Werk

Titel: Hoehere Arithmetik
Jahr: 1863
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN23599524X
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN23599524X
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=23599524X

LOG Id: LOG_0032
LOG Titel: Caput octavum. Disquisitiones generales de congruentiis
LOG Typ: chapter

Übergeordnetes Werk

Werk Id: PPN235957348
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235957348
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=235957348

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

DISQUISITIONES GENERALES DE CONGRUENTIIS.

ANALYSIS RESIDUORUM CAPUT OCTAVUM.

330.

Quae in Sectionibus praecedentibus de congruentiis sunt tradita, simplicissimos tantum casus attinent methodisque particularibus plerumque sunt eruta. In hac Sectione periculum faciemus congruentiarum theoriam, quantum quidem adhuc licet, ad altiora principia reducere, simili fere modo ut *aequationum* theoria considerari solet, quacum insignis intercedit analogia, uti iam saepius observavimus. Quoniam igitur omnes congruentiae algebraicae unicam incognitam involventes ad hanc formam reduci possunt

$$X \equiv 0$$

ubi X est functio algebraica incognitae x, nullas fractiones involvens, huiusmodi functiones imprimis erunt considerandae.

331.

Si P, Q sint functiones indeterminatae x huius formae

$$A+Bx+Cxx+Dx^3+\ldots$$
$$H+Ix+Kxx+Lx^3+\ldots$$

(quales abhinc semper per *functiones* simpliciter designamus) et in utraque coëfficientes similium ipsius x potestatum secundum quemcunque modulum sint con-

grui, *functiones secundum hunc modulum congruae* dicentur. Perspicuum autem est, functiones congruas, si pro indeterminata valores aequales aut congrui accipiantur, valores congruos nancisci. Quae in Capp. I. et II. de *numeris* demonstravimus, plerumque etiam de functionibus sunt tenenda; ita si $P \equiv P'$, $Q \equiv Q'$, $R \equiv R'$ etc., patet, fore $P+Q+R+$ etc. $\equiv P'+Q'+R'+$ etc.; $P-Q \equiv P'-Q'$; $PQ \equiv P'Q'$; PQR etc. $\equiv P'Q'R'$ etc. Demonstrationes facillimae, possuntque simili modo adornari ut Cap. I^mo.

Si $PQ \equiv R$, functionem Q per $\frac{R}{P}$ designabimus apposito modulo, dicemusque, Q esse quotientem, si R per P secundum hunc modulum dividatur. Manifestum autem est, loco ipsius Q omnes functiones ipsi congruas accipi posse, quas omnes tamquam *unicum* valorem spectabimus. Infra vero ostendemus, quibus casibus talis quotiens plures valores (i. e. incongruos) nancisci possit.

332.

Si modulus sit numerus primus et divisor Q unicum tantum terminum involvat Hx^h, cuius coëfficiens H per modulum non dividitur, i. e. si modo H non sit $\equiv 0$, quotiens plures valores habere nequit. Si enim esset $QA \equiv P$ et $QB \equiv P$, foret $Q(A-B) \equiv 0$. Iam sit

$$Q \equiv \ldots + Hx^h + Ix^{h+1} + \text{etc.}$$

ita ut H per p non dividatur, et

$$A-B \equiv Lx^l + Mx^{l+1} + \text{etc.}$$

ita ut L per p non dividatur (hanc autem formam $A-B$ habebit, quia supponimus A non $\equiv B$). Foretque $Q(A-B) \equiv HLx^{h+l} + \text{etc.} \equiv 0$. Q. E. A., quia HL non $\equiv 0$.

Facile iam regulae dantur functionem P per Q, siquidem fieri potest, dividendi; sit

$$P \equiv ax^\alpha + bx^{\alpha+1} + cx^{\alpha+2} + \text{etc.} + kx^\varkappa$$
$$Q \equiv mx^\mu + nx^{\mu+1} + qx^{\mu+2} + \text{etc.} + tx^\tau$$

ita ut a, k, m, t per modulum non dividantur, debetque esse α non $< \mu$, $\varkappa$ non $< \tau$. Divisio autem simili modo institui potest, ut in calculo logistico communi, modo semper pro quotiente numerus integer accipiatur; scilicet quotiens semper

hanc formam habebit $\frac{r}{m}$, quod secundum modulum determinari debet. Iam si postquam $\varkappa+\mu-\alpha-\tau+1$ termini sunt inventi, residuum remaneat, quod erit formae

$$Ax^{\varkappa+\mu-\tau+1}+Bx^{\varkappa+\mu-\tau+2}+..+Cx^{\varkappa}$$

neque omnes coëfficientes $A, B, C..$ sint $\equiv 0$, P per Q dividi nequit.

Ceterum patet, divisionem etiam a terminis, qui maximas dimensiones habent, $kx^{\varkappa}$, tx^{τ} incipi potuisse; operatio facilitabitur, si Q ad formam redigatur

$$mx^{\mu}(1+qx+rxx+\text{ etc.})$$

unde fiet posito $mv \equiv 1$

$$\frac{P}{Q} \equiv \frac{vP:x^{\mu}}{1+qx+\text{ etc.}}$$

tunc vero divisio per methodos communes perfici potest.

333.

Theorema. *Si $x \equiv a$ fuerit radix congruentiae $\xi \equiv 0$, ξ per $x-a$ dividi poterit secundum congruentiae modulum.*

Demonstratio. Si enim dividi non posset, foret $\xi \equiv (x-a)\xi'+b$, ita ut b per modulum dividi non posset. Iam si x ponatur $\equiv a$, ξ fiet $\equiv 0$ (hyp.), quare $(x-a)\xi'+b \equiv 0$; sed tunc etiam $(x-a)\xi' \equiv 0$, quare b necessario erit $\equiv 0$.

334.

Problema. *Datis binis functionibus, earum communem divisorem (maximae dimensionis) invenire secundum modulum datum.*

Solutio. Sint functiones A, B. Habeat A totidem aut plures dimensiones quam B; dividatur A per B, si fieri potest sine residuo, B erit divisor communis quaesitus. Si residuum maneat C, hoc inferiorem dimensionem habebit quam B. Sit itaque

$$A \equiv aB+C, \quad B \equiv bC+D, \quad C \equiv cD+E, \text{ etc.}$$

ita ut A, B, C, D, a, b, c etc. sint functiones, et dimensiones functionum A, B, C, D etc. constituant seriem decrescentem. Iam si tandem aliqua divisio succedat, ex. gr. $D \equiv dE$, ultimus divisor erit divisor communis quaesitus; si vero nulla succedat, tandem ad residuum pervenietur, quod nullam dimensionem

habeat i. e. ad *numerum*; hoc autem casu functiones A, B communem divisorem non habent.

Demonstr. Si divisor E functionem praecedentem sine residuo dividat, omnes antecendentes dividere facile perspicitur; quare E erit divisor communis functionum A, B. Q. E. Pr. Si autem daretur divisor maioris dimensionis, puta E', hic propter $C \equiv A - aB$ etiam C similique argumento etiam D etc. adeoque E divideret, functio maioris dimensionis functionem minoris. Q. E. A. Q. E. Scd. Hinc etiam patet, si divisor communis ullius dimensionis datur, ad residuum nullius dimensionis perveniri non posse; alias enim functio nullius dimensionis per functionem alicuius dimensionis divideretur. Q. E. A.

335.

THEOREMA. *Si A, B sint functiones inter se primae secundum modulum p; A autem dimensionis α, B dimensionis β; inveniri poterunt functiones P, Q, dimensionum quae sunt respective $< \beta$, $< \alpha$, ita ut*

$$PA + QB \equiv 1 \pmod{p}$$

Demonstr. Hoc enim casu erit

$$A \equiv aB + C, \quad B \equiv bC + D, \text{ etc.} \quad K \equiv kL + M$$

ita ut dimensiones functionum A, B, C, D, .. K, L, M continuo decrescant et M nullam dimensionem habeat. Iam formentur series

$$\begin{array}{l} a,\ a',\ a'',\ a''',\ \ldots\ a^{(\varkappa)} \\ 1,\ b,\ b',\ b'',\ \ldots\ b^{(\varkappa-1)} \end{array}$$

ita ut

$$\begin{array}{lll} a' \equiv ba + 1 & a'' \equiv ca' + a & a''' \equiv da'' + a' \text{ etc.} \\ b' \equiv cb + 1 & b'' \equiv db' + b & b''' \equiv eb'' + b' \text{ etc.} \end{array}$$

eritque

$$A - aB \equiv +C, \quad bA - a'B \equiv -D, \quad b'A - a''B \equiv +E, \text{ etc.}$$

uti sine negotio perspicitur; hinc tandem

$$b^{(\varkappa-1)}A - a^{(\varkappa)}B \equiv \pm M$$

Iam sit $\frac{1}{\pm M} \equiv \mu$, eritque ponendo $P \equiv \mu b^{(\varkappa-1)}$, $Q \equiv -\mu a^{(\varkappa)}$

$$PA + QB \equiv 1$$

Porro vero manifestum est,

Dimens. ipsius B + Dim. ipsius a esse = Dim. A

$$\text{Dim. } C + \text{Dim. } b = \text{Dim. } B$$

etc.

$$\text{Dim. } L + \text{Dim. } k = \text{Dim. } K.$$

Quare

$$\text{Dim. } L + \text{Sum. Dim. } a, b, \ldots k = \text{Dim. } A$$

Patet vero dimensionem ipsius $a^{(\varkappa)}$ adeoque etiam

$$\text{Dim. ipsius } Q \text{ esse} = \text{Sum. Dim. } a, b, c, \ldots \text{ i. e. } = \alpha - \text{Dim. } L$$

itemque

$$\text{Dim. ipsius } P = \acute{\alpha} - \text{Dim. } L \quad \text{Q. E. D.}$$

336.

Hinc autem sequitur, si M est divisor communis maximae dimensionis functionum A, B, semper poni posse

$$AP + BQ \equiv M$$

Exempla praecedentis theorematis brevitatis gratia omitto, sed lectores non negligent, per ea facilitatem huius generis problemata tractandi sibi comparare. Ceterum operae pretium erit admonere, theorema praecedens etiam de functionibus absolute sumtis valere, quarum quidem coëfficientes sint numeri rationales. Hoc ex demonstrationis modo per se elucebit. Nobis autem ei rei immorari non licet. Similia lector etiam non admonitus in sequentibus observabit.

