

Werk

Titel: Analysis residuorum. Caput sextum [et septimum]. [237 - 302] (Manuskripttitel), O...

Autor: Gauß, Carl Friedrich

Ort: Ohne Ort

Jahr: 1796

Kollektion: nachlaesse

Gattung: Werk

Signatur: Cod. Ms. Gauß Manusk. 50

Werk Id: DE-611-HS-3373298

PURL: <http://resolver.sub.uni-goettingen.de/purl?PID=DE-611-HS-3373298> | DE-611-HS-3373298

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

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

Caput sextum.

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

237.

In Capite tertio docuimus, congruentiam $x^n \equiv 1$, si
pro modulo accipiatur numerus primus, p , habere μ radi-
ces quando μ est maxima communis mensura numerorum
 n et $p-1$ hasque radices ~~radices~~ ^{hunc cum} cum radicibus $x^n \equiv 1$ penitus
conuenire. Quamobrem ~~tunc tantummodo~~ casum considerare sufficit
conuenit ubi n est pars aliquota numeri $p-1$. Quod autem
non modo congruentiae $x^n - 1 \equiv 0$ sed cuiusvis alius solutio
pro modulis ^{quibuscunque} ~~haberi~~ ~~possit~~ ~~quod est qui sunt numeri primi~~
~~hinc~~ ex solutione pro modulis qui sunt numeri primi possit derivari

iam passim est ostensum infraque (Cap. 8) fusius docebitur.

238.

Sed ne hic quidem subsistere opus est; namque eodem Capite⁸ exposuimus (§) ^{congruentiae} aequationis $x^n \equiv 1$ solutionem a resolutione similium congruentiarum pendere $x^a \equiv 1$, $x^b \equiv 1$, &c ubi a , b &c sunt numeri primi aut numerorum primorum potestates et n productum ex his numeris. Si scilicet A , B &c sunt respectivae radices quaecunque congr. $x^a \equiv 1$; $x^b \equiv 1$ &c productum ex his $AB...$ erit aliqua e radicibus congruentiae $x^n \equiv 1$. Nostrae igitur investigationes ad solutionem congruentiae $x^n \equiv 1 \pmod{p}$ restringentur quando p est numerus primus, n numerus primus aut numeri primi potestas, et simulque passim aliquotia numeri $p-1$.

239.

Porro ex Cap. 3 constat inter congruentiae $x^n \equiv 1$ radices semper aliquas dari per quorum potestates omnes ceterae exhiberi possunt.

Ita si r designet huiusmodi radicem (primitivam supra diximus quando $n = p-1$) omnes congr. propos. radices erunt

$1, r, r^2, r^3, \dots, r^{n-1}$. ~~Idem itaque agenda valde erit ut~~
~~in huiusmodi radices~~ huiusmodi ergo radices omni modo sunt investigandae quoniam his inveniatis ceterae sponte patebunt. Brevitatis gratia quaecunque ipsius r potestatem r^k per exponentem unius inclusum designamus ita ut (0) denotet unitatem, (1) radicem quaecunque

#haecque
expressionum
haec quaecunque
significatione
rationi retine
bimus

primitivam,

congruentiae $x^n \equiv 1$ — ~~quae indolis et per ipsius potestates successivas~~
~~omnes ceterae exhiberi possunt~~; (2) ipsius (1) quadratum &c. (2)
ita ut in hac serie (0); (1); (2); (3) (n-1) omnes radices
amplectatur. Ceterum constat (k) semper fore talem rad. primitivam
quoties k ad n est primus; i.e. nostro casu (ubi n est numeri primi potestas
 $= t^v$) quoties t ipsum k non dividit. Manifesto vero signa (1) (2) &c. per
se sunt indeterminata; ~~sed~~ sed simulac ipsi (1) valor aliquis determinatus
tribuitur omnia cetera determinata fiunt.

240.

Quoniam radices primitivas prae ceteris investigare propositum est
has a ceteris primum separare oportet. Quod fiet si ex serie (0), (1),
(2) ... (n-1) omnes terminos (k) eiiciamus ubi k per t dividitur;
quod si autem n est numerus primus seu $v=1$; unus (0) erit
abrogandus. Priusquam vero ad disquisitionem ~~h.~~ radicum superfluum
abrogandus. Priusquam vero ad disquisitionem ~~h.~~ radicum superfluum
progre- redulo
diamur lectorem ad monemus, exempla aliquot sibi conficere ut omnia
sine his forsan generalius dicta viderentur in concreto intueri possit
Nos aliquod apponimus: sed non ideo superfluum erit ut ipse sibi alia
propriis Marte elaborare.

Est $p = 29$; $n = 7$ et septemae aequae congruentiae $x^7 \equiv 1 \pmod{29}$
radices erunt 1, 7, 16, 20, 23, 24, 25. Quoniam n est num. prim. omnes
hae radices praeter 1 erunt primitivae posito igitur $7 = (1)$ radices
signa haec significabunt:

Ne lector ignarus sit quorsum disquisitiones sequentes tendant theorema quod demonstrandum atque dilucidandum nobis proponimus indicare iuvabit.

~~Resolutio congruentiae $x^n - 1$~~

" Si numerus λ (qui est $= t^{n-1} \cdot t - 1$) habeat factores simplices

" $a, b, c, d, \dots$ (nihil interest quolibetibus quicunque ~~hanc~~ ~~divisum~~

" et sit $\lambda = a^a b^b c^c \dots$ resolutio congruentiae $x^n - 1$ pendet a

" resolutione $\alpha + \beta + \gamma \dots$ congruentiarum inferiorum quorum

" α modus gradus a ; β gradus b , γ gradus c &c."

Ita in nostro exemplo congruentiae $x^7 \equiv 1$ resolutio pendet ~~ab~~^a congruentia secundi et ab alia tertii gradus; perspiciturque in genere nunquam gradum ^{harum} aequationum a modulo p pendere. Ut autem ad huius theorematism demonstrationem perveniamus necesse est aliquas propositiones ad uerum inter congruentias earumque radices praemittere, quamquam proprie in Cap. octavo haec disquisitiones ulterius (sunt persequendae

243

Theorema. Si congruentia $x^m + Ax^{m-1} + Bx^{m-2} \dots + N = 0$ (Mod. primus

habeat m radices $r, r', r'', r''', \dots$ (quod si habet repetitum Cap. [2]) formeturque productum

ita ut comparata ut confecto producto ex m factoribus

$(x-r); (x-r'), (x-r''), (x-r'''), \dots$ quod sit $x^m + ax^{m-1} + bx^{m-2} \dots + n$

sit $A \equiv a, B \equiv b, C \equiv c$ &c secund. Mod. p , quantitates
 $x, x', x'' \dots$ erunt radices congruentiae propositae nullasque alias
 habebit.

Demonstratio I. Erit semper $x^m + Ax^{m-1} + Bx^{m-2} \dots \equiv x^m + ax^{m-1} + bx^{m-2} \dots$

Mod. p . Sed posterioris congruentiae pars sit $= 0$ ponendo
 $x = r, x = r', x = r''$ &c. quare pro his quibus x valoribus
 prior pars fiet $\equiv 0$ (Mod. p) Q. E. Primum.

II si autem ~~prae aliis alijs~~ ^{alijs, adhuc} valori ξ , nulli horum r, r' &c congruus
 congruentiae propositae satisfaceret foret

$$0 \equiv \frac{x^m}{\xi} + A \frac{x^{m-1}}{\xi} + B \frac{x^{m-2}}{\xi} \dots \equiv \xi^{m-1} + a \xi^{m-2} + b \xi^{m-3} \dots \equiv (\xi - r)(\xi - r') \dots$$

sed quoniam nullus factorum $\xi - r, \xi - r', \xi - r'' \dots$ &c est $\equiv 0$
 productum ex omnibus ~~non potest esse~~ fieri $\equiv 0$, ob p primum
 est absurdum (§) Quare praeter radices r, r' &c nullae
 dantur aliae Q. E. Secundum.

248

Problema Sint $r, r', r'' \dots$ quantitates incognitae quorum
 multitudo sit $= m$, quorum summa sit $= \alpha$, summa quadratorum
 $= \beta$, summa cuborum $= \gamma \dots$ summae potestatis cuius exponens est
 $m, = \mu$ danturque non hi numeri (quorum multitudo etiam $= m$)
 ipsi, sed aliae singulis congruae secundum modulum p qui sit numerus
 $\alpha', \beta', \gamma', \delta' \dots$ &c

primus et $> m$, inuenire congruentiam m^{ti} gradus cuius (4) 271
radices sint ~~ipsae~~ quant r, r', r'' &c.

Solutio. Considerentur ~~a', a'', a'''~~ & α', β', γ' &c quasi radices
alicuius aequationis (determinenturque eius coefficients A, B, C

$$x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \dots = 0$$

(adhibendo tantummodo congruentiam loco aequalitatis)

ad methodum cognitam faciendo scilicet

$$-A \equiv +\alpha'$$

$$-2B \equiv \beta' + A\alpha'$$

$$-3C \equiv \gamma' + A\beta' + B\alpha'$$

$$-4D \equiv \delta' + A\gamma' + B\beta' + C\alpha'$$

&c &c

$$-mN \equiv \mu' + A\lambda' + \text{&c.}$$

Haec vero coefficients non possunt esse indeterminatae, quia ~~nulli~~ ^{omnes}
numeri $1, 2, 3, \dots, m < p$.

Dico congruentiam

$$x^m + Ax^{m-1} + Bx^{m-2} + \dots + N \equiv 0$$

esse quaesitam.

Demonstr. Ponatur aequatio cuius radices sunt ~~α, β, γ~~ r, r', r'', r''' &c

$$\text{esse hanc } x^m + ax^{m-1} + bx^{m-2} + \dots = 0 \text{ eritque}$$

$$-a \equiv \alpha$$

$$-2b \equiv \beta + a\alpha$$

$$-3c \equiv \gamma + a\beta + b\alpha$$

$$-4c \equiv \delta + a\gamma + b\beta + c\alpha$$

Cuique autem manifestum ^{hinc} erit fore $a \equiv A, b \equiv B, c \equiv C$ (eti. mod. p.)

quare per δ praec. numeri r, r', r'' &c qui sunt radices
 aequationis $x^m + ax^{m-1} + bx^{m-2} \dots = 0$ erunt ^{simples} eodem ~~tempore~~
 radices congruentiae $x^m + Ax^{m-1} + Bx^{m-2} \dots \equiv 0$. Q. E. D.

Exempla componenda lectoribus linquimus.

246.

Ad propositum nostrum reuertimus. Retentis caracteribus
 §§ 242 et antec. adhibitis ostendere aggredimur si λ ~~habent~~ factum
 sit productum e factoribus quibuscunque efg &c, radices congruen-
 tiae $x^n \equiv 1$ harum primitivas quorum multitudo est λ , ita in e ^{classe} ~~partes~~ discerpi
 posse ut ~~habet~~ aggregata radicum in eadem ⁿ classe reatorum
 per aequationem congruentiam gradus e $\frac{n}{\lambda}$ dentur; his vero tanquam
 cognitis suppositis, quodvis ~~ex~~ classe ita in f ~~partes~~ ordines
 subdividi posse ut aggregata cuiusvis ordinis per congruentiam $f \frac{n}{\lambda}$
 gradus datus, ~~habet~~ ^{habet} ordines itersus subdividi possunt etc.
 usque dum ad singulos divisores perveniamus.

Defin.

Complexum terminorum omnium in hac tali forma

completum siue simplicitate periodum Mm ~~(e^{α})~~ $(e^{ke+\alpha})$ contentarum periodum dicemus. Designat

vero e diuisorem aliquem numeri λ ; α numerum quemcunque datum
 k omnes numeros integros ab 0 usque ad $\frac{\lambda}{e} - 1$; breuitatis vero gratia
 ita designamus $(e * \alpha)$. Ita in exemplo nostro termini

$(1), (2), (4)$ } periodos $(2 * 0)$ constituent hi vero
 $(3), (6), (5)$ } $(2 * 1)$

$(1), (6)$ } phase $(3 * 0)$
 $(3), (4)$ } ~~phase~~ $(3 * 1)$
 $(2), (5)$ } $(3 * 2)$

quomodocunque

Item, ~~si pro~~ si omnes termini in periodis distribuantur, singulaeque periodi
 alterum in periodos minores et sic porro, dicimus, id ~~non~~ obtineri quod
 in § praec. promissimus. Antequam vero hanc expositionem ipsam
 aggrediamur ostendamus formationi harum periodi, quamquam a duabus
 quantitatibus ^{quodammodo} arbitrariis r, e dependeat, nihil tamen vaji in esso, seu quoma
 docunque hae quantitates eligantur, semper eosdem terminos in eandem periodum
 concurrere (siquidem & quot terminos periodus continere debeat fuerit praec.
 scriptum). Primo quidem facile intelligitur

Criterium, quos terminos A, B in eadem periodo esse inde petitur
 quod uterque in tali forma continetur: $(e^{ke+\alpha})$ siue esse

$A \equiv r e^{ke+\alpha}$; $B \equiv r e^{ke+\alpha} \pmod{p}$. Nunc autem r est radix prima
 tua congruentiae $x^n \equiv 1 \pmod{p}$; e vero radix primitiva congruentiae

$$x^\lambda \equiv 1 \pmod{n} \text{ vid. supra.}$$

Demonstrandum est si loco numerorum r, ℓ alii eligantur
puta' s, σ , ~~et tunc~~ ~~constituitur~~ ~~et tunc~~ ^{is} A ~~et~~ B in similibus formis

~~$$s^{\sigma^{le+b}} \times s^{\sigma^{le+b}}$$~~
$$s^{\sigma^{le+b}} \times s^{\sigma^{le+b}}$$
 comprehendendi.

$$\text{et } m \equiv \sigma^2 \pmod{n}$$

Sit $s^m \equiv r \pmod{p}$; $\sigma^m \equiv \ell \pmod{n}$ quod fieri potest quia
 r, ℓ sunt radic. prim. — erit vero m primus ad n , μ ad λ

(Cap. 3). ~~Est autem~~
~~Jam $A e^{ke+\alpha} = B e^{ke+\alpha}$~~

Per debitas substitutiones obtinebimus

$$A \equiv s^{\sigma^{\mu k e + \mu \alpha + ?}}$$

$$B \equiv s^{\sigma^{\mu k \ell e + \mu \alpha + ?}}$$

Q. E. D.

247

(independenter a numero p)

Theorema. Productum e binis periodis similibus componi potest
per additionem periodorum similitum et numerorum datorum.

(Periodos similes vocamus ~~ex~~ ~~ea~~ quae aequè multos terminos
comprehendant siue ubi numerus e est idem.)

Exempl. sit $n \equiv 7$ productum e periodis

$$1+2+3+4 \quad (1)+(2)+(4)+(8) \quad (1)+(6) \quad \text{et} \quad (2)+(5) \quad \text{erit}$$

$$\left[\text{propter } (a) \times (b) \equiv (a+b) \right] \quad (3)+(6)+(8)+(11) \quad \text{siue } \equiv \quad \text{constat e periodis}$$

$$(3)+(4) \quad \text{et} \quad (1)+(6).$$

Demonstratio Lint periodi datae $(e^{\alpha} \cdot \alpha)$ et $(e^{\beta} \cdot \beta)$ 44/275
 seu aggregata et $\frac{1}{e} = f$ (6)

$$(e^{\alpha}) + (e^{\alpha+e}) + (e^{\alpha+2e}) \dots + (e^{\alpha+(f-1)e}) \dots \dots \dots (p)$$

$$(e^{\beta}) + (e^{\beta+e}) + (e^{\beta+2e}) \dots \dots \dots (e^{\beta+(f-1)e}) \dots \dots \dots (q)$$

Productum PQ ex f^2 terminis constat. Hi vero ita sunt ordinandi:

Formantur f series quarum singulae ex f terminis consistit.

Prima complectatur productum ipsius P in e^{β} ; secunda productum P
 $e^{\beta+e}$ &c. &c. In prima serie primum locum occupet productum
 ex parte (e^{α}) oriundum, secundum productum ex $e^{\alpha+e}$ et sic ceteri
 deinceps; in secunda vero primus locus producto e parte $e^{\alpha+e}$ oriundo
 tribuatur, secundus producto e parte $e^{\alpha+2e}$ &c.; ~~intertia inchoet~~
 a ~~producto e parte~~ $e^{\alpha+2e}$ ultimus denique ^{producto e} parte e^{α} ; ~~tertia inchoet~~
 et a prod. e parte $e^{\alpha+2e}$ et sic porro, ^{post} productum e parte ultima
 sequatur productum e parte prima et secunda &c. &c.

sive partibus ^{successive} consecut $\neq$ periodi P per 1, 2, 3 ... ∞ et periodi
 Q per I, II, III &c. ∞ designatis ita producti PQ partes constituantur

$$1. I + 1. II + 1. III + 1. IV \dots + 1. Z$$

$$2. II + 2. III + 2. IV + \dots + 2. I$$

$$3. III + 3. IV + \dots + 3. I + 3. II$$

$$\text{&c. &c.}$$

omnes ordinis termini erunt $\equiv (0) \text{ i.e. } \equiv 1 \text{ Q.E.D. } (7) 277$

Annot.

Demonstratio haec simul methodum facillimam ostendit productum evolvendi. Aliam ~~adiciamus~~ infra dabimus quae hoc quidem praerogativa caret sed ob simplicitatem non contemnenda videtur.

248.

Periodos omnes ^{minores} quae periodum maiorem constituent periodorum systema nominamus. Ita periodi:

$(ef * \alpha) ; (ef * f + \alpha) ; (ef * 2f + \alpha) \dots (ef * (e-1)f + \alpha)$ e quibus componitur periodus $(f * \alpha)$ hoc nomine designabitur. Rite ordinatum erit si numeri ^{ut hic} $\alpha, f + \alpha, 2f + \alpha$ ^{secundum} ^(cuius diff. est, f) ^{post} ^{signum * positi} ^{seriem arithmeticeam} ^{progreantur}; similia denique erunt systemata, si tam minores quam maiores periodi sint similes.

Theorema si periodi ^{duorum} ~~binorum~~ ^{similium} rite ordinatorum inuicem multiplicentur, prima scilicet in primam; secunda in secundam, tertia in tertiam &c summa omnium productorum e periodi maiori similibus ~~et~~ ^{est} et numeri dati, componi potest.

sint systemata $\begin{cases} (ef * \alpha) & (ef * \alpha + f) & (ef * \alpha + 2f) & \dots \\ (ef * b) & (ef * b + f) & (ef * b + 2f) & \dots \end{cases}$

~~##~~ Propositio paullo aliter exprimi debet ~~quia~~ si generaliter numeri primi potestatem denotat, quando vero est numerus primus nihil immutatur.

Demonstr. Productum e ~~tem~~ singulis periodis systematis prioris in periodos respondentis posterioris constabunt (8 praec) e numeris integ³ et periodis similibus. Sed parvula attentio ^{ad genus hanc} docebit si

$(ef * A) \times (ef * B)$ constat ex numero integro N et periodis $(ef * A); (ef * B); (ef * C)$ _{et}
tum ~~per~~ constare producta

$(ef * a + f) \times (ef * b + f)$ ex N et per. $(ef * A + f); (ef * B + f); (ef * C + f)$ &
 $(ef * a + f) \times (ef * b + f)$ ex N et per. $(ef * A + f); (ef * B + f); (ef * C + f)$ &
et generaliter

$(ef * a + f) \times (ef * b + f)$ ex N et per. $(ef * A + f); (ef * B + f); (ef * C + f)$ &
Unde sponte patet omnium periodorum summam fore

$$1 \text{ e } N + (f * A) + (f * B) + (f * C) \text{ &c. } Q. E. D.$$

Etiā haec demonstratio methodum suppeditat summam illam inveniendi.

249.

Facile est hoc theorema generatius adhuc reddere. Scilicet si habeantur quocunque systemata rite ordinata similia sicutque producta ex omnibus periodis primis, secundis &c., omnium horum productorum summam constare e numeris et periodis maioribus. Si omnia haec systemata aequalia assumantur, ^{summa} potestates ^{sum} quocunque omnium periodorum additae ^{sum} ~~fi~~ constabit e numeris et periodis maiori similibus. Jam hinc patet quorsum haec tendant. Sit $A = efgh \dots$; diverpantur

omnes radices primae in e periodos, quacuis harum iterum in f, harum 8
 Singulae in g &c. &c. Jam omnium periodorum summa datur est scilicet

$\equiv -1$. si ~~est numerus primus~~. Ex B secundum ea quae modo
 diximus datus sumus gradatorum, cuborum ~~omnium~~ ^{et sic porro} omnium potestatum
 periodorum datus etiam $(A)^2 + (A')^2 + (A'')^2 + (A''')^2 + \&c$
 $(A)^3 + (A')^3 + (A'')^3 + (A''')^3 + \&c$
 &c &c

Hinc §. 244 Congruentia gradus $e \frac{L}{i}$ inveniri poterit cuius radices sint
 A, A', A'' &c &c. Jam his tanquam cognitis suppositis, quacuis periodos
 disceperat in minores A in B, B', B''
 A' in B'', B''+1, B''+2 &c &c

Datur ergo $B+B'+B'' \dots \equiv A$
 Sed constat $(B)^2 + (B')^2 + (B'')^2 + \&c \dots$ } ex unitatibus et periodi A, A',
 $(B)^3 + (B')^3 + (B'')^3 + \&c \dots$ } A'' &c
 &c

Quare B, B', B'' &c dabantur per congruentiam gradus $f \frac{L}{i}$
 ex qua inveniri possunt similique modo periodi ex quibus constat A', A''
 poterant determinari. Quisquis autem hinc videbit, & propterea simili
 methodo quacuis periodum in minores subdividi posse donec ad radices ipsas
 perveniat.

Et in harum regularum applicatione difficultas occurrit quam dimovere debemus. Quoniam scilicet quacumque congruentia plures radices habeat, ~~quod~~ quod cuique signum tribuendum sit ut ab invicem rite distinguantur est videndum.

~~Ostendimus. Prae cunctis praedictis est ut radices quamprimum sunt~~
custodito ~~rite adinveniantur~~. Quoniam periodorum designatio a numeri
 r, s pendet qui ad libitum assumi possunt facile per necessarium
etiam designationi aliquid arbitrarii inhaerere debet.

Numerus quidem s iam ab initio est stabiliscendus ~~sed numeri~~ x

Methodi nostri indices in eo ^{potissimum} consistit ut ex periodis maioribus periodos menores
deducamus. Sed hoc sine debita periodorum ordine quem per signa assignati
sumus fieri nequit. Quare ~~et~~ eo nitendum est ut omnes periodi quamprimum
sint invicem signis suis distinguantur. ~~Atque~~

Sit ^{per $(e * x)$} periodus A designatus atque in s periodos B, C, D etc. dissectus quos
designare oportet. Patet quoniam in tali forma fore contentam $(e * (k + \alpha))$
Sed hoc pro aliquo eorum B numerum k ad libitum assumi posse et inde
alterarum collationem derivari posse.

Sit R radix aliqua prima ~~ad~~ congr. $x^n \equiv 1$ constetque B terminis $R'' + R' + R$

Sit $\frac{s^{k+\alpha}}{u} \equiv v \pmod{n}$ et quoniam valor ipsius s est arbitrarius

(si autem A designatur signum $(e * x)$ quod hoc fieri manifestum est) ponatur

$s \equiv R^v$; quare aliquis terminus ipsius B erit s^k et R per $(e * (k + \alpha))$

designare licet. R loco ipsius R^u terminum R^v considerauimus
 alium ipsius p valorem formae effecimus nacti; sed sine negotio perspicui
 potest u ut et e ; $\frac{1}{e}$ valores diuersos habere posse.

251

9 44af 281.

Analysis Residuorum

Nn

Iam quomodo ex designatione unius periodi ceterae lignis suis distinguantur
 videamus. ~~Hic autem inde peti~~ Ad hanc vero finem aliam methodum
 quaeere oportet reliquas periodos inueniendi; quae namque quatenus reliquae
 ut ipsa A radices alicuius congruentiae sunt nullus in illis ordo certitus.

ponamus ipsum A ita esse designatum $(ef * 0)$; tum patet ~~tu~~ ex proec. signis
 fore

$$A^2 \text{ formae } M + N(ef * 0) + O(ef * 1) + P(ef * 2) + \dots$$

$$A^3 \text{ formae } M' + N'(ef * 0) + O'(ef * 1) +$$

bc

$$A^{ef-1} \text{ formae } M^* + N^*(ef * 0) + O^*(ef * 1) \dots$$

Hic accedit congruentia $(ef * 0) + (ef * 1) \dots (ef * (ef - 1)) \equiv -1$
 habentur itaque $ef - 1$ congruentiae lineares totidemque quantitates incognitae
 quae igitur per eliminationem determinari possunt.

Ans. Casus occurrere potest, quo quantitates incognitae per huiusmodi expressiones
 datur $\frac{v}{m_p}$; quomodo vero hic difficultati remedium offerri possit infra docuimus.

~~quem contra methodum~~. Hic quoniam hic casus peraro occurrere potest
 ei immorari nolimus.

Hæc in genere de solutione congruentiarum purarum sufficiant. Passim infra multa adhuc de ipsis dicentur; præsertim quæ multe ex solutione æquationum purarum huc trahi possunt: quæ loco suo annectere non augebimus. Exemplum adhuc apponimus quod cum irracionalis collato omnino minus peritis clariora fient.

Sit $n = 31$ $p = 311$. Sive investigandæ sunt radices congruentiæ

$$x^{31} - 1 \equiv 0 \pmod{311}$$

Statim radix prima congruentiæ $x^{30} - 1 \equiv 0 \pmod{31}$ est quærendæ qualis est $x \equiv 3$. Ponamus itaque $\xi \equiv 3$, habebimusque et omnes congruentiæ præpositæ radices primas primum in 5 periodas discrepamus

$$\begin{array}{l} \text{scilicet } (5*0) \dots\dots (1) + (26) + (25) + (30) + (5) + (6) \\ (5*1) \dots\dots (3) + (16) + (13) + (28) + (15) + (18) \\ (5*2) \dots\dots (9) + (17) + (8) + (22) + (14) + (23) \\ (5*3) \dots\dots (27) + (20) + (24) + (4) + (11) + (7) \\ (5*4) \dots\dots (19) + (29) + (10) + (12) + (2) + (21) \end{array}$$

Per ~~æ~~ calculos requisitos inuenietur

$$\begin{array}{ll} \text{Summa periodæ.} & \equiv -1 \\ \text{quadrat.} & \equiv 25 \\ \text{cub.} & \equiv 26 \\ \text{biquadr.} & \equiv 249 \\ \text{pot. quint.} & \equiv 564 \end{array} \quad \begin{array}{l} \text{Quare periodi erunt radices congruentiæ} \\ x^5 + x^4 - 12x^3 - 4x^2 + x + 5 \equiv 0 \end{array}$$

Porro autem inuenitur

$$\begin{array}{l} (5*0)^2 \equiv 6 + 2(5*0) + 2(5*3) + (5*4) \\ (5*0)^3 \equiv 12 + 15(5*0) + 4(5*1) - 13(5*2) + 6(5*3) + 6(5*4) \\ (5*0)^4 \equiv 90 + 60(5*0) + 28(5*1) + 26(5*2) + 49(5*3) + 38(5*4) \end{array}$$

et hinc per eliminationem

Manuscr. 50

(10)

41 of 283

$$S(S*1) \equiv 3(S*0)^4 - (S*0)^3 - 33(S*0)^2 - 24(S*0) + 19$$

$$S(S*2) \equiv -2(S*0)^4 + (S*0)^3 + 22(S*0)^2 + 31(S*0) + 0$$

$$S(S*3) \equiv (S*0)^4 - 2(S*0)^3$$

$$S(S*4) \equiv -2(S*0)^4 + 4(S*0)^3$$

Congruentiarum vero inventae una radix est $\equiv 17$. Quare si ponatur

$$(S*0) \equiv 17 \text{ erit}$$

$$(S*1) \equiv 183$$

$$(S*2) \equiv 263$$

$$(S*3) \equiv 91$$

$$(S*4) \equiv 67$$

Jam periodi inventae iterum discrepantur singulae in ternas;
scilicet

$$(S*0) \text{ in } (15*0); (15*5); (15*10) \text{ nunc in } (11+30); (26)+(5); (25)+(6).$$

$$(S*1) \text{ in } (15*1); (15*6); (15*11) \text{ nunc in } (3)+(28); (16)+(15); (13)+(18).$$

Ponatur &c &c.

~~Inveniturque simili modo~~ periodos in quas discrepant est

$$\left. \begin{array}{l} (S*0) \\ (S*1) \\ (S*2) \end{array} \right\} \text{ fore esse radices congruentiarum} \left\{ \begin{array}{l} x^3 + Ax^2 + Bx + C \equiv 0 \\ x^3 + A'x^2 + B'x + C' \equiv 0 \\ x^3 + A''x^2 + B''x + C'' \equiv 0 \end{array} \right.$$

&c.

eritque

$$\begin{array}{l} A \equiv -(S*0) \\ A' \equiv -(S*1) \end{array} \left| \begin{array}{l} B \equiv (S*0) + (S*3) \\ B' \equiv (S*1) + (S*4) \end{array} \right. \left\{ \begin{array}{l} C \equiv -2(S*4) \\ C' \equiv -2(S*0) \end{array} \right.$$

&c

&c

&c

284
Quare

$(15 \times 0); (15 \times 5); (15 \times 10)$
 $(15 \times 1); (15 \times 6); (15 \times 11)$
 $(15 \times 2); (15 \times 7); (15 \times 12)$
 $(15 \times 3); (15 \times 8); (15 \times 13)$
 $(15 \times 4); (15 \times 9); (15 \times 14)$

$a^2 = x^3 - 17x^2 + 108x - 69$
 $a^2 = x^3 - 17x^2 + 108x - 69$
 $a^2 = x^3 - 17x^2 + 108x - 69$

$(4, 1) + 2(4, 9) + 3(4, 13)$
 $(4, 1) + 2(4, 9) + 3(4, 13)$
 $(4, 1) + 2(4, 9) + 3(4, 13)$

Nic autem habetur $(15 \times 0)^3 - 3(15 \times 0)(15 \times 1) = (15 \times 1)^3 - 3(15 \times 1)(15 \times 2)$

Unde si una radicum primae congruentiae, 10, ponatur (15×0) habetur

$(15 \times 0) \equiv 10$
 $(15 \times 1) \equiv 37$
 $(15 \times 2) \equiv$
 $(15 \times 3) \equiv$
 $(15 \times 4) \equiv$
 $(15 \times 5) \equiv$

$(15 \times 6) \equiv$
 $(15 \times 7) \equiv$
 $(15 \times 8) \equiv$
 $(15 \times 9) \equiv$
 $(15 \times 10) \equiv$
 $(15 \times 11) \equiv$

$(15 \times 12) \equiv$
 $(15 \times 13) \equiv$
 $(15 \times 14) \equiv$

Pandem harum singularum periodarum capiantur termini constituentes

eruntque $(1); (30)$ radices congruentiae $x^2 - (15 \times 0)x + 1$
 $(3); (28)$ — — — — — $x^2 - (15 \times 1)x + 1$

Primae congr. radices sunt 126 et 195 quae igitur erunt radices primae congruentiae $x^3 \equiv 1$ et ea his reliquae sine negotio deducuntur

$(7, 1), (7, 9), (7, 13)$
 $(7, 1), (7, 9), (7, 13)$
 $(7, 1), (7, 9), (7, 13)$

$(15 \times 0) \equiv 10$
 $(15 \times 1) \equiv 37$
 $(15 \times 2) \equiv$
 $(15 \times 3) \equiv$
 $(15 \times 4) \equiv$
 $(15 \times 5) \equiv$

$(15 \times 6) \equiv$
 $(15 \times 7) \equiv$
 $(15 \times 8) \equiv$
 $(15 \times 9) \equiv$
 $(15 \times 10) \equiv$
 $(15 \times 11) \equiv$

$(15 \times 12) \equiv$
 $(15 \times 13) \equiv$
 $(15 \times 14) \equiv$

$(15 \times 0) \equiv 10$
 $(15 \times 1) \equiv 37$
 $(15 \times 2) \equiv$
 $(15 \times 3) \equiv$
 $(15 \times 4) \equiv$
 $(15 \times 5) \equiv$

$(15 \times 6) \equiv$
 $(15 \times 7) \equiv$
 $(15 \times 8) \equiv$
 $(15 \times 9) \equiv$
 $(15 \times 10) \equiv$
 $(15 \times 11) \equiv$

$(15 \times 12) \equiv$
 $(15 \times 13) \equiv$
 $(15 \times 14) \equiv$

Ad alteram huius Capituli partem disquisitionem scilicet
aequationum $x^n - 1 = 0$ transgredimur. Quae in priori tenuius
sunt pertractata hic quam accuratius sumus perscrutaturi multa
adiumenta suppedit: sed ideo potissimum congruentiarum consideratione
praemisimus quia facilius hic est in concretis intueri quas nimis
abstractas ab primo aspectu videri possent.

Ex iisdem rationibus ex quibus § 237 congruentias $x^n - 1 \equiv 0$
exclusimus ubi n est nec numerus primus nec numeri primi
potestas, etiam hic tales aequationes omittimus: ceterum si qui nostra
principia prope penetraverunt facile intelligunt hosce casus etiam
simili modo tractari posse ut reliquos. Notis igitur semper erit
 n numerus primus aut numeri primi potestas

254.

Radix prima aequationis $x^n = 1$ erit cuius ~~nulla~~ potestates omnes
usque ad n tam (exclusive) unitati sunt inaequales. Facile quidamque
sit, quavis aequationis $x^n = 1$ radixⁿ, erit radix prima aequationis
cuiusdam $x^v = 0$ ita ut v sit pars aliquota numeri n . Si enim negas
hac numerorum v, n divisorem communem maximum $= m$ qui
igitur deberet esse $< v$, essent igitur $\frac{v}{m}, \frac{n}{m}$ numeri inter se primi
fiat $t \frac{v}{m} + u \frac{n}{m} = 1$ (Cap. 2) sine $tv + un = m$ eritque ob $r^v = 1$ et $r^n = 1$
etiam $r^{tv} = r^{m - un} \neq 1$ et $r^{un} = 1$ quare etiam $r^{tv + un} = r^m = 1$. hyp.

i.e. ~~non~~ non omnes potestates ipsius x intra x^n unitati sunt
inaequales Q. E. A.

Si igitur $x^n = 1$ est numeri primi potestas omnes aequationis $x^n = 1$
radices erunt radices primae siue huius ipsius aequationis
siue aequationis aliae $x^n = 1$ ita ut x sit eiusdem numeri
primae potestas aliqua inferior.

At quoties n est numerus primus omnes aeq: $x^n = 1$ radices praeter
erunt radices primae.

Nunc denotante p numerum primum habebit aequatio

$$x^p = 1 \quad \text{radices primae } p$$

$$x^{p^2} = 1$$

$$x^{p^3} = 1$$

$$\text{etc.}$$

$$x^{p^4} = 1$$

$$p \cdot p - 1$$

$$p^2 \cdot p - 1$$

$$p^{p-1} \cdot p - 1$$

Generaliter autem facile probari
potest aequationem $x^n = 1$ totidem
radices primas habere quot infra
numerum n sunt numeri ad ipsum
primi.

255.

Omnes aequationis $x^n = 1$ radices sunt inaequales et irrationales
si enim aequales habeat hae etiam aequationis $n x^{n-1} = 0$ radices esse
deberent i.e. $= 0$ Q. E. A. Si vero aliqua radix esset rationalis

et posset realis esse $= 1$, si vero imagineria tunc
huius formae $\frac{a}{b} + \frac{c}{d} \sqrt{-1}$ etiam $\frac{a}{b} - \frac{c}{d} \sqrt{-1}$ foret radix
siue $x + \frac{aadd + bbcc}{bbdd}$ erit similis ipsius $x^n = 1$

Quare $\frac{2a}{b}$ et $\frac{aadd + bbcc}{bbdd}$ deberent esse numeri integri
et quidem $\frac{aadd + bbcc}{bbdd} = 1$ (Cap. 2) Nunc $bb > aa$ (namque $Cx^n = 0$)
Quare aut $a = 0$ aut $a = \pm b$ priori casu foret $x = \sqrt{-1}$ quod ob n impar

est absurd. ^{namque} posteriori fit $\frac{3cc}{4} = dd$ quare $\frac{3}{4}$ irrat. P.E.D.
44/287

256.

(12)

radicum congruentiae $x^n \equiv 1$
Quae supra de distributione in periodos sunt exposita eadem etiam hic
locum habent. Omnibus scilicet radicibus primis hoc modo
expressis r^e ubi r radicem aliquam determinatam aequationis
 ζ vero radicem primam congruentiae $(x^n \equiv 1) \bmod n$ significant
periodus erit complexus radicum talium ut valores ipsius n constituent progre-
arithmetica completam. Quorum terminorum numerus ζ sit ζ et $n - \zeta$ et
etiam hic ita exprimat $(e * m)$. Periodorum systema etiam hic vocatur periodus
maior in minores subdivisus. ~~Supplementum~~ foret ea quae huius pro solutione congru-
deduximus hic iterum repetere; quisque per se videt omnia etiam hanc applicari
posse immo omnes congruentiae auxiliares hic tantummodo in auxiliares mutari.
Quare certum est si factores numeri n i.e. $t^{r-1} t - 1$ si $t^r = n$ et t primus
sint $a, b, c, \dots$ ~~et~~ $a^b c^d \dots$ et $a, b, c, \dots$ primi ad solutionem aequationis $x^n = 1$
quis esse solutione a aequationum gradus a , b gradus b , c gradus c . —
Quod si igitur n est numerus primus formae $2^m + 1$ solutio aequationis
 $x^n - 1 = 0$ per ~~radicem~~ aequat. mere quadraticas solui potest adeoque geometricae
constitui poterit ut si $n = 3:5:17:257:65537$ &c. V. infra
Sed ea quae in l. 251 sunt exposita dubio adhuc obscuriora esse possunt. Videlicet
quoniam ibi solidem aequationes quam incognitas habeamus timendum est ne

foran aliqua illarum ~~fiat~~ ~~id~~ ex reliquis sponte sequantur. Hoc autem nunquam fieri posse per sequentia redarguetur.

257.

Supponamus igitur aliquam (aut plures) ex aequationum

$$\begin{aligned} 0 &= 1 + A + B + C + D \dots \\ 0 &= A^2 + M + \alpha A + \beta B + \gamma C + \delta D \dots \\ 0 &= A^3 + M' + \alpha' A + \beta' B + \gamma' C + \delta' D \dots \\ 0 &= A^4 + M'' + \alpha'' A + \beta'' B + \gamma'' C + \delta'' D \dots \\ &\vdots \\ 0 &= A^{ef-1} + M^* + \alpha^* A + \beta^* B + \gamma^* C + \delta^* D \dots \end{aligned}$$

*In videretur fore
Rursus quoniam in
Causa
omissis*

3weile

III

3. 4. 5. 15. 17. 18.

$$\begin{aligned} p &= 1. 7. 8. 11. 12. 18 \\ p' &= 2. 3. 5. 14. 16. 17 \\ p'' &= 4. 6. 9. 10. 13. 15 \\ p''' &= 2p + p' + 2p'' \\ p'''' &= 2p + p' + 3p'' \end{aligned}$$

$$\begin{aligned} p + p' + p'' &= -1 \\ p + p' + p'' + p''' &= -6 \\ p + p'' &= 7 \end{aligned}$$

sed ex theoria aequationum linearium constat si plures formae habeantur

$$\begin{aligned} 0 &= h + ax + by + \dots \\ 0 &= h' + a'x + b'y + \dots \end{aligned} \quad \begin{pmatrix} Z \\ Z' \end{pmatrix}$$

et

quarum aliqua ex reliquis deduci possit, tunc etiam fieri posse

$$mZ + m'Z' + m''Z'' + \dots = 0 \quad \text{seu}$$

$$mh + m'h' + m''h'' + \dots = 0$$

ab arg. i. e. a' b' c' pendentia

determinati: Quare in nostro exemplo haberetur huiusmodi aequatio

$$mA^{ef-1} + m'A^{ef-2} + m''A^{ef-3} + \dots + m^* = 0 \dots (C)$$

ubi m, m', m'' erunt numeri rationales

Ad ~~pro~~ quoniam in aequationibus ex quibus haecce est deducta pro A etiam $B, C, D, \dots$ substituere licet si modo etiam ceterae quantitates rite mutantur, patet aequationi (C) etiam $B, C, D, \dots$ satisfacere debere. quarum quantitatum numerus quum sit ef , aequatio autem gradus $ef-1$ radices inaequales tantummodo habere possit perspicuum

est ~~bon~~ duas, ad minimum, quantitates inter has $A, B, C \dots$ Analysis Residuorum
 aequales esse debere.

Oo

258.

~~Hoc vero fieri non posse ita probamus.~~ Primo ostendemus hinc sequi
 omnes periodos fore rationales hinc huius sectarii absurditatem
 patefaciemus.

I. Supponatur itaque $(e * \alpha) = (e * \beta)$

(2

$$\text{sitque } (e * \alpha) = \cancel{e^x + e^{\lambda}} + \cancel{e^{\mu}} \rho^x + e^{\lambda} + \cancel{e^{\mu}} \rho^x \quad (\lambda + \mu) (x, \lambda) + \theta^{\mu} (x, \lambda g^{\lambda})$$

$$(e * \beta) =$$

$$(e * 0) =$$

$$\rho^{\mu} + \rho^{\nu} + \rho^{\omega}$$

$$+ \theta^{2\mu} (x, \lambda g^{2x})$$

Ita ut $\lambda, \mu, \nu, \dots$ constituent series decrecentes et

$\mu, \nu, \dots \leq n$. Erunt itaque posito $x > \mu$ q. e. p. (ρ^{μ}, λ)

$$\rho^x + \rho^{\lambda} + \rho^{\mu} - \rho^{\mu} - \rho^{\nu} = 0$$

$$[\theta^{\mu}; \lambda]^{\epsilon}$$

$$[\theta^{\mu}, \lambda]$$

$$[\theta^{\mu}; \lambda]$$

Quaeratur maximus divisor communis functionum $\{x^{\mu} + x^{\lambda} + \dots\}$ et $x^{\mu-1} + x^{\lambda-1} + \dots$

quod fit $x^{\omega} + Ax^{\omega-1} + Bx^{\omega-2} \dots$. Si hanc expressionem circa
 aequationem ponamus aequatio ~~et~~ radices aequationis $x^{\omega} = 1$ involuet (excepta
 radice, 1) quae simul aequationi $x^{\mu} + x^{\lambda} \dots = x^{\mu} + x^{\lambda} \dots$ satisficiant

Quare statim videtur radices fore $\rho, \rho^{\nu}, \rho^{\omega}$ et generatiles omnes terminos
 e quibus constat $(e * 0)$. Si autem haec aequationem nondum exhaustiant
 dico ceteros omnes finitos periodos ipsi $e * 0$ similes formare.

Satis sit radix aliqua ρ^1 et periodus cuius haec radix est terminus sit $(e * d)$ patet omnes alios facile est intelligere omnes reliquos periodos terminos radices fore. Scilicet

$$\text{sit } \rho^{1x} + \rho^{1x} \dots \neq \rho^{1u} + \rho^{1u} \dots \quad \text{i.e. } (e * \alpha + d) = (e * (\beta + d))$$

sed $(e * \alpha + d) ; (e * \beta + d)$ non immutantur si pro ρ^1 quavis alius terminus eiusdem periodi substituatur. Patet autem totidem hinc periodos aequaliter distantes (i.e. formae $(e * \alpha + d), (e * \beta + d)$) aequales fore quod periodos formantur a radicibus aequationis $x^w + Ax^{w-1} + Bx^{w-2} \dots = 0$

259.

II. ~~Sed constat ex~~ Deducantur ex ~~potestates~~ ^{coefficientibus} huius aequationis summae potestates quarum exponentes sint $1, x, x^2, x^3 \dots$ (Memores factores eruat per x designari abis ~~potestates~~ congruentiae $x^{n-1} \equiv 1 \pmod{n}$ ~~quae~~ cui periodorum designat et ordo sint ~~superiorum~~) Sintque haec $A, A', A'' \dots$ porro sint ~~radix~~ periodi a radicibus aequationis formatae

$$(e * 0) ; (e * d) ; (e * d') ; (e * d'') \dots \text{ eruntque}$$

$$(e * 0) + (e * d) + (e * d') \dots = A$$

$$(e * 1) + (e * d) + (e * d') \dots = B$$

sint periodia radice. Seq. $x^w + Ax^{w-1} \dots$ formatar

$$(e * 0) ; (e * d) ; (e * d') ; (e * d'') \dots$$

et primo
supponatur primo

ubi supponimus $d, d', d'' \dots$ constituit seriem crescentem, ~~dis~~ numeros

d, d', d'' constituit non potest seriem arithmetica completam (i.e. talem ut nullus
desit terminus et qui ultimum terminum ultimum ultimum integratus e
sit $d' = 2d; d'' = 3d \dots$ Et est ultimus $= e - d$.)

~~Demonstrat foret enim hinc~~ $(e * \alpha) = (e * \beta)$
 ~~$(e * \alpha + d) = (e * \beta + d)$~~

Tunc igitur erit $(e * 0) + (e * d) + (e * 2d) + \dots = -A$ i.e.
Periodus $(e * 0) \#$ erit $= -A$

Ita ut periodus habeatur numero rationali aequalis.

Pateat autem Superest autem ut demonstremus esse non posse $d = 1$

Alias enim foret $(e * \alpha) = (e * \beta)$ et

$$(e * \alpha + k) = (e * \beta + k) \text{ denotante } k \text{ quocumque numero}$$

integrum. Jam $\beta - \alpha$ ad e est primus hinc sequeretur
omnes periodos ex $\frac{n-1}{e}$ terminis constantes aequales esse

Quare omnes aequationes ~~has~~ radices ~~has~~ periodos quorum radices constituant
singulos terminos eadem essent adeoque ~~egales~~ radices sed ex omnibus productum
est $= \frac{x^n - 1}{x - 1}$ quam expressiorem potestatem esse non posse iam supra est ~~est~~

Si vero $\beta - \alpha$ et e factorem comm. 3 habeant
semper erit $(e * u) = (e * u + 3)$ qui quid sit u adeoque

$$(e * u) = \frac{2}{e} (3 * u) \text{ hinc } (e * u) + (e * u + 1) + (e * u + 2) \dots (e * u + 3 - 1)$$

$$= -\frac{3}{e}$$

aequatio $x^w + Ax^{w-1} \dots = 0$ omnes $n-1$ radices inducet q.e.d. quoniam necessarii
sunt $n-1$.

Si vero a, d, d' seriem arithmeticum non compleant ostendemus, semper aliquem periodum rationalem inde deduci posse.

Sit $x^w + A'x^{w-1} + B'x^{w-2} + \dots = 0$ aequatio cuius radices sint potestates ~~et~~ exponentis r^d aeq. radicum aequationis $x^w + Ax^{w-1} + \dots = 0$. Constat quomodo A', B' etc. ex $A, B, \dots$ inveniri possint.

Constituent igitur radices aequationis huius periodos

$(e + d)$; $(e + 2d)$; $(e + d' + d)$ quia periodorum complexus ab hoc $(e + d)$; $(e + d')$; $(e + d'')$... $(e + 0)$ diversus erit. Sint utriusque communes ~~$(e + d)$ et $(e + d')$~~ Quare etiam duo aequationes erunt diversae sit ambarum communis divisor

$x^v + A''x^{v-1} + \dots = 0$ quae citra aequato aequales obtinebunt cuius radices constituent ~~per~~ periodos $(e + d)$ et si qui sunt alii utriusque complexui communes. Patet propterea simili modo semper ulterius procedere donec tandem ad periodum unicam perveniatur quae sit rationalis. Manifestum autem potest tunc omnes reliquas etiam fore racionales.

261.

Sit enim aequatio periodo alicui $(e + k)$ conveniens

$$x^{(n-1)e} + ax^{(n-1)e-1} + \dots = 0$$

Sintque radicum dignitates $1, r, r^2, r^3$ &c. successive

a, a', a'', a''' &c. eritque

$$r^k(e + k) = a; (e + k + 1) = a'; (e + k + 2) = a'' \text{ &c.}$$

Hoc vero denique absurdum esse facile monstrari potest.

~~Sit productum ex~~

Constat periodus $(e \neq 0)$ ex hinc: $e^{\pm}, \sigma, \gamma$ &c
 $(e \neq 1)$ ex e', σ', γ' &c
 &c

~~Sit~~ Evaluaturque productum

$$\begin{aligned} (1-e)(1-\sigma) \dots &= p \\ (1-e')(1-\sigma') \dots &= p' \\ (1-e'')(1-\sigma'') \dots &= p'' \end{aligned}$$

Quibusque

$$\begin{aligned} N + a(e \neq 0) + a'(e \neq 1) + \dots \\ N + a(e \neq 1) + a'(e \neq 2) + \dots \\ N + a(e \neq 2) + a'(e \neq 3) + \dots \\ \vdots \end{aligned} \quad \left. \begin{array}{l} \text{Haec } N, a, a' \text{ sint} \\ \text{numeri integri} \end{array} \right\}$$

Ex omnibus autem productum $p p' p'' \dots$ erit = n namque
 seu $(1-e)(1-e')(1-e'') \dots (1-\sigma)(1-\sigma') \dots$ &c. &c.

namque? $e', \sigma, \sigma' \dots$ &c omnes complex: radices pr. $x^n = 1$ quare
 quia generaliter sit $(x-e)(x-e')/x(x-\sigma)(x-\sigma') \dots = x^{n-1} + x^{n-2} + \dots + 1$
 est substituendo prod: prae. $= 1+1+1 \dots = n$.

II. Porro omnes producta $p, p' \dots$ erunt numeri positivi integri. Integer esse ex
 hypothese nostra leg. positivus tunc: si p est in periodo aliquo $e \neq k$
 etiam $\frac{1}{p}$ ibi erit quare p etiam ita exhiberi potest $(2 - (e + \frac{1}{e})) (2 - (\sigma + \frac{1}{\sigma}))$ &c
 sed $\sigma + \frac{1}{\sigma}$ semper ≤ 2 et realis. Quare p erit prod.
 ex quantt. real: positivis

8082

III Quum igitur $\#^n$ sit numerus primus Omnes $p, p', \dots$ praeter unum erunt
 $= 1$ ille vero $= n$ hinc omnium summa $= n + e - 1$

Quare

$$eN - (a + a' + a'' \dots) = n + e - 1$$

IV. Sed si in p loco p ponatur 1 p transit in 0 ,

$$N + a(e+0) + a'(e+1) \dots \text{vero in}$$

$$N + \frac{n-1}{e} (a + a' + a'' \dots) \text{ quare}$$

$$eN + (n-1)(a + a' + a'' \dots) = 0$$

$$\text{hinc } n(a + a' + a'' \dots) = -(n + e - 1)$$

Sed quoniam $e-1 > 0$ et $< n$ $n+e-1$ per n dividi nequit

Adcoque $(a + a' + a'' \dots)$ numerus integer esse requiritur. Hinc sequitur
 suppositionem nostram esse scilicet periodum aliquam ~~at~~ integram
 seu binas aequales consistere non posse.

Quare in δ . eliminatio semper succedat nullaque amplius intro
 methodus hac esse potest subacta. Ceterum ad congruentias omnia
 haec applicare non posse per se est perspicuum.

262

Post illustrissimorum Geometrarum labores repetitos nulla spes
 superesse videtur Aequationum solutionum generalis possibilitatem esse
 (i.e. reductionem ad aequationes puras. *)

Id tamen maxime est memorabile, aequationes omnes ad quae
 solutio aequationis $x^n = 1$ dicit resolvi. sive ad puras eiusdem gradus reduci
 posse. Sit Periodus maior $(e * a)$ qui ex hisce ^{minoribus} est compositus
 $(e * a) ; (e * a + e) ; (e * a + 2e)$ &c. Demonstravimus hos periodos
 minores esse radices gradus $\frac{n}{e}$ cuius coefficients per periodum $(e * a)$ et
 similes datur. Nunc rem paullo aliter aggrediamur. Sit θ radix prima ^{determinata} aequationis
 $x^{\frac{n}{e}} - 1 = 0$, formeturque expressio

$$\theta (e * a) + \theta (e * a + e) + \theta^2 (e * a + 2e) + \dots + \theta^{t-1} (e * a + (t-1)e)$$

quam brevitatis gratia per $(\theta ; a)$ designamus. Similitergue aliae finitae expressiones
 exhibebuntur. His ita factis habeturs sequens

263

Theorema

Productum e duabus expr. formarum $(\theta^m ; a)$, $(\theta^n ; b)$ ad hanc formam
 reduci potest $A + B(\theta^{m+n} ; 0) + C(\theta^{m+n} ; 1) + D(\theta^{m+n} ; 2) + \text{ec}$
 ita ut $A, B, C, \dots$ designent functiones racionales quantitatis θ .

Demonstratis.

* Nos etiam huic rei multum operae impedimus; et tantum non de impossibilitate sumus certi. Forsam
 quae in hoc genere meditati sumus et quae forsam ad demonstrationem rigorosam tunc impossibili-
 tatis ducere possunt alia occasione publici iuris faciemus.

296 Per se constat

Productum e ~~primis~~ ~~constat~~ huius ~~formae~~ hanc formam habere

$$\begin{aligned} & A(e f * 0) + A'(e f * e) + A''(e f * 2e) \dots + A^*(e f * e f - e) \\ & + B(e f * 1) + B'(e f * e + 1) + B''(e f * 2e + 1) \dots + B^*(e f * e f + 1 - e) \\ & \vdots \\ & + M(e f * e - 1) + M'(e f * 2e - 1) + M''(e f * 3e - 1) \dots + M^*(e f * e f - 1) \\ & + Z \end{aligned}$$

ubi $A, A', B, B' \dots$; $bc. M, M' \dots$; Z designant functiones rationales ipsius

Jam patet si loco ipsius a substituatur $a+e, a+2e, a+3e \dots$

$$(\theta^m; a) \text{ transire in } \frac{1}{\theta^m}(\theta^m; a) ; \frac{1}{\theta^{2m}}(\theta^m; a) ; \frac{1}{\theta^{3m}}(\theta^m; a) \dots$$

similiterque est ~~$(\theta^n; b)$~~ $(\theta^n; b+e) = (\frac{1}{\theta^n}; b)$ &c...

Sed si a, b transeant in $a+e, b+e$ in productum illud transeunt in

$$\begin{aligned} & A(e f * e) + A'(e f * 2e) + \dots \text{ substituendum erit} \\ & + B(e f * e + 1) + B'(e f * e + 2) + \dots \end{aligned}$$

A loco ipsius A' , A' loco ipsius A'' et d. &c. B pro B' , B' et sic semper antecedens pro consequente; Z manet.

Similiterque si a transeat in $a+2e$ &c. b &c. hinc patet fore

$$\begin{aligned} & (\theta^m; a) \cdot (\theta^n; b) + \theta^{m+n}(\theta^m; a+e)(\theta^n; b+e) + \theta^{2m+2n}(\theta^m; a+2e)(\theta^n; b+2e) \dots \text{ donec} \\ & \text{habeantur } \frac{1}{\theta^{m+n}} = \\ & \quad (A + \theta^{m+n} A^* + \dots)(e f * 0) + (A' + \theta^{m+n} A'' + \theta^{2m+2n} A^* + \dots)(e f * e) \dots \\ & \quad (B + \theta^{m+n} B^* + \dots)(e f * 1) + (B' + \theta^{m+n} B'' + \theta^{2m+2n} B^* + \dots)(e f * e + 1) \dots \\ & \quad \vdots \\ & \quad + Z \end{aligned}$$

Sed per prima aequationis est $= f(\theta^m; a)(\theta^n; b)$ secunda vero hanc

$$\begin{aligned}
& \text{circa } (A + \frac{1}{\theta^{m+n}} A' + \frac{1}{\theta^{2m+2n}} A'' \dots) (\theta^{m+n}; 0) \\
& + (B + \frac{1}{\theta^{m+n}} B' + \frac{1}{\theta^{2m+2n}} B'' \dots) (\theta^{m+n}; 1) \\
& + \text{etc} \\
& + f^2
\end{aligned}$$

Sp.

Unde sponte theoremati veritas derivatur.

Annot. Potuissimus quoque (ut supra pluries fecimus) expressiones in suas partes solvendo singulasque multiplicando ostendere esse $A' = \theta^{m+n} A$; $A'' = \theta^{2m+2n} A$; $A''' = \theta^{3m+3n} \dots$ etc. $B' = \theta^{m+n} B$ &c &c sed brevitatis gratia hocce negotio supersemus lectoribusque reliquimus.

264.

Nunc statim sequitur si ~~hinc~~ duae expressiones formarum

$$A + B(\theta^m; 0) + C(\theta^m; 1) + D(\theta^m; 2) + E(\theta^m; 3) + \text{etc}$$

$$A' + B'(\theta^n; 0) + C'(\theta^n; 1) + D'(\theta^n; 2) + E'(\theta^n; 3) + \text{etc}$$

$A, A', B, B' \dots$ Designantibus functiones racionales quibus θ productum fore formae $P + Q(\theta^{m+n}; 0) + R(\theta^{m+n}; 1) \dots$ quippe cuius partes singulae huius sunt formae. Generaliter si per $Q(\theta^m)$ denotetur functio quaecumque expressio huius formae $A + B(\theta^m; 0) + C(\theta^m; 1) + \text{etc}$ et si in similibus erit $Q(\theta^m) \cdot Q(\theta^n) \cdot Q(\theta^p) \dots$ in forma

$$Q(\theta^{m+n+p+\dots}).$$

Nunc patet $(\theta^m; a)^{t-1}$ fore in forma $Q(\theta^m; t)$ i.e. in hac

$$A + B(\theta^m; 0) + C(\theta^m; 1) + \text{etc} \quad \text{At}$$

At generaliter $(\theta^{mn-m}; k)$ significat hoc (propter $\theta^{\frac{1}{n}} = 1$)

$$(e/k) + (e/k+e) + (e/k+e) + \dots \quad \text{i.e.}$$

(e/k) Quare

$(\theta^m; a)^{\frac{1}{n}}$ erit in forma $A + B(e \times 0) + C(e \times 1) + \dots$

i.e. quoniam A, B, C sunt functiones rationales ipsius θ quod tunc
cognitum consideramus, insuperque periodi maiores $(e \times 0)(e \times 1)$ &c. supponunt
esse cognitae, $(\theta^m; a)$ per aequationis purae $f^{\frac{1}{n}}$ gradus solui potest

265.

Sed quoniam haec aequatio pura f radices diversas habet quamnon
pro $(\theta^m; a)$ accipere oportet dubium videri potest. Ex similibus
rationibus ~~pot~~ supra (ex indeterminata electione quantitatis ρ) facile
derivatur semel hanc selectionem arbitrio relinquere si modo m
cum f factorem communem habeat (eo vero casu ubi factor communis
adest, x , $(\theta^m; a)$ per aequationem puram gradus $\frac{f}{x}$ $\frac{1}{n}$ determinatur
neque hic inter $\frac{f}{x}$ radices ulla praerogativam habet) simulat vero
hooce casu aliqua radix signis aliquo est distincta omnes alii non amplius
arbitrarii manent. ^{itaque} hic ~~et~~ supra d. methodum docebimus ex
invento valore expressionis $(\theta^m; a)$ Ex.gr. $(\theta; a)$ ceteros deducendi.

$(\theta^2; a); (\theta^3; a)$ &c.

Determinari oportet $(\theta^k; a)$.

~~Est~~ Evolvatur $(\theta; a)^k; (\theta; a)^{k+f}; (\theta; a)^{k+2f}$ usque ad $(\theta; a)^{k+(e-1)f}$

quae expr. cognitae erant ex $(\theta; a)$. Sunt autem omnes in tali formae

propter $\theta^t = 1$

(18) 44 of 299

$$A + B(\theta^k; 0) + C(\theta^k; 1) + \dots + M(\theta^k; e-1)$$

Habentur itaque e quantitates incognitae $(\theta^k; 0); (\theta^k; 1); (\theta^k; 2)$ &c &c
solidemque aequationes lineares; unde singulae determinari poterant.

266

Haec vero conclusio hallucinaretur si possibile esset ut aliqua aut plures harum
aequationum e reliquis sequantur. Tum autem per simile ratiocinium (ut
supra δ talis aequatio daretur

$$A(\theta * a)^{k+(e-1)t} + B(\theta * a)^{k+(e-2)t} + \dots = 0$$

(ita ut A, B, C esset functiones rati. ipsius θ .) seu dividendo per $(\theta * a)^k$

$$A(\theta * a)^t + B(\theta * a)^{t-1} + \dots = 0$$

$$A\theta^{e-1} + B\theta^{e-2} + C\theta^{e-3} + \dots = 0$$

et quoniam haec aequatio etiam locum habere debeat si pro a substituaturs
0, 1, 2 usque ad e-1 sequitur binas ad minimum expressiones huius formae
 $(\theta; 0); (\theta; 1); (\theta; 2)$ aequales esse. Si vero hoc esset, etiam conclusio
valeret si pro θ , θ^t i.e. 1 substituaturs; nempe omnes conclusiones
hactenus factae valorem singularem ipsius θ non supponunt sed tantum ut sit
radix aequationis $x^t = 1$. Sed $(\theta^t; \alpha)$ est $= (e * \alpha)$ et $(\theta^t; e)$ est $= e * e$.
Quod autem duae tales periodi aequales esse aequant iam supra est
demonstratum.



2.29
32.35
36.4
29

93

26
10

7,8125444
1,9822712
1,7948156
8,2418553
3,5529603

3000

3572 550 3000
549 44 4000
0,4771213
0,755913
0,7185300
0,2418783
0,9604073

Postquam per hanc methodum $(\theta; a); (\theta^2; a); (\theta^3 a) \dots$ sunt determinatae
i.e.

$$(ef * a) + \theta (ef * a + e) + \theta^2 (ef * a + re) + \text{etc.}$$

$$(ef * a) + \theta^2 (ef * a + e) + \theta^4 (ef * a + re) + \text{etc.}$$

$$\text{Et sic ad quod accedit } (\theta^5; a) \text{ seu } (e * a) \text{ i.e.}$$

$$ef * a + (ef * a + e) + (ef * a + re) + \text{etc.}$$

facile per eliminationem singulas inveniuntur. ~~et~~ seu brevius
ad huc omnes addendo erit habebimus

$$f(ef * a) \text{ namque } \theta + \theta^2 + \theta^3 \dots = 0 \text{ et sic ceteri coefficientes.}$$

$$\text{Similiter erit } f(ef * a + e) = \frac{1}{\theta} (\theta; a) + \frac{1}{\theta^2} (\theta^2; a) + \text{etc.}$$

~~Quare~~ Et sic

~~Ad idem~~ ~~igitur~~ ~~periodi~~ ~~minoris~~ ~~ex~~ ~~maioribus~~ ~~per~~ ~~solutionem~~ ~~aeguationis~~
parae 268

Hoc itaque modo per aeguationis purae solutionem ad periodorum
maiorum in minores divisionem pervenimus. Patet ceterum hocce
modo statim a periodo maximo (omnes radices primas comprehendit)
ad radices singulas transiri posse quo casu eliminatio illa s. 266 hanc
parum facilitatur. ^{Quoties} ~~Quoties~~ enim ~~hic~~ $e = 1$, potestas $(\theta; a)^k$ hanc formam
habet $A + B(\theta^k; 0)$. Unde $(\theta^k; 0)$ sponte fluit.

Ceterum hic adhuc annotari debet hanc methodum semper etiam
ad congruentias (mutatis mutandis) applicari posse quod congruentia
 $\theta^k \equiv 1$ habet omnes suas radices reales. Sed eliminatio (266) etiam
hic et supra difficultates parere potest quae octavo demum capite dissolvemus.

Exempla adhuc quaedam adidere non inutile erit, beneque faciet lector si plures adhuc ipse elaboraverit.

I. Quaerendae sint radices aequationis $x^{12} = 1$; quae hic ergo ob $12 = 2 \cdot 2 \cdot 3$ per solutionem unius aequationis tertiae, duarumque secundae gradus locum attingemus. Quaeatur primo radix prima congruentiae $x^{12} \equiv 1$ v. g. $\underline{2}$ utque eruntque radices ita rite ordinati

$$e, e^2, e^4, e^8, e^3, e^6, e^{12}, e^{11}, e^9, e^{10}, e^7.$$

~~Et~~ Distribuantur haec radices in tres periodos

$$e + e^8 + e^{12} + e^5 = A$$

$$e^2 + e^3 + e^4 + e^{10} = B$$

$$e^6 + e^9 + e^7 + e^1 = C$$

$$\text{erit } A + B + C = -1$$

$$AA = 4 + B + 2C$$

$$AB = A + 2B + C$$

$$AC = 2A + B + C$$

$$\text{hinc } A^3 = 9A + 4B + 3C$$

hinc porro

$$A^2 + B^2 + C^2 = 9$$

$$A^3 + B^3 + C^3 = -16$$

Quare A, B, C erunt radices huius aequationis

Jam quatenus periodus in duas subditi datur

$$A \text{ in } e + e^{12} \text{ et } e^8 + e^5$$

Quae sunt radices aequationis $xx - Ax + C = 0$

$$\text{Quae erunt sunt vero } x = \frac{1}{2}A \pm \sqrt{\left(\frac{1}{4}AA - C\right)} = \frac{1}{2}A \pm \sqrt{1 + \frac{1}{4}B - \frac{1}{2}C}$$

$$= 0,1369452775 \pm 1,6339667738$$

$$x^3 + x^2 - 4x + 1 = 0$$

Una harum radicum quam ponamus = A per approximationem invenitur = $+0,273890554964212$

Sed ex

$$A + B + C + 1 = 0$$

$$AA = 4 + B + 2C \text{ sequitur}$$

$$AA + A - 3 = C$$

$$-AA - 2A + 2 = B$$

$$\text{hinc } B = +1,377202853972963$$

$$C = -2,651093408937173$$

Quod si ponatur $\rho + \rho^{12} = 1,770912051306417$
 erit $\rho^8 + \rho^5 = -1,497021496342205$

Hinc quoniam $(\rho + \rho^{12})^2 = \rho^2 + \rho^{10} + 2$

erit $\rho^2 + \rho^{10} = 1,136129493462315$

Et $\rho^3 + \rho^9 = 3 - \rho^2 - \rho^{10} = 0,2410733606510648$

Denique quoniam $(\rho^2 + \rho^{10})^2 = 2 + \rho^4 + \rho^8$ erit

$\rho^4 + \rho^8 = 0,7092097742$ ^{0.85071} et hinc ob $\rho = \rho^4 \rho^9 + \rho^6 + \rho^7$

$\rho^6 + \rho^7 = -1,941883634852102$

Hinc iam ad terminos singulos perveniri potest.

ρ et ρ^{12} sunt radices aequationis

$$x^2 - (\rho + \rho^{12})x + 1 = 0$$

Hinc haec autem sunt $\frac{1}{2}(\rho + \rho^{12}) \pm \sqrt{\left(\frac{1}{4}(\rho + \rho^{12})^2 - 1\right)}$

$$= \frac{1}{2}(\rho + \rho^{12}) \pm \sqrt{\left(\frac{1}{4}\rho^2 + \frac{1}{4}\rho^{10} - \frac{1}{2}\right)}$$

$$= 0,8854560256 \pm 0,4647231721 \sqrt{-1}$$

Hinc porro deducuntur ³¹¹⁵⁸ assumpto ~~signo superius~~ pro ρ inferiori pro ρ^{12}

$\rho^2; \rho^{10} = 0,5680647467 \pm$

$\rho^3; \rho^9 = 0,1205366803 \pm$ ^{2.55324} $0,992708873918568$

$\rho^4; \rho^8 = -0,3546048871 \pm$ ^{0.42535.5} $0,935016242685412$

$\rho^5; \rho^7 = -0,7485107481 \pm$ ⁷¹¹⁰²⁺

$\rho^6; \rho^{11} = -0,9709418174 \pm$ ²⁶⁰⁵¹ $0,239315664287557$

II. Quaerantur radices aequationis

$$x^{17} = 1.$$

Radix prima congruentiae $x^{16} \equiv 1 \pmod{17}$ est 3 secundum quos
radices rite ordinatae erunt ita

$$p, p^3, p^9, p^{10}, p^{13}, p^5, p^{15}, p^{11}, p^{16}, p^{14}, p^8, p^7, p^4, p^{12}, p^2, p^6$$

~~Quare~~

haec in binas periodos ita distribuantur

$$(2*0) = p + p^9 + p^{13} + p^{15} + p^{16} + p^8 + p^4 + p^2 \dots$$

$$(2*1) = p^3 + p^{10} + p^5 + p^{11} + p^{14} + p^7 + p^{12} + p^6 \dots$$

eruntque $2*0$ $2*1$ radices aequationis

$xx + x - 4$. quare statuemus

$$(2*0) = -\frac{1}{2} + \frac{1}{2}\sqrt{17} = 3, \cancel{623/85} \sqrt{6256} \quad 1,56155$$

$$(2*1) = -\frac{1}{2} - \frac{1}{2}\sqrt{17} = -4,62 \quad -2,56$$

Periodi $(4*0)$; $(4*2)$ i. e. $p + p^{13} + p^{16} + p^4$ et $p^9 + p^{15} + p^8 + p^2$ sunt radices
huius aequationis

$$x^2 - (2*0)x + 1 \text{ quare quia propter } (2*0)^2 = 8 + 3(2*0) + 4(2*1)$$

$$\text{erunt } \frac{1}{2}(2*0) \pm \frac{1}{2}\sqrt{(4 + 3(2*0) + 4(2*1))}$$

$$= -\frac{1}{4} + \frac{1}{4}\sqrt{17} \pm \frac{1}{2}\sqrt{\left(\frac{17}{2} - \frac{1}{2}\sqrt{17}\right)} = \pm$$

statuemus igitur $(4*0) =$

eritque $(4*2) =$

et propter $(4*0)^2 = 4 + (4*0) + 2(4*1)$ erit per reductiones debitas:

$$(4*1) = -\frac{1}{4} - \frac{1}{4}\sqrt{17} - \sqrt{\left(\frac{17}{2} + \frac{1}{2}\sqrt{17}\right)} =$$

$$\text{et } (4*3) = -\frac{1}{4} - \frac{1}{4}\sqrt{17} - \sqrt{\left(\frac{17}{2} + \frac{1}{2}\sqrt{17}\right)} =$$

Manuscr. 50. $p + p^{16}$ et $p^7 + p^{13}$

(8×0) et (8×4) sunt radices aequationis:

(27) 44af 305

Analysis Residuorum

Eg.

$$xx - (4 \times 0)x + (4 \times 1) = 0$$

$$\text{Quare } x = +\frac{1}{2}(4 \times 0) \pm \sqrt{\left(\frac{1}{4}(4 \times 0)^2 - (4 \times 1)\right)}$$

$$= +\frac{1}{2}(4 \times 0) \pm \sqrt{\left(1 + \frac{1}{4}(4 \times 0) - \frac{1}{2}(4 \times 1)\right)}$$

$$= -\frac{1}{2} + \frac{1}{8}\sqrt{17} \pm \frac{1}{4}\sqrt{\left(\frac{17}{2} - \frac{1}{2}\sqrt{17}\right)} \pm \sqrt{\left(\frac{17}{16} - \frac{1}{16}\sqrt{17} + \frac{1}{8}\sqrt{\left(\frac{17}{2} - \frac{1}{2}\sqrt{17}\right)} - \frac{1}{4}\sqrt{\left(\frac{17}{2} + \frac{1}{2}\sqrt{17}\right)}\right)}$$

Pars ultima sub signo radicali ita etiam exprimi potest:

$$\pm \sqrt{\left(\frac{17}{16} - \frac{1}{16}\sqrt{17} + \frac{1}{8}\sqrt{\left(\frac{85}{2} - \frac{13}{2}\sqrt{17}\right)}\right)}$$

Tum autem

$$(8 \times 2); (8 \times 6) \text{ inveniuntur} =$$

$$(8 \times 1); (8 \times 5) \text{ erunt} =$$

$$(8 \times 3); (8 \times 7) \text{ erunt} =$$

His autem inuentis

e, e^{16} erunt radice aequat: $x^2 - (8 \times 0)x + 1 = 0$. Sed valores ipsas expressiones apponere evolueret lectoribus reliquimus. Valores autem tandem hanc inveniuntur

$$e; e^{16} =$$

$$e^2; e^{15} =$$

$$e^3; e^{14} =$$

$$e^4; e^{13} =$$

$$e^5; e^{12} =$$

$$e^6; e^{11} =$$

$$e^7; e^{10} =$$

$$e^8; e^9 =$$

Signa superiora pro e, e^2, e^3 ; inferiora pro e^{16}, e^{15}, e^{14} sumenda sunt; seu sumenda quod inferiora pro his superiora pro his.

Perspicuum ~~est~~ est ad computum valorum numericorum

271

Exempla hae methodi nostrae indolem abunde declarabunt. Observationes autem
adhuc aliquas ~~aspe~~ adiciemus. — Resolutionem aequationis $x^n = 1$ ^{et} ~~per~~
et congruentiarum $x^n \equiv 1$ per aequationes (seu congruentias) quasdam auxiliares
quarum dimensio a factoribus numeri $n-1$ si n supponatur esse primus
seu numeri $t-1$ si $n = t^m$ et t primus pendere eliciemus.

Quodsi itaque praeter haec aequationes auxiliares semper referri
i.e. ad puras aeq.
suo ad sectionem Rationum et Arcuum reduci possent. Si itaque n est primus
et $n-1$ ~~factores primos praeter 2~~ est formae 2^n ^{aequationis} ~~auxiliaris~~ ^{quadratae}
tantum requiruntur si, praeterea factorem 3 continet ~~quadratae~~

per quadrat. et trisectionem Rationis et Arcus res expeditas b. c.

Ita ^{per aeq.} quadrat. solvantur aeq. $x^3 = 1$; $x^5 = 1$; $x^7 = 1$; $x^{237} = 1$; $x^{65537} = 1$ &c.

per quadr. et Cubic. $x^7 = 1$; $x^{13} = 1$; $x^9 = 1$; $x^{37} = 1$; $x^{73} = 1$; $x^{97} = 1$ &c. ad

Aequationes quinti gradus ascendere oportet pro aequat. $x^{11} = 1$; $x^{31} = 1$; $x^{41} = 1$
 $x^{61} = 1$; $x^{101} = 1$ &c. et sic porro. ~~Ita~~ Geometrice itaque construere ~~possunt~~

possunt aequat. $x^n = 1$ radices (i.e. pars realis et quantitates imaginariae $\sqrt{-1}$ multi-
plicatas reales) ^{quodlibet} n est primus et $n-1$ potestas ipsius 2. Facile autem
demonstrare potest has conditiones una consistere non posse nisi ipse huius potestatis
exponens sit potestas binarii. Si enim $n = 2^a + 1$ et a factorem impari
h. inuoluit constat $2^a + 1$ per $2^b + 1$ diuidi posse, quocirca n non foret
numerus ~~integer~~ primus. n igitur debet esse formae $2^{2^m} + 1$ et substituendo
pro m successiue 0, 1, 2, 3, 4 habebuntur valores modo prolatis. Sed hinc non sequi-
tur et olim Fermatius per hanc inductionem deceptus praepropere concluderat

Opera Mathematica

omnes numeros huius formae $2^{2^n} + 1$ esse primos. M. Euler iam observavit
 numerum. insequenti scilicet $2^{32} + 1$ pro 641 divi. Comment. Acad.
 272.

Hae vero ipsae aequationes auxiliares omni attentione sunt dignissimae
 praesertim eae a quibus periodi primae pendent, neque dubitamus quin multa
 egregia hic ~~adhuc~~ in posterum hic adhuc detegerentur. Specimina aliquot
 dabimus.

Primo. Si omnes ^{radices} periodi in binas periodos coniciantur. Quos hic casus
 separare convenit.

I. Sit n numerus primus formae $4\alpha + 1$, adeoque p et q in eadem
 periodo. Sint binae periodi

$$\begin{aligned} (2 \times 0) &= p + p^{\alpha} + p^{\beta} + p^{\gamma} + p^{\delta} + \dots + p^{-1} \\ (2 \times 1) &= p^2 + p^6 + p^9 + p^{12} + \dots \end{aligned}$$

determinentur per aequationem
 $x^2 + Ax + B$ eritque ~~et quoniam~~
 $A = 1$.

$(2 \times 0)^2$ autem hanc habebit formam $2\alpha + p(2 \times 0) + q(2 \times 1)$
 p scilicet designabit quot termini in serie $1, \alpha, \beta, \gamma, \dots$ si unitate augeantur
 adhuc in serie sint; q quot ~~in~~ in altera serie $a, b, c, \dots$ facile patet praeter
 terminum -1 omnes unitate auctos in altera serie esse quare erit $p + q = 2\alpha - 1$
 Sed tum $(2 \times 1)^2$ erit $= 2\alpha + q(2 \times 0) + p(2 \times 1)$ Quare summa quadratorum
 $= 4\alpha + (2\alpha - 1)((2 \times 0) + (2 \times 1)) = 2\alpha + 1$ hinc sequitur $B = -\alpha$ Quare
 $(2 \times 0), (2 \times 1)$ erunt ^{radices aeq.} $x^2 + x - \alpha$ i.e. $= -\frac{1}{2} \pm \frac{1}{2}\sqrt{n}$.

II. Si n est primus formae $4\alpha - 1$ per simile ratiocinium quod praec.
 latis gratia omittimus invenietur summa quadratorum periodorum $= -2\alpha - 1$ unde
 Aequatio ~~quae~~ radices sunt periodi erit $xx + x + \alpha$ unde radices erunt autem $=$
 $-\frac{1}{2} \pm \frac{1}{2}\sqrt{-n}$.

Ceterum facile perspicitur omnia haec etiam de congruentiis valere ubi tantummodo conditio accedere debet, ut n sit divisor moduli congruentiae unitate minuti, quoniam ad hunc casum disquisitionem hanc pariter restrinximus. Hinc autem sequitur theorema elegans
(quod proprie partem constituit theorematum nostrum fundamentalis in Cap. 4^{to}). Quoniam scilicet semper de praec. erit legitime fore pro aequationibus $((2 \times 0) - (2 \times 1))^2 \equiv \pm n$ prout n est formae $4n+1$ et pro congruentiis $((2 \times 0) - (2 \times 1))^2 \equiv \pm n$.

Quare si a et b sint numeri primi atque b formae $4n+1$ $\pm a$ erit residuum quadraticum ipsius b prout a est formae $4n+1$

273.

Hoc theorema alio etiam modo derivari potest. Sint omnes ^{termini} radices quae periodum (2×0) constituent radices aequationis

$$(P) \quad x^m + A x^{m-1} + B x^{m-2} + C x^{m-3} + \dots + 1 = 0$$

omnes vero qui constituent periodum (2×1) formant aequationem

$$(Q) \quad x^m + A' x^{m-1} + B' x^{m-2} + C' x^{m-3} + \dots = 0$$

Habebitque coefficientis quicunque K talem formam $a + b(2 \times 0) + c(2 \times 1)$ in altera autem aeq. coefficientis correspondens K' erit $= a + b(2 \times 1) + c(2 \times 0)$ ita ut a, b, c sint integri quare K, K' haec habebunt formas $e + f\sqrt{\pm n}$; $e - f\sqrt{\pm n}$ (prout $a \pm b$ secund. formas ipsius n), et e et f erunt aut integri aut integri dimidiati.

Quare $P)$ ad hanc formam potest reduci

$$x^m + E x^{m-1} + F x^{m-2} + \dots + \frac{1}{2}(e x^{m-1} + f x^{m-2} + \dots + e x) \sqrt{\pm n}$$

$$A(Q) = x^m + E x^{m-1} + F x^{m-2} + \dots - \frac{1}{2}(e x^{m-1} + f x^{m-2} + \dots + e x) \sqrt{\pm n}$$

Quare ^{genu} productum ex (P/Q) sit $= x^{n-1} + x^{n-2} + x^{n-3} \dots + 1$
~~si ponit~~ habetur

Theorema. si n est numerus primus formae $4k \pm 1$ functio

$x^{n-1} + x^{n-2} + x^{n-3} \dots + 1$ ita exhiberi potest

$X^2 \mp n Y^2$ ita ut X , sit functio formae

$x^m + Ax^{m-1} + Bx^{m-2} \dots$ Quare formae $Ex^{m-1} + Fx^{m-2} \dots + Ex$

ita ut $A, B, \dots E, F \dots$ sint numeri aut integri aut impares dimidiati.

Ita habetur

n	X	Y
3	$x + \frac{1}{2}$	$\frac{1}{2}$
5	$xx + \frac{1}{2}x + 1$	$\frac{1}{2}x$
7		
11		

3c

~~Nulla adhuc addere possumus de proprietatibus fractionum~~

X, Y

Ubi perspicuum est $(x^n - 1)$ semper ita exhiberi posse $(x-1)XX \mp nYY$

Quare si t est numerus primus formae $kn \pm 1$ constat

propter unitatem dandi $n-1$ alias radices congruentiae $x^n \equiv 1$. pro quavis autem
 $XX \pm nYY$ per t erit divisibilis. Hinc deduci potest $\mp n$ esse residuum
 quadr. ipsius t quavis non sine ambagibus demonstrari possit Y nunquam per t
 divisibilem esse

Aliud adhuc Theorema afferemus huius simile per quod eodem pervenire possumus.
Scilicet si n est numerus primus formae $4n \pm 1$

$\frac{x^n - 1}{x - 1}$ semper ad hanc formam redigi potest $X^2 \pm nxY^2$ ita ut X sit formae

$x^m + Ax^{m-1} + Bx^{m-2} + \dots + Ax + 1$ et Y formae $x^{m-1} + Ex^{m-2} + \dots + Ex + 1$

Eccae tabulam

$n \quad X, Y$

3	$x-1$
5	x^2+3x+1
7	x^3

Monstrabimus autem quomodo generaliter haec ex iis quae d. praec. docemus
derivari possint. Sit igitur

$$\frac{x^n - 1}{x - 1} = (x^m + Ax^{m-1} + Bx^{m-2} + Cx^{m-3} + \dots)^2 \pm n(Ex^{m-1} + Fx^{m-2} + Gx^{m-3} + \dots)^2 = XX \pm nYY$$

Nunc etiam erit ponendo loco ipsius x , $-x$

$$\frac{x^n + 1}{x + 1} = (x^m - Ax^{m-1} + Bx^{m-2} - Cx^{m-3} + \dots)^2 \pm n(Ex^{m-1} - Fx^{m-2} + Gx^{m-3} + \dots)^2 = X'X' \pm nY'Y'$$

Quare

$$\frac{x^{2n} - 1}{xx - 1} = (XX' \pm nYY')^2 \pm n(XY' - X'Y)^2 \quad (6)$$

sed facile perspicitur fore $XX' \pm nYY'$ formae functionem ipsius x
~~Quare etiam formae $x^{2m} + Kx^{2m-2} + Lx^{2m-4} + \dots$~~

$XY' + X'Y$ autem formae $Kx^{2m-1} + Lx^{2m-3} + Mx^{2m-5} + \dots$ Nunc si pro xx
substituat x erit

$$\frac{x^n - 1}{x - 1} = (x^m + Kx^{m-1} + \dots)^2 \pm nx(Nx^{m-1} + \dots)$$

Sint periodi

$$(3*0) = e + e^{-1} + e^a + e^b + \dots$$

$$(3*1) = e + e^e + e^f + \dots$$

$$(3*2) = e^g + e^h + e^i + \dots$$

quae sint radices Aequationis

$$x^3 + Ax^2 + Bx + C$$

primo patet fore A = 1.

facile perspicitur fore $(3*0)^2 = m + a(3*0) + b(3*1) + c(3*2)$

eritque $a + b + c = m$. ~~Tunc autem Patet erit~~ Tum vero

$$(3*1) = m + a(3*1) + b(3*2) + c(3*0)$$

$$(3*1)^2 = m + a(3*2) + b(3*0) + c(3*1)$$

$$\text{Quare } (3*0)^2 + (3*1)^2 + (3*2)^2 = 3m - a - b - c = 2m + 1. \text{ Nunc}$$

$$B = -m.$$

Tum ponatur

$$(3*0)(3*1) = e + f(3*1) + g(3*2) \text{ eritque } e + f + g = m \text{ et}$$

$$(3*0)(3*2) = e(3*2) + f(3*0) + g(3*1)$$

$$(3*1)(3*2) = e(3*1) + f(3*2) + g(3*0)$$

Tum autem $(3*0)((3*0) + (3*1) + (3*2))$ erit $= m + (a + e + f)(3*0) + (b + f + g)(3*1) + (c + g + e)(3*2) = -(3*0)$ Quare quum $1 + (3*0) + (3*1) + (3*2) = 0$

$$\text{erit } b + f + g = c + g + e = m + e + f + 1 = m$$

facile vero perspicitur esse $b = f$; $c = g$ quare $a = 1 + g$ Nunc

$$(3*0)^2 = m + a(3*0) + b(3*1) + c(3*2)$$

$$(3*0)(3*1) = b(3*0) + c(3*1) + (a-1)(3*2)$$

$$(3*0)(3*2) = c(3*0) + (a-1)(3*1) + b(3*2)$$

$$\text{Quare } (3*0)(3*1)(3*2) = m(a-1) + a(a-1)(3*0) + b(a-1)(3*1) + c(a-1)(3*2) \\ + bb + bc + b(a-1) \\ + cc + (a-1)c + bc$$

Sed patet oportere esse

$$a(a-1) + bb + cc = b(a-1) + bc + (a-1)c$$

277.

quibus

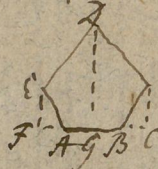
Vulgo notum iam est ^{quibus} ~~quomodo~~ radices aequationis
 $x^n = 1$ cum divisione peripheriae circuli in n partes aequales
 axum habeant. Constat enim si $n\phi$ est angulus peripheriae
 integralis multiplex fore $\cos \phi + i \sin \phi \cdot \sqrt[n]{-1}$ radicem aequationis
 $x^n = 1$. Quare si habeantur omnes ^{haec} radices, habebuntur etiam
 cosinus et sinus angulorum $\frac{1}{n} \cdot 2\pi, \frac{2}{n} \cdot 2\pi, \frac{3}{n} \cdot 2\pi \dots$ Designante
 ρ semiperipheriam. et e contra si ρ est radix, patet natis
 erit $\rho + \rho^{-1}$ duplex cosinus alicuius horum arcuum, $\frac{\rho - \rho^{-1}}{\sqrt[n]{-1}}$
 autem duplex sinus. Hinc omnia theorematata quae supra
 dedimus facile ad doctrinam de sectione circuli transferuntur.
 Quod si igitur Circulus in n partes aequalis sit secundus
 et $n = a \cdot b \cdot c \dots$, a, b, c primi res absolutas
 eae autem numeri numeri autem $a-1, b-1, c-1$ habeant factores
 simplices $e, f, g \dots$ res absolutas per sectionem arcus et rationem
 in e, f, g partes; insuperque in $a, b, c \dots$ partes si α, β, γ sint > 1
 hinc patet circulum geometricae in $2^m, 3, 5, 17, 257$ &c partes
 diuidi posse ut et in $2^m \times 3 \times 5 \times 17$ &c partes, ad divisionem in $7, 9$
 $13, 19 \dots$ partes insuper anguli et rationis trisectio requiritur &c.
 Nullam difficultatem habet omnia haec etiam independentes
 ab aequatione monstrare, peritis vero hoc proorsus superfluum foret
 Potis ergo sufficeret rem pro sectione in septemdecim partes ostendere
 unde etiam minus exercitati via sine nullo auxilio colligere poterant.

Analysis Residuorum
Rr

Qui autem
 cuius horum
 angulorum
 conveniant
 facile inde
~~per se~~ ind. col.
 quod angulus
 a 0 aut
 per aut est
 minimum
 diuersus
 maximus
 cosinus
 minimus per
 sinus habet
 et deinceps
 magis
 diuersus
 quoniam
 cosinus
 minor
 vero
 sinus

Ex elementis constat et per simplicissimam constructionem monstrari potest summam cosinum omnium angulorum

$0, \frac{2\pi}{n}, \frac{4\pi}{n}, \frac{6\pi}{n} \dots \frac{(n-2)\pi}{n}$ esse $= 0$. Ut in figura pro $n = 5$



Ubi $AB = \cos 0^\circ$

$BC = \cos 72^\circ$

$CG(\text{negat.}) = \cos 144^\circ$

$GF(\text{negat.}) = \cos 216^\circ$

$FA \text{ Pos.} = \cos 288^\circ$

Porro ex trigonometria notum est esse

$$\cos a \cdot \cos b = \frac{1}{2} \cos(a+b) + \frac{1}{2} \cos(a-b)$$

Hinc propter $\cos \frac{1}{17} \cdot 2\pi = \cos \frac{16}{17} \cdot 2\pi$; $\cos \frac{2}{17} \cdot 2\pi = \cos \frac{15}{17} \cdot 2\pi$ &c
erit $\cos 0 + 2 \cos \frac{1}{17} \cdot 2\pi + 2 \cos \frac{2}{17} \cdot 2\pi + \dots + 2 \cos \frac{8}{17} \cdot 2\pi = 0$
adeoque

$$\cos \frac{1}{17} \cdot 2\pi + \cos \frac{2}{17} \cdot 2\pi + \dots + \cos \frac{8}{17} \cdot 2\pi = -\frac{1}{2}$$

cum dicatur $\cos \frac{1}{17} \cdot 2\pi + \cos \frac{2}{17} \cdot 2\pi + \cos \frac{4}{17} \cdot 2\pi + \cos \frac{8}{17} \cdot 2\pi$ A
 $\cos \frac{2}{17} \cdot 2\pi + \cos \frac{6}{17} \cdot 2\pi + \cos$

De la Granjii error

Caput septimum

Variae quarundam investigationum praecedentium
applicationes

I. ^{279.} De fractionum communium transmutationibus.

Nullum est dubium quin multae investigationes quas hactenus pertractamus etiam in aliis matheseos partibus utiliter applicari possint. Complures quidem applicationes iam ab initio interspersimus sed ne investigationes nimis interromperentur quasdam hinc segregare visum est.

Problemata

Problema Fractionem $\frac{m}{ab}$, a, b existentibus inter se primis in duas alias discerpere quarum denominatores sint a, b . (Numeratores vero positivè seu negativè.)

Solutio Sit $\alpha \equiv \frac{m}{b} \pmod{a}$ (i.e. $b\alpha \equiv m$) et
 ~~$\beta \equiv \frac{m}{a} \pmod{b}$~~

H. p. 117

eritque Eritque $m - b\alpha = ab$ eritque

$$\frac{\alpha}{a} + \frac{\beta}{b} = \frac{m}{ab} \quad \text{Q.E.D.}$$

Exempl. Proponatur fractio $\frac{362}{209}$; quoniam $209 = 11 \cdot 19$ quare.

$$\frac{362}{19} \pmod{11} \equiv 4 \quad \text{Hinc invenitur } \frac{362}{209} = \frac{4}{11} + \frac{26}{19}.$$

280.

Problema propositâ fractione $\frac{m}{n}$ cuius denominatus n sit productum e factoribus inter se primis $a, b, c, \&c$ eam in alias fractiones discerpere quarum denominatores sint $a, b, c, \&c...$

Solutio Sit $\alpha \equiv \frac{m}{bcd...} \pmod{a}$; $\beta \equiv \frac{m}{acd...} \pmod{b}$; $\gamma \equiv \frac{m}{abd} \pmod{c}$ &c

dico fore $\frac{m}{n} - \frac{\alpha}{a} - \frac{\beta}{b} - \frac{\gamma}{c} \dots$ numerum integrum. Namque quoniam $m - \alpha bcd - \beta acd - \gamma abd \dots$ per omnes numeros $a, b, c \dots$ dividitur qui inter se sunt primi etiam per omnium productum i.e. n dividitur. Quod si cum quotiens alicui fractionum $\frac{\alpha}{a}, \frac{\beta}{b} \dots$ adducatur seu inter plures distribuat

factum erit quod requirebatur.

Exempl. Ceterum non opus est ut m, n recipiâ habeantur plerumque sufficit. mediate ipsorum valores assignare ut ex exempla ad hoc loco palam fiet.

$$\text{sit } m = \frac{2 \cdot 55224^2 - 1}{2 \cdot 55224 \cdot 2 \cdot 55224 \cdot 11515}$$

$$\frac{6099' \ 380351}{1271 \ 808720}$$

Quoniam quoniam denominator ^{est} productum e factoribus inter se primis

16. 9. 13. 59. 5. 49. 47. Quareatur ergo:

$$\frac{2 \cdot 55224^2 - 1}{9 \cdot 13 \cdot 59 \cdot 5 \cdot 49 \cdot 47} \pmod{16} \equiv \frac{-1}{13} \equiv 11$$

$$\frac{2 \cdot 55224^2 - 1}{16 \cdot 13 \cdot 59 \cdot 5 \cdot 49 \cdot 47} \pmod{9} \equiv \frac{-1}{2} \equiv 4$$

h. Unde habebuntur fractiones

$\frac{11}{16}, \frac{4}{9}, \frac{5}{13}, \frac{52}{59}, \frac{4}{5}, \frac{22}{49}, \frac{7}{47}$. Quorum aggregatum cum unitate sit minus quam $\frac{m}{n}$ erit $\frac{m}{n} = 1 + \frac{11}{16} + \frac{4}{9} + \frac{5}{13} + \frac{52}{59} + \frac{4}{5} + \frac{22}{49} + \frac{7}{47}$.

281.

Quoniam numeratores $\alpha, \beta, \gamma, \delta$ per congruentiam inveniuntur eorum valores absoluti non penitus sunt determinati. Attamen plerumque commodius est omnes positivos accipere (Vid. infra) et, quae uniformes ^{sem} observare volumus omnes denominatore suo minores accipi possunt.

Hoc itaque modo omnes numeratores exasse sunt determinati. Facile vero potest eandem fractionem ad hanc normam pluribus modis diversis discepi inquirere:

$$\text{hinc esset } \frac{m}{n} = A + \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} \dots = A' + \frac{\alpha'}{a} + \frac{\beta'}{b} + \frac{\gamma'}{c} + \frac{\delta'}{d}$$

$$\text{et } \alpha, \alpha' < a \text{ non autem } \alpha = \alpha' \text{ ponatur } \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} \dots = \frac{f}{bcd} \text{ est } \frac{\alpha'}{a} + \frac{\beta'}{b} + \frac{\gamma'}{c} + \frac{\delta'}{d}$$

$$= \frac{f}{bcd} \text{ sit forte } \frac{\alpha}{a} + \frac{f}{bcd} = \frac{\alpha'}{a} + \frac{f'}{bcd} \text{ hinc forte } \alpha > \alpha' \text{ quod licet.}$$

$$\frac{\alpha - \alpha'}{a} = \frac{f' - f}{bcd} \text{ Quoniam autem } a \text{ ad } bcd \dots \text{ est primus deberet esse.}$$

$$\frac{\alpha - \alpha'}{a} \text{ numerus integer Q.E.D. (Cap. 2.)}$$

Quoniam ^{Mauro 50} quinus numerus ita in factores inter se primos resolui potest ut quinus ²⁸
 sit aut numerus primus aut numeri primi potestas, perspicuum est quamvis fractionem
 in alias fractiones diuidi posse, quarum denominatores sint numeri primi aut
 numerorum primorum potestates, fractionis proportionem deaonitorem mediantes.

Ceterum in applicatione facillime compendia sibi offerunt quae autem per
 usum ~~tantum~~ modo edisci possunt. ~~Tampam~~ Ut calculus comprobetur inuabit, postquam
 aliquorum fractionum numeratores sint inuentae, harum summa a proposita fractione
 subducere, reliquarumque numeratores duplici modo scilicet ex fractione proposita quam
 ex hac differentia determinare. Sed Calculatores magis minusue exercitati non eadem methodi
 uti uolent; nec regulae generales hic dari possunt.

282.

De fractionum Communium in decimales Conversione.

Brevitatis gratia ad systema commune decadarum sequentia tantummodo
 adaptamus; facillime autem quisquis intelligit quomodo omnia in propositione
 generales conuerti possint.

Definitio Si fractio communis $\frac{m}{n}$ in decimalem conuoluta series figurarum
 decimalium (exclusa scilicet siquis adest numero integro) siue sit finita siue infinita
 fractionis mantissam vocamus. Permittetur nobis hanc expressionem generaliter
 accipere, quam vulgo tantum de logarithmis adhibeatur.

Ita fractionis $\frac{1}{8}$ mantissa erit 125; fractionis $\frac{33}{16}$, 0625 fractionis $\frac{4}{11}$

963636... in infin.

In infinitum
 sequens

Quand mantissa

Angla miffi



1796

In infinitum
 sequens
 Gallien
 Mant non in Angla miffi

et vice versa Pabet, fractionem quae eandem denominatorem, numeratores vero secundum hunc denominatorem congruos habent eandem ^{fore} mantissam esse; porro fractionis $\frac{m}{n}$ debita prima figura esse mantissam fractionis $\frac{10 \cdot m}{n}$, debita duabus primis ~~fra~~ mantissam fractionis $\frac{10^2 \cdot m}{n}$ et generaliter debita a primis figuris mantissam fractionis $\frac{10^a \cdot m}{n}$. Si vero m per n dividitur mantissa nulla erit.

Si fractionem $\frac{a}{b}$, $\frac{10^4 \cdot a}{b}$, $\frac{10^8 \cdot a}{b}$... mantissae secundum regulas communes addantur (scilicet, iungendo omnes figuras primum locum, a laeva, occupantes omnes porro secundum locum, et sic deinceps, decenario alteri fig. qui proveniunt tanquam unitates ad ^{aggregata} praefigendo fig. e figuris loci praecedentis adiungantur ommissis iis qui ex primo loco oriuntur) summa erit mantissa summae fractionum $\frac{a}{b} + \frac{10^4 \cdot a}{b} + \frac{10^8 \cdot a}{b}$...

Ex gr. fractionum $\frac{1}{7}$, $\frac{2}{11}$, $\frac{8}{13}$ Mantissae sunt

2857142...
4545454...
6153846...

Quae summa autem $\frac{286 + 455 + 616}{1001} = \frac{1357}{1001}$ summae mantissarum vero 3556442...

hocce casu ut semper quoties mantissae in infinitum progrediantur ultima figura est dubia ob decenarios qui proveniunt si figuras sequentes non affluerimus. (pro 2 scilicet hic esse debet 3).

Hinc sequitur quoniam quavis fractio in alias discerni potest Analysis Residuor.
 quarum denominatores sint numeri primi aut numerorum primorum
 potestates huiusmodi fractiones tantummodo considerare oportere; quoniam
 de reliquis locum habent hinc deduci poterunt. Sit igitur proporia
 fractio $\frac{m}{p^n}$, ubi p est numerus primus. Supponimus quae m per p non dividitur.
 S.S.

Primum ponamus p esse $= 2$ aut $= 5$ tum ~~dicta~~ fractionis mantissa ex n figuris
 constabit quoniam enim 10^n per p^n dividitur et id quod de mantissa demit
 n primis figuris relinquens sit mantissa fractionis $\frac{10^n \cdot m}{p^n}$, quae nulla est
 patet mantissam ad has n figuras limitari cohiberi; quod vero non prius
 finitum inde patet quod $\frac{10^k \cdot m}{p^n}$ si $k < n$ non est numerus integer.

Cacterum hanc mantissam ~~obtinere potest~~ si ~~identica~~ est cum n infimis
 figuris numeri $m \cdot \left(\frac{10}{p}\right)^{n,n}$

285

¶ Si vero p nec est $= 2$ nec $= 5$, mantissa in infinitum progreditur
 Quantumvis enim magnus k accipiat $\frac{10^k \cdot m}{p^n}$ nunquam erit numerus integer
 Sed in Capite ostendimus semper dari potestates numeri 10 ; 10^e unitati
 secundum p^n congruam et si 10^e sit infima huiusmodi potestas esse e ~~divi~~
 aut $= (p-1)p^{n-1}$ aut partem aliquotam huius numeri

Sunt autem $\frac{10^e m}{p^n}$ et $\frac{m}{p^n}$ eandem mantissam habebunt
 quocirca figura 2^a huius mantissae eadem erit quam prima
 $e + 2^a$ eadem cum secunda et sic porro, figura antea $e + 1^a$
 iterum cum prima eadem erit. Hinc sequitur primas e figuris
 periodum quasi formare quae in infinitum p^n repetita mantissam
 efficit. Multitudo vero figurarum periodi a p non vero a m
 Ita si m dividet eritque semper aut $= p-1$ p^{n-1} aut pars aliquas
 huius numeri.

Ista fractionis quoniam pro $p^n = 13$; $e = 6$ fractionis $\frac{2}{13}$
 habet mantissam 1538461538... quae constat e periodis infinitis
 153846. Periodos autem minores quos quae ex e terminis constant
 accipi non posse inde patet quod si post figuram k tam $k < e$
 omnes iterum ibidem recurrant esse debet $10^k m \equiv m \pmod{p^n}$
 seu $10^k \equiv 1$ contra hypothesis.
 Denique manifestum est ~~periodi~~ figurarum numerum periodum constanter
 tunc semper esse $= p-1 \cdot p^{n-1}$ quoties 10 est id quod in p^n radicem
 primitivam pro modulo p^n dixerimus.

286.

Si itaque mantissae aliorum periodos habeatur i.e. primae illae figurae
 in infinitum recurrentes, quousque libet continuari poterit. In tabula
 ipsius mantissarum conficienda periodi tantummodo tradi oportet. ~~Tabula~~
 Celeb. Robertson (Philosophic. Trans.) periodos per binas fere
 figurae ultimas primae et ultimas superscriptis designare proposuit; quo

quod signandi modum etiam C. M. W. d. b. g. secutus est (30) 414/222
 in libello (Kernich l. c. p.) Ita fractionis $\frac{2}{13}$ periodus hoc modo
 designatur 153846.

Si $m \cdot 10^k \equiv h \pmod{p^n}$ perspicuum est fractionis $\frac{h}{p^n}$ mantissa orietur
 si a fractionis $\frac{m}{p^n}$ mantissa primi k figurae reponentur; et si $k < e$
 id quod semper supponere licet periodus mantissae fractionis $\frac{h}{p^n}$ obtinetur
 si a periodo fractionis $\frac{m}{p^n}$ primae k figurae demantur et post ultimam
 reponentur. Quamobrem si fractionis $\frac{m}{p^n}$ periodus habeatur etiam fractionis
 $\frac{h}{p^n}$ periodus tamquam cognata potest speculari si $h \equiv 10^k m$.

887.

Quod si igitur 10 sit radix primitiva pro modulo p^n , i.e. quibus numeris
 alicuius per p non divisibilis potestati alicuius ipsius 10 sit congruus, e fractionis $\frac{1}{p^n}$ periodo
 cuiusvis alius fractionis $\frac{m}{p^n}$, (m per p non div.) cognitus erit. Et autem dividendum
 quot a periodo fractionis $\frac{1}{p^n}$ figurae rescari debeant tabula qualem Capite 3^o adinvenimus
 servare potest, unde demantur cuius ipsius 10 potestati m sit congruus. Et ut semper
 in hac tabula finius pro hocce cum 10 pro basi assumatur index numeri n quaestum
 statim ostendit; si vero alia basis esset supposita operatio requiratur de qua in eodem
 Capite fusius tractavimus.

Si vero periodus non est nimis magna calculabor exercitatus tali tabula etiam carere
 noverit. Computabit scilicet poterit tot figuras primas quot requiruntur ad hanc
 fractionem ab aliis diversis numeratoribus distinguendam. Facile has ^{eodem ordine} Vbi has in periodo invenit
 fieri autem quandoque aliquando potest et aliquae harum figurarum in periodi fine alia in iustis

sint locatae) ibi periodus initium erit statuendum. ~~Exercitatus~~ Exercitatus abso-
luti non molestus erit hoc modo figuras distinctas in periodo non ultra eorum
figuras complexitate invenire; commodius autem erit si plures aliquot figurae
insuper eis quae absolute sunt necessariae adiungantur: tunc enim inquirentis oculus
super vis poterunt. — Ceterum per se clarum est hanc methodum
~~appet~~ nunquam applicandam esse si pauculae mentibus figurae tractando des-
derentur; tunc enim tabula proorsus careri poterit.

Exempl. si $p^n = 29$ periodus erit 0344827586206896551724137931
quod si requiratur mentibus fractionis $\frac{7}{29}$, primae figurae erunt 24 quae
sine negotio in periodo inveniuntur reservandae sunt figurae 20
i. e. etiam ex tabula supra data apparet.

Itaque computus figurarum distinctarum etiam ~~per~~ ita perficere possumus multipli-
cando periodum fractionis $\frac{1}{p^n}$ per m .

288

Si vero 10 non est radix primitiva pro modulo p^n in fractionis
 $\frac{1}{p^n}$ periodus eorum tantum modo fractionis ~~mentibus~~ periodus dabitur quam numeratores
alicui ipsius 10 potestati sint congrui. Sit 10^e minima potestas, ~~terminus~~ terminus periodus ex
e figuris constabit ponatis quae $\frac{p-1, p^{n-1}}{e} = f$. Sit radix prima aliqua pro modulo p^n ,
 p , erit p^k potestati alicui ipsius 10 congrua (scilicet si $10 = e^{kf}$, maxima numerus
 $p-1, p^{n-1}$, et kf divisor communis erit f , ~~quae~~ $\frac{k}{f}$ et e inter se habent prima
Quod autem $t \cdot f \equiv \frac{1}{k} \pmod{e}$ erit $10^t \equiv e^t \pmod{p^n}$ Quare fractionis $\frac{e^t}{p^n}$ peri-
odus in periodo fractionis $\frac{1}{p^n}$ continetur. fractionum autem omnium $\frac{e}{p^n}, \frac{e^2}{p^n}, \frac{e^3}{p^n}$ vgae

ad $\frac{e^{t-1}}{p^n}$ periodi neque in periodo fractionis $\frac{1}{p^n}$, nec alterius periodi an alterius periodo continetur. Hinc perspicitur, si habeantur periodi fractionum

$\frac{1}{p^n}, \frac{e}{p^n}, \frac{e^2}{p^n}$ usque ad $\frac{e^{t-1}}{p^n}$, in his omnia aliarum fractionum periodos contineri.

~~Si quæritur~~ Data ergo harum periodorum tabula periodi eius fractionis

inveniri potest ~~tandem~~ ex primis figuris distinctis; sine etiam ope tabulae indicium ~~pro~~ capiti lectio annexae Proponitur scilicet fractione $\frac{m}{p^n}$ sit

$$m \equiv e^h. \text{ Dividatur hoc sit } 10 \equiv e^{kf} \text{ et } 10^t \equiv e^t$$

Dividatur h per f itaque $h = \lambda f + v$ ita ut $v < f$ erit ergo

$$m \equiv e^{\lambda f + v} \equiv 10^{\lambda t} \cdot e^v. \text{ Invenietur igitur periodus fractionis } \frac{m}{p^n} \text{ in periodo fractionis}$$

e^v resecandaeque sunt λ primae figurae (λ semper erit accipipossit $< e$ ob $h <$

289

ad
Quoniam radix primitiva e tam proportionum praesens quæ tum quæ basis in tabula d. ita eam semper accipere licet ut sit $t \equiv 1$. Ad hanc

normam tam tabula supra data quam ea quam ut specimen tabulae fractionum anneximus sunt adornatae; et quoniam plerumque etiam huiusmodi ipsius e inter plures eligere licet ~~non~~ ut aliquando fixi adhibetur omnium minima semper adhibuimus. Hinc usus huius tabulae per se clarus est. Si requiratur Periodus exhibet fractionum $\frac{1}{p^n}, \frac{e}{p^n}, \frac{e^2}{p^n}$ etc. per numeros 0, 1, 2, etc. distinctos

quodsi desideretur periodus fractionis $\frac{m}{p^n}$ ^{capitulus} sit index ipsius m ex tabula

qui si sit, h dividatur h per f more solito ~~residuum quotiens et residuum~~ indicant quæ ~~operati~~ ^{non} e qua periodo petenda sit quæsitum, quæritur autem quod

figurae a periodi huius initio sint resicandae et post finem restituendae.

Qui vero paullulus tantum ^{est} exercitatus, ceto ad hanc quidem tabulae extensi-
onem ceto malet binas periodi figuras primas computare ^{eorumque in} ~~longue in~~ periodo
~~perstruendo~~ ^{hic} locum preclustranda invenire.

290.

$$\begin{array}{r} 27 \\ 4x2+1 \\ 4x6+3 \end{array} \quad !!$$

Hanc

Tabulam hanc ~~vix~~ ad pro omnibus denominatoribus millenario minoribus
perfecimus; quam hic communicamus specimen tantummodo est, integram post
haec forsam ~~seu~~ si otium competat productam publici iuris faciemus.

Aliquas tantummodo observationes ad iuvimus quas pluribus lectoribus non
ingratis fore. Quoniam pro nostro calculo decimali numeri e, f (periodorum
magnitudo et quantitas multitudo) tantummodo a p^n pendent, eas ~~quae~~ p^n

colligere possumus quae eadem e; et e contra eas quae eodem f habent
illorum numerus semper erit finita namque $\neq p^n$ semper est divisor

numeri $10^e - 1$ ^{et numeri} huius divisores quoniam sunt finiti ~~per~~; horum autem
multitudo est infinita. Ecce excerptum ex tabula nostra, quae 166 numeris

primis comprehendit inter hos sunt

pro quibus $f =$				e autem = pro $p =$	
60	1	3	12	1	3
54	2	1	14	2	11
15	3	1	17	3	37
10	4	1	20	4	101
2	5	1	28	5	41.271
6	6	1	28	6	7.13
2	7	1	33	7	239
2	8	1	34	8	73.137
1	9	1	54	9	59.73
2	10			10	31
1	11				

60.

$$\frac{p-1}{p}$$

$$\frac{p-1}{p^2}$$

$$\frac{p-1}{p^3}$$

$$p \frac{p-1-1}{p-p} = a$$

$$1 \dots a$$

$$2 \dots a$$

$$3 \dots a$$

$$45$$

$$p-1$$

$$p-2$$

$$+ \frac{p-1}{p}$$

$$8490 \quad 2 \quad 1 \quad 2 \quad 4 \quad 5 \quad 7 \quad 8$$

$$4248 \quad 1 \quad 2 \quad 1 \quad 3 \quad 1$$

$$294 \quad \frac{1}{3} \quad \frac{1}{3} \quad \frac{2}{9}$$

$$1 \quad 45 \quad \frac{1}{6}$$

$$\frac{1}{2} \cdot \frac{5}{6} \cdot \frac{19}{20}$$

$$\frac{p-1}{p-p}$$

$$1 - \frac{1}{p} - \frac{1}{p^2} - \frac{1}{p^4} \text{ etc.}$$

$$1 - \frac{1}{4} - \frac{1}{8} - \frac{1}{9} - \frac{1}{16} - \frac{1}{25} + \frac{1}{36}$$

Ex praecedentibus patet quomodo fractionem cuius denominator in
factores inter se primos millenario minores resolui potest per opera
tabulae nostrae in fractionem decimalem converti posse. Ostendimus enim quomodo
fractio haec in alias discepi possit cuius denomin. sint primi aut primorum
potestates; dein quomodo haec in fractionem decimalem converti possint.
Restat igitur ut haec in summam uniantur. Superfluum est hoc modo fractionis
decimale figurae ultimam (aut si fractionem addendam numerus denarius
superat, ~~ultima~~ ultimam et penultimam &c. &c.) circoscribere. Exemplum adhuc adducimus
Supra p. 280 fractionem $\frac{6099380351}{1271808720}$ ita discepiamus $1 + \frac{1}{16} + \frac{4}{9} + \frac{5}{13} + \frac{52}{59} + \frac{22}{49} + \frac{7}{47}$
Quae hoc modo ex tabula nostra in fractionem decimalem convertuntur.

$1 = 1$						
$\frac{1}{16} = 0,6875$						
$\frac{4}{9} = 0,8$						
$\frac{5}{13} = 0,444444$	444444	444444	444444	444444	4 +	444444
$\frac{52}{59} = 0,881355$	384615	984615	384615	384615	4 -	384615
$\frac{22}{49} = 0,448979$	932203	389830	508474	6 -		57627
$\frac{7}{47} = 0,148936$	591836	734693	877551	0 +		02040
	170212	765957	446808	5 +		51063
						93637
	4,795831	523312	709541	661893	9	

figurae ultimae aut $1\frac{1}{2}$ addendum aut 1 demendum erit; unde patet quousque
sit exacte.

$$23 + \frac{1}{aa} = \frac{bb}{aa}$$

$$\sqrt{23} = \frac{b}{a} - \frac{1}{2ab}$$

Quod ad earum fractionum quarum denominatores sunt numeri e pluribus primis
 compositi attinet paucis ea tantummodo erunt ~~attinenda~~ ^{mantiffa} ~~attinenda~~. si denominator
 ad 10 factorem 2 aut 5 non contineat mantiffa e periodis erit composita
 tum enim semper datus potestas ipsius 10 unitati secundum fractionis denomi-
 natorem congrua, huiusque exponens periodi magnitudinem determinabit.

Hic autem exponens ex principis Cap. Ii facile determinari potest.
 Tandem si ~~de~~ fractionis determinator est formae $2^a 5^b$ puta
 ut p ad 10 sit primus ~~fra~~ fractionis mantiffa post ~~ter~~ figuram a aut
b ~~ter~~ prout a maior aut minor quam b e periodis confare incipiet

Omnia haec facillime tum ex iis quae Cap. Iio exposuimus quam
 inde ~~deducatur~~ ^{deducatur}, quod fractionis hae in alias quarum denominatores
 numerorum primorum potestates, quare superfluum foret diutius

 Quaedam
 monenda
 de methodo
 tabulas
 huiusmodi
 conscribendi.

hinc rei immorari.

293.

De resolutione aequationis indeterminatae $xx = a + by$

In Capite ~~tertio~~ quarto regulae sunt expositae secundum quas iudicari
 debet utrum haec aequatio ubi a et b sunt datus sit resolutibilis
 nec ne (i.e. utrum a sit ipsius b residuum quadraticum seu non-residuum)
 Sed plus quomodo easu priori x et y determinari possint plerumque
 regulae ~~admodum~~ magis ob elegantiam quam quod in applicatione

sint commodae commendandas videntur (Vid. 88)
 His itaque methodum communicabimus indirectam quidem
 sed quae plerumque satis facile percipitur suppeditat.

Analysis Residuorum

It

Nititur ea principio exclusionum quod per universam
 arithmetica singularia enolumenta praebet.

Primum limitis sunt investigandi intra quos valor ipsius y necessario
 cadere debet. Jam quoniam notum est x semper ita affigere posse ut
 non sit maior quam $\frac{1}{2}b$, ~~patet~~ et a semper $< b$, (absolute sine respectu
 signi) patet y fore positivum et ~~non~~ ^{minor} minus quam $\frac{1}{2}b + 1$. Jam pro y omnes
 valores numeri ab 1 usque ad $\frac{1}{2}b$ substituendi essent isque eligendus pro
 quo $a + by$ fit quadratum. Sed ostendemus quomodo maxima pars
 horum numerorum tamquam inepti ab hoc examine excludi possint, ita
 ut valor idoneus (sive valores si dantes plures) tantum modo supersit
 aut de reliquis tam pauci ut eos fortissime huic examini subicere
 possimus.

294

Assumatur pro lubitu numerus integer ^p sitque eius non-residu quadratum
 $\alpha, b, \gamma \dots$ Solvantur congruentiae $\alpha \equiv a + by$, $b \equiv a + by$, $\gamma \equiv a + by$ (Mod p)
 etc. sintque valores omnes ipsius y hinc oriundae $\equiv \lambda, \mu, \nu$ &c
 tum ex numeris 1, 2, ... usque ad $\frac{1}{2}b$ omnes ii erunt evicendi qui alicui horum
 numerorum $\lambda, \mu, \nu \dots$ secundum p sunt congrui. Si enim tales valores pro y substituamus

$a + by$ nonresiduo ipsius p congruum fiet adeoque gradatum esse reperit.
 Manifestum est pro p aliis aliisque numeros accipi posse adeoque numerorum
 ex serie $1, 2 \dots$ usque ad $\frac{1}{4}b$ superstitum multitudinem continuo dirimui posse.

295

Exemplum Proponatur aequatio $xx = -5 + 61y$. hic itaque y non erit
 minor quam 15. Ponatur $\parallel p = 3$ cuius non residuum est 2
 est vero $\frac{2+5}{61} \pmod{3} \equiv 1$ quare y non potest esse $\equiv 1 \pmod{3}$ excludunturque
 $1, 4, 7, 10, 13$; et restant $2, 3, 5, 6, 8, 9, 11, 12, 14, 15$. Jam sit $p = 4$
 erunt Non Residua 2, 3 est autem $\frac{2+5}{61}, \frac{3+5}{61} \equiv 3, 0 \pmod{4}$ hinc excluduntur
 iterum 3, 8, 11, 12, 15 restabuntque 2, 5, 6, 9, 14. Simili modo pro $p = 5$ excludendi
 erunt numeri qui sunt $\equiv 2, 3$ i.e. 2. restant 5, 6, 9, 14 pro $p = 6$ nulli
 excluduntur pro $p = 7$ abest 5 et 9. restant 6 et 14 quod si etiam $p = 9$ posueris
 relinquitur etiam 14 aliud est autem $19^2 = -5 + 61 \cdot 6$
 296.

Manifesta per huiusmodi operationem omnes numeri excluduntur pro
 quibus $a + by$ ipsius p fit Non Resid. Quare ^{pro utris} omnes qui restabant
 $a + by$ ipsius p fit Residuum. Per binas itaque ^{operationes} excluduntur omnes qui
 alterius aut utriusque dant Non Residua. omnes autem qui dant utriusque
 Residua remanebunt. Quod si binum numeri p, q ad quos hoc examen instituitur
 sint inter se primi, patet per Cap. 4tm omnes numeros excludi qui
 producti pq sint nonresidua, omnes autem remanentes huius producti fore

residua. Quae binae operationes cum potq aequivalent uniae cum p q.
 si p et q inter se sint primi. Hinc ratio perspicitur cur in exemplo praec. ponendo
 $p = 6$ nullae exclusi fuerint. Porro patet facile, si ponatur $p = t^2$ aut
 generalius p^k tunc eodem numeros infusperque alios (sic p non vero per p^2 , per
 p^3 non vero per p^4 divisihi) excludi. ~~Ad hoc Quae quavis quae excluderentur~~
~~ponendo $p = t$.~~ ^{aut generalius $p = t^k a$} ^{excl. 2^k} ~~sed potestas impari exponente non plus potest quam potestas~~
~~procedens. Hinc colligitur, quod quoniam arbitrio rebus quae potissimum~~
~~pro p valores sint eligenda. Scilicet numeri primi, numerorumque potestates~~
~~pares. ex. gr. 3, 8, 5, 7, 9, 11, 13, 17, 19 &c~~

297.

Lectio

Ad calculus adhuc ~~relati~~ commodius potest adornari. Quoniam agitur
 omnes valores expressimus $\frac{x-a}{b} \pmod{p}$ habere, si pro x omnes ipsius
 p non residua substituantur. Supponitis semper bad p primus fiat igitur
 $mb \equiv 1 \pmod{p}$ eritque $\frac{x-a}{b} \equiv mx - mb \pmod{p}$ Quod si iam m ipsius
 p residuum sit ~~etiam omnes~~ ^{ipsius} ~~omnia~~ ^{omnia} valores non residua comprehendit, si autem
 m ipsius p sit Non Res: ~~omnia~~ ^{residua} Residua comprehendit (exclusis ^{residua o} ~~ita quae~~
~~potestati pari ipsius aut si p primus; si vero p primus potestas t^k , exclusis~~
~~quae sunt formae $\pm rt^{2k}$)~~ (Cap. 4) Prout igitur seu hoc seu illud locum habet
 ab omnibus tantummodo residuis (excl. debiti factis) seu ab omnibus non residuis subtrahen-
 dum est mb, ~~quod reliquum~~ Habebuntur quae omnes numeri quibus y per p. iacognum esse de-
 bet.

Exempl. 2. Proponitur aequatio $xx = 7 + 139 \cdot y$

ponatur 1) $p = 5$ excludenda erunt $\frac{Non R. - 7}{139} \equiv 4 \cdot Non R. 3$ i.e. $N.R. + 2$

seu 4 et 0 simili modo habebit:

p | Encl.

7 | 1. 2. 4

8 | 0. 1. 2. 4. 5

9 | 1. 2. 4. 7. 8

11 | 0. 2. 3. 4. 8

Quoniam autem y non erit > 34

Exclusis hisce numeris restabunt: 6 et 27

$$29^2 = 7 + 6 \cdot 139$$

Annotati adhuc convenit per hanc operationem numerorum qui superserent multitudinem ad semissem ferè reduci et quamvis plures et pauciores remanere possint praesertim si haec multitudo iam sit satis modica.

Ceterum facile est subsidia comminisci quibus haec exclusiones mechanice possint institui; hoc tamen lectori perito relinquimus.

298.

De Resolutione aequationis indeterminatae $axx + byy = c$

In Capite quinto regulas generales et directas dedimus aequationem hanc resolveri sed in praxi plerumque multo facilius est indirecte quando a et b sint potestates rem indirecte aggredi; quare insuper etiam illae methodi solutionem aequationis huiusmodi in d. 181... 197 tractatus supponat quae commodissime indirecte perfici possunt.

Methodus hanc aequationem solvendi ei quae in praeco. descripsimus propius est similis sed explici modo applicari potest prout scilicet aut x aut y inue. siturus. Ponamus aequationis possibilitatem ex principis Capitis.

quinti Deductam esse quaevis x . Primo determinanda sunt limites
^{ipius} infra quos x et y cadunt ^{ad} quoniam scilicet byy ex hyp: semper positum.

44af 333 (35)

R+2

axx maior quam c fieri aequit; quare x necessario inter 0 et $\sqrt{\frac{c}{a}}$ iacebit.
 Jam ~~per~~ praesentibus omnia affirmatus numerus quicunque (ex similibus rationibus
 et s. conueniet primos tantum primos namque potestates pares accipere)

p cuius omnia non residua quadratica sunt $a, b, x \dots$
 Jam quaeantur ~~ex~~ omnes valores fractionum $\frac{c-bx}{a}, \frac{c-b^2}{a}, \frac{c-b^3}{a}$

ent
nec

ria

ex (Mod. p) eliganturque ii qui ipsius p sunt residua, horum radices
 sint $\pm A, B, C \dots$ Tum perspicuum est x nulli horum numerorum
 secundum modulum p congruum esse posse quia alias yy non residua congru-
 fieret. Omnes igitur numeri ex serie $1 \dots$ Vtique ad $\sqrt{\frac{a}{c}}$, harmonizationi
 congrui statim sunt reiciendi. Manifestum est pro p semper alios aliosque
 valores subspici et ita remanentium continui diminui posse

299



1
enice

Etiam hic calculus per sequentes reflexiones contrahi potest.
 Quoniam facile perspicitur p semper ad a primum accipi oportere sit
 $ka \equiv 1 \text{ Mod. } p$ Hinc patet omnes expressiones $\frac{c-bk}{a}$ Non R in

$ck - bk$ Non R. transire quod si iam $-bk$ sit residuum ~~et~~ ck si omnia Residua

hinc expressioni aequalebit haec $ck + bk$ Res. + ck si omnia Residua
 substituantur, si vero $-bk$ sit Non Res. hinc Res. + ck si omnia Residua
 substituantur. Exceptiones et hic simili modo et supra sunt determinandae.
 Facile autem per principia cap. 1^o exposita (p) ~~est~~ demonstratur

Let Genius live in all eternity
 Let Genius live in all eternity

in utraque expressione, $Res + ck$, $Non k. + ck$ necessaria
Residua comprehendendi et quidem ad minimus. Quare ad minimus
valores dantur per A, B, C quibus x congruum esse requirit.

300.

Exempla. Sit aequatio proposita $xx + 344 = 88801$

Quaeraturque x . ^{quod est ≤ 298} Ponendo $p = 5$, erit $88801 - 3 \cdot Non. R$ sine

~~88801~~ + Res. (exclusa res. = 0) i.e. 0, et 2 Quare xx non potest

esse $\equiv 0$ neque $x \equiv 0 \pmod{5}$ simili modo habebitur

p	Numeri ipsi x incongrui
5	0
7	2, 4, 6
8	0, 2, 4, 6 i.e.
9	0
11	0

x non potest esse $\equiv$

0	Mod 3	His vero eiectis restabunt				
± 1	Mod 9	7	79	151	223	295
± 2	Mod 2	23	95	167	239	
± 3	Mod. 8	25	97	169	241	
		31	103	175	247	
		41	113	185	257	
		47	119	191	263	
		49	121	193	265	
		65	137	209	281	

Porro non $\equiv$ | Eiectis his remanebunt

$\pm 2, 3$ Mod 7 | 7. 41. 97. 113. 119. 167. 169. 209. 223. 239. 295.

$\pm 1, 5$ Mod. 11

Porro non

$\equiv 0$ Mod 5

~~$\pm 2, 3, 5$~~ Mod. 25

$\pm 4, 6, 9, 11$

Quibus eiectis supererunt

~~7, 97~~ 7. 97. 113. 167. 223.

R ponamus $p = 13$ eiiciendi illi qui sunt $\equiv \pm 0, 2, 3, 4$ Quo facto remanebunt

7. 97. est vero $3.172^2 + 7^2 = 88809$

Si malimus y ~~primam~~ ante inuenire Calculus ita esset instituendus

$$y \text{ erit } < \sqrt{\frac{88801}{3}} \text{ i.e. } < 173$$

Jam inuenietur y ~~non~~ debere esse incongruum secundum modulum

$$\begin{array}{c|c} 2 & 1 \\ 4 & 2 \end{array}$$

Hinc poni poterit $yx = 172$ quare

$$xx + 48zz = 88801 \text{ eritque } z < 44$$

Debet autem z esse incongruum secundum

modulum

$$\begin{array}{c|c} 5 & \pm 1 \\ 7 & \pm 0, 2 \\ 11 & \pm 3, 5 \\ 13 & \pm 0, 1, 3, 5 \end{array}$$

Quibus ceteris remanent

$$15, 20, 22, 32, 43$$

Quod si adhuc poneremus

$p = 17$ etiam 15, 20, 32 abiret

est autem ut vidimus $z = 43$

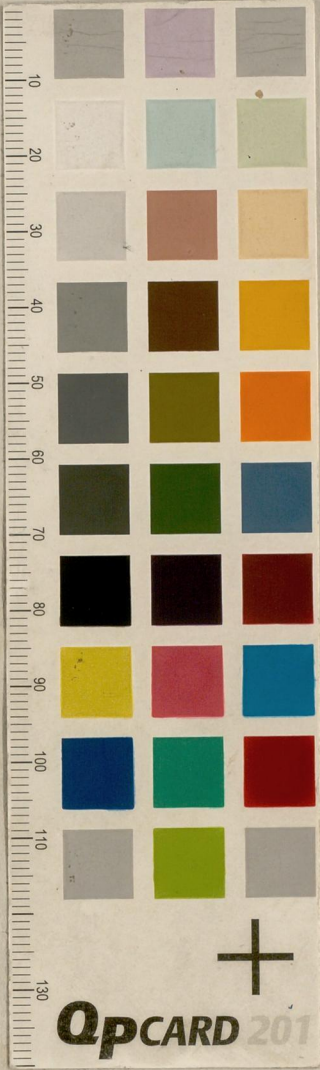
Simul per hunc methodum colligitur 88801 vixit tantum modo in forma $\square + 3\square$ esse contentum.

301

Facile intelligitur si quaeratur x ~~non~~ ^{imaginarium} ~~non~~ ^{ipsum} ~~non~~ ^{dividere non} ~~non~~ ^{debet} ~~non~~ ^{primum esse} debere. Alias enim $\frac{c-bN.A.}{p}$ semper fit ~~indeterminatum~~ ^{imaginarium} quoniam $\frac{c}{b} \pmod{a}$ adeoque etiam

$\frac{c}{b} \pmod{p}$ semper est Residuum. Si itaque ut in nostro exemplo $a = 1$, $b = 3$ y quidem iam per se intra archiores limites includitur quam x adeoque numerorum qui examini subiacendorum multitudo erit minor; sed hoc in eo compensatur quod si y quaeratur $p = 3$ ponere non licet, adeoque hoc criterio caremus.

In genere tamen ^{expedite} ~~conueniens~~ est x quaerere si $a < b$ et y si $b < a$. cuius rationem



© SUB GÖTTINGEN/GDZ