Werk

Titel: Disquisitiones arithmeticae
Jahr: 1863
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN235993352
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN235993352
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=235993352

LOG Id: LOG_0007
LOG Titel: Sectio Secunda De Congruentiis Primi Gradus
LOG Typ: chapter

Übergeordnetes Werk

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

Contact

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

SECTIO SECUNDA

DE

CONGRUENTIIS PRIMI GRADUS.

Theoremata praeliminaria de numeris primis, factoribus etc.

13.

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

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

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

14.

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

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

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

15.

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

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

16.

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

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

17.

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

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

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

divisores diversos, inclusis etiam 1 et A.

18.

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

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

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

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

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

19.

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

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

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

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

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

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

20.

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

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

21.

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

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

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

integer. Similiter de reliquis b, c etc.

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

22.

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

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

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

23.

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

Hoc est tantum conversio theor. art. praec.

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

24.

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

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

25.

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

Solutio congruentiarum primi gradus.

26.

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

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

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

27.

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

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

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

brevitatis gratia ita eas designamus,

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

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

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

ita ut $\alpha, \mathfrak{b}, \gamma$ etc. c, d, e etc. sint integri positivi, et b, c, d, e continuo decrescentes, donec perveniatur ad $m = \mu n + 1$

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

1°. $[\alpha, \mathfrak{b}, \gamma \ldots . \lambda, \mu].\ [\mathfrak{b}, \gamma \ldots . \lambda] - [\alpha, \mathfrak{b}, \gamma \ldots \lambda]\ [\mathfrak{b}, \gamma, \ldots \lambda, \mu] = \pm 1,$

ubi signum superius accipiendum quando numerorum $\alpha, \mathfrak{b}, \gamma \ldots \lambda, \mu$ multitudo par, inferius quando impar.

2°. Numerorum $\alpha, \mathfrak{b}, \gamma$ etc. ordo inverti potest, $[\alpha, \mathfrak{b}, \gamma \ldots \lambda, \mu] = [\mu, \lambda \ldots \gamma, \mathfrak{b}, \alpha]$.

Demonstrationes quae non sunt difficiles hic supprimimus.

quod tandem evenire debere constat. Erit itaque

$$a = [n, \mu, \ldots . \gamma, \mathfrak{6}, \alpha], \quad b = [n, \mu \ldots . \gamma, \mathfrak{6}]$$

Tum fiat $x = [\mu, \ldots . \gamma, \mathfrak{6}], \qquad y = [\mu, \ldots . \gamma, \mathfrak{6}, \alpha]$

eritque $ax = by + 1$, quando numerorum $\alpha, \mathfrak{6}, \gamma \ldots . \mu, n$ multitudo est par, aut $ax = by - 1$, quando est impar. *Q. E. F.*

28.

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

$$\cfrac{1}{\alpha + \cfrac{1}{\mathfrak{6} + \cfrac{1}{\gamma + \text{etc.} + \cfrac{1}{\mu + \frac{x}{n}}}}}$$

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

29.

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

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

30.

Quando modulus est compositus, nonnumquam praestat sequenti methodo uti.

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

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

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

31.

Simili modo ut aequationis $ax = b$ radix per $\frac{b}{a}$ exprimitur, etiam congruentiae $ax \equiv b$ radicem quamcunque per $\frac{b}{a}$ designabimus, congruentiae modulum, distinctionis gratia, apponentes. Ita e. g. $\frac{19}{17} \pmod{12}$ denotat quemvis numerum, qui est $\equiv 11 \pmod{12}$ *). Generaliter ex praecedentibus patet, $\frac{a}{b} \pmod c$ nihil reale significare (aut si quis malit aliquid imaginarii), si a, c habeant divisorem communem, qui ipsum b non metiatur. At hoc casu excepto, expressio $\frac{b}{a} \pmod c$ semper valores reales habebit, et quidem infinitos: hi vero omnes secundum c erunt congrui quando a ad c primus, aut secundum $\frac{c}{\delta}$, quando δ numerorum c, a divisor communis maximus.

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

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

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

De inveniendo numero secundum modulos datos residuis datis congruo.

32.

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

*) id quod ex analogia per $\frac{11}{1} \pmod{12}$ designari potest.

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

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

33.

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

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

34.

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

35.

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

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

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

36.

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

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

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

quum valor expressionis $\frac{1}{19.28} \pmod{15}$, sive $\frac{1}{532} \pmod{15}$, sit 13, erit $\alpha = 6916$. Similiter pro δ invenitur 4200, et pro γ 4845, quare numerus quaesitus erit residuum minimum numeri $6916a + 4200b + 4845c$, denotantibus a indictionem, b numerum aureum, c cyclum solarem.

Congruentiae lineares quae plures incognitas implicant.

37.

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

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

2) Propositae sint igitur congruentiae

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

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

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

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

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

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

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

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

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

quas brevitatis gratia ita exhibemus:

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

4) Iam plures casus sunt distinguendi.

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

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

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

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

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

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

Propositae sint congruentiae

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

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

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

quibus facile intelligitur aequivalere has

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

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

$$\begin{aligned} x &\equiv 2, \quad 5, \quad 8, \quad 11 \pmod{12} \\ y &\equiv 11, \quad 11, \quad 11, \quad 11 \\ z &\equiv 3, \quad 6, \quad 9, \quad 0 \end{aligned}$$

* * *

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

Theoremata varia.

38.

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

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

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

$$\phi A = A - 1$$

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

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

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

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

quae ita demonstratur. Sint numeri ad M primi ipsoque M minores m, m', m'' etc. quorum itaque multitudo $= \phi M$. Similiter sint numeri ad N, P etc. respective primi ipsisque minores n, n', n'' etc.; p, p', p'' etc. etc., quorum multitudo $\phi N, \phi P$ etc. Iam constat omnes numeros ad productum A primos etiam ad factores singulos M, N, P etc. primos fore et vice versa (art. 19); porro omnes numeros qui horum m, m', m'' etc. alicui sint congrui secundum modulum M ad M primos fore et vice versa, similiterque de N, P etc. Quaestio itaque huc reducta est: determinare quot dentur numeri infra A, qui secundum modulum M, alicui numerorum m, m', m'' etc. secundum N, alicui ex his n, n', n''

etc. etc. sint congrui. Sed ex art. 32 sequitur, omnes numeros, secundum singulos modulos M, N, P etc. residua determinata dantes, congruos secundum eorum productum A fore, adeoque infra A unicum tantum dari, secundum singulos M, N, P etc. residuis datis congruum. Quare numerus quaesitus aequalis erit numero combinationum singulorum numerorum m, m', m'' cum singulis n, n', n'' atque p, p', p'' etc. etc. Hunc vero esse $= \phi M . \phi N . \phi P$ etc. ex theoria combinationum constat. *Q. E. D.*

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

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

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

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

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

39.

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

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

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

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

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

$+\phi a''+$ etc. numeri, omnes ipso A non maiores. At

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

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

3) Hinc colligitur horum numerorum multitudinem esse A, quare

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

40.

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

$$aA + bB + cC + etc. = \mu$$

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

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

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

---

*) Metietur enim manifesto λ' omnes A, B, C. Si vero non esset divisor communis *maximus*: maximus foret maior quam λ'. Iam quoniam hic divisor maximus metitur ipsos A, B, C, metietur etiam ipsum $k\alpha A + k\mathfrak{b}B + \gamma C$ i. e. ipsum λ', maior minorem *Q. E. A.* — Facilius adhuc hoc ex art. 15 deduci potest.

Simili modo procedi potest, quotcunque alii numeri accedant.

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

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

41.

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

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

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

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

numerus permutationum erit

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

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

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

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

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

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

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

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

42.

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

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

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

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

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

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

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

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

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

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

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

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

43.

Congruentia m^{ti} *gradus*

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

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

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

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

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

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

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

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

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

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

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

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

44.

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

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