Si A nec cum B nec cum C divisorem ullius dimensionis communem habeat, etiam cum producto BC nullum habebit divisorem communem. Sit enim

$$PA + QB \equiv 1, \quad \text{erit} \quad PAC + QBC \equiv C$$

Iam si A cum BC divisorem M communem haberet, hic etiam ipsam C divideret contra hyp. Hinc generaliter si functio A ad B, C, D etc. prima, etiam ad omnium productum erit prima.

Si A, B, C, D etc. nullum divisorem habeant omnibus communem, fieri potest

$$PA+QB+RC+SD+\text{etc.} \equiv 1$$

Sit divisor maximae dimensionis inter A et B, M; inter M et C, M'; inter M' et D, M'' etc.: patet, ultimum huius seriei terminum fore nullius dimensionis (hyp.). Quare poni poterit

$$aA+bB \equiv M, \quad mM+cC \equiv M', \quad m'M'+dD \equiv M'', \text{ etc.}$$

unde substitutionibus factis theorematis veritas apparet.

337.

THEOREMA. *Si A, B, C etc. sint functiones inter se primae (quarum binae quaeque nullum habeant divisorem communem) secundum modulum p, et functio M secundum eundem modulum per singulas sit divisibilis; etiam per omnium productum erit divisibilis.*

Demonstr. Poni enim potest $PA+QB \equiv 1$, quare erit

$$\frac{M}{A}Q+\frac{M}{B}P \equiv \frac{M}{AB}$$

Iam quum C ad AB prima, erit etiam M per ABC divisibilis similique ratiocinio per $ABCD$ etc.

338.

Si congruentia $\xi \equiv 0$ habeat radices $x \equiv a$, $x \equiv b$, $x \equiv c$ etc., ξ per productum ex $(x-a)$, $(x-b)$, $(x-c)$ etc. dividi poterit; cum enim a, b, c, etc. supponantur incongrui, functiones $x-a$, $x-b$, $x-c$ etc. erunt primae inter se, et quum ξ per singulas dividatur. etiam per productum ex omnibus dividetur. Hinc patet, radicum multitudinem congruentiae dimensionem superare non posse: quae est demonstratio huius theorematis, quam polliciti sumus.

Sed simul hinc perspicitur, quomodo congruentiarum solutio partem tantummodo constituat multo altioris disquisitionis, scilicet de resolutione functionum in factores. Manifestum est, congruentiam $\xi \equiv 0$ nullas habere radices reales, si ξ nullos factores unius dimensionis habeat; at hinc nihil obstat, quominus ξ in factores duarum, trium pluriumve dimensionum resolvi possit, unde radices quasi *imaginariae* illi attribui possint. Revera, si simili licentia, quam recentiores mathematici usurparunt, uti talesque quantitates imaginarias introducere vo-

luissemus, omnes nostras disquisitiones sequentes incomparabiliter contrahere licuisset; sed nihilominus maluimus omnia ex primis principiis deducere *).

339.

Functiones secundum modulum determinatum *primae* vocantur, quae per nullas functiones inferiorum dimensionum secundum hunc modulum dividi possunt.

Ita omnes functiones unius dimensionis erunt primae, functiones autem duarum dimensionum aut erunt primae aut ex binis unius dimensionis compositae: quare ξ erit functio prima duarum dimensionum, si congruentia $\xi \equiv 0$ nullas radices reales admittit. Ex. gr. $xx+x+1$ pro modulo 5 est prima, quia

$$xx+x+1 \equiv (x-2)^2-3 \pmod 5$$

et 3 non-residuum quadraticum numeri 5.

Hae vero functiones primae prae omnibus attentionem nostram desiderant. Quamvis enim aliae quam primi gradus ad inveniendas radices reales inservire non possint, amplior earum consideratio tum ob insignes ipsarum proprietates tum ob alias egregias veritates ex his deducendas sese commendat.

340.

THEOREMA. *Functio quaecunque aut est prima aut ex functionibus primis composita; posteriorique casu unico tantum modo e functionibus primis componi potest.*

Demonstr. Nisi enim functio proposita A sit prima, per aliam inferioris dimensionis B dividetur. Si B non est functio prima, per aliam C inferioris gradus dividetur, itaque pergendo patet, tandem ad functionem primam deveniri, quoniam alias haec series foret infinita, quod, quoniam dimensiones perpetuo decrescunt, absurdum est. Jam si ultima functio prima sit L, haec omnes antecedentes metietur. Quare $A \equiv LA'$ eritque A' inferioris dimensionis quam A. Quod iterum fiet $A' \equiv L'A''$ etc., patet, tandem ad functionem primam perveniri, adeoque A erit $\equiv$ producto e functionibus primis L, L', L'' etc. Q. E. Pr.

Iam si etiam esset $A \equiv MM'M''$ etc. neque omnes L, L', L'' etc. eaedem cum omnibus M, M', M'' etc., eiiciantur eae, quae utrique seriei communes

*) Alia forsan occasione de hac re opinionem nostram fusius explicabimus.

sunt. Remaneantque $\lambda, \lambda', \lambda'' \ldots$; $\mu, \mu', \mu'', \ldots$ eritque μ ad $\lambda, \lambda', \lambda''$ etc. prima, quare etiam ad productum $\lambda\lambda'\lambda''$ etc.; tamen esse debet

$$\lambda\lambda'\lambda'' \ldots \equiv \mu\mu'\mu \ldots \text{ i. e. } \frac{\lambda\lambda'\lambda'' \ldots}{\mu} \equiv \mu'\mu'' \ldots \text{ Q. E. A.}$$

341.

Primum caput harum investigationum in eo consistet, ut functionum primarum cuiusvis dimensionis multitudinem determinemus. Quoniam enim pro modulo determinato numerus omnium functionum diversarum (incongruarum) cuiuslibet gradus est definitus, ex his vero aliae sunt ex primis inferiorum graduum compositae, aliae primae, etiam harum numerus finitus erit. Rigorosa huius rei evolutio satis est lubrica; a casibus simplicioribus incipiemus.

Posito modulo $= p$, numerus omnium functionum diversarum n^{ti} gradus huius formae

$$x^n + Ax^{n-1} + Bx^{n-2} + Cx^{n-3} + \text{etc.}$$

erit p^n; coëfficientium enim A, B, C etc. numerus est n; et quum quivis independenter a reliquis possit esse $\equiv 0, 1, 2, 3 \ldots (p-1) (\text{mod.} p)$, ex combinationum theoria sequitur, p^n combinationes diversas haberi; quae igitur omnium functionum diversarum huius gradus complexum definiunt.

Ita functiones unius dimensionis erunt p, scilicet x, $x+1$, $x+2$ usque ad $x+p-1$; functiones duarum dimensionum pp etc.

342.

Iam supra monuimus, omnes functiones primi gradus pro primis habendas esse; si igitur, quod ad propositum nostrum sufficit, ad eas functiones nos restringamus, quarum terminus summus habet coëfficientem 1, erunt p functiones primi gradus seu unius dimensionis.

Functiones secundi gradus omnes aut e binis primi gradus erunt compositae aut primae. Jam ex combinationum theoria constat, p res diversas admissis repetitionibus $\frac{p \cdot p+1}{1 \cdot 2}$ modis diversis combinari posse, quare totidem functiones erunt e binis primis unius dimensionis compositae, adeoque $pp - \frac{p \cdot p+1}{1 \cdot 2} = \frac{1}{2}(pp-p)$ functiones primae duarum dimensionum.

Simili modo e functionibus omnibus tertii gradus, quarum numerus est p^3, excludendae sunt eae, quae e ternis primis unius dimensionis componuntur, quarum numerus est $\frac{p.p+1.p+2}{1.2.3}$; insuperque eae, quae e functione prima unius aliaque duarum dimensionum componuntur, quarum numerus est $p.\frac{1}{2}(pp-p)$; quibus deletis restabunt $\frac{1}{3}(p^3-p)$; tot igitur sunt primae trium dimensionum. Elucet hoc modo semper continuari posse.

343.

Ut autem hae operationes facilius absolvantur simulque ad evolutionem legis generalis via sternatur, rem generaliter considerabimus. Brevitatis gratia designamus per (1) multitudinem functionum primarum unius dimensionis, per (2) numerum functionum primarum duarum dimensionum, sic porro per (1^2) multitudinem functionum e binis primis unius dimensionis compositarum etc. etc., generaliter per $(1^\alpha 2^\beta 3^\gamma \ldots)$ multitudinem functionum omnium, quae e functionibus primis compositae sunt, scilicet ex α unius, β duarum, γ trium etc. dimensionum, quarum itaque dimensio erit $\alpha+2\beta+3\gamma+$ etc. Tum per praecedentia theoriamque combinationum elucet, fore

$$(1^\alpha 2^\beta 3^\gamma 4^\delta \ldots) = (1^\alpha)(2^\beta)(3^\gamma)(4^\delta)\ldots$$

$$(1^\alpha) = \frac{(1).(1)+1.(1)+2.(1)+3\ldots(1)+\alpha-1}{1.2.3.4\ldots\alpha}$$

seu generaliter

$$(a^\alpha) = \frac{(a).(a)+1.(a)+2.(a)+3\ldots(a)+\alpha-1}{1.2.3.4\ldots\alpha}$$

Denique manifestum est, si omnes modi diversi numerum n e numeris $1, 2, 3, \ldots$ per additionem componendi colligantur, qui designentur per $\alpha.1+\beta.2+\gamma.3+$ etc., summam omnium harum expressionum $(1^\alpha 2^\beta 3^\gamma \ldots)$ aequalem fore multitudini omnium functionum n dimensionum, i. e. $= p^n$. Ita

$$\begin{aligned} p &= (1) \\ pp &= (1^2)+(2) \\ p^3 &= (1^3)+(1.2)+(3) \\ p^4 &= (1^4)+(1^2.2)+(1.3)+(2^2)+(4) \\ &\text{etc.} \end{aligned}$$

Perspicuum est, in expressione p^n praeter quantitates (1), (2), (3) etc. etiam hanc

ingredi (n), unde patet, quomodo omnes quantitates per praecedentes sint determinandae. Ita invenitur

$$\begin{array}{lll} (1) = p & (4) = \frac{1}{4}(p^4 - pp) & (7) = \frac{1}{7}(p^7 - p) \\ (2) = \frac{1}{2}(pp - p) & (5) = \frac{1}{5}(p^5 - p) & (8) = \frac{1}{8}(p^8 - p^4) \\ (3) = \frac{1}{3}(p^3 - p) & (6) = \frac{1}{6}(p^6 - p^3 - pp + p) & \text{etc.} \end{array}$$

344 — 346.

Observatur ex hoc seriei initio, summum terminum expressionis (n) esse $\frac{1}{n}p^n$, ad quem, si n est primus, accedit $-\frac{1}{n}p$; at si n est compositus, lex minus elucet. Si vero attentius rem consideramus, videmus esse

$$\begin{array}{ll} p = (1) & p^5 = 5(5) + (1) \\ pp = 2(2) + (1) & p^6 = 6(6) + 3(3) + 2(2) + (1) \\ p^3 = 3(3) + (1) & p^7 = 7(7) + (1) \\ p^4 = 4(4) + 2(2) + (1) & p^8 = 8(8) + 4(4) + 2(2) + (1) \text{ etc.} \end{array}$$

ubi lex progressionis est manifesta; scilicet si omnes numeri n divisores sint α, $\mathfrak{b}$, γ, δ etc., erit

$$p^n = \alpha(\alpha) + \mathfrak{b}(\mathfrak{b}) + \gamma(\gamma) + \delta(\delta) + \text{ etc.}$$

Huius observationis generalitatem iam demonstrare accingimur.

Ostendimus summam omnium talium expressionum $(1^\alpha)(2^\mathfrak{b})(3^\gamma)\ldots$ si semper $\alpha + 2\mathfrak{b} + 3\gamma + \ldots = n$, exhaurire omnes functiones n dimensionum adeoque esse $= p^n$. Hinc patet, — — —. Si

$$\left(\frac{1}{1-x}\right)^{(1)}\left(\frac{1}{1-xx}\right)^{(2)}\left(\frac{1}{1-x^3}\right)^{(3)}\ldots \text{ evolvatur in seriem } 1 + Ax + Bx^2 \ldots = P,$$

erit

$$A = p, \quad B = p^2, \quad C = p^3 \text{ etc.}$$

$$\frac{x\,dP}{P\,dx} = \frac{(1)x}{1-x} + \frac{2(2)x^2}{1-x^2} + \frac{3(3)x^3}{1-x^3}\ldots$$

— — — —

[hinc substituendo $\frac{px}{1-px}$ pro $\frac{x\,dP}{P\,dx}$ et evolvendo singulas fractiones in series infinitas theorematis veritas sponte elucet.]

347.

Theorema hoc etiam alio modo exprimi potest. Scilicet si numeri n divisores omnes sint n, 1, δ, δ', δ'', δ''' etc., theorema in eo consistit, ut sit

$$p^n = n(n) + (1) + \delta(\delta) + \delta'(\delta') + \text{ etc.}$$

Iam patet, productum ex (n) functionibus primis, quae sunt n dimensionum, habere $n(n)$ dimensiones et sic de reliquis, quare

Productum ex omnibus functionibus primis dimensionis unius, dimensionum n, δ, δ' etc. habebit p^n dimensiones.

Facile nunc est ex hoc theoremate valorem expressionis (n) ipsum deducere; sed brevitatis gratia analysin, quae non est difficilis, supprimimus. Sit itaque $n = a^\alpha b^\beta c^\gamma$ etc., ita ut a, b, c etc. sint numeri primi diversi, eritque

$$n(n) = p^n - \Sigma p^{\frac{n}{a}} + \Sigma p^{\frac{n}{ab}} - \Sigma p^{\frac{n}{abc}} \text{ etc.}$$

ubi $\Sigma p^{\frac{n}{abc\cdots}}$ significat complexum omnium expressionum huic $p^{\frac{n}{abc\cdots}}$ similium, si quantitates $a, b, c \ldots$ quomodocunque inter se permutentur. Ita pro $n = 36$ erit $36(36) = p^{36} - p^{18} - p^{12} + p^6$.

Unam adhuc observationem adiicere liceat. Si n est formae a^α et a primus, erit $n(n) = p^n - p^{\frac{n}{a}}$, quare, quum (n) necessario sit integer, erit quicquid sit p,

$$p^n \equiv p^{\frac{n}{a}} \pmod{n}$$

quare, si p ad a primus erit,

$$p^{n-\frac{n}{a}} \equiv 1 \pmod{n}$$

et pro $\alpha = 1$

$$p^{a-1} \equiv 1 \pmod{a}$$

Memorabile est, haec theoremata tam diversis modis erui posse.

348.

Problema. *Data aequatione*

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \text{ etc.} + M = 0$$

cuius radices sunt $x = a$, $x = b$, $x = c$ etc., invenire aequationem, cuius radices sint $x = a^\tau$, $x = b^\tau$, $x = c^\tau$ etc.

Solutio prima. Quaerantur per theorema notum summae radicum aequationis propositae, earum quadratorum, cuborum etc. usque ad potestatem $m\tau^{\text{tam}}$. Hinc igitur habentur etiam summae radicum aequationis quaesitae nec non quadratorum etc. scilicet Σa^τ, $\Sigma a^{2\tau}$ etc., unde per idem theorema coëfficientes determinari possunt.

Ad praxin quidem haec solutio est facilior; sed ad institutum nostrum nec non ad ostendendum, coëfficientes aequationis quaesitae fore integros, si aequationis propositae coëfficientes fuerint integri, quae sequitur magis est accomodata.

Solutio secunda. Sit θ radix prima aequationis $x^\tau = 1$, fiatque productum ex

$$\begin{aligned}
&x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.}\\
&x^m + A\theta x^{m-1} + B\theta\theta x^{m-2} + \text{etc.}\\
&x^m + A\theta\theta x^{m-1} + B\theta^4 x^{m-2} + \text{etc.}\\
&\quad \text{etc.}\\
&x^m + A\theta^{\tau-1} x^{m-1} + B\theta^{2\tau-2} x^{m-2} + \text{etc.}
\end{aligned}$$

Huius itaque producti radices erunt

$$\begin{aligned}
&a,\ \theta a,\ \theta\theta a \text{ etc.}\\
&b,\ \theta b,\ \theta\theta b \text{ etc.}\\
&c,\ \theta c,\ \theta\theta c \text{ etc.}
\end{aligned}$$

i. e. productum aequale erit huic

$$(x^\tau - a^\tau)(x^\tau - b^\tau)(x^\tau - c^\tau) \ldots$$

adeoque huius formae

$$x^{\tau m} + A'x^{\tau(m-1)} + B'x^{\tau(m-2)} + \text{etc.}$$

Iam si pro x^τ scribatur x, erit

$$x^m + A'x^{m-1} + B'x^{m-2} + \text{etc.} = (x - a^\tau)(x - b^\tau)(x - c^\tau)\ldots$$

adeoque

$$x^m + A'x^{m-1} + B'x^{m-2} + \text{etc.} = 0$$

aequatio quaesita. Quod vero hic A', B' etc. sint non solum rationales sed etiam integri, facile ex theoria aequationis $x^\tau = 1$ deducitur.

Quoniam hac operatione in sequentibus saepe utemur, per (P, ρ^τ) indica-

bimus functionem, qua cifrae aequali posita aequatio proveniens habeat radices, quae sunt potestates τ^{tae} radicum aequationis $P = 0$.

Si $P \equiv Q$ secundum modulum quemcunque, erit etiam $(P, \rho^\tau) \equiv (Q, \rho^\tau)$ secundum eundem modulum.

349.

THEOREMA. *Coëfficiens termini* x^n *in* (P, ρ^τ) *congruus est secundum modulum* τ *coëfficienti termini* $x^{\tau n}$ *in* P^τ, *siquidem* τ *est numerus primus* (quod pro hoc casu est tertia solutio problematis praecedentis).

Demonstr. Ex capite sexto sequitur, producti

$$(x^m + Ax^{m-1} + \text{etc.})(x^m + A\theta x^{m-1} + \text{etc.}) \ldots$$

coëfficientem quemcunque habere hanc formam, postquam pro θ^τ substituta est unitas,

$$E + (1 + \theta + \theta\theta + \text{etc.} + \theta^{\tau-1})F$$

Quodsi iam θ consideretur tamquam radix prima aequationis $x^\tau = 1$, totum productum abibit in E; si vero ponatur $\theta = 1$, totum productum abibit in $P^\tau = E + \tau F$, quare erit coëfficiens termini $x^{n\tau}$ in P^τ congruus secundum modulum τ coëfficienti termini $x^{n\tau}$ in E, i. e. coëfficienti termini x^n in (P, ρ^τ).

350.

THEOREMA. *Si* τ *est numerus primus, erit*

$$(P, \rho^\tau) \equiv P \ (mod. \tau)$$

Demonstr. Sit coëfficiens termini x^n in $(P, \rho^\tau) = N'$, in P vero eiusdem termini coëfficiens $= N$. Tunc posito

$$P = x^m + Ax^{m-1} + \text{etc.} + Nx^n + \text{etc.}$$

erit

$$P^\tau \equiv x^{m\tau} + A^\tau x^{(m-1)\tau} + \text{etc.} + N^\tau x^{n\tau} + \text{etc.} \ (\text{mod.}\, \tau)$$

adeoque (§. praec.) $N' \equiv N^\tau \ (\text{mod.}\, \tau)$; quare, quum $N^\tau \equiv N$, erit $N' \equiv N$. Q.E.D.

Hinc etiam patet, esse $(P, \rho^\alpha) \equiv (P, \rho^{\alpha\tau})$ et $(P, \rho^\tau) \equiv (P, \rho^{\tau\tau})$, unde generaliter

$$(P, \rho^\alpha) \equiv (P, \rho^{\alpha\tau^k}) \ (\text{mod.}\, \tau)$$

351.

THEOREMA. *Datur valor numeri* ν *minor quam* p^m, *ita ut functio* $x^\nu - 1$ *per functionem propositam* P m *dimensionum, cuius pars infima indeterminatam* x *non involvit, secundum modulum* p *dividi possit.*

Dem. Dividatur per P series functionum $1, x, xx \ldots$ usque ad x^{p^m-1}, simulac dimensionem m superant, et quoniam nulla per P sine residuo dividi poterit, omnia residua ad hanc formam redigi poterunt

$$Ax^{m-1} + Bx^{m-2} + \ldots + N$$

ita ut omnes coëfficientes sint positivi et $< p$. Sed patet, quum nunquam omnes possint esse $= 0$, $p^m - 1$ tantummodo functiones dari, quarum alicui singulae aequales esse debent, quare quum usque ad potestatem ipsius x, cuius exponens est $p^m - 1$, p^m residua habeantur, necessario duo ad minimum eadem esse debent. Prodeat igitur idem residuum, si x^a et $x^{a+\nu}$ per P dividantur, ita ut $a + \nu < p^m$. Quare $x^{a+\nu} - x^a$ per P dividi poterit. Hinc quoniam (hyp.) x adeoque etiam x^a functio est ad P prima, etiam $x^\nu - 1$ per P dividi poterit. Q. E. D.

Coroll. Si $x^\nu - 1$ per P dividatur, etiam $x^{k\nu} - 1$ per P dividi poterit, denotante k numerum quemcunque integrum.

352.

THEOREMA. *Manentibus denominationibus ut in §. praec., si* P *fuerit functio prima et* x^ν *infima potestas, quae unitate mulctata per* P *dividi possit, erit* ν *aut* $= p^m - 1$ *aut pars aliquota huius numeri, excepto unico casu, ubi* $P \equiv x$.

Dem. Quoniam P est functio prima m dimensionum, dabuntur $p^m - 1$ functiones diversae pauciorum quam m dimensionum (exclusa scilicet ab omnium numero functione 0), quae omnes ad P erunt primae. Iam quum x^ν supponatur esse infima potestas, quae per P divisa unitatem relinquit, palam est, si omnes inferiores potestates ab $1, x, \ldots$ usque ad $x^{\nu-1}$ per P dividantur, ν residua diversa prodire, quae per A generaliter designentur. Iam si haec exhauriant omnia quae sunt possibilia, theorema erit demonstratum; sin vero quaedam nondum sint in eorum numero, sit quodcunque eorum B; iam perspicuum est, functionem Bx^ν per P divisam residuum B dare et generaliter esse $Bx^{\nu+k} \equiv Bx^k \pmod{P}$; sed omnes functiones ab B usque ad $Bx^{\nu-1}$ diversa inter se et ab residuis A

dabunt residua; si scilicet esset $Bx^\lambda \equiv Bx^{\lambda+\delta} \pmod P$, foret etiam $1 \equiv x^\delta \pmod P$, et $\delta < \nu$ contra hyp.; si vero esset $Bx^\lambda \equiv x^\mu \pmod P$, foret $B \equiv x^{\mu+\nu-\lambda} \pmod P$ adeoque B unum ex residuis A contra hyp. . Quare patet haberi adhuc ν nova residua. Simili modo ulterius progredi licebit (omnino ut supra §. .) apparebitque numerum omnium residuorum possibilium $p^m - 1$ esse aut $= \nu$, aut $= 2\nu$, aut $= 3\nu$, aut generaliter multiplum numeri ν. Q. E. D.

353.

Ex theoremate praec. et Coroll. §. 351 sequitur, quamvis functionem primam n dimensionum metiri functionem $x^{p^n-1} - 1$ secundum modulum p. Omnes itaque functiones unius dimensionis excepta unica, quae est $\equiv x$, metientur $x^{p-1} - 1$, quod est theorema FERMATianum; omnes autem functiones primae secundi gradus i. e. formae $xx + Ax + B$ metientur functionem $x^{pp-1} - 1$ etc. Iam sint numeri n divisores omnes $n, \delta, \delta', \delta''$ etc.. 1, patetque, $p^n - 1$ etiam per $p^\delta - 1$ $p^{\delta'} - 1$, $p^{\delta''} - 1$ etc. $p - 1$ dividi posse, quare functio $x^{p^n-1} - 1$ per *omnes functiones primas dimensionum* $n, \delta, \delta', \delta''$ *etc. usque ad functiones primas unius dimensionis (exclusa functione* x*)* dividi poterit, quare etiam (quum omnes hae functiones sint absolute adeoque etiam inter se primae) per *productum ex omnibus.* Sed idem hoc productum habet $p^n - 1$ dimensiones (§. 347.) (ob deficientiam unius functionis x); quare patet, *hoc productum ipsum ipsi* $x^{p^n-1} - 1$ *(mod.* p*) congruum esse debere.*

354.

THEOREMA. *Si functio* $x^\nu - 1$ *per functionem* P *dividitur, erit*

$$(P, \rho^{k\nu+t}) \equiv (P, \rho^t)$$

denotantibus k, t *numeros quoscunque integros.*

Dem. Sit

$$P = x^m + Ax^{m-1} + Bx^{m-2} + \text{etc.}$$

notum est, si

$$\frac{mx^{m-1} + (m-1)Ax^{m-2} + \text{etc.}}{x^m + Ax^{m-1} + \text{etc.}}$$

in seriem infinitam formae

$$m\frac{1}{x} + \alpha\frac{1}{xx} + \beta\frac{1}{x^3} + \gamma\frac{1}{x^4} + \text{etc.}$$

evolvatur, fore α summam radicum aequationis $P = 0$, $\mathfrak{G}$ summam quadratorum etc. Unde sine labore deducitur, potestatum $\nu+1$, $\nu+2$ etc.[tarum] summam congruam esse summae radicum, quadratorum etc. Hinc vero nisi modulus est aequalis aut inferior numero dimensionum functionis P, sequitur esse

$$(P, \rho^{\nu+1}) \equiv P, \quad (P, \rho^{\nu+2}) \equiv (P, \rho^2), \quad (P, \rho^{\nu+3}) \equiv (P, \rho^3) \text{ etc.}$$

Istum autem casum infra considerabimus.

355.

THEOREMA. *Si in serie*

$$(P, \rho^0), (P, \rho) (P, \rho^2), (P, \rho^3) \text{ etc.}$$

post terminum ν^{tum} *sequentes primis deinceps sunt congrui,* $x^\nu - 1$ *per* P *dividi poterit, siquidem* P *nullum factorem pluries contineat.*

Dem. Posito $\frac{\mathrm{d}P}{\mathrm{d}x} = Q$, erit Q functio ad P prima. Sit

$$\frac{Q}{P} \equiv \frac{A}{x} + \frac{B}{xx} + \frac{C}{x^3} + \text{etc.}$$

tum post terminum $\frac{N}{x^\nu}$ sequetur (hyp.)

$$\frac{A}{x^{\nu+1}} + \frac{B}{x^{\nu+2}} + \frac{C}{x^{\nu+3}} + \text{etc.}$$

Quare erit

$$\frac{Q}{P} \equiv \frac{Ax^{\nu-1} + Bx^{\nu-2} + \text{etc.}}{x^\nu - 1}$$

unde patet, functionem $x^\nu - 1$ per P dividi posse. Q. E. D.

356.

THEOREMA. *Si* P *sit functio ipsius* x *prima* m *dimensionum et* X *functio ipsorum* x, x^p, x^{pp}, $x^{p^3} \ldots x^{p^{m-1}}$, *in quam omnes hae quantitates aequaliter ingrediantur, i.e. quae eadem maneat, quomodocunque eae inter se permutentur, functio* X *per* P *divisa dabit residuum, quod erit numerus.*

Dem. Sit residuum

$$\equiv Ax^{m-1} + Bx^{m-2} + \ldots + N \equiv \xi$$

omnes coëfficientes $A, B, C \ldots$ usque ad N exclusive erunt $\equiv 0$. Hoc ita demonstratur. Quum $X - \xi$ per P dividatur, etiam $X^p - \xi^p$ per P dividi pote-

rit. Sed facile perspicitur, X^p esse id, quod fit X, si pro x ponatur x^p, pro x^p, x^{pp} etc... et pro $x^{p^{m-1}}$, x^{p^m} seu quod idem est x. Hinc patet, esse $X^p \equiv X \pmod{P}$; quare, quum $X^p \equiv \xi^p$ et $X \equiv \xi \pmod{P}$, erit etiam $\xi^p \equiv \xi \pmod{P}$ seu

$$\xi^p - \xi \equiv 0 \pmod{P}$$

At $\xi^p - \xi$ secundum modulum p congruum est producto ex ξ, $\xi+1$, $\xi+2$, .. usque ad $\xi+p-1$, qui factores omnes ad P primi erunt, nisi ξ sit simpliciter numerus. Quare etiam $\xi^p - \xi$ alio modo per P divisibilis non erit. Q. E. D.

Huiusmodi functiones sunt summa omnium, summa quadratorum, cuborum etc., summa productorum e binis, ternis etc. Quis vero sit ille numerus, per § sq. determinabimus.

357.

THEOREMA. *Sit functio prima § praec.*

$$P \equiv x^m - Ax^{m-1} + Bx^{m-2} - Cx^{m-3} + \text{etc.}$$

erit residuum, si summa quantitatum x, x^p *etc.* $x^{p^{m-1}}$ *per* P *dividatur,* $\equiv A$, *si summa productorum e binis,* $\equiv B$, *si summa productorum e ternis,* $\equiv C$ *etc.*

Dem. Sint functiones illae X, Y, Z etc. earumque residua ordine suo numeri A', B', C' etc. Iam facile intelligitur, esse x, x^p, x^{pp} etc. radices aequationis

$$z^m - Xz^{m-1} + Yz^{m-2} - Zz^{m-3} + \text{etc.} = 0$$

Quare erit ponendo $z = x$

$$x^m - Xx^{m-1} + Yx^{m-2} - Zx^{m-3} + \text{etc.} = 0$$

Sed functiones $X - A'$, $Y - B'$, $Z - C'$ etc. per P dividi possunt, quare etiam functio

$$x^m - A'x^{m-1} + B'x^{m-2} - C'x^{m-3} + \text{etc.}$$

Hoc autem aliter fieri nequit, nisi sit $A' \equiv A$, $B' \equiv B$, $C' \equiv C$ etc. Q. E. D.

Ceterum notum est, quaecunque alia functio sit X ipsorum x, x^p etc. [in quam omnes hae quantitates aequaliter ingrediantur,] eam semper ex his deduci posse. Ita erit

$$x^2+x^{2p}+x^{2pp}+\text{etc.} \equiv AA-2B \pmod{P} \text{ etc. etc.}$$

Exempl. Sit $p=5$ et $P\equiv x^2+2x+3$, erit functio $x+x^5$ per P divisa $\equiv -2$, $x^6\equiv 3$ etc. etc.

358. 359.

THEOREMA. *Sit P functio prima et x^ν infima potestas ipsius x, quae per P divisa dat residuum 1; porro sit $P\equiv(P,\rho^n)$, erit n alicui numeri p potestati secundum ν congruus.*

Dem. Supra ostendimus, si P sit

$$=x^m+Ax^{m-1}+Bx^{m-2}+\text{etc.}$$

fore

$$z^m+Az^{m-1}+Bz^{m-2}+\text{etc.}-(z-x)\,(z-x^p)\,..\,(z-x^{p^{m-1}})$$

per P divisibilem. Simili modo sequeretur esse

$$z^m+Az^{m-1}+Bz^{m-2}+\text{etc.}-(z-x^n)\,(z-x^{np})\,..\,(z-x^{np^{m-1}})$$

per P divisibilem. Quoniam autem hi factores inter se sunt primi, necessario singuli singulis secundum P, p congrui esse debent. Quare $z-x^n$ debet esse $\equiv z-x^{p^\varkappa}$ i. e. $p^\varkappa\equiv n \pmod{\nu}$. Q. E. D.*)

De inventione divisorum primorum functionis $x^\nu-1$ secundum modulum primum.

360.

Si ν per modulum p seu per aliquam eius potestatem est divisibilis, sit $\nu=p^k\lambda$, eritque

$$x^\nu-1\equiv(x^\lambda-1)^{p^k} \pmod{p}.$$

Unde manifestum est, eum tantummodo casum considerari oportere, ubi ν per p non dividitur.

*) Si $(P,\rho^a)\equiv(P,\rho^b) \pmod{p}$ erit $a\equiv p^\varkappa b \pmod{\nu}$.

Demonstratio. Sit $z^m+Az^{m-1}+Bz^{m-2}+..=\Pi$ erit $(\Pi,\rho^a)\equiv(\Pi,\rho^b) \pmod{P}$; est autem

$(\Pi,\rho^a)\equiv(z-x^a)\,(z-x^{ap})\,(z-x^{app})\,..\,(z-x^{ap^{m-1}})$, $(\Pi,\rho^b)\equiv(z-x^b)(z-x^{bp})(z-x^{bpp})\,..\,(z-x^{bp^{m-1}})$

unde patet propositio.

Productum ex Π, (Π,ρ^2), (Π,ρ^3) etc. (Π,ρ^ν) est $\equiv(z^\nu-1)^m \pmod{P}$; est enim

$$(z-x)\,(z-x^2)\,(z-x^3)\,\ldots\,(z-x^\nu)\equiv(z-x^p)\,(z-x^{2p})\,(z-x^{3p})\,..\,(z-x^{\nu p})\equiv\text{etc.}\equiv z^\nu-1$$

In serie P, (P,ρ^2), (P,ρ^3) etc. $\ldots$ (P,ρ^ν) omnes divisores primi functionis $x^\nu-1$ occurrunt, et quidem quisque m vicibus. Inde patet, productum ex omnibus esse $\equiv(x^\nu-1)^m$.

Si $p^m \equiv 1 \pmod{\nu}$ et quidem m quam minimus, tum patet $x^{p^m-1}-1$ per $x^\nu - 1$ dividi posse. Quamobrem $x^\nu - 1$ alios divisores habere nequit quam $x^{p^m-1}-1$. At haecce expressio habet divisores primos m dimensionum aliosque, quorum dimensionum numerus est divisor numeri m. Tales igitur etiam $x^\nu - 1$ habebit. Quot autem cuiusvis generis habeat, per exemplum declaramus, unde facile lex generalis deduci poterit.

Sit $\nu = 63$ et $p = 13$, erit $m = 6$. Quare $x^{63}-1$ secundum modulum 13 factores primos habebit sex, trium, duarum dimensionum uniusque. Iam palam est, productum ex factoribus unius dimensionis fore divisorem communem (maximae dimensionis) functionum $x^{63}-1$ et $x^{12}-1$ i. e. x^3-1; quare tres erunt factores primi unius dimensionis. Productum ex omnibus factoribus primis duarum dimensionum uniusque erit divisor communis functionum $x^{63}-1$ et $x^{168}-1$ i. e. $x^{21}-1$; quare erunt $\frac{21-3}{2}$ sive 9 factores duarum dimensionum. Productum ex factoribus primis trium dimensionum uniusque erit divisor communis functionum $x^{63}-1$ et $x^{2196}-1$ i. e. x^9-1; quare erunt $\frac{9-3}{3}$ i. e. 2 divisores trium dimensionum. Tandem reliqui erunt sex dimensionum, quorum igitur numerus $= \frac{63-6-18-3}{6}$ i. e. 6.

Facile per attentam huius rei ponderationem sequens regula generalis deducitur:

Sit δ divisor ipsius m, sint omnes numeri δ divisores ipso δ minores $\delta', \delta'', \delta'''$ etc. Sint divisores communes maximi ipsius ν cum $p^\delta - 1$, $p^{\delta'}-1$, $p^{\delta''}-1$ etc. respective μ, μ', μ'' etc., sit $\frac{\mu}{\mu'}, \frac{\mu}{\mu''}, \frac{\mu}{\mu'''}$ etc. $= \lambda', \lambda'', \lambda'''$ etc. habebitque $x^\nu - 1$ $\frac{1}{\delta}$ ties tot divisores primos δ dimensionum, quot infra numerum μ sunt numeri per nullum numerorum $\lambda', \lambda'', \lambda'''$ etc. divisibiles.

361.

THEOREMA. *Si functio X indeterminatae x per aliam ξ dividi possit et X si pro x scribatur x^k, transeat in X', X' per $(\xi, \rho^{\frac{1}{k}})$ dividi poterit.*

Dem. Sit $X \equiv \xi\upsilon$ transeantque ξ, υ in ξ', υ', si pro x scribatur x^k. Patet, fore $X' \equiv \xi'\upsilon'$. At ξ' per $(\xi, \rho^{\frac{1}{k}})$ dividi potest. Quare etiam X'. Q.E.D.

362.

His principiis positis facili negotio divisores primos functionis $x^\nu - 1$ determinare possumus. Supponimus, omnes eos divisores, qui etiam functionem ali-

quam $x^{\nu'}-1$ dividunt, existente $\nu'<\nu$, iam inventos esse, reliquosque investigare proponi. Hi autem omnes in hac expressione comprehendi possunt (P, ρ^k), si P sit unus ex ipsis et pro k omnes numeri minores quam ν ad ipsumque primi substituantur.

In Cap. VI ostendimus, quomodo radices primae aequationis $x^\nu = 1$ ita in classes discerpi possint, ut, omnibus per alicuius potestates expressis, eadem in classes distributio habeatur, quaecunque radix prima pro hac basi accipiatur; *periodos* huiusmodi radicum complexus vocavimus. Iam patet, functiones x, x^α, x^β, x^γ etc., designantibus α, β, γ etc. omnes numeros ad ν primos, simili modo in periodos resolvi posse, quamque periodum maiorem rursus in minores donec tandem ad periodos formae x^k, x^{kp}, x^{kpp} . . . $x^{kp^{m-1}}$ perveniatur. Hoc ita facto patet

1° Quoniam periodus quaeque ex huiusmodi periodis minimis $x^k+x^{kp}+$ etc. composita est, si per quamcunque functionem primam m dimensionum dividatur, residuum fore numerum.

2°. Quum omnes periodi termini semper ad hanc formam reduci queant $x^{\varkappa . a^\alpha b^\beta c^\gamma \cdots}$, ubi $\varkappa, a, b, c$ . . sunt numeri determinati, pro α, β, γ . . autem omnes valores substitui possunt; patet, periodum in se ipsam mutari, si pro x substituatur x^k et k sit formae $a^\alpha b^\beta c^\gamma$ . . (mod. ν), unde facile perspicitur omnes functiones $P, (P, \rho^k)$ etc., designante k huiusmodi numerum, si periodus per eas dividatur, idem residuum dare.

3°. Quare periodus subducto tali residuo per productum ex omnibus functionibus (P, ρ^k) dividi poterit.

363.

Summa rei in hoc vertitur, ut haec residua determinentur. Primo quaeratur residuum, quod periodus maxima per productum ex omnibus functionibus primis idoneis dabit. Si hoc productum sit

$$\equiv x^\lambda - Ax^{\lambda-1} + \text{ etc.}$$

erit residuum hoc $\equiv A$. Huius autem producti forma facile invenitur et ex Cap. VI sequitur esse $A = 0$, si ν per quadratum dividi possit, contra esse A aut $= +1$ aut $= -1$, prout multitudo factorum primorum numeri ν sit par aut impar.

Iam resolvatur haec periodus maxima in periodos inferiores repraesententurque periodi cuiusvis termini per $x^{kp^\pi u}$, ita ut k in quavis periodo sit numerus

determinatus, pro diversis vero variabilis, π et u autem in quavis periodo variabiles, eos autem valores, quos in aliqua periodo habent, etiam in reliquis adipisci possint. Supponatur aliquantisper aliqua functio prima P pro basi sitque residuum, quod periodi $\Sigma x^{p^\pi u}$, $\Sigma x^{k'p^\pi u}$ etc. per eam divisae praebent respective A, A' etc., erit $\Sigma x^{p^\pi u} - A$ per productum ex omnibus functionibus (P, ρ^u) divisibilis, $\Sigma x^{k'p^\pi u} - A'$ per productum ex omnibus functionibus $(P, \rho^{k'u})$ etc. etc. At facile liquet, quantitates A, A' etc. esse radices congruentiae datae. Scilicet sint periodi radicum aequationis $x^\nu = 1$ periodis praecedentibus correspondentes radices aequationis $Q = 0$, erunt A, A' etc. radices congruentiae $Q \equiv 0$. Namque erit

$$A + A' + \text{etc.} \equiv \text{summae periodorum},$$
$$AA + A'A' + \text{etc.} \equiv \text{summae quadratorum periodorum}$$

etc. etc. Calculus enim prorsus similis erit ei, quem Cap. VI exposuimus, si pro ρ substituatur x, quoniam etiam hic poni potest pro x^ν unitas, uti illic pro ρ^ν.

Inventis radicibus A, A' etc. aliqua pro residuo periodi $\Sigma x^{p^\pi u}$ eligatur et inde reliquarum residua simili modo uti Cap. VI ordinentur. Namque illud etiam hic arbitrio relinquitur, quum functio P sit prorsus hactenus indeterminata. Calculus sequens omnino analogus est ei, quem Cap. VI pertractavimus, singula exponere nimis prolixum nobis foret. Tandem postquam ad Σx^{p^π} perventum est, rei summa perfecta est. Namque posito

$$P \equiv x^m + a x^{m-1} + b x^{m-2} + \text{etc.}$$

erit $-a \equiv \Sigma x^{p^\pi}$, eodem modo coëfficiens secundus reliquarum functionum (P, ρ^k) habebitur, unde reliqui ipsius P determinari possunt. Saepius evenire potest, ut ad congruentias identicas perveniatur, ex quibus nihil derivari posse videtur. Quomodo huic difficultati obveniri possit, infra monstrabitur.

364.

Omnia haec per exemplum multo clariora fient. Resolvenda proponitur functio $x^{15} - 1$ secundum modulum 17 in factores. Erit $m = 4$ et quoniam productum ex omnibus functionibus elementaribus

$$\equiv \frac{x^{15}-1 \,.\, x-1}{x^3-1 \,.\, x^5-1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

Quare duo tantummodo erunt factores primi quatuor dimensionum P et P'. Iam x, xx, x^4, x^7, x^8, x^{11}, x^{13}, x^{14} in has duas periodos distribuantur

$$\Sigma x^{17^\alpha} \equiv x + xx + x^4 + x^8, \quad \Sigma x^{7\cdot 17^\alpha} \equiv x^7 + x^{11} + x^{13} + x^{14}$$

Sit secundum alteram functionem P, P'

$$\Sigma\, x^{17^\alpha} \equiv A, \quad \Sigma x^{7\cdot 17^\alpha} \equiv A'.$$

eritque

$$A + A' \equiv 1$$
$$AA \equiv \Sigma x^{2\cdot 17^\alpha} + \Sigma x^{3\cdot 17^\alpha} + \Sigma x^{5\cdot 17^\alpha} + \Sigma x^{9\cdot 17^\alpha}$$
$$A'A' \equiv \Sigma x^{14\cdot 17^\alpha} + \Sigma x^{6\cdot 17^\alpha} + \Sigma x^{5\cdot 17^\alpha} + \Sigma x^{3\cdot 17^\alpha}$$

quare

$$AA + A'A' \equiv \Sigma x^{17^\alpha} + \Sigma x^{7\cdot 17^\alpha} + 4\Sigma x^{3\cdot 17^\alpha} + 2\Sigma x^{5\cdot 17^\alpha} \equiv 1 - 4 - 4 \equiv -7$$

Hinc A et A' erunt radices congruentiae

$$xx - x + 4 \equiv 0 \pmod{17}$$

quae sunt 6, 12. Hinc P dividet

$$x^8 + x^4 + xx + x - 6$$

eritque

$$\equiv x^4 - 6x^3 - 2xx - 12x + 1$$

P' autem erit $\equiv (P, \rho^7)$ eritque

$$\equiv x^4 - 12x^3 - 2xx - 6x + 1$$

365.

Sufficit nobis hic possibilitatem solutionum harum monstravisse. Multa artificia, quibus hae operationes sublevari possunt, praeterimus brevitatis gratia. At consequentias quasdam pergraves praetermittere non possumus.

Per praecedentia demonstratum est, omnes aequationes auxiliares pro solutione aequationis $x^\nu = 1$, si in congruentias convertantur, habere radices possibiles, quando periodus

$$x+x^p+x^{pp}+\ldots+x^{p^{m-1}}$$

nondum est disiuncta. Subsistamus in casu, ubi ν est numerus primus; erit m divisor ipsius $\nu-1$. Hic itaque congruentiae auxiliares, si numerus periodorum, quae per illas inveniuntur, est pars aliquota numeri $\frac{\nu-1}{m}$, habebunt radices reales. Si itaque $\frac{\nu-1}{m}$ est par i. e. si m est divisor numeri $\frac{\nu-1}{2}$ seu si $p^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}$ seu si p est residuum quadraticum numeri primi ν, aequatio quadratica, per quam radices in duas periodos dividuntur, habebit radices reales secundum modulum p. At in Cap. VI monstravimus hanc aequationem posito $\nu = 4n \pm 1$ semper esse $xx+x\mp n = 0$. Quare habetur insigne

THEOREMA. *Si numerus primus p est residuum quadraticum numeri primi $4n \pm 1$, congruentia*

$$xx+x\mp n \equiv 0 \,(mod.\, p)$$

habebit radices reales, adeoque etiam congruentia

$$4xx+4x\mp 4n \equiv 0 \quad seu \quad (2x+1)^2 \mp \nu \equiv 0$$

i. e. $\pm\nu$ erit residuum quadraticum numeri p.

366.

Haec igitur est tertia theorematis fundamentalis Capitis IV completa demonstratio, eo magis attentione digna, quod principia, e quibus est petita, ab iis quibus ad priores usi sumus, prorsus sunt diversa. At ex eodem hoc fonte, sed via opposita quartam deducamus. Scilicet sit ν numerus primus formae $4n \pm 1$, p alius primus quicunque, sitque $\pm\nu$ residuum quadraticum numeri primi p, demonstrabimus, p fore residuum quadraticum numeri ν.

Sit p^m minima potestas numeri p, quae sit $\equiv 1 \pmod{\nu}$. Divisores elementares functionis $\frac{x^\nu-1}{x-1}$ secundum p habebunt m dimensiones, quare omnium numerus erit $= \frac{\nu-1}{m}$. Iam quoniam $\pm\nu Rp$, congruentia

$$xx+x\mp n \equiv 0 \,(\mathrm{mod.}\, p)$$

erit resolubilis; sint radices A, A'. Distribuantur functiones $x, xx, \ldots x^{\nu-1}$ in binas classes per ξ, ξ' designandas, erit

$$\xi+\xi' \equiv A+A'+(1+x+xx+\ldots+x^{\nu-1})$$
$$\xi\xi' \equiv AA'+\lambda(1+x+xx+\ldots+x^{\nu-1})$$

quare

$$(z-\xi)(z-\xi')-(z-A)(z-A')$$

per quemvis divisorem elementarem functionis $\frac{x^\nu-1}{x-1}$ erit divisibilis. Hinc autem quivis horum divisorum elementarium aut $\xi-A$ et $\xi'-A'$, aut $\xi-A'$ et $\xi'-A$ dividet. Hinc patet (quoniam A non $\equiv A'$), si pro x ponatur x^p, ξ et ξ' non immutari. Si enim ξ in ξ' et vice versa transiret, $\xi-A$ et $\xi-A'$ per eandem functionem primam dividerentur. Q. E. A. Hinc denique sequitur, $\frac{\nu-1}{2}$ per m dividi seu $p^{\frac{\nu-1}{2}}-1$ per ν. Quare p erit residuum quadraticum ipsius ν. Q. E. D.

Facile autem est omnes theorematis fundamentalis casus ex utroque theoremate derivare.

367.

Quamvis ad casum, ubi ν est numerus primus, hic nos restrinxerimus, tamen etiam, si ν sit compositus, theoremata analoga haud magno negotio determinari possunt, quod fusius exponere brevitatis gratia nunc non licet.

Manifestum est, similes observationes etiam de maiori periodorum multitudine formari posse. Ita si $\frac{\nu-1}{m}$ per 3 dividitur i. e. si p est residuum cubicum numeri primi ν, aequatio, per quam radices aequationis $x^\nu = 1$ in tres periodos distribuuntur quamque in Cap. VI a priori determinandam docuimus, solubilis erit secundum modulum p et vice versa. Ita ex. gr. congruentia $x^3+xx-2x-1 \equiv 0$ secundum modulum primum quemcunque, qui est formae $7n\pm 1$, resolvi potest, si vero aliam formam habeat, non poterit.

Non difficile nobis foret hoc Caput multis aliis observationibus locupletare, nisi limites, intra quos restringi oportet, vetarent. Iis qui ulterius progredi amant, haec principia viam saltem addigitare poterunt.

368.

Congruentiam aliquam $X \equiv 0$ radices seu generalius divisores *aequales* habere dicimus, si per functionis alicuius potestatem dividi possit.

Num congruentia proposita divisores aequales habeat, eodem modo diiudicatur, uti in aequationum theoria. Ponamus

$$X \equiv \xi^m P$$

patet fore

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv \xi^{m-1}\left(mP\frac{\mathrm{d}\xi}{\mathrm{d}x} + \xi\frac{\mathrm{d}P}{\mathrm{d}x}\right)$$

quare $\frac{\mathrm{d}X}{\mathrm{d}x}$ per ξ^{m-1} dividetur. Generaliter sit

$$X \equiv A^a B^b C^c \text{ etc.}$$

ubi A, B, C etc. denotant functiones primas diversas, erit

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv X\left(\frac{a\,\mathrm{d}A}{A\,\mathrm{d}x} + \frac{b\,\mathrm{d}B}{B\,\mathrm{d}x} + \frac{c\,\mathrm{d}C}{C\,\mathrm{d}x} + \text{etc.}\right)$$

unde patet, nisi aliquis numerorum a, b, c etc. per modulum dividatur, $\frac{\mathrm{d}X}{\mathrm{d}x}$ per $A^{a-1}B^{b-1}C^{c-1}$ etc. dividi posse, non autem per A^a, B^b, C^c etc. Hinc sequitur

THEOREMA. *Si functionum X et $\frac{\mathrm{d}X}{\mathrm{d}x}$ divisor communis maximae dimensionis sit ξ, omnes factores primos, quos ξ habet, etiam X habebit et quidem quemvis toties $+1$ vice quoties ξ; si igitur X et $\frac{\mathrm{d}X}{\mathrm{d}x}$ sint functiones inter se primae, X nullos factores aequales habebit.*

369.

Exemplum I. Quaeritur an functio

$$x^5 + 3x^4 - 6x^3 + 3x - 4 \ldots (X)$$

secundum modulum 17 divisores aequales habeat. Erit

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv 5x^4 - 5x^3 - xx + 3$$

Hinc invenitur, functiones X et $\frac{\mathrm{d}X}{\mathrm{d}x}$ inter se esse primas, quare X divisores aequales non habet.

Exemplum II. Sit

$$X \equiv x^5 + 6x^4 - 3x^3 - 4xx + 2x - 3 \text{ (mod. 13)}$$

erit

$$\frac{\mathrm{d}X}{\mathrm{d}x} \equiv 5x^4 - 2x^3 + 4xx + 5x + 2$$

maxima vero functionum X, $\frac{\mathrm{d}X}{\mathrm{d}x}$ communis mensura $\equiv 5xx + 7x + 7$ seu mul-

tiplicata per 8: $xx+4x+4$; at quum hic divisor sit $\equiv (x+2)^2$, functio X per $(x+2)^3$ dividi poterit quotiensque (qui est $xx+11$) nullum amplius divisorem duplicem involvit.

370. 371.

Si ex §.§. praecc. functio X ita est exhibita $A^a B^b C^c$ etc., ita ut A, B, C etc. inter se sint primae et numeri a, b, c etc. inaequales, resolutio etiam ulterius extendi potest. Sit itaque X functio, quae nullos amplius divisores aequales involvit. Supra vidimus, $x^p - x$ esse productum ex omnibus functionibus primis unius dimensionis. Sit ξ divisor communis maximae dimensionis functionum X et $x^p - x$, erit ξ productum ex omnibus divisoribus ipsius X unius dimensionis, et $\frac{X}{\xi}$ huiusmodi divisores non amplius habebit. Quodsi autem inveniatur, functiones X et $x^p - x$ esse inter se primas, X nullum divisorem unius dimensionis habebit adeoque congruentia $X \equiv 0$ radices reales non habebit. Porro quoniam $x^{pp} - x$ est productum ex omnibus functionibus primis duarum dimensionum uniusque, divisor communis maximae dimensionis functionum $x^{pp} - x$ et $\frac{X}{\xi}$, ξ' involvet omnes divisores ipsius X, qui sunt duarum dimensionum. Hinc ulterius progrediendo perspicitur, X hoc modo in factores ξ, ξ', ξ'' etc. resolvi, qui continent respective omnes divisores unius, duarum, trium etc. dimensionum.

372.

Si autem productum ex pluribus functionibus primis eiusdem dimensionis datum est, singulae functiones tentando erui debebunt. Magnam analogiam habet hoc problema cum eo, quod numerorum compositorum factores quaerere iubet. Hic vero iam a priori determinatur, an functio proposita in factores adhuc discerpi possit. Quum et hic factorum omnium possibilium multitudo sit finita, simili subsidio ut supra uti possumus. Sed huic rei inhaerere nolumus, nam calculator exercitatus principia probe assecutus, quando opus est, facile artificia particularia reperiet.

Progredimur ad aliud caput, scilicet ad considerationem congruentiarum, si modulus non est numerus primus, uti hactenus semper supposuimus. Praesertim vero hic ille casus attentione dignus est, ubi modulus est numeri primi potestas, tum per se tum quod ad aliqua dubia removenda (§.§. . .) necessarius sit.

373.

PROBLEMA. *Si functio* X *secundum modulum* p *in factores inter se primos* ξ, ξ', ξ'' *etc. sit resoluta,* X *secundum modulum* pp *in similes factores* Ξ, Ξ', Ξ'' *etc. resolvere ita, ut sit*

$$\xi \equiv \Xi, \quad \xi' \equiv \Xi', \quad \xi'' \equiv \Xi'', \text{ etc. } (\text{mod. } p)$$

Sol. Sit $X \equiv \xi\psi (\text{mod. } p)$ seu $X = \xi\psi + p\Sigma$. Ponatur

$$\Xi = \xi + p\varphi, \quad \Psi = \psi + p\omega$$

erit

$$\Xi\Psi = X - p\Sigma + (\varphi\psi + \xi\omega)p + pp\varphi\omega$$

Si igitur $\Xi\Psi$ esse debet $\equiv X (\text{mod. } pp)$, necessario debet esse $\varphi\psi + \xi\omega - \Sigma$ per p divisibilis. At cum ψ et ξ secundum modulum p sint functiones inter se primae, φ et ω ita determinari poterunt, ut haec conditio adimpleatur (§. 336), et quidem insuper ita, ut dimensiones ipsarum φ et ω sint respective unitate minores dimensionibus functionum ξ, ψ. Hinc erit $X \equiv \Xi\Psi (\text{mod. } pp)$. Patet, simili modo Ψ rursus in factores $\Xi'\Omega$ discerpi posse, ita ut alter Ξ' sit $\equiv \xi' (\text{mod. } p)$ et ita porro, unde tandem

$$X \equiv \Xi\,\Xi'\,\Xi'' \text{ etc. } (\text{mod. } pp). \quad \text{Q. E. Fac.}$$

374.

Facile hinc probari potest, functionem X etiam secundum modulos p^3. p^4 etc. in factores resolvi posse. Generaliter sit

$$X \equiv PQ (\text{mod. } p^m) \text{ seu } X = PQ + p^m R$$

et functio P ad ipsam Q prima secundum modulum p; posito

$$P' = P + Ap^m, \quad Q' = Q + Bp^m$$

erit

$$P'Q' = X - p^m R + (AQ + BP)p^m + ABp^{2m}$$

Hinc pro quovis modulo p^ν (ν existente $> m$ et $< 2m+1$) erit

$$P'Q' \equiv X, \quad \text{si} \quad R \equiv AQ + BP (\text{mod. } p^{\nu - m})$$

Ex his perspicitur, si functio X aequales non habeat divisores secundum modulum p, eam secundum modulum p^k similiter in factores discerpi posse, uti secundum modulum p. At si X divisores aequales habeat, res fit multo magis complicata neque adeo ex principiis praecedentibus prorsus exhauriri potest. Quare quum quae huc pertineant cuncta communicare non possimus, unicum casum tantummodo considerabimus, qui plurimum occurrit cuiusque enodatio ad quaedam in praecedentibus dubia solvenda requiritur. Hic est, si factores aequales unius dimensionis tantum respiciantur. Hic proprie etiam ad congruentiarum radices inveniendas adhiberi potest. Generaliter alia occasione hanc rem pertractabimus.

375.

Sit igitur $X \equiv X'(x-a)^m \pmod{p}$ et functio X' ad $x-a$ prima; desiderantur omnes divisores unius dimensionis huic $x-a$ secundum modulum p congrui ipsius X secundum modulos pp, p^3 etc. (Supponimus, functionem X absolute per $x-a$ dividi non posse; alias enim $x-a$ secundum modulum quemcunque functionem X divideret). Si substituatur $z+a$ pro x, habebitur

$$Z \equiv Z'z^m \pmod{p} \quad \text{seu} \quad Z = Z'z^m + pA$$

Iam si Z secundum modulum pp per aliquem divisorem formae $z+\alpha p$ dividi potest, necessario A debet esse formae $zZ''+pB$. Nisi hoc sit, disquisitio iam est finita. Ponamus igitur

$$Z \equiv Z'z^m + pZ''z \pmod{pp} \quad \text{seu} \quad Z = Z'z^m + pZ''z + ppB$$

patetque, Z per z ac quemcunque alium divisorem huic secundum modulum p congruum dividi posse;

Ut attentio fixetur. ponemus $m = 4$, facile perspicietur, quemvis alium casum simili modo tractari posse. Iam si Z secundum modulum p^3 per aliquem divisorem formae $z+\alpha p$ dividi potest, erit

$$0 \equiv -\alpha pp Z'' + ppB \pmod{z+\alpha p, p^3} \quad \text{seu} \quad \alpha Z'' \equiv B \pmod{z, p}$$

Iam tres casus esse possunt

1) si $Z'' \equiv 0 \pmod{z, p}$ et B non $\equiv 0$, tunc patet, nullum ipsius α valorem congruentiae satisfacere adeoque Z secundum modulum p^3 nullum divisorem formae $z+\alpha p$ habere. Quare disquisitio erit finita

2) si nec Z'' nec $B \equiv 0 \,(\text{modd.}\, z, p)$; tunc α unicum valorem habebit, scilicet

$$\alpha \equiv \frac{B}{Z''} \,(\text{modd.}\, z, p).$$

Quare erit unicus divisor $\equiv z + \alpha p \,(\text{mod.}\, pp)$ ipsius Z secundum modulum p^3; eritque

$$Z \equiv V\,(z + \alpha p) + p^3 W$$

Iam ponatur divisor ipsius $Z (\text{mod.}\, p^4)$ $z + \alpha p + \delta pp$ eritque

$$0 \equiv$$

BEMERKUNGEN ZUR ANALYSIS RESIDUORUM.

Die beiden vorstehenden Abhandlungen sind einem umfangreichen Manuscripte entnommen, welches den Titel Analysis Residuorum führt und vermuthlich aus dem Jahre 1797 oder 1798 stammt; durch eine gänzliche Umarbeitung sind aus demselben später die Disquisitiones Arithmeticae entstanden. Der vollständige Titel des Caput sextum lautet:

Solutio congruentiae $x^m - 1 \equiv 0$ et aequationis $x^m - 1 = 0$; cum dilucidationibus super theoria polygonorum regularium.

Der zweite Theil desselben (§§. 253—278) ist seinem wesentlichen Inhalte nach in die siebente Section der Disqq. Arithm. übergegangen.

Ausserdem ist noch zum Theil erhalten das Caput septimum. Variae quarundam investigationum praecedentium applicationes (§§. 279—302). Es zerfällt in folgende Unterabtheilungen:

De fractionum communium transmutationibus (§§. 279—281).

De fractionum communium in decimales conversione (§§. 282—292).

De resolutione aequationis indeterminatae $xx = a + by$ (§§. 293—297).

De resolutione aequationis indeterminatae $axx + byy = c$ (§§. 298—301).

De investigatione divisorum numerorum (§. 302; die folgenden Bogen fehlen).

Dies alles ist fast wörtlich in die sechste Section der Disqq. Arithm. aufgenommen.

Die beiden hier mitgetheilten Abschnitte behandeln die Gegenstände, welche, wie aus der Vorrede und den Artikeln 11, 44, 61, 62, 65, 84 der Disqq. Arithm. hervorgeht, den Inhalt der achten Section dieses Werkes bilden sollten. Es verdient indessen bemerkt zu werden, dass dieser Plan später wieder abgeändert ist; es findet sich nemlich unter den Manuscripten ein Fragment mit der Ueberschrift Sectio octava: Quarundam disquisitionum ad circuli sectionem pertinentium uberior consideratio. Dasselbe be-

ginnt mit Art. 367 und sollte also die Fortsetzung der Disqq. Arithm. bilden; die wenigen noch vorhandenen Artikel sind aber später ihrem Inhalte nach in die Abhandlung Summatio quarumdam serierum singularium übergegangen, und deshalb wird dieses Fragment von der gegenwärtigen Ausgabe ausgeschlossen.

In dem vorstehenden Abdruck der beiden Theile der Analysis Residuorum ist der Text des Originals im Wesentlichen treu beibehalten, obgleich dasselbe in formeller Beziehung nicht druckfertig zu nennen ist; in den folgenden Bemerkungen sind die wichtigsten Abänderungen bezeichnet, und zugleich einige Erläuterungen hinzugefügt.

§. 237. Vergl. Disqq. Arithm. artt. 61, 62.

§. 239. Vergl. Disqq. Arithm. artt. 53, 54, 65.

§. 241. Wenn $n = 2^\nu$ und $\nu \geqq 3$ ist, so existirt zwar keine Zahl ρ von der angegebenen Art, aber die ganze Untersuchung wird hierdurch nicht wesentlich geändert.

§. 251. Vermuthlich sollte die hier bemerkte Schwierigkeit durch die Einführung höherer Potenzen von p als Moduln beseitigt werden. Vergl. §§. 363, 372, 373.

§. 332. Die Voraussetzung, dass der Modulus eine Primzahl ist, wird bis §. 372 incl. beibehalten.

§. 338. Das unvollständige Citat kann auf Disqq. Arithm. art. 44 bezogen werden.

§§. 344—346. Von den beiden im Manuscript vorhandenen Beweisen ist hier der erste, welcher mit den Worten iam demonstrare accingimur eingeleitet wird und sich auf eine nähere Untersuchung der Ausdrücke $(1^\alpha 2^\beta 3^\gamma \ldots)$ gründet, nach der eigenen Vorschrift des Verfassers ganz unterdrückt ('Tota prae cedens demonstratio una cum altera theorematis praec., quam adiicere mens erat, supprimenda erit, quoniam aliam infinities simpliciorem deteximus. Nititur ea huic fundamento'.); in dem obigen Abdruck ist ferner der zweite Beweis dadurch abgekürzt, dass die Entwicklung von $\frac{x\,\mathrm{d}P}{P\,\mathrm{d}x}$ statt derjenigen von $\frac{x\,\mathrm{d}P}{\mathrm{d}x}$ betrachtet wird, wodurch zugleich eine im Original enthaltene Beziehung auf den unterdrückten ersten Beweis umgangen wird.

§. 348. Der Ausdruck radix prima ist hier in derselben Bedeutung zu nehmen, wie der Ausdruck radix propria in der Abhandlung Summatio quarumdam serierum singularium art. 11. — Bei der Behauptung, dass die Coëfficienten $A', B' \ldots$ des entwickelten Productes ganze rationale Zahlen sind, wird auf das sechste Capitel verwiesen, in welchem aber die Theorie der Gleichung $x^\tau - 1 = 0$ nur für den Fall behandelt wird, dass τ eine Primzahl ist; die Form des Beweises in §. 349 führt zunächst auf folgende Ergänzung. Wird das entwickelte Product in die (für alle Wurzeln der Gleichung $\theta^\tau = 1$ geltende) Form

$$S = E + F\theta + \ldots + N\theta^{\tau-1}$$

gebracht, so sind die Coëfficienten $E, F \ldots N$ ganze rationale Functionen von x mit ganzen rationalen Coëfficienten; da ferner das Product ungeändert bleibt, wenn θ durch θ^k ersetzt wird, wo k irgend eine relative Primzahl zu τ bedeutet, so gilt dasselbe von dem Ausdruck S, und hieraus ergibt sich ohne Schwierigkeit, dass alle diejenigen in S enthaltenen Potenzen von θ, deren Exponenten s einen und denselben grössten gemeinschaftlichen Divisor mit τ haben, auch identische Coëfficienten haben müssen; da endlich eine jede Summe solcher Potenzen θ^s immer eine ganze Zahl ist, so leuchtet ein, dass der Ausdruck S, und folglich auch das in Rede stehende Product eine ganze Function von x mit ganzen Coëfficienten ist, was zu zeigen war. Ebenso geht aus dieser Betrachtung zugleich die Richtigkeit der Bemerkung am Schlusse des Paragraphen hervor. Andere Grunde lassen indessen vermuthen, dass dem Verfasser schon damals das allgemeine Theorem über die Transformation der symmetrischen Functionen (Demonstratio nova altera theorematis omnem functionem etc. art. 4) bekannt war, aus welchem sich die obigen Sätze als unmittelbare Folgerungen ergeben.

§. 352. Das Zeichen $R \equiv S (\mathrm{mod.}\ P)$ oder auch $R \equiv S (\mathrm{mod.}\ P, p)$ bedeutet hier und im Folgen-

den, dass die Differenz $R-S$ nach dem Modul p den Divisor P hat. — Das unvollständige Citat kann auf Disqq. Arithm. art. 49 bezogen werden.

§. 354. Durch Multiplication mit $x^\nu-1$ ergibt sich, dass die Summen gleich hoher Potenzen der Wurzeln der beiden Gleichungen $(P, \rho^{k\nu+t}) = 0, (P, \rho^t) = 0$ einander congruent sind (mod. p), und hieraus folgt die Congruenz $(P, \rho^{k\nu+t}) \equiv (P, \rho^t) (\mathrm{mod}.p)$, sobald $m < p$ ist (vergl. §. 244); ist aber $m \geq p$, so lässt sich der Coëfficient der Potenz x^{m-p} in einer Gleichung nicht mehr aus den gegebenen Potenzsummen ihrer Wurzeln nach dem Modul p bestimmen, weil er in den hierzu dienenden Newton'schen Formeln mit dem Factor p behaftet ist. In der That darf man aus der Congruenz je zweier gleich hoher Potenzsummen der Wurzeln der Gleichungen $A = 0$, $B = 0$ allgemein nur folgern, dass $A \equiv \mathfrak{A}^p \mathfrak{C}$, $B \equiv \mathfrak{B}^p \mathfrak{C} (\mathrm{mod}.p)$ ist, wo $\mathfrak{C}$ den grössten gemeinschaftlichen Divisor der beiden Functionen A, B nach dem Primzahl-Modulus p bezeichnet, $\mathfrak{A}$ und $\mathfrak{B}$ aber ganz unbestimmte Functionen sind. Es ist zu vermuthen, dass der Verfasser die Allgemeingültigkeit des Satzes aus der Theorie der Transformation der symmetrischen Functionen und speciell aus dem folgenden Satze abgeleitet hat: Ist in Bezug auf einen beliebigen Modulus p die Differenz $R(x)-S(x)$ theilbar durch die Function $P(x)$, und sind $a, b, c \ldots$ die Wurzeln der Gleichung $P(x) = 0$, so sind die Functionen

$$(x-R(a))(x-R(b))(x-R(c))\ldots \quad \text{und} \quad (x-S(a))(x-S(b))(x-S(c))\ldots$$

einander nach dem Modul p congruent.

§. 355. Es wird in §. 368 gezeigt, dass P und $\frac{\mathrm{d}P}{\mathrm{d}x}$ keinen gemeinschaftlichen Divisor haben, wenn P keinen Factor mehr als einmal enthält.

§§. 358, 359. Die unter den Text gesetzte Note ist einem einzelnen Blatt entnommen, welches wahrscheinlich den schon in der Handschrift gestrichenen §. 359 ersetzen sollte.

§. 360. In dem Ausdruck des Theorems ist eine Ungenauigkeit der Handschrift berichtigt.

§. 361. Hier bedeutet der Exponent $\frac{1}{k}$ in dem Zeichen $(\xi, \rho^{\frac{1}{k}})$ jede positive ganze Zahl k' von der Beschaffenheit, dass $kk' \equiv 1 (\mathrm{mod}.\nu)$ wird, wo ν die kleinste positive ganze Zahl ist, für welche $x^\nu-1$ durch ξ nach dem Modul p theilbar wird; hierbei ist vorauszusetzen, dass ξ nicht durch x theilbar nach dem Modul p, und ausserdem, dass k relative Primzahl zu ν ist. Die Richtigkeit der Behauptung, dass ξ' durch $(\xi, \rho^{\frac{1}{k}})$ theilbar ist (mod. p), ergibt sich aus §. 354.

§. 363. Die Schlussbemerkung bezieht sich vermuthlich auf die Einführung von Moduln, welche Potenzen der Primzahl p sind; vergl. §§. 251, 372, 373.

§. 367. Die Wurzeln der Gleichung $x^3+xx-2x-1 = 0$ sind die zweigliedrigen Perioden, in welche die Wurzeln der Gleichung $\frac{x^7-1}{x-1} = 0$ zerfallen. Dasselbe Beispiel findet sich auch auf einem einzelnen Blatt, wo das Hauptresultat der §§. 362, 363 unter dem Titel 'der goldene Lehrsatz' ausgesprochen ist.

§. 371. Dieser Paragraph sollte ein Beispiel enthalten; doch ist dasselbe nicht ausgeführt.

R. Dedekind.