodus similis adhiberi potest, ut in art. 101; vid. etiam art. 88. — Denique de numeris paribus eadem valent, quae art. 102 generaliter exposuimus.

104.

Circa multitudinem valorum diversorum (*i. e.* secundum modulum incongruorum), quos expressio talis $V \equiv \sqrt{A} \pmod{p^n}$ admittit, siquidem A est residuum ipsius p^n, facile e praecc. colliguntur haec. (Numerum p supponimus esse primum, ut ante, et brevitatis caussa casum $n=1$ statim includimus). I. Si A per p non est divisibilis, V *unum* valorem habet pro $p=2$, $n=1$, puta $V \equiv 1$; *duos*, quando p est impar, nec non pro $p=2$, $n=2$, puta ponendo unum $\equiv v$, alter erit $\equiv -v$; *quatuor* pro $p=2, n>2$, scilicet ponendo unum $\equiv v$, reliqui erunt $\equiv -v$, $2^{n-1}+v$, $2^{n-1}-v$. II. Si A per p divisibilis est, neque vero per p^n, sit potestas altissima ipsius p ipsum A metiens $p^{2\mu}$ (manifesto enim ipsius exponens par esse debebit) atque $A = ap^{2\mu}$. Tunc patet, omnes valores ipsius V per p^μ divisibiles esse, et quotientes e divisione ortos fieri valores expr. $V' \equiv \sqrt{a} \pmod{p^{n-2\mu}}$; hinc omnes valores diversi ipsius V prodibunt, multiplicando omnes valores expr. V' inter 0 et $p^{n-\mu}$ sitos per p^μ; quare illi exhibebuntur per

$$vp^\mu,\ vp^\mu + p^{n-\mu},\ vp^\mu + 2p^{n-\mu} \ldots vp^\mu + (p^\mu - 1)p^{n-\mu}$$

si v indefinite omnes valores *diversos* expr. V' exprimit, ita ut illorum multitudo fiat p^μ, $2p^\mu$ vel $4p^\mu$, prout multitudo horum (per casum I) est 1, 2 vel 4. III. Si A per p^m divisibilis est, facile perspicietur, statuendo $n = 2m$ vel $= 2m-1$, prout par est vel impar, omnes numeros per p^m divisibiles, neque ullos alios, esse valores ipsius V; quare omnes valores diversi hi erunt $0, p^m, 2p^m \ldots (p^{n-m}-1)p^m$, quorum multitudo p^{n-m}.

*) Puta quoniam multitudo numerorum imparium infra 2^{n-2} est 2^{n-3}.

105.

Superest casus, ubi modulus m e pluribus numeris primis compositus est. Sit $m = abc \ldots$, designantibus a, b, c etc. numeros primos diversos aut primorum diversorum potestates, patetque statim, si n sit residuum ipsius m, fore etiam n residuum singulorum a, b, c etc., adeoque n certo non-residuum ipsius m esse, si fuerit NR. ullius e numeris a, b, c etc. Vice versa autem, si n singulorum a, b, c etc. residuum est, etiam residuum producti m erit. Supponendo enim, $n \equiv A^2$, B^2, C^2 etc. sec. mod. a, b, c etc. resp., patet, si numerus N ipsis A, B, C etc. sec. mod. a, b, c etc. resp. congruus eruatur (art. 32), fore $n \equiv NN$ secundum omnes hos modulos adeoque etiam secundum productum m. — Quum facile perspiciatur, hoc modo e combinatione *cuiusvis* valoris ipsius A sive expr. $\sqrt{n} \pmod{a}$ cum *quovis* valore ipsius B cum *quovis* valore ipsius C etc. oriri valorem ipsius N sive expr. $\sqrt{n} \pmod{m}$, nec non e combinationibus diversis produci diversos N, et e cunctis cunctos: multitudo omnium valorum diversorum ipsius N aequalis erit producto e multitudinibus valorum ipsorum A, B, C etc. quas determinare in art. praec. docuimus. — Porro manifestum est, si unus valor expressionis $\sqrt{n} \pmod{m}$ sive ipsius N fuerit notus, hunc simul fore valorem omnium A, B, C etc.; et quum hinc per art. praec. omnes reliqui valores harum quantitatum deduci possint, facile sequitur, ex uno valore ipsius N omnes reliquos obtineri posse.

Ex. Sit modulus 315 cuius residuum an non-residuum sit 46, quaeritur. Divisores primi numeri 315 sunt 3, 5, 7, atque numerus 46 residuum cuiusvis eorum quare etiam ipsius 315 erit residuum. Porro, quia $46 \equiv 1$, et $\equiv 64 \pmod{9}$; $\equiv 1$ et $\equiv 16 \pmod{5}$; $\equiv 4$ et $\equiv 25 \pmod{7}$, inveniuntur radices quadratorum, quibus 46 secundum modulum 315 congruus. 19, 26, 44, 89, 226, 271, 289, 296.

Criterium generale, utrum numerus datus numeri primi dati residuum sit an non-residuum.

106.

Ex praecedentibus colligitur, si tantummodo semper dignosci possit utrum *numerus primus* datus numeri *primi dati* residuum sit an non-residuum, omnes reliquos casus ad hunc reduci posse. Pro illo itaque casu criteria certa omni studio nobis erunt indaganda. Antequam autem hanc perquisitionem aggrediamur, criterium quoddam exhibemus ex Sect. praec. petitum, quod quamvis in praxi nul-

lum fere usum habeat, tamen propter simplicitatem atque generalitatem memoratu dignum est.

Numerus quicunque A per numerum primum $2m+1$ non divisibilis, huius primi residuum est vel non-residuum, prout $A^m \equiv +1$ vel $\equiv -1 \pmod{2m+1}$.

Sit enim pro modulo $2m+1$ in systemate quocunque numeri A index a, eritque a par quando A est residuum ipsius $2m+1$, impar vero quando A non-residuum. At numeri A^m index erit ma, *i. e.* $\equiv 0$ vel $\equiv m \pmod{2m}$, prout a par vel impar. Hinc denique A^m in priori casu erit $\equiv +1$, in posteriori vero $\equiv -1 \pmod{2m+1}$. V. artt. 57, 62.

Ex. 3 ipsius 13 est residuum quia $3^6 \equiv 1 \pmod{13}$, 2 vero ipsius 13 non-residuum, quoniam $2^6 \equiv -1 \pmod{13}$.

At quoties numeri examinandi mediocriter sunt magni, hoc criterium ob calculi immensitatem prorsus inutile erit.

Disquisitiones de numeris primis quorum residua aut non-residua sint numeri dati.

107.

Facillimum quidem est, proposito modulo, omnes assignare numeros, qui ipsius residua sunt vel non-residua. Scilicet si ille numerus ponitur $= m$, determinari debent quadrata, quorum radices semissem ipsius m non superant, sive etiam numeri his quadratis secundum m congrui (ad praxin methodi adhuc expeditiores dantur), tuncque omnes numeri horum alicui secundum m congrui, erunt residua ipsius m, omnes autem numeri nulli istorum congrui erunt non-residua. — At quaestio inversa, *proposito numero aliquo, assignare omnes numeros quorum ille sit residuum vel non-residuum*, multo altioris est indaginis. Hoc itaque problema, a cuius solutione illud quod in art. praec. nobis proposuimus pendet, in sequentibus perscrutabimur, a casibus simplicissimis inchoantes.

Residuum -1.

108.

Theorema. *Omnium numerorum primorum formae $4n+1$, -1 est residuum quadraticum, omnium vero numerorum primorum formae $4n+3$, non-residuum.*

Ex. -1 est residuum numerorum 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97 etc., e quadratis numerorum 2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22 etc. respective oriundum; contra non-residuum est numerorum 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83 etc.

Mentionem huius theor. iam in art. 64 fecimus. Demonstratio vero facile ex art. 106 petitur. Etenim pro numero primo formae $4n+1$ est $(-1)^{2n} \equiv 1$, pro numero autem formae $4n+3$ habetur $(-1)^{2n+1} \equiv -1$. Convenit haec demonstratio cum ea quam l. c. tradidimus. Sed propter theorematis elegantiam atque utilitatem non superfluum erit, alio adhuc modo idem ostendisse.

109.

Designemus complexum omnium residuorum numeri primi p, quae ipso p sunt minora, excluso residuo 0, per literam C, et quoniam horum residuorum multitudo semper $= \frac{p-1}{2}$, manifestum est, eam fore parem, quoties p sit formae $4n+1$, imparem vero, quoties p sit formae $4n+3$. Dicantur, ad instar art. 77, ubi de numeris in genere agebatur, *residua socia* talia, quorum productum $\equiv 1 \pmod{p}$; manifesto enim si r est residuum, etiam $\frac{1}{r} \pmod{p}$ residuum erit. Et quoniam idem residuum plura socia inter residua C habere nequit, patet omnia residua C in classes distribui posse, quarum quaevis bina residua socia contineat. Iam perspicuum est, si nullum residuum daretur, quod sibi ipsi esset socium, *i. e.* si quaevis classis bina residua *inaequalia* contineret, omnium residuorum numerum fore duplum numeri omnium classium; quodsi vero aliqua dantur residua sibi ipsis socia *i. e.* aliquae classes quae unicum tantum residuum aut, si quis malit, idem residuum bis continent, posita harum classium multitudine $= a$, reliquarumque multitudine $= b$; erit omnium residuorum C numerus $= a+2b$: Quare quando p est formae $4n+1$, erit a numerus par; quando autem p est formae $4n+3$, erit a impar. At numeri ipso p minores alii, quam 1 et $p-1$, sibi ipsis socii esse nequeunt (vid. art. 77); priorque 1 certo inter residua occurrit; unde in priori casu $p-1$ (seu quod hic idem valet, -1) debet esse residuum, in posteriori vero non-residuum; alias enim in illo casu foret $a = 1$, in hoc autem $= 2$, quod fieri nequit.

110.

Etiam haec demonstratio ill. Eulero debetur, qui et priorem primus invenit V. *Opusc. Anal.* T. I. p. 135. — Facile quisquis videbit eam similibus principiis innixam esse, ut demonstratio nostra secunda theor. Wilsoniani art. 77. Si

vero hoc theorema supponere velimus, facilius adhuc demonstratio exhiberi poterit. Scilicet inter numeros $1, 2, 3 \ldots p-1$ erunt $\frac{p-1}{2}$ residua quadratica ipsius p totidemque non-residua; quare non-residuorum multitudo erit par, quando p est formae $4n+1$; impar quando p est formae $4n+3$. Hinc productum ex omnibus numeris $1, 2, 3 \ldots p-1$ in priori casu erit residuum, in posteriori non-residuum (art. 99). At productum hoc semper $\equiv -1 \pmod p$; adeoque etiam -1 in priori casu residuum, in posteriori non-residuum erit.

111.

Si itaque r est residuum numeri alicuius primi formae $4n+1$, etiam $-r$ huius primi residuum erit, omnia autem talis numeri non-residua, etiam signo contrario sumta non-residua manebunt *). Contrarium evenit pro numeris primis formae $4n+3$, quorum residua quando signum mutatur, non-residua fiunt et vice versa, vid. art. 98.

Ceterum facile ex praecedentibus derivatur regula generalis: -1 *est residuum omnium numerorum qui neque per* 4 *neque per ullum numerum primum formae* $4n+3$ *dividi possunt; omnium reliquorum non-residuum.* V. artt. 103 et 105.

Residua $+2$ *et* -2.

112.

Progredimur ad residua $+2$ et -2.

Si ex tabula II colligimus omnes numeros primos quorum residuum est $+2$, hos habebimus: 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Facile autem animadvertitur, inter hos numeros nullos inveniri formarum $8n+3$ et $8n+5$.

Videamus itaque, num haec inductio ad certitudinem evehi possit.

Primum observamus quemvis numerum compositum formae $8n+3$ vel $8n+5$ necessario factorem primum alterutrius formae $8n+3$ vel $8n+5$, involvere; manifesto enim e solis numeris primis formarum $8n+1$, $8n+7$, alii numeri quam qui sunt formae $8n+1$ vel $8n+7$, componi nequeunt. Quodsi itaque inductio nostra generaliter est vera, nullus omnino numerus formae

*) Quando igitur de numero quocunque loquemur quatenus numeri formae $4n+1$ residuum vel non-residuum est, ipsius signum omnino negligere sive etiam signum anceps $\pm$ ipsi tribuere poterimus.

$8n+3$, $8n+5$ dabitur, cuius residuum $+2$; sicque nullus certe numerus huius formae infra 100 exstat, cuius residuum sit $+2$. Si autem ultra hunc limitem tales numeri reperirentur, ponamus minimum omnium $=t$. Erit itaque t vel formae $8n+3$ vel $8n+5$; $+2$ ipsius residuum erit, omnium autem numerorum similium minorum non-residuum. Ponatur $2 \equiv aa \pmod t$ poteritque a ita semper accipi ut sit impar simulque $< t$, (habebit enim a ad minimum duos valores positivos ipso t minores quorum summa $= t$, quorumque adeo alter par alter impar v. artt. 104. 105). Quo facto sit $aa = 2 + tu$, sive $tu = aa - 2$, eritque aa formae $8n+1$, tu igitur formae $8n-1$, adeoque u formae $8n+3$ vel $8n+5$, prout t est formae posterioris vel prioris. At ex aequatione $aa = 2 + tu$ sequitur, etiam $2 \equiv aa \pmod u$ *i. e.* 2 etiam ipsius u residuum fore. Facile vero perspicitur, esse $u < t$, quare t non est minimus numerus inductioni nostrae contrarius contra hyp. Unde manifesto sequitur id quod per inductionem inveneramus generaliter verum esse.

Combinando haec cum prop. art. 111 sequentia theoremata nanciscimur.

I. *Numerorum omnium primorum formae* $8n+3$, $+2$ *erit non-residuum,* -2 *vero residuum.*

II. *Numerorum omnium primorum formae* $8n+5$ *tum* $+2$ *tum* -2 *erunt non-residua.*

113.

Per similem inductionem ex tab. II inveniuntur numeri primi quorum residuum est -2 hi: 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97 *). Inter quos quum nulli inveniantur formarum $8n+5$, $8n+7$, num etiam haec inductio theorematis generalis vim adipisci possit investigemus. Ostenditur simili modo ut in art. praec. quemvis numerum compositum formae $8n+5$ vel $8n+7$, factorem primum involvere formae $8n+5$ vel formae $8n+7$, ita ut, si inductio nostra generaliter vera, -2 nullius omnino numeri formae $8n+5$ vel $8n+7$ residuum esse possit. Si autem tales numeri darentur, ponatur omnium minimus $= t$, fiatque $-2 = aa - tu$. Ubi si uti supra a impar ipsoque t minor accipitur, u erit formae $8n+5$ vel $8n+7$, prout t formae $8n+7$ vel $8n+5$. At ex eo quod $aa + 2 = tu$ atque $a < t$, quisquis facile derivare poterit, etiam

*) Considerando scilicet -2 tamquam productum ex $+2$ et -1 V. art. 111.

u ipso t minorem fore. Denique -2 etiam ipsius u residuum erit, *i. e.* t non erit minimus numerus qui inductioni nostrae adversatur, contra hyp. Quare necessario -2 omnium numerorum formarum $8n+5$, $8n+7$ non-residuum.

Combinando haec cum prop. art. 111, prodeunt theoremata haec:

I. *Omnium numerorum primorum* $8n+5$, *tum* -2 *tum* $+2$ *sunt non-residua*, uti iam in art. praec. invenimus.

II. *Omnium numerorum primorum formae* $8n+7$, -2 *est non-residuum*, $+2$ *vero residuum.*

Ceterum in utraque demonstratione pro a etiam valorem parem accipere potuissemus; tunc autem casum ubi a fuisset formae $4n+2$, ab eo distinguere oportuisset, ubi a formae $4n$. Evolutio autem perinde procedit uti supra, nullique difficultati est obnoxia.

114.

Unus adhuc superest casus, scilicet ubi numerus primus est formae $8n+1$ Hic vero methodum praecedentem eludit, artificiaque prorsus peculiaria postulat.

Sit pro modulo primo $8n+1$, radix quaecunque primitiva a, eritque (art. 62) $a^{4n} \equiv -1 \pmod{8n+1}$, quae congruentia ita etiam exhiberi potest, $(a^{2n}+1)^2 \equiv 2a^{2n} \pmod{8n+1}$, sive etiam ita, $(a^{2n}-1)^2 \equiv -2a^{2n}$. Unde sequitur tum $2a^{2n}$ tum $-2a^{2n}$ ipsius $8n+1$ esse residuum: at quia a^{2n} est quadratum per modulum non divisibile, manifesto etiam tum $+2$ tum -2 residua erunt (art. 98).

115.

Haud inutile erit, adhuc aliam huius theorematis demonstrationem adiicere, quae similem relationem ad praecedentem habet, ut theorematis art. 108 demonstratio secunda (art. 109) ad primam (art. 108). Periti facilius tunc perspicient, binas demonstrationes tam illas quam has non adeo heterogeneas esse, quam primo forsan aspectu videantur.

I. Pro modulo quocunque primo formae $4m+1$, inter numeros ipso minores $1, 2, 3 \ldots 4m$, reperientur m qui biquadrato congrui esse possunt, reliqui vero $3m$ non poterunt.

Facile quidem hoc ex principiis Sect. praec. derivatur, sed etiam absque his demonstratio haud difficilis. Demonstravimus enim pro tali modulo -1 semper esse residuum quadraticum. Sit itaque $ff \equiv -1$ patetque, si z fuerit numerus quicunque per modulum non divisibilis, quaternorum numerorum $+z$, $-z$, $+fz$, $-fz$ (quos incongruos esse facile perspicitur) biquadrata inter se congrua fore; porro manifestum est biquadratum numeri cuiuscunque, qui nulli ex his quatuor congruus, illorum biquadratis congruum fieri non posse, (alias enim congruentia $x^4 \equiv z^4$ quae est quarti gradus plures quam 4 radices haberet, contra art. 43). Hinc facile colligitur, omnes numeros $1, 2, 3, \ldots 4m$, tantummodo m biquadrata incongrua praebere, quibus inter eosdem numeros m congrui reperientur, reliqui autem nulli biquadrato congrui esse poterunt.

II. Secundum modulum primum formae $8n+1$, -1 biquadrato congruus fieri poterit (-1 erit *residuum biquadraticum* huius numeri primi).

Omnium enim residuorum biquadraticorum ipso $8n+1$ minorum (cifra exclusa) multitudo erit $=2n$ *i. e.* par. Porro facile probatur, si r fuerit residuum biquadraticum ipsius $8n+1$, etiam valorem expr. $\frac{1}{r} \pmod{8n+1}$ fore tale residuum. Hinc omnia residua biquadratica in classes simili modo distribui poterunt, uti in art. 109 residua quadratica distribuimus: nec non reliqua demonstrationis pars prorsus eodem modo procedit ut illic.

III. Iam sit $g^4 \equiv -1$, et h valor expr. $\frac{1}{g} \pmod{8n+1}$. Tunc erit

$$(g \pm h)^2 = g^2 + h^2 \pm 2gh \equiv g^2 + h^2 \pm 2$$

(propter $gh \equiv 1$). At $g^4 \equiv -1$, adeoque $-h^2 \equiv g^4 h^2 \equiv g^2$, unde tandem $g^2 + h^2 \equiv 0$, atque $(g \pm h)^2 \equiv \pm 2$ *i. e.* tum $+2$ tum -2 residuum quadraticum ipsius $8n+1$. *Q. E. D.*

116.

Ceterum ex praecc. facile regula sequens generalis deducitur: $+2$ *est residuum numeri cuiusvis, qui neque per* 4, *neque per ullum primum formae* $8n+3$ *vel* $8n+5$ *dividi potest, reliquorum autem* (*ex. gr.* omnium numerorum formarum $8n+3$, $8n+5$, sive sint primi, sive compositi) *non-residuum:*

-2 *est residuum numeri cuiusvis, qui neque per* 4, *neque per ullum primum formae* $8n+5$ *vel* $8n+7$ *dividi potest, omnium autem reliquorum non-residuum.*

Theoremata haec elegantia iam sagaci Fermatio innotuerunt, *Op. Mathem. p.* 168. Demonstrationem vero quam se habere professus est, nusquam commu-

nicavit. Postea ab ill. Eulero frustra semper est investigata: at ill. La Grange primus demonstrationem rigorosam reperit, *Nouv. Mém. de l'Ac. de Berlin* 1775. *p.* 349, 351. Quod ill. Eulerum adhuc latuisse videtur, quando scripsit diss. in *Opusc. Analyt.* conservatam, T. I. p. 259.

Residua $+3$ *et* -3.

117.

Pergimus ad residua $+3$ et -3. A posteriori initium faciamus.

Reperiuntur ex tab. II. numeri primi quorum residuum est -3 hi: 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, inter quos nullus invenitur formae $6n+5$. Quod vero etiam ultra tabulae limites nulli primi huius formae dantur quorum residuum -3, ita demonstramus: Primo patet quemvis numerum compositum formae $6n+5$ necessario factorem primum aliquem eiusdem formae involvere. Quousque igitur nulli numeri primi formae $6n+5$ dantur, quorum residuum -3, eousque tales etiam compositi non dabuntur. Quodsi vero ultra tabulae nostrae limites tales numeri darentur, sit omnium minimus $=t$, ponaturque $-3=aa-tu$. Tunc erit, si acceperis a parem ipsoque t minorem, $u<t$, atque -3 residuum ipsius u. Sed quando a formae $6n\pm 2$, tu erit formae $6n+1$, adeoque u formae $6n+5$. *Q. E. A.* quia t minimum esse numerum inductioni nostrae adversantem supposuimus. Quando vero a formae $6n$, erit tu formae $36n+3$ adeoque $\frac{1}{3}tu$ formae $12n+1$, quare $\frac{1}{3}u$ erit formae $6n+5$; patet autem -3 etiam ipsius $\frac{1}{3}u$ residuum fore, atque esse $\frac{1}{3}u<t$, *Q. E. A.* Manifestum itaque, -3 nullius numeri formae $6n+5$ residuum esse posse.

Quoniam quisque numerus formae $6n+5$ necessario vel sub forma $12n+5$, vel sub hac $12n+11$ continetur, prior autem forma sub hac $4n+1$, posterior sub hac $4n+3$, haec habentur theoremata:

I. *Cuiusvis numeri primi formae* $12n+5$, *tum* -3 *tum* $+3$ *non-residuum est.*

II. *Cuiusvis numeri primi formae* $12n+11$, -3 *est non-residuum*, $+3$ *vero residuum.*

118.

Numeri quorum residuum est $+3$ ex tabula II. inveniuntur hi: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97, inter quos nulli sunt formae $12n+5$ vel $12n+7$. Nullos autem omnino numeros formarum $12n+5$, $12n+7$ dari quorum $+3$ sit residuum, eodem prorsus modo, ut in artt. 112, 113, 117, comprobari potest, quare hoc negotio supersedemus. Habemus itaque collato art. 111 theoremata:

I. *Numeri cuiusvis primi formae* $12n+5$ *non-residua sunt tum* $+3$ *tum* -3 (uti iam in art praec. invenimus).

II. *Numeri cuiusvis primi formae* $12n+7$ *non-residuum est* $+3$, -3 *vero residuum.*

119.

Nihil autem per hanc methodum pro numeris formae $12n+1$ inveniri potest, qui proin artificia singularia requirunt. Ex inductione quidem facile colligitur, omnium numerorum primorum huius formae residua esse $+3$ et -3. Manifesto autem demonstrari tantummodo debet, numerorum talium residuum esse -3, quia tunc necessario etiam $+3$ residuum esse debet (art. 111). Ostendemus autem generalius, -3 esse residuum numeri cuiusvis primi formae $3n+1$.

Sit p huiusmodi primus atque a numerus pro modulo p ad exponentem 3 pertinens (quales dari ex art. 54 manifestum, quia 3 submultiplum ipsius $p-1$). Erit itaque $a^3\equiv 1 \pmod p$ *i. e.* a^3-1 sive $(a^2+a+1)(a-1)$ per p divisibilis. Sed patet a esse non posse $\equiv 1 \pmod p$, quia 1 ad exponentem 1 pertinet, quare $a-1$ per p divisibilis non erit, sed a^2+a+1 erit, hincque etiam $4aa+4a+4$, *i. e.* erit $(2a+1)^2\equiv -3 \pmod p$ sive -3 residuum ipsius p. *Q. E. D.*

Ceterum patet, hanc demonstrationem (quae a praecedentibus est independens) etiam numeros primos formae $12n+7$ complecti quos iam in art. praec. absolvimus.

Observare adhuc convenit, hanc analysin ad instar methodi in artt. 109, 115 usitatae exhiberi posse, at brevitatis gratia huic rei non immoramur.

120.

Colliguntur facile ex praecc. theoremata haec (vid. artt. 102, 103, 105).

I. -3 *est residuum omnium numerorum, qui neque per* 8, *neque per* 9, *neque per ullum numerum primum formae* $6n+5$ *dividi possunt, non-residuum autem omnium reliquorum.*

II. $+3$ *est residuum omnium numerorum, qui neque per* 4, *neque per* 9, *neque per ullum primum formae* $12n+5$ *vel* $12n+7$ *dividi possunt, omnium reliquorum non-residuum.*

Teneatur imprimis casus particularis hic: -3 est *residuum* omnium numerorum primorum formae $3n+1$, seu quod idem est *omnium; qui ipsius* 3 *sunt residua, non-residuum* vero omnium numerorum primorum formae $6n+5$, seu, excluso numero 2, omnium formae $3n+2$, *i.e. omnium qui ipsius* 3 *sunt non-residua.* Facile vero perspicitur omnes reliquos casus ex hoc sponte sequi.

Propositiones ad residua $+3$ et -3 pertinentes iam Fermatio notae fuerunt, *Opera Wallisii T.* II. *p.* 857. At ill. Euler primus demonstrationes tradidit, *Comm. nov. Petr. T.* VIII. *p.* 105 sqq. Eo magis est mirandum, demonstrationes propositionum ad residua $+2$ et -2 pertinentium, prorsus similibus artificiis innixas, semper ipsius sagacitatem fugisse. Vid. etiam comment. ill. La Grange, *Nouv. Mém. de l'Ac. de Berlin*, 1775 *p.* 352.

Residua $+5$ *et* -5.

121.

Per inductionem deprehenditur, $+5$ nullius numeri imparis formae $5n+2$ vel $5n+3$ residuum esse, *i.e.* nullius numeri imparis qui ipsius 5 non-residuum sit. Hanc vero regulam nullam exceptionem pati, ita demonstratur. Sit numerus minimus, si quis datur, ab hac regula excipiendus $=t$, qui itaque numeri 5 est non-residuum, 5 autem ipsius t residuum. Sit $aa=5+tu$, ita ut a sit par ipsoque t minor. Erit igitur u impar ipsoque t minor, $+5$ autem ipsius u residuum erit. Quodsi iam a per 5 non est divisibilis, etiam u non erit; manifesto autem tu ipsius 5 est residuum, quare quum t ipsius 5 sit non-residuum, etiam u non-residuum erit; *i.e.* datur non-residuum impar numeri 5, cuius residuum est $+5$, ipso t minus, contra hyp. Si vero a per 5 est divisibilis, ponatur $a=5b$, atque $u=5v$, unde $tv\equiv -1\equiv 4 \pmod 5$, *i.e.* tv erit residuum numeri 5. In reliquis demonstratio perinde procedit ut in casu priori.

122.

Omnium igitur numerorum primorum, qui simul sunt ipsius 5 non-residua simulque formae $4n+1$, *i.e.* omnium numerorum primorum formae $20n+13$ vel $20n+17$, tum $+5$ quam -5 non-residua erunt; omnium autem numerorum primorum formae $20n+3$ vel $20n+7$, non-residuum erit $+5$, -5 residuum.

Potest vero prorsus simili modo demonstrari, -5 esse non-residuum omnium numerorum primorum formarum $20n+11$, $20n+13$, $20n+17$, $20n+19$, facileque perspicitur hinc sequi, $+5$ esse residuum omnium numerorum primorum formae $20n+11$ vel $20n+19$, non-residuum autem omnium formae $20n+13$ vel $20n+17$. Et quoniam quivis numerus primus, praeter 2 et 5 (quorum residuum ± 5), in aliqua harum formarum continetur $20n+1, 3, 7, 9, 11, 13, 17, 19$, patet, de omnibus iam iudicium ferri posse, exceptis iis qui sint formae $20n+1$ vel formae $20n+9$.

123.

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

At verificatio illius inductionis non adeo facilis. Quando numerus primus formae $20n+1$, sive generalius formae $5n+1$ proponitur, res simili modo absolvi potest, ut in artt. 114, 119. Sit scilicet numerus quicunque pro modulo $5n+1$ ad exponentem 5 pertinens a, quales dari ex Sect. praec. manifestum,

eritque $a^5 \equiv 1$, sive $(a-1)(a^4+a^3+a^2+a+1) \equiv 0 \pmod{5n+1}$. At quia nequit esse $a \equiv 1$, neque adeo $a-1 \equiv 0$; necessario erit $a^4+a^3+a^2+a+1 \equiv 0$. Quare etiam $4(a^4+a^3+a^2+a+1) = (2aa+a+2)^2 - 5a^2$ erit $\equiv 0$ *i. e.* $5a^2$ erit residuum ipsius $5n+1$, adeoque etiam 5, quia a^2 est residuum per $5n+1$ non divisibile (a enim per $5n+1$ non divisibilis propter $a^5 \equiv 1$). *Q. E. D.*

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

I. Si p est numerus primus atque b non-residuum quadraticum datum ipsius p, valor expressionis

$$(A) \ldots \frac{(x+\sqrt{b})^{p+1} - (x-\sqrt{b})^{p+1}}{\sqrt{b}}$$

(ex qua evoluta irrationalitatem abire facile perspicitur), semper per p divisibilis erit, quicunque numerus pro x assumatur. Patet enim ex inspectione coefficientium qui ex evolutione ipsius A obtinentur, omnes terminos a secundo usque ad penultimum (incl.) per p divisibiles fore, adeoque esse $A \equiv 2(p+1)(x^p + xb^{\frac{p-1}{2}}) \pmod{p}$. At quoniam b ipsius p non-residuum est, erit $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, (art. 106); x^p autem semper est $\equiv x$ (Sect. praec.), unde fit $A \equiv 0$. *Q. E. D.*

II. In congruentia $A \equiv 0 \pmod{p}$, indeterminata x habet p dimensiones omnesque numeri $0, 1, 2 \ldots p-1$ illius radices erunt. Iam ponatur e esse divisorem ipsius $p+1$ eritque expressio

$$\frac{(x+\sqrt{b})^e - (x-\sqrt{b})^e}{\sqrt{b}}$$

(quam per B designamus) si evolvitur, ab irrationalitate libera, indeterminata x in ipsa $e-1$ dimensiones habebit, constatque ex analyseos primis elementis, A per B (indefinite) esse divisibilem. Iam dico $e-1$ valores ipsius x dari, quibus in B substitutis, B per p divisibilis evadat. Ponatur enim $A \equiv BC$, habebitque x in C dimensiones $p-e+1$, adeoque congruentia $C \equiv 0 \pmod{p}$ non plures quam $p-e+1$ radices. Unde facile patet, omnes reliquos numeros ex his $0, 1, 2, 3 \ldots p-1$, quorum multitudo $= e-1$, congruentiae $B \equiv 0$ radices fore.

III. Iam ponatur p esse formae $5n+4$, $e = 5$, b non-residuum ipsius p, atque numerum a ita determinatum, ut sit

$$\frac{(a+\sqrt{b})^5 - (a-\sqrt{b})^5}{\sqrt{b}}$$

per p divisibilis. At illa expressio fit

$$= 10a^4 + 20aab + 2bb = 2((b+5aa)^2 - 20a^4)$$

Erit igitur etiam $(b+5aa)^2 - 20a^4$ per p divisibilis *i. e.* $20a^4$ residuum ipsius p; at quoniam $4a^4$ residuum est per p non divisibile (facile enim intelligitur, a per p dividi non posse), etiam 5 residuum ipsius p erit. *Q. E. D.*

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

Observamus adhuc, demonstrationes pro utroque casu ill. La Grange deberi, *Mém. de l'Ac. de Berlin* 1775, *p.* 352 sqq.

De ± 7.

124.

Per similem methodum demonstratur,

-7 *esse non-residuum cuiusvis numeri qui ipsius* 7 *sit non-residuum.*

Ex inductione vero concludi potest,

-7 *esse residuum cuiusvis numeri primi qui ipsius* 7 *sit residuum.*

At hoc a nemine hactenus rigorose demonstratum. Pro iis quidem residuis ipsius 7, quae sunt formae $4n-1$, facilis est demonstratio; etenim per methodum ex praecc. abunde notam ostendi potest, $+7$ semper esse talium numerorum primorum non-residuum, adeoque -7 residuum. Sed parum hinc lucramur: reliqui enim casus per hanc methodum tractari nequeunt. Unum quidem adhuc casum simili modo ut artt. 119, 123 absolvere possumus. Scilicet si p est numerus primus formae $7n+1$, atque a pro modulo p ad exponentem 7 pertinens, facile perspicitur

$$\frac{4(a^7-1)}{a-1} = (2a^3+a^2-a-2)^2 + 7(a^2+a)^2$$

per p divisibilem, adeoque $-7(a^2+a)^2$ ipsius p residuum fore. At $(a^2+a)^2$, tamquam quadratum, ipsius p residuum est, insuperque per p non divisibile; quum enim a ad exponentem 7 pertinere supponatur, neque $\equiv 0$, neque $\equiv -1 \pmod{p}$ esse potest, *i. e.* neque a neque $a+1$ per p divisibilis erit, adeoque etiam quadratum $(a+1)^2 a^2$. Unde manifesto etiam 7 ipsius p residuum

erit. *Q. E. D.* — At primi numeri formae $7n+2$ vel $7n+4$ omnes methodos hucusque traditas eludunt. Ceterum etiam haec demonstratio ab ill. La Grange primum est detecta l. c. — Infra Sect. VII. docebimus generaliter, expressionem $\frac{t(x^p-1)}{x-1}$ semper ad formam $X^2 \mp pY^2$ reduci posse, (ubi signum superius est accipiendum quando p est numerus primus formae $4n+1$, inferius quando est formae $4n+3$), denotantibus X, Y functiones rationales ipsius x, a fractionibus liberas. Hanc discerptionem ill. La Grange ultra casum $p=7$ non perfecit v. l. c. p. 352.

Praeparatio ad disquisitionem generalem.

125.

Quoniam igitur methodi praecedentes ad demonstrationes generales stabilendas non sufficiunt, iam tempus est, aliam ab hoc defectu liberam exponere. Initium facimus a theoremate, cuius demonstratio satis diu operam nostram elusit, quamvis primo aspectu tam obvium videatur, ut quidam ne necessitatem quidem demonstrationis intellexerint. Est vero hoc: *Quemvis numerum, praeter quadrata positive sumta, aliquorum numerorum primorum non-residuum esse.* Quia vero hoc theoremate tantummodo tamquam auxiliari ad alia demonstranda usuri sumus, alios casus hic non explicamus quam quibus ad hunc finem indigemus. De reliquis casibus postea sponte idem constabit. Ostendemus itaque, *quemvis numerum primum formae* $4n+1$, *sive positive sive negative accipiatur* *), *non-residuum esse aliquorum numerorum primorum*, et (si >5) quidem talium qui ipso sint minores.

Primo, quando numerus primus p, formae $4n+1$ (>17; sed $-13 N 3$, $-17 N 5$), *negative* sumendus proponitur, sit $2a$ numerus par proxime maior quam $\sqrt{p}$; tum facile perspicitur, $4aa$ semper fore $<2p$ sive $4aa-p<p$. At $4aa-p$ est formae $4n+3$, $+p$ autem residuum quadraticum ipsius $4aa-p$, (quoniam $p \equiv 4aa \pmod{4aa-p}$); quodsi igitur $4aa-p$ est numerus primus, $-p$ ipsius non-residuum erit; sin minus, necessario factor aliquis ipsius $4aa-p$ formae $4n+3$ erit; et quum $+p$ etiam huius residuum esse debeat, $-p$ ipsius non-residuum erit. *Q. E. D.*

Pro numeris primis *positive* sumendis duos casus distinguimus. *Primo* sit p numerus primus formae $8n+5$. Sit a numerus quicunque positivus $<\sqrt{\frac{1}{2}p}$. Tum $8n+5-2aa$ erit numerus positivus formae $8n+5$ vel $8n+3$ (prout a

*) $+1$ autem excipi oportere per se manifestum est.

par vel impar), adeoque necessario per numerum aliquem primum formae $8n+3$ vel $8n+5$ divisibilis, productum enim ex quotcunque numeris formae $8n+1$ et $8n+7$ neque formam $8n+3$ neque hanc $8n+5$ habere potest. Sit hic q, eritque $8n+5 \equiv 2a^2 \pmod{q}$. At 2 ipsius q non-residuum erit (art. 112), adeoque etiam $2a^2$ *) et $8n+5$. *Q. E. D.*

126.

Sed numerum quemvis primum formae $8n+1$ positive acceptum semper alicuius numeri primi ipso minoris non residuum esse, per artificia tam obvia demonstrari nequit. Quum autem haec veritas maximi sit momenti, demonstrationem rigorosam, quamvis aliquantum prolixa sit, praeterire non possumus. Praemittimus sequens

LEMMA. *Si habentur duae series numerorum*

$$A, B, C \text{ etc.} \ldots\ldots \text{(I)}, \quad A', B', C' \text{ etc.} \ldots\ldots \text{(II)}$$

(utrum terminorum multitudo in utraque eadem sit necne nihil interest) *ita comparatae, ut, denotante p numerum quemcunque primum aut numeri primi potestatem, terminum aliquem secundae seriei (sive etiam plures) metientem, totidem ad minimum termini in serie prima sint per p divisibiles, quot sunt in secunda: tum dico productum ex omnibus numeris* (I) *divisibile fore per productum ex omnibus numeris* (II).

Exempl. Constet (I) e numeris 12, 18, 45; (II) ex his 3, 4, 5, 6, 9. Tum divisibiles erunt per 2, 4, 3, 9, 5 in (I) 2, 1, 3, 2, 1 termini, in (II) 2, 1, 3, 1, 1 termini, respective; productum autem omnium terminorum (I) $=9720$ divisibile est per productum omnium terminorum (II), 3240.

Demonstr. Sit productum ex omnibus terminis (I), $=Q$, productum omnium terminorum seriei (II), $=Q'$. Patet quemvis numerum primum qui sit divisor ipsius Q' etiam ipsius Q divisorem fore. Iam ostendemus quemvis factorem primum ipsius Q', in Q totidem ad minimum dimensiones habere quot habeat in Q'. Esto talis divisor p, ponaturque, in serie (I) a terminos esse per p divisibiles, b terminos per p^2 divisibiles, c terminos per p^3 divisibiles etc., similia denotent literae a', b', c' etc. pro serie (II), perspicieturque facile, p in Q habere

*) Art. 93. Patet enim a^2 esse residuum ipsius q per q non divisibile, nam alias etiam numerus primus p per q foret divisibilis. *Q. E. A.*

$a+b+c+$ etc. dimensiones, in Q' vero $a'+b'+c'+$ etc. At a' certe non maior quam a, b' non maior quam b etc. (hyp.); quare $a'+b'+c'$ etc. certo non erit $>a+b+c$ etc. — Quum itaque nullus numerus primus in Q' plures dimensiones habere possit, quam in Q, Q per Q' divisibilis erit (art. 17). *Q. E. D.*

127.

Lemma. *In progressione* $1, 2, 3, 4, \ldots . n$, *plures termini esse nequeunt per numerum quemcunque* h *divisibiles, quam in hac* $a, a+1, a+2 \ldots . a+n-1$ *ex totidem terminis constante.*

Nullo enim negotio perspicitur si n fuerit multiplum ipsius h, in utraque progressione $\frac{n}{h}$ terminos fore per h divisibiles; sin minus, ponatur $n=eh+f$, ita ut f sit $<h$, eruntque in priori serie e termini per h divisibiles, in posteriori autem vel totidem vel $e+1$.

Hinc tamquam Coroll. sequitur propositio ex numerorum figuratorum theoria nota, sed a nemine, ni fallimur, hactenus directe demonstrata,

$$\frac{a \,.\, a+1 \,.\, a+2 \ldots . a+n-1}{1 \,.\, 2 \,.\, 3 \ldots . n}$$

semper esse numerum integrum.

Denique Lemma hoc generalius ita proponi potuisset:

In progressione $a, a+1, a+2, \ldots . a+n-1$ totidem ad minimum dantur termini secundum modulum h numero cuicunque dato, r, congrui, quot in hac $1, 2, 3 \ldots . n$ termini per h divisibiles.

128.

Theorema. *Sit* a *numerus quicunque formae* $8n+1$, p *numerus quicunque ad* a *primus, cuius residuum* $+a$, *tandem* m *numerus arbitrarius: tum dico, in progressione*

$$a, \tfrac{1}{2}(a-1), 2(a-4), \tfrac{1}{2}(a-9), 2(a-16), \ldots . 2(a-m^2), \text{ vel } \tfrac{1}{2}(a-m^2)$$

prout m *par vel impar, totidem ad minimum dari terminos per* p *divisibiles quot dentur in hac*

$$1, 2, 3, \ldots . 2m+1$$

Priorem progressionem designamus per (I), posteriorem per (II).

Demonstr. I. Quando $p=2$, in (I) omnes termini praeter primum, *i. e.* m termini divisibiles erunt; totidem autem erunt in (II).

II. Sit p numerus impar vel numeri imparis duplum vel quadruplum, atque $a \equiv rr \pmod p$. Tum in progressione $-m, -(m-1), -(m-2), \ldots . +m$ (quae terminorum multitudine cum (II) convenit et per (III) designabitur) totidem ad minimum termini erunt secundum modulum p ipsi r congrui, quot in serie (II) per p divisibiles (art. praec.). Inter illos autem bini, qui signo tantum, non magnitudine, discrepent, occurrere nequeunt*). Tandem quisque eorum correspondentem habebit in serie (I), qui per p erit divisibilis. Scilicet si fuerit $\pm b$ aliquis terminus seriei (III) ipsi r secundum p congruus, erit $a-bb$ per p divisibilis. Quodsi igitur b est par, terminus seriei (I), $2(a-bb)$, per p divisibilis erit. Si vero b impar, terminus $\frac{1}{2}(a-bb)$ per p divisibilis erit: namque manifesto $\frac{a-bb}{p}$ erit integer *par*, quoniam $a-bb$ per 8, p autem ad summum per 4 divisibilis (*a* enim per hyp. est formae $8n+1$, bb autem ideo quod est numeri imparis quadratum eiusdem formae erit, quare differentia erit formae $8n$). Hinc tandem concluditur, in serie (I) totidem terminos esse per p divisibiles, quot in (III) sint ipsi r secundum p congrui *i. e.* totidem aut plures quam in (II) sint per p divisibiles. *Q. E. D.*

III. Sit p formae $8n$, atque $a \equiv rr \pmod{2p}$. Facile enim perspicitur, a, quum ex hyp. ipsius p sit residuum, etiam ipsius $2p$ residuum fore. Tum in serie (III) totidem ad minimum termini erunt ipsi r secundum p congrui, quot in (II) sunt per p divisibiles, illique omnes magnitudine erunt inaequales. At cuique eorum respondebit aliquis in (I) per p divisibilis. Si enim $+b$ vel $-b \equiv r \pmod p$, erit $bb \equiv rr \pmod{2p}$†), adeoque terminus $\frac{1}{2}(a-bb)$ per p divisibilis. Quare in (I) totidem ad minimum termini erunt per p divisibiles quam in (II). *Q. E. D.*

129.

Theorema. *Si* a *est numerus primus formae* $8n+1$, *necessario infra* $2\sqrt{a}+1$ *dabitur aliquis numerus primus cuius non-residuum sit* a.

*) Si enim esset $r \equiv -f \equiv +f \pmod p$, fieret $2f$ per p divisibilis, adeoque etiam $2\dot{a}$ (propter $ff \equiv a \pmod p$). Hoc autem aliter fieri nequit, quam si $p=2$, quum per hyp. a ad p sit primus. Sed de hoc casu iam seorsim diximus.

†) Erit scilicet $bb-rr=(b-r)(b+r)$ e duobus factoribus compositus, quorum alter per p divisibilis (hyp.), alter per 2 (quia tum b tum r sunt impares); adeoque $bb-rr$ per $2p$ divisibilis.

Demonstr. Esto, si fieri potest, a residuum omnium primorum ipso $2\sqrt{a}+1$ minorum. Tum facile perspicietur, a etiam omnium numerorum compositorum ipso $2\sqrt{a}+1$ minorum residuum fore (conferantur praecepta per quae diiudicare docuimus, utrum numerus propositus sit numeri compositi residuum necne; art. 105). Sit numerus proxime minor quam $\sqrt{a}$, $=m$. Tum in serie

$$(\mathrm{I}) \ldots\ldots a,\ \tfrac{1}{2}(a-1),\ 2(a-4),\ \tfrac{1}{2}(a-9) \ldots . 2(a-mm) \text{ vel } \tfrac{1}{2}(a-mm)$$

totidem aut plures termini erunt per numerum quemcunque ipso $2\sqrt{a}+1$ minorem divisibiles, quam in hac

$$(\mathrm{II}) \ldots\ldots 1,\ 2,\ 3,\ 4 \ldots . 2m+1 \text{ (art. praec.)}$$

Hinc vero sequitur, productum ex omnibus terminis (I) per productum omnium terminorum (II) divisibile esse, (art. 126). At illud est aut $=a(a-1)(a-4)\ldots.(a-mm)$ aut semissis huius producti (prout m aut par aut impar). Quare productum $a(a-1)(a-4)\ldots.(a-mm)$ certo per productum omnium terminorum (II) dividi poterit, et, quia omnes hi termini ad a sunt primi, etiam productum illud omisso factore a. Sed productum ex omnibus terminis (II) ita etiam exhiberi potest,

$$(m+1).((m+1)^2-1).((m+1)^2-4)\ldots.((m+1)^2-m^2)$$

Fiet igitur

$$\frac{1}{m+1}\cdot\frac{a-1}{(m+1)^2-1}\cdot\frac{a-4}{(m+1)^2-4}\cdots\frac{a-m^2}{(m+1)^2-m^2}$$

numerus integer, quamquam sit productum ex fractionibus unitate minoribus: quia enim necessario $\sqrt{a}$ irrationalis esse debet, erit $m+1>\sqrt{a}$, adeoque $(m+1)^2>a$. Hinc tandem concluditur suppositionem nostram locum habere non posse. *Q. E. D.*

Iam quia a certo >9, erit $2\sqrt{a}+1<a$, dabiturque adeo aliquis primus $<a$, cuius non-residuum a.

Per inductionem theorema generale (fundamentale) stabilitur, conclusionesque inde deducuntur.

130.

Postquam rigorose demonstravimus quemvis numerum primum formae $4n+1$, et positive et negative acceptum, alicuius numeri primi ipso minoris non-residuum esse, ad comparationem exactiorem et generaliorem numerorum primorum, quatenus unus alterius residuum vel non-residuum est, statim transimus.

Omni rigore supra demonstravimus, -3 et $+5$ esse residua vel non-residua omnium numerorum primorum, qui ipsorum 3, 5 respective sint residua vel non-residua.

Per inductionem autem circa numeros sequentes institutam invenitur: -7, -11, $+13$, $+17$, -19, -23, $+29$, -31, $+37$, $+41$, -43, -47, $+53$, -59 etc. esse residua vel non-residua omnium numerorum primorum, qui, positive sumti, illorum primorum respective sint residua vel non-residua. Inductio haec perfacile adiumento tabulae II confici potest.

Quivis autem levi attentione adhibita observabit, ex his numeris primis signo positivo affectos esse eos, qui sint formae $4n+1$, negativo autem eos, qui sint formae $4n+3$.

131.

Quod hic per inductionem deteximus, generaliter locum habere mox demonstrabimus. Antequam autem hoc negotium adeamus, necesse erit, omnia quae ex theoremate, si verum esse supponitur, sequuntur, eruere. Theorema ipsum ita enunciamus.

Si p est numerus primus formae $4n+1$, erit $+p$, si vero p formae $4n+3$, erit $-p$ residuum vel non-residuum cuiuscis numeri primi qui positive acceptus ipsius p est residuum vel non-residuum.

Quia omnia fere quae de residuis quadraticis dici possunt, huic theoremati innituntur, denominatio *theorematis fundamentalis*, qua in sequentibus utemur, haud absona erit.

Ut ratiocinia nostra quam brevissime exhiberi possint, per a, a', a'' etc. numeros primos formae $4n+1$, per b, b', b'' etc. numeros primos formae $4n+3$ denotabimus; per A, A', A'' etc. numeros quoscunque formae $4n+1$, per B, B', B'' etc. autem numeros quoscunque formae $4n+3$; tandem litera R duabus quantitatibus interposita indicabit, priorem sequentis esse residuum, sicuti litera N significationem contrariam habebit. *Ex. gr.* $+5R11$, $\pm 2N5$, indicabit $+5$ ipsius 11 esse residuum, $+2$ vel -2 esse ipsius 5 non-residuum. Iam col-

lato theoremate fundamentali cum theorematibus art. 111, sequentes propositiones facile deducentur.

	Si	erit
1.	$\pm aRa'$	$\pm a'Ra$
2.	$\pm aNa'$	$\pm a'Na$
3.	$\begin{cases} +aRb \\ -aNb \end{cases}$	$\pm bRa$
4.	$\begin{cases} +aNb \\ -aRb \end{cases}$	$\pm bNa$
5.	$\pm bRa$	$\begin{cases} +aRb \\ -aNb \end{cases}$
6.	$\pm bNa$	$\begin{cases} +aNb \\ -aRb \end{cases}$
7.	$\begin{cases} +bRb' \\ -bNb' \end{cases}$	$\begin{cases} +b'Nb \\ -b'Rb \end{cases}$
8.	$\begin{cases} +bNb' \\ -bRb' \end{cases}$	$\begin{cases} +b'Rb \\ -b'Nb \end{cases}$

132.

In his omnes casus, qui, duos numeros primos comparando, occurrere possunt, continentur: quae sequuntur, ad numeros quoscunque pertinent: sed harum demonstrationes minus sunt obviae.

	Si	erit
9.	$\pm aRA$	$\pm ARa$
10.	$\pm bRA$	$\begin{cases} +ARb \\ -ANb \end{cases}$
11.	$+aRB$	$\pm BRa$
12.	$-aRB$	$\pm BNa$
13.	$+bRB$	$\begin{cases} -BRb \\ +BNb \end{cases}$
14.	$-bRB$	$\begin{cases} +BRb \\ -BNb \end{cases}$

Quum omnium harum propositionum demonstrationes ex iisdem principiis sint petendae, necesse non erit omnes evolvere: demonstratio prop. 9, quam apponimus tamquam exemplum inservire potest. Ante omnia autem observetur, quemvis numerum formae $4n+1$ aut nullum factorem formae $4n+3$ habere, aut duos, aut quatuor etc., *i. e.* multitudinem talium factorum (inter quos etiam aequales esse possunt) semper fore parem: quemvis vero formae $4n+3$ multitudinem imparem factorum formae $4n+3$ (*i. e.* aut unum aut tres aut quinque etc.) implicare. Multitudo factorum formae $4n+1$ indeterminata manet.

Prop. 9 ita demonstratur. Sit A productum e factoribus primis a', a'', a''' etc., b, b', b'' etc.; eritque factorum b, b', b'' etc. multitudo par (possunt etiam nulli adesse, quod eodem redit). Iam si a est residuum ipsius A, erit residuum etiam omnium factorum a', a'', a''' etc. b, b', b'' etc. quare per propp. 1, 3 art. prace. singuli hi factores erunt residua ipsius a, adeoque etiam productum A. $-A$ vero idem esse debet. — Quodsi vero $-a$ est residuum ipsius A, eoque ipso omnium factorum a', a'' etc. b, b etc.; singuli a', a'' etc. erunt ipsius a residua, singuli b, b' etc. autem non-residua. Sed quum posteriorum multitudo sit par, productum ex omnibus, *i. e.* A, ipsius a residuum erit, hincque etiam $-A$.

133.

Investigationem adhuc generalius instituamus. Contemplemur duos numeros quoscunque impares inter se primos, signis quibuscunque affectos, P et Q. Concipiatur P sine respectu signi sui in factores suos primos resolutus, designeturque per p, quot inter hos reperiantur quorum non-residuum sit Q. Si vero aliquis numerus primus, cuius non-residuum est Q, pluries inter factores ipsius P occurrit, pluries etiam numerandus erit. Similiter sit q multitudo factorum primorum ipsius Q, quorum non-residuum est P. Tum numeri p, q certam relationem mutuam habebunt ab indole numerorum P, Q pendentem. Scilicet si alter numerorum p, q est par vel impar, numerorum P, Q forma docebit, utrum alter par sit vel impar. Haec relatio in sequenti tabula exhibetur.

Erunt p, q simul pares vel simul impares, quando numeri P, Q habent formas:

1. $+A, \quad +A'$
2. $+A, \quad -A'$

3. $+A$, $+B$
4. $+A$, $-B$
5. $-A$, $-A'$
6. $+B$, $-B'$

Contra numerorum p, q alter erit par, alter impar, quando numeri P, Q habent formas:

7. $-A$, $+B$
8. $-A$, $-B$
9. $+B$, $+B'$
10. $-B$, $-B'$ *)

Ex. Sint numeri propositi -55 et $+1197$, qui ad casum quartum erunt referendi. Est autem 1197 non-residuum unius factoris primi ipsius 55, scilicet numeri 5, -55 autem non-residuum trium factorum primorum ipsius 1197, scilicet numerorum 3, 3, 19.

Si P et Q numeros primos designant, propositiones hae abeunt in eas quas art. 131 tradidimus. Hic scilicet p et q maiores quam 1 fieri nequeunt, quare quando p ponitur esse par necessario erit $=0$ *i. e.* Q erit residuum ipsius P, quando vero p est impar, Q ipsius P non-residuum erit. Et vice versa. Ita scriptis a, b loco ipsorum A, B, ex 8 sequitur, si $-a$ fuerit residuum vel non-residuum ipsius b, fore $-b$ non-residuum vel residuum ipsius a, quod cum 3 et 4 art. 131 convenit.

Generaliter vero patet, Q residuum ipsius P esse non posse nisi fuerit $p=0$; si igitur p impar, Q certo ipsius P non-residuum erit.

Hinc etiam propp. art. praec. sine difficultate derivari possunt.

Ceterum mox patebit, hanc repraesentationem generalem plus esse quam speculationem sterilem, quum theorematis fundamentalis demonstratio completa absque ea vix perfici possit.

*) Sit $l=1$ si uterque $P, Q \equiv 3 \pmod 4$, alioquin $l=0$
$m=1$ si uterque P, Q negativus, alioquin $m=0$
tunc relatio pendet ab $l+m$.

134.

Aggrediamur nunc deductionem harum propositionum.

I. Concipiatur, ut ante, P in factores suos primos resolutus, signis neglectis, insuperque etiam Q in factores quomodocunque resolvatur, ita tamen ut signi ipsius Q ratio habeatur. Combinentur illi singuli cum singulis his. Tum si s designat multitudinem omnium combinationum, in quibus factor ipsius Q est non-residuum factoris ipsius P, p et s vel simul pares vel simul impares erunt. Sint enim factores primi ipsius P, hi f, f', f'' etc. et inter factores in quibus Q est resolutus, sint m qui ipsius f sint non-residua, m' non-residua ipsius f', m'' non-residua ipsius f'' etc. Tum facile quisquis perspiciet, fore

$$s = m + m' + m'' + \text{etc.}$$

p autem exprimere quot numeri inter ipsos m, m', m'' etc. sint impares. Unde sponte patet, s fore parem quando p sit par, imparem quando p sit impar.

II. Haec generaliter valent, quomodocunque Q in factores sit resolutus. Descendamus ad casus particulares. Contemplemur primo casus, ubi alter numerorum, P, est positivus, alter vero, Q, vel formae $+A$ vel formae $-B$. Resolvantur P, Q in factores suos primos, attribuatur singulis factoribus ipsius P signum positivum, singulis autem factoribus ipsius Q signum positivum vel negativum, prout sunt formae a vel b; tunc autem manifesto Q fiet vel formae $+A$ vel $-B$ uti requiritur. Combinentur factores singuli ipsius P cum singulis factoribus ipsius Q, designetque ut ante s multitudinem combinationum in quibus factor ipsius Q est non-residuum factoris ipsius P, similiterque t multitudinem combinationum in quibus factor ipsius P est non-residuum factoris ipsius Q. At ex theoremate fundamentali sequitur illas combinationes identicas fore cum his adeoque $s=t$. Tandem ex iis quae modo demonstravimus sequitur esse $p \equiv s \pmod 2$, $q \equiv t \pmod 2$, unde fit $p \equiv q \pmod 2$.

Habentur itaque propp. 1, 3, 4 et 6 art. 133.

Propositiones reliquae per methodum similem directe erui possunt, sed una consideratione nova indigent; facilius autem ex praecedentibus sequenti modo derivantur.

III. Denotent rursus P, Q, numeros quoscunque impares inter se primos, p, q multitudinem factorum primorum ipsorum P, Q, quorum non-residua Q, P respective. Tandem sit p' multitudo factorum primorum ipsius P, quorum

non-residuum est $-Q$ (quando Q per se est negativus, manifesto $-Q$ numerum positivum indicabit). Iam omnes factores primi ipsius P in quatuor classes distribuantur.

1) in factores formae a, quorum residuum est Q.

2) factores formae b, quorum residuum Q. Horum multitudo sit χ.

3) factores formae a, quorum non-residuum est Q. Horum multitudo sit ψ.

4) factores formae b, quorum non-residuum Q. Quorum multitudo $= \omega$.

Tum facile perspicitur fore $p' = \psi + \omega$, $p' = \chi + \psi$.

Iam quando P est formae $\pm A$, erit $\chi + \omega$ adeoque etiam $\chi - \omega$ numerus par; quare fiet $p' = p + \chi - \omega \equiv p \pmod 2$; quando vero P est formae $\pm B$, per simile ratiocinium invenitur, numeros p, p' sec. mod. 2 incongruos fore.

IV. Applicemus haec ad casus singulos. Sit primo tum P tum Q formae $+A$, eritque ex prop. 1 $p \equiv q \pmod 2$; at erit $p' \equiv p \pmod 2$; quare etiam $p' \equiv q \pmod 2$. Quod convenit cum prop. 2. — Simili modo si P est formae $-A$, Q formae $+A$, erit $p \equiv q \pmod 2$ ex prop. 2 quam modo demonstravimus; hinc, ob $p' \equiv p$, erit $p' \equiv q$. Est itaque etiam prop. 5 demonstrata.

Eodem modo prop. 7 ex 3; prop. 8 vel ex 4 vel ex 7; prop. 9 ex 6; ex eademque prop. 10 derivantur.

Demonstratio rigorosa theorematis fundamentalis.

135.

Per art. praec. propositiones art. 133 non quidem sunt demonstratae, sed tamen earum veritas a veritate theorematis fundamentalis quam aliquantisper supposuimus pendere ostensa est. At ex ipsa deductionis methodo manifestum est, illas valere pro numeris P, Q, si modo theorema fundamentale pro omnibus factoribus primis horum numerorum inter se comparatis locum habeat, etiamsi generaliter verum non sit. Nunc igitur ipsius theorematis fundamentalis demonstrationem aggrediamur. Cui praemittimus sequentem explicationem.

Theorema fundamentale usque ad numerum aliquem M verum esse dicemus, si valet pro duobus numeris primis quibuscunque, quorum neuter ipsum M superat.

Simili modo intelligi debet, si theoremata artt. 131, 132, 133 usque ad aliquem terminum vera esse dicemus. Facile vero perspicitur, si de veritate theorematis fundamentalis usque ad aliquem terminum constet, has propositiones usque ad eundem terminum locum esse habituras.

136.

Theorema fundamentale pro numeris parvis verum esse, per inductionem facile confirmari, atque sic limes determinari potest usque ad quem certo locum teneat. Hanc inductionem institutam esse postulamus; prorsus autem indifferens est quousque eam persecuti simus; sufficeret adeo, si tantummodo usque ad numerum 5 eam confirmavissemus, hoc autem per unicam observationem absolvitur, quod est $+5 N 3$, $\pm 3 N 5$.

Iam si theorema fundamentale generaliter verum non est, dabitur limes aliquis, T, vsque ad quem valebit, ita tamen ut usque ad numerum proxime maiorem, $T+1$, non amplius valeat. Hoc autem idem est ac si dicamus, dari duos numeros primos quorum maior sit $T+1$, et qui inter se comparati theoremati fundamentali repugnent, binos autem alios numeros primos quoscunque, si modo ambo ipso $T+1$ sint minores, huic theoremati esse consentaneos. Unde sequitur, propositiones artt. 131, 132, 133 usque ad T etiam locum habituras. Hanc vero suppositionem consistere non posse nunc ostendemus. Erunt autem secundum formas diversas, quas tum $T+1$, tum numerus primus ipso $T+1$ minor, quem cum $T+1$ comparatum theoremati repugnare supposuimus, habere possunt, casus sequentes distinguendi. Numerum istum primum per p designamus.

Quando tum $T+1$ tum p sunt formae $4n+1$, theorema fundamentale duobus modis falsum esse posset, scilicet si simul esset, *vel*

$$\pm p R (T+1) \text{ et } \pm (T+1) N p$$

vel simul

$$\pm p N (T+1) \text{ et } \pm (T+1) R p$$

Quando tum $T+1$ tum p sunt formae $4n+3$, theor. fund. falsum erit si simul fuerit *vel*

$$+ p R (T+1) \text{ et } - (T+1) N p$$

(sive quod eodem redit $- p N (T+1)$ et $+ (T+1) R p$)

vel

$$+ p N (T+1) \text{ et } - (T+1) R p$$

(sive

$$- p R (T+1) \text{ et } + (T+1) N p)$$

Quando $T+1$ est formae $4n+1$, p vero formae $4n+3$, theor. fund. falsum erit, si fuerit *vel*

$$\pm p R (T+1) \text{ et } + (T+1) N p \text{ (sive } - (T+1) R p)$$

vel

$$\pm p N (T+1) \text{ et } - (T+1) N p \text{ (sive } + (T+1) R p)$$

Quando $T+1$ est formae $4n+3$, p vero formae $4n+1$, theor. fund. falsum erit, si fuerit *vel*

$$+pR(T+1) \text{ (sive } -pN(T+1)) \text{ et } \pm(T+1)Np$$

vel

$$+pN(T+1) \text{ (sive } -pR(T+1)) \text{ et } \pm(T+1)Rp$$

Si demonstrari poterit, nullum horum octo casuum locum habere posse, simul certum erit, theorematis fundamentalis veritatem nullis limitibus circumscriptam esse. Hoc itaque negotium nunc aggredimur: at quoniam alii horum casuum ab aliis sunt dependentes, eundem ordinem, quo eos hic enumeravimus, servare non licebit.

137.

Casus primus. Quando $T+1$ est formae $4n+1$ $(=a)$, atque p eiusdem formae; insuper vero $\pm pRa$, non potest esse $\pm aNp$. Hic casus supra fuit primus.

Sit $+p \equiv e^2 \pmod a$, atque e par et $<a$ (quod semper obtineri potest). Iam duo casus sunt distinguendi.

I. Quando e per p non est divisibilis. Ponatur $e^2 = p + af$, eritque f positivus, formae $4n+3$ (sive formae B), $<a$, et per p non divisibilis. Porro erit $e^2 \equiv p \pmod f$, *i. e.* pRf adeoque ex prop. 11 art. 132 $\pm fRp$ (quia enim $p, f < a$, pro his propositiones istae valebunt). At est etiam $afRp$, quare fiet quoque $\pm aRp$.

II. Quando e per p est divisibilis, ponatur $e = gp$, atque $e^2 = p + aph$, sive $pg^2 = 1 + ah$. Tum erit h formae $4n+3$ (B), atque ad p et g^2 primus. Porro erit pg^2Rh, adeoque etiam pRh, hinc (prop. 11 art. 132) $\pm hRp$. At est etiam $-ahRp$, quia $-ah \equiv 1 \pmod p$; quare fiet etiam $\mp aRp$.

138.

Casus secundus. Quando $T+1$ est formae $4n+1$ $(=a)$, p formae $4n+3$, atque $\pm pR(T+1)$, non potest esse $+(T+1)Np$ sive $-(T+1)Rp$. Hic casus supra fuit quintus.

Sit ut supra $e^2 = p + fa$ atque e par et $< a$.

I. Quando e per p non est divisibilis, erit etiam f per p non divisibilis. Praeterea autem erit f positivus, formae $4n+1$ (sive A), atque $< a$; $+pRf$,

adeoque (prop. 10 art. 132) $+fRp$. Sed est etiam $+faRp$, quare fiet $+aRp$, sive $-aNp$.

II. Quando e per p est divisibilis, sit $e = pg$, atque $f = ph$. Erit itaque $g^2p = 1 + ha$. Tum h erit positivus, formae $4n+3$ (B), et ad p et g^2 primus. Porro $+g^2pRh$, adeoque $+pRh$; hinc fit (prop. 13 art. 132) $-hRp$. At est $-haRp$, unde fit $+aRp$ atque $-aNp$.

139.

Casus tertius. Quando $T+1$ est formae $4n+1$ $(=a)$, p eiusdem formae, atque $\pm pNa$: non potest esse $\pm aRp$. (Supra casus secundus).

Capiatur aliquis numerus primus ipso a minor, cuius non-residuum sit $+a$, quales dari supra demonstravimus (artt. 125, 129). Sed hic duos casus seorsim considerare oportet, prout hic numerus primus fuerit formae $4n+1$ vel $4n+3$, non enim demonstratum fuit, dari tales numeros primos *utriusque* formae.

I. Sit iste numerus primus formae $4n+1$ et $= a'$. Tum erit $\pm a'Na$ (art. 131) adeoque $\pm a'pRa$. Sit igitur $e^2 \equiv a'p \pmod a$ atque e par, $< a$. Tunc iterum quatuor casus erunt distinguendi.

1) Quando e neque per p neque per a' est divisibilis. Ponatur $e^2 = a'p \pm af$, signis ita acceptis ut f fiat positivus. Tum erit $f < a$, ad a' et p primus atque pro signo superiori formae $4n+3$, pro inferiori formae $4n+1$. Designemus brevitatis gratia per $[x, y]$ multitudinem factorum primorum numeri y quorum non-residuum est x. Tum erit $a'pRf$ adeoque $[a'p, f] = 0$. Hinc erit $[f, a'p]$ numerus par (propp. 1, 3, art. 133), *i. e.* aut $= 0$ aut $= 2$. Quare erit f aut residuum utriusque numerorum a', p, aut neutrius. Illud autem est impossibile, quum $\pm af$ sit residuum ipsius a', atque $\pm aNa'$ (hyp.); unde fit $\pm fNa'$. Hinc f debet esse utriusque numerorum a', p non-residuum. At propter $\pm afRp$ erit $\pm aNp$. *Q. E. D.*

2) Quando e per p, neque vero per a' est divisibilis, sit $e = gp$, atque $g^2p = a' \pm ah$, signo ita determinato, ut h fiat positivus. Tum erit $h < a'$, ad a', g et p primus, atque pro signo superiori formae $4n+3$, pro inferiori vero formae $4n+1$. Ex aequatione $g^2p = a' \pm ah$ si per p et a' multiplicatur, nullo negotio deduci potest, $pa'Rh$ ..... (α); $\pm ahpRa'$ .... (6); $aa'hRp$ ..... (γ). Ex (α) sequitur $[pa', h] = 0$, adeoque (propp. 1, 3, art. 133) $[h, pa']$ par, *i. e.*

erit h non-residuum vel utriusque p, a', vel neutrius. *Priori in casu* ex (6) sequitur $\pm apNa'$, et quum per hyp. sit $\pm aNa'$, erit $\pm pRa'$. Hinc per theor. fundam. quod pro numeris p, a' ipso $T+1$ minoribus valet, $\pm a'Rp$. Hinc et ex eo quod hNp, fit per (γ) $\pm aNp$. *Q. E. D.* *Posteriori casu* ex (6) sequitur $\pm apRa'$, hinc $\pm pNa'$, $\pm a'Np$, hincque tandem et ex hRp fit ex (γ) $\pm aNp$. *Q. E. D.*

3) Quando e per a' non autem per p est divisibilis. Pro hoc casu demonstratio tantum non eodem modo procedit ut in praec., neminemque qui hanc penetravit poterit morari.

4) Quando e tum per a' tum per p est divisibilis adeoque etiam per productum $a'p$ (numeros a', p enim *inaequales* esse supponimus, quia alias id quod demonstrare operam damus, esse aNp iam in hypothesi aNa' contentum foret), sit $e=ga'p$ atque $g^2a'p=1+ah$. Tum erit $h<a$, ad a' et p primus atque pro signo superiori formae $4n+3$, pro inferiori formae $4n+1$. Facile vero perspicitur, ex ista aequatione deduci posse haec $a'pRh$ .... (α); $\pm ahRa'$ .... (6); $\pm ahRp$ .... (γ). Ex (α) quod convenit cum (α) in (2) sequitur perinde ut illic, esse vel simul hRp, hRa', vel hNp, hNa'. Sed in casu priori foret per (6), aRa', contra hyp.; quare erit hNp, adeoque per (γ) etiam aNp.

II. Quando iste numerus primus est formae $4n+3$, demonstratio praecedenti tam similis est, ut eam apponere superfluum nobis visum sit. In eorum gratiam qui per se eam evolvere gestiunt (quod maxime commendamus), id tantum observamus, postquam ad talem aequationem $e^2=bp\pm af$ (designante b illum numerum primum) perventum fuerit, ad perspicuitatem profuturum, si utrumque signum seorsim consideretur.

140.

Casus quartus. *Quando* $T+1$ *est formae* $4n+1 (=a)$, p *formae* $4n+3$, *atque* $\pm pNa$, *non poterit esse* $+aRp$ *sive* $-aNp$. (Casus sextus supra).

Etiam huius casus demonstrationem, quum prorsus similis sit demonstrationi casus tertii, brevitatis gratia omittimus.

141.

Casus quintus. *Quando* $T+1$ *est formae* $4n+3 (=b)$, p *eiusdem formae, atque* $+pRb$ *sive* $-pNb$, *nequit esse* $+bRp$ *sive* $-bNp$. (Casus tertius supra).

Sit $p\equiv e^2 \pmod b$, atque e par et $<b$.

I. Quando e per p non est divisibilis. Ponatur $e^2=p+bf$, eritque f positivus, formae $4n+3$, $<b$ atque ad p primus. Porro erit pRf adeoque per prop. 13 art. 132, $-fRp$. Hinc et ex $+bfRp$ fit $-bRp$ adeoque $+bNp$. *Q. E. D.*

II. Quando e per p est divisibilis, sit $e=pg$, atque $ggp=1+bh$. Tum erit h formae $4n+1$ atque ad p primus, $p\equiv g^2p^2 \pmod h$, adeoque pRh; hinc fit $+hRp$ (prop. 10 art. 132), unde et ex $-bhRp$ sequitur $-bRp$, sive $+bNp$. *Q. E. D.*

142.

Casus sextus. *Quando* $T+1$ *est formae* $4n+3 (=b)$, p *formae* $4n+1$, *atque* pRb, *non poterit esse* $\pm bNp$. (Supra casus septimus).

Demonstrationem praecedenti omnino similem omittimus.

143.

Casus septimus. *Quando* $T+1$ *est formae* $4n+3 (=b)$, p *eiusdem formae, atque* $+pNb$ *sive* $-pRb$, *non poterit esse* $+bNp$ *sive* $-bRp$. (Casus quartus supra).

Sit $-p\equiv e^2 \pmod b$, atque e par et $<b$.

I. Quando e per p non divisibilis. Sit $-p=e^2-bf$ eritque f positivus, formae $4n+1$, ad p primus ipsoque b minor (etenim e certo non maior quam $b-1$, $p<b-1$, quare erit $bf=e^2+p<b^2-b$, *i.e.* $f<b-1$). Porro erit $-pRf$, hinc (prop. 10 art. 132) $+fRp$, unde et ex $+bfRp$ fit $+bRp$, sive $-bNp$.

II. Quando e per p est divisibilis, sit $e=pg$, atque $g^2p=-1+bh$. Tum erit h positivus, formae $4n+3$, ad p primus et $<b$. Porro erit $-pRh$, unde fit (prop. 14 art. 132) $+hRp$. Hinc et ex $bhRp$ sequitur $+bRp$ sive $-bNp$. *Q. E. D.*

144.

Casus octavus. *Quando* $T+1$ *est formae* $4n+3$ $(=b)$, p *formae* $4n+1$, *atque* $+pNb$ *sive* $-pRb$, *non poterit esse* $\pm bRp$. (Casus ultimus supra).

Demonstratio perinde procedit ut in casu praecedente.

Methodus analoga theorema art. 114 demonstrandi.

145.

In demonstratt. praecc. semper pro e valorem parem accepimus (artt. 137.. 144); observare convenit, etiam valorem imparem adhiberi potuisse, sed tum plures adhuc distinctiones introducendae fuissent. Qui his disquisitionibus delectantur, haud inutile facient, si vires suas in evolutione horum casuum exercitent. Praeterea theoremata ad residua $+2$ et -2 pertinentia tunc supponi debuissent; quum vero nostra demonstratio absque his theorematibus sit perfecta, novam hinc methodum nanciscimur, illa demonstrandi. Quae minime est contemnenda, quum methodi, quibus supra pro demonstratione theorematis, ± 2 esse residuum cuiusvis numeri primi formae $8n+1$, usi sumus, minus directae videri possint. Reliquos casus (qui ad numeros primos formarum $8n+3$, $8n+5$, $8n+7$ spectant) per methodos supra traditas demonstratos, illudque theorema tantummodo per inductionem inventum esse supponemus; hanc autem inductionem per sequentes reflexiones ad certitudinis gradum evehemus.

Si ± 2 omnium numerorum primorum formae $8n+1$ residuum non esset, ponatur minimus primus huius formae, cuius non-residuum ± 2, $=a$, ita ut pro omnibus primis ipso a minoribus theorema valeat. Tum accipiatur numerus aliquis primus $< \frac{1}{2}a$, cuius non-residuum a (qualem dari ex art. 129 facile deducitur). Sit hic $=p$ eritque per theor. fund. pNa. Hinc fit $\pm 2pRa$. — Sit itaque $e^2 \equiv 2p \pmod{a}$ ita ut e sit impar atque $< a$. Tum duo casus erunt distinguendi.

I. Quando e per p non est divisibilis. Sit $e^2 = 2p + aq$ eritque q positivus, formae $8n+7$ vel formae $8n+3$ (prout p est formae $4n+1$ vel $4n+3$), $< a$, atque per p non divisibilis. Iam omnes factores primi ipsius q in quatuor classes distribuantur, sint scilicet e formae $8n+1$, f formae $8n+3$, g formae $8n+5$, h formae $8n+7$; productum e factoribus primae classis sit E, producta e factoribus secundae, tertiae, quartae classis respective F, G, H*).

*) Si ex aliqua classe nulli factores adessent, loco-producti ex his 1 scribere oporteret.

His ita factis, consideremus *primo* casum ubi p est formae $4n+1$, sive q formae $8n+7$. Tum facile perspicitur fore $2RE$, $2RH$, unde pRE, pRH, hincque tandem ERp, HRp. Porro erit 2 non-residuum cuiusvis factoris formae $8n+3$ aut $8n+5$, adeoque etiam p; hinc quivis talis factor non-residuum ipsius p; unde facile concluditur FG fore ipsius p residuum si $f+g$ fuerit par, non-residuum si $f+g$ fuerit impar. At $f+g$ impar esse non potest; facile enim perspicietur omnes casus enumerando. $EFGH$ sive q fieri vel formae $8n+3$ vel $8n+5$, si fuerit $f+g$ impar, quidquid sint singuli e,f,g,h, contra hyp. Erit igitur $FGRp$, $EFGHRp$, sive qRp, hincque tandem, propter $aqRp$, aRp contra hyp. *Secundo* quando p est formae $4n+3$, simili modo ostendi potest, fore pRE adeoque ERp, $-pRF$ adeoque FRp, tandem $g+h$ parem hincque $GHRp$, unde tandem sequitur qRp, aRp contra hyp.

II. Quando e per p divisibilis, demonstratio simili modo adornari, et a peritis (quibus solis hic articulus est scriptus) haud difficulter evolvi poterit. Nos brevitatis gratia eam omittimus.

Solutio problematis generalis.

146.

Per theorema fundamentale atque propositiones ad residua -1 et ± 2 pertinentes semper determinari potest utrum numerus quicunque datus numeri primi dati residuum sit an non-residuum. At haud inutile erit, reliqua etiam quae supra tradidimus hic iterum in conspectum producere, ut omnia coniuncta habeantur quae sunt necessaria ad solutionem

Problematis: *Propositis duobus numeris quibuscunque* P, Q, *invenire, utrum alter* Q, *alterius* P *residuum sit an non-residuum.*

Sol. I. Sit $P = a^\alpha b^\beta c^\gamma$ etc. designantibus a, b, c etc. numeros primos inaequales positive acceptos (nam P manifesto absolute est sumendus). Brevitatis gratia in hoc art. *relationem* duorum numerorum x, y simpliciter dicemus eam quatenus prior x posterioris y residuum est vel non-residuum. Pendet igitur relatio ipsorum Q, P a relationibus ipsorum Q, a^α; Q, b^β etc. (art. 105).

II. Ut relatio ipsorum Q, a^α (de reliquis enim Q, b^β etc. idem valet) innotescat, duo casus distinguendi.

1. Quando Q per a est divisibilis. Ponatur $Q = Qa^e$, ita ut Q per a non sit divisibilis. Tunc si $e = \alpha$ vel $e > \alpha$, erit QRa^α; si vero $e < \alpha$ atque impar, erit QNa^e: tandem si $e < \alpha$ atque par, habebit Q ad a^e eandem relationem quam habet Q' ad a^{e-e}. Reductus est itaque hic casus ad

2. Quando Q per a non est divisibilis. Hic denuo duos casus distinguimus.

(*A*) Quando $a = 2$. Tunc semper erit QRa^α, quando $\alpha = 1$; quando vero $\alpha = 2$, requiritur, ut sit Q formae $4n+1$: denique quando $\alpha = 3$ vel > 3, Q debet esse formae $8n+1$. Quae conditio si locum habet, erit QRa^α.

(*B*) Quando a est alius numerus primus. Tunc Q ad a^α eandem relationem habebit quam habet ad a. (V. art. 101).

III. Relatio numeri cuiuscunque Q ad numerum primum a (imparem) ita investigatur. Quando $Q > a$, substituatur loco ipsius Q ipsius residuum minimum positivum secundum modulum a *). Hoc ad a eandem relationem habebit quam habet Q.

Porro resolvatur Q, sive numerus ipsius loco assumtus, in factores suos primos p, p', p'' etc., quibus adiungendus factor -1, quando Q est negativus. Tum constat relationem ipsius Q ad a pendere a relationibus singulorum p, p', p'' etc. ad a. Scilicet si inter illos factores sunt $2m$ non-residua ipsius a, erit QRa, si vera $2m+1$, erit QNa. Facile autem perspicitur, si inter factores p, p', p'' etc., bini aut quaterni aut seni aut generaliter $2k$ aequales occurrant, hos tuto oiici posse.

IV. Si inter factores p, p', p'' reperiuntur -1 et 2, horum relatio ad a ex artt. 108, 112, 113, 114 inveniri potest. Reliquorum autem relatio ad a pendet a relatione ipsius a ad ipsos (theor. fund., atque propp. art. 131). Sit p unus ex ipsis, invenieturque, tractando numeros a, p eodem modo ut antea Q et a illis respective maiores, relationem ipsius a ad p aut per artt. 108 — 114 determinari posse (si scilicet residuum minimum ipsius a (mod. p) nullos factores primos impares habeat), aut insuper a relatione ipsius p ad numeros quosdam primos ipso p minores pendere. Idem valet de reliquis factoribus p', p'' etc. Facile iam

*) *Residuum* in signific. art. 1. — Plerumque praestat residuum *absolute* minimum accipere.

perspicitur per continuationem huius operationis tandem ad numeros perventum iri quorum relationes per propp. artt. 108 — 114 determinari possint. Per exemplum haec clariora fient.

Ex. Quaeritur relatio numeri $+453$ ad 1236. Est $1236 = 4.3.103$; $+453 R 4$ per II, 2 (*A*); $+453 R 3$ per II, 1. Superest igitur ut relatio ipsius $+453$ ad 103 exploretur. Eadem autem erit quam habet $+41$ ($\equiv 453$, mod. 103) ad 103; eadem ipsius $+103$ ad 41 (theor. fund.), sive ipsius -20 ad 41. At est $-20 R 41$; namque $-20 = -1.2.2.5$; $-1 R 41$ (art. 108); atque $+5 R 41$ ideo quod $41 \equiv 1$ adeoque ipsius 5 residuum est (theor. fund.). Hinc sequitur $+453 R 103$, hincque tandem $+453 R 1236$. Est autem revera $453 \equiv 297^2 \pmod{1236}$.

De formis linearibus omnes numeros primos continentibus, quorum vel residuum vel non-residuum est numerus quicunque datus.

147.

Proposito numero quocunque A, *formulae* certae exhiberi possunt, sub quibus omnes numeri ad A primi quorum residuum est A continentur, sive omnes qui esse possunt *divisores* numerorum formae $xx - A$ (designante xx quadratum indeterminatum) *). Sed brevitatis gratia ad eos tantum divisores respiciemus, qui sunt impares atque ad A primi, quum ad hos casus reliqui facile reduci possint.

Sit primo A aut numerus primus positivus formae $4n+1$, aut negativus formae $4n-1$. Tum secundum theorema fundamentale omnes numeri primi, qui, positive sumti, sunt residua ipsius A, erunt divisores ipsius $xx - A$: omnes autem numeri primi (excepto numero 2 qui semper est divisor) qui ipsius A sunt non-residua erunt non-divisores ipsius $xx - A$. Sint omnia residua ipsius A ipso A minora (exclusa cifra) r, r', r'' etc. omnia non-residua vero n, n', n'' etc. Tum quivis numerus primus, in aliqua formarum $Ak+r$, $Ak+r'$, $Ak+r''$ etc. contentus, erit divisor ipsius $xx - A$, quivis autem primus in aliqua formarum $Ak+n$, $Ak+n'$ etc. contentus non-divisor erit, designante k numerum integrum indeterminatum. Illas formas dicimus *formas divisorum ipsius* $xx - A$, has vero *formas non-divisorum*. Utrorumque multitudo erit $\frac{1}{2}(A-1)$. Porro si B est numerus compositus impar atque ARB, omnes factores primi ipsius B in aliqua for-

*) Huiusmodi numeros simpliciter *divisores ipsius* $xx - A$ dicemus unde sponte patet quid sint *non-divisores*.

marum priorum continentur adeoque etiam B. Quare *quivis* numerus impar in forma non-divisorum contentus, erit non-divisor formae $xx-A$. Sed hoc theorema convertere non licet; nam si B est non-divisor compositus impar formae $xx-A$, inter factores primos ipsius B aliqui non-divisores erunt, quorum multitudo si est *par*, B nihilominus in aliqua forma divisorum reperietur. V. art. 99.

Ex. Hoc modo pro $A=-11$ formae divisorum ipsius $xx+11$ inveniuntur hae: $11k+1, 3, 4, 5, 9$; formae non-divisorum autem erunt $11k+2, 6, 7, 8, 10$. Erit itaque -11 non-residuum omnium numerorum imparium, qui in aliqua posteriorum formarum continentur, residuum autem omnium primorum ad aliquam priorum pertinentium.

Similes formae dantur pro divisoribus atque non-divisoribus ipsius $xx-A$, quemcunque numerum designet A. Sed facile perspicitur, eos ipsius A valores tantummodo considerari oportere, qui per nullum quadratum sint divisibiles; patet enim si fuerit $A=a^2A'$, omnes divisores *) ipsius $xx-A$ etiam fore divisores ipsius $xx-A'$, similiterque non-divisores. — Distinguemus autem tres casus, 1) quando A est formae $+(4n+1)$ vel $-(4n-1)$. 2) quando A est formae $-(4n+1)$ vel $+(4n-1)$. 3) quando A est par sive formae $\pm(4n+2)$.

148.

Casus primus, quando A est formae $+(4n+1)$ vel $-(4n-1)$. Resolvatur A in factores suos primos, tribuaturque iis qui sunt formae $4n+1$ signum positivum, iis vero qui sunt formae $4n-1$ signum negativum (unde fiet productum ex ipsis $=A$): Sint hi factores a, b, c, d etc. Distribuantur omnes numeri ipso A minores et ad A primi in duas classes, et quidem in primam classem omnes numeri qui sunt nullius ex numeris a, b, c, d etc. non-residua, aut duorum, aut quatuor aut generaliter multitudinis paris; in secundam vero ii, qui sunt non-residua unius ex numeris a, b, c etc. aut trium etc. aut generaliter multitudinis imparis. Designentur priores per r, r', r'' etc., posteriores per n, n', n'' etc. Tum formae $Ak+r$, $Ak+r'$, $Ak+r''$ etc. erunt formae divisorum ipsius $xx-A$, formae vero $Ak+n$, $Ak+n'$ etc. erunt formae non-divisorum ipsius $xx-A$ (*i.e. numerus quicunque primus, praeter 2, erit divisor aut non-divisor ipsius $xx-A$, prout in aliqua formarum priorum aut posteriorum continetur*). Si enim p est numerus primus positivus atque alicuius ex numeris a, b, c etc. residuum vel non-residuum, hic ipse numerus ipsius p residuum vel non-residuum erit (theor. fund.). Quare si inter numeros a, b, c etc. sunt m, quorum non-residuum est p, totidem erunt non-residua ipsius p, adeoque si p in aliqua formarum priorum continetur, erit m par et ARp, si vero in aliqua posteriorum, erit m impar atque ANp.

*) Nempe qui sint primi ad A.

Ex. Sit $A=+105=-3\times+5\times-7$. Tum numeri r, r', r'' etc. erunt hi: 1, 4, 16, 46, 64, 79 (qui sunt non-residua nullius numerorum 3, 5, 7); 2, 8, 23, 32, 53, 92 (qui sunt non-residua numerorum 3, 5); 26, 41, 59, 89, 101, 104 (qui sunt non-residua numerorum 3, 7); 13, 52, 73, 82, 97, 103 (qui sunt non-residua numerorum 5, 7). — Numeri autem n, n', n'' etc. erunt hi: 11, 29, 44, 71, 74, 86; 22, 37, 43, 58, 67, 88; 19, 31, 34, 61, 76, 94; 17, 38, 47, 62, 68, 83. Seni primi sunt non-residua ipsius 3, seni posteriores non-residua ipsius 5, tum sequuntur non-residua ipsius 7, tandem ii qui sunt non-residua omnium trium simul.

Facile ex combinationum theoria atque artt. 32, 96 deducitur, numerorum r, r', r'' etc. multitudinem fore

$$= t\left(1+\frac{l.l-1}{1.2}+\frac{l.l-1.l-2.l-3}{1.2.3.4}+\cdots\cdots\right)$$

numerorum n, n', n'' etc. multitudinem

$$= t\left(l+\frac{l.l-1.l-2}{1.2.3}+\frac{l.l-1.\ldots.l-4}{1.2.\ldots.5}+\cdots\right)$$

ubi l designat multitudinem numerorum a, b, c etc.;

$$t=2^{-l}(a-1)(b-1)(c-1) \text{ etc.}$$

et utraque series continuanda donec abrumpatur. (Dabuntur scilicet t numeri qui sunt residua omnium a, b, c etc., $\frac{t.l.l-1}{1.2}$ qui sunt non-residua duorum, etc. sed demonstrationem hanc fusius explicare brevitas non permittit). Utriusque autem seriei summa *) est $=2^{l-1}$. Scilicet prior prodit ex hac

$$1+(l-1)+\frac{l-1.l-2}{1.2}+\cdots$$

iungendo terminum secundum et tertium, quartum et quintum etc., posterior vero ex eadem iungendo terminum primum atque secundum, tertium et quartum etc. Dabuntur itaque tot formae divisorum ipsius $xx-A$, quot dantur formae non-divisorum, scilicet $\frac{1}{2}(a-1)(b-1)(c-1)$ etc.

*) Neglecto factore t.

149.

Casum secundum et tertium hic simul contemplari possumus. Poterit scilicet A semper hic poni $=(-1)Q$, aut $=(+2)Q$, aut $=(-2)Q$, designante Q numerum formae $+(4n+1)$, aut $-(4n-1)$, quales in art. praec. consideravimus. Sit generaliter $A=\alpha Q$, ita ut sit α aut $=-1$, aut $=\pm 2$. Tum erit A residuum omnium numerorum, quorum residuum est aut uterque α et Q, aut neuter; non-residuum autem omnium, quorum non-residuum alteruter tantum numerorum α, Q. Hinc formae divisorum ac non-divisorum ipsius $xx-A$ facile derivantur. Si $\alpha=-1$, distribuantur omnes numeri ipso $4A$ minores ad ipsumque primi in duas classes, in priorem ii, qui sunt in aliqua forma divisorum ipsius $xx-Q$ simulque in forma $4n+1$, iique, qui sunt in aliqua forma non-divisorum ipsius $xx-Q$ simulque in forma $4n+3$; in posteriorem reliqui. Sint priores r, r', r'' etc., posteriores n, n', n'' etc., eritque A residuum omnium numerorum primorum in aliqua formarum $4Ak+r$, $4Ak+r'$, $4Ak+r''$ etc. contentorum, non-residuum autem omnium primorum in aliqua formarum $4Ak+n$, $4Ak+n'$ etc. contentorum. — Si $\alpha=\pm 2$, distribuantur omnes numeri ipso $8Q$ minores ad ipsumque primi in duas classes: in primam ii, qui continentur in aliqua forma divisorum ipsius $xx-Q$ simulque in aliqua formarum $8n+1$, $8n+7$ pro signo superiori, vel formarum $8n+1$, $8n+3$ pro inferiori, iique qui contenti sunt in aliqua forma non-divisorum ipsius $xx-Q$ simulque in aliqua harum $8n+3$, $8n+5$ pro signo superiori, vel harum $8n+5$, $8n+7$ pro inferiori, — in secundam reliqui. Tum designatis numeris classis prioris per r, r', r'' etc., numerisque classis posterioris per n, n', n'' etc., $\pm 2Q$ erit residuum omnium numerorum primorum in aliqua formarum $8Qk+r$, $8Qk+r'$, $8Qk+r''$ etc. contentorum, omnium autem primorum in aliqua formarum $8Qk+n$, $8Qk+n'$, $8Qk+n''$ etc. non-residuum. Ceterum facile demonstrari potest, etiam hic totidem formas divisorum ipsius $xx-A$ datum iri ac non-divisorum.

Ex. Hoc modo invenitur $+10$ esse residuum omnium numerorum primorum in aliqua formarum $40k+1, 3, 9, 13, 27, 31, 37, 39$ contentorum, non-residuum vero omnium primorum, qui sub aliqua formarum $40k+7, 11, 17, 19, 21, 23, 29, 33$ continentur.

150.

Formae hae plures habent proprietates satis memorabiles, quarum tamen unam tantummodo apponimus. Si B est numerus compositus ad A primus, inter cuius factores primos occurrunt $2m$, qui in aliqua forma non-divisorum ipsius $xx-A$ continentur, B in aliqua forma divisorum ipsius $xx-A$ contentus erit; si vero multitudo factorum primorum ipsius B in aliqua forma non-divisorum ipsius $xx-A$ contentorum impar est, B quoque in forma non-divisorum contentus erit. Demonstrationem quae non est difficilis omittimus. Hinc vero sequitur, non modo quemvis numerum primum sed etiam quemvis compositum imparem ad A primum, qui in aliqua forma non-divisorum contineatur, non-divisorem fore; necessario enim aliquis factor primus talis numeri debet esse non-divisor.

De aliorum laboribus circa has investigationes.

151.

Theorema fundamentale, quod sane inter elegantissima in hoc genere est referendum, in eadem forma simplici, in qua supra propositum est, a nemine hucusque fuit prolatum. Quod eo magis est mirandum, quum aliae quaedam propositiones illi superstruendae, ex quibus ad illud facile reveniri potuisset, ill. Eulero iam innotuerint. Formas certas dari, in quibus omnes divisores primi numerorum formae $xx+A$ continentur, aliasque in quibus omnes non-divisores primi numerorum eiusdem formae sint comprehensi, ita ut hae illas excludant, noverat methodumque illas formas inveniendi eruerat: sed omnes ipsius conatus ad demonstrationem perveniendi semper irriti fuerunt, veritatique illi per inductionem inventae maiorem tantummodo verisimilitudinem conciliaverunt. In aliqua quidem tractatione, *Novae demonstrationes circa divisores numerorum formae* $xx+nyy$, quae in Acad. Petrop. recitata est 1775 Nov. 20, et post mortem viri summi in *T.* I, *Nov. Act.* huius Ac. p. 47 sqq. est conservata, voti se compotem credidisse videtur: sed hic error irrepsit, scilicet p. 65 *tacite* supposuit, formas tales divisorum et non-divisorum exstare *) unde non difficile erat *quales* esse debeant derivare: methodus autem qua usus est ad comprobationem illius suppositionis haud

*) Nempe dari numeros r, r', r'' etc., n, n', n'' etc. omnes diversos et $<4A$ tales ut omnes divisores primi ipsius $xx-A$ sub aliqua formarum $4Ak+r$, $4Ak+r'$ etc. contineantur, omnesque non-divisores primi sub aliqua harum $4Ak+n$, $4Ak+n'$ etc. (designante k numerum indeterminatum).

idonea videtur. In alio schediasmate, *De criteriis aequationis* $fxx+gyy=hzz$ *utrumque resolutionem admittat necne*, Opusc. Anal. T. I. (ubi f,g,h sunt dati, x,y,z indeterminati) per inductionem invenit, si aequatio pro aliquo valore ipsius $h=s$ solubilis sit, eandem pro quovis alio valore ipsi s secundum mod. $4fg$ congruo, siquidem sit numerus primus, solubilem fore, ex qua propositione suppositio de qua diximus haud difficile demonstrari potest. Sed etiam huius theorematis demonstratio omnes ipsius labores elusit *), quod non est mirandum, quia nostro iudicio a theoremate fundamentali erat proficiscendum. Ceterum veritas huius propositionis ex iis quae in Sect. sequenti docebimus sponte demanabit.

Post Eulerum, clar. Le Gendre eidem argumento operam navavit, in egregia tract. *Recherches d'analyse indéterminée*, Hist. de l'Ac. des Sc. 1785 p. 465 sqq., ubi pervenit ad theorema, quod si rem ipsam spectas cum th. fund. idem est, scilicet designantibus p,q duos numeros primos positivos, fore residua absolute minima potestatum $p^{\frac{q-1}{2}}$, $q^{\frac{p-1}{2}}$ sec. mod. q,p resp. aut ambo $+1$, aut ambo -1, quando aut p aut q sit formae $4n+1$; quando vero tum p tum q sit formae $4n+3$, alterum res. min. fore $+1$, alterum -1, p. 516, ex quo sec. art. 106 derivatur, *relationem* (in signif. art. 146 acceptam) ipsius p ad q ipsiusque q ad p *eandem* esse, quando aut p aut q sit formae $4n+1$, *oppositam*, quando tum p tum q sit formae $4n+3$. Propos. haec inter propp. art. 131 est contenta, sequitur etiam ex 1, 3, 9, art. 133; vicissim autem theor. fund. ex ipsa derivari potest. Clar. Le Gendre etiam demonstrationem tentavit, de qua quum perquam ingeniosa sit in Sect. seq. fusius loquemur. Sed quoniam in ea plura sine demonstratione supposuit (uti ipse fatetur p. 520 *Nous avons supposé seulement* etc.), quae partim a nemine hucusque sunt demonstrata, partim nostro quidem iudicio sine theor. fund. ipso demonstrari nequeunt: via quam ingressus est, ad scopum deducere non posse videtur, nostraque demonstratio pro prima erit habenda. — Ceterum infra *duas alias demonstrationes* eiusdem gravissimi theorematis trademus, a praec. et inter se toto coelo diversas.

*) Uti ipse fatetur, l. c. p. 216: „Huius elegantissimi theorematis demonstratio adhuc desideratur, postquam a pluribus iamdudum frustra est investigata.... Quocirca plurimum is praestitisse censendus erit, cui successerit demonstrationem huius theorematis invenire.“ — Quanto ardore vir immortalis demonstrationem huius theorematis aliorumque, quae tantummodo casus speciales theor. fundam. sunt, desideraverit, videre licet ex multis aliis locis Opusce. Anall. Conf. *Additamentum ad diss.* VIII, T. I. et *diss.* XIII, T. II. pluresque diss. in Comment. Petrop., iam passim laudatae.

De congruentiis secundi gradus non puris.

152.

Hactenus congruentiam puram $xx\equiv A \pmod m$ tractavimus, ipsiusque resolubilitatem dignoscere docuimus. *Radicum ipsarum* investigatio per art. 105 ad eum casum est reducta, ubi m est aut primus aut primi potestas, posterior vero per art. 101 ad eum, ubi m est primus. Pro hoc autem casu ea quae in art. 61 sqq. tradidimus una cum iis quae in Sectt. V et VIII docebimus, omnia fere complectuntur quae per methodos directas erui possunt. Sed hae ubi sunt applicabiles plerumque infinities prolixiores sunt quam indirectae quas in Sect. VI docebimus, adeoque non tam propter utilitatem suam in praxi quam propter pulcritudinem memorabiles. — *Congruentiae secundi gradus non purae* ad puras facile reduci possunt. Proposita congruentia

$$axx+bx+c \equiv 0$$

secundum mod. m solvenda, huic aequivalebit congruentia

$$4aaxx+4abx+4ac \equiv 0 \pmod{4am}$$

i. e. quivis numerus alteri satisfaciens etiam alteri satisfaciet. Haec vero ita exhiberi potest

$$(2ax+b)^2 \equiv bb-4ac \pmod{4am}$$

unde omnes valores ipsius $2ax+b$ minores quam $4am$, si qui dantur inveniri possunt. Quibus per r,r',r'' etc. designatis, omnes solutiones congr. prop. deducentur ex solutionibus congruentiarum

$$2ax \equiv r-b,\quad 2ax \equiv r'-b \text{ etc. } \pmod{4am}$$

quas in Sect. II invenire docuimus. Ceterum observamus, solutionem plerumque per varia artificia contrahi posse, *ex. gr.* loco congr. prop. aliam inveniri posse

$$a'xx+2b'x+c' \equiv 0$$

illi aequipollentem, et in qua a' ipsum m metiatur; haec vero de quibus Sect. ultima conferri potest, hic explicare brevitas non permittit